Cohomology of groups with applications to number theory

Dietrich Burde

Lecture Notes 2009

Contents

Introduction

Group homology and cohomology has its origins in topology, starting with the work of Riemann (1857), Betti (1871) and Poincaré (1895) on "homology numbers" of manifolds. Although Emmy Noether observed in 1925 that homology was an abelian group rather than just Betti numbers, homology remained a part of the realm of topology until about 1945. During the period of $1940-1955$ came the rise of algebraic methods. The homology and cohomology of several algebraic systems were defined and explored: Tor and Ext for abelian groups, homology and cohomology of groups and Lie algebras, the cohomology of associative algebras, sheaves, sheaf cohomology and spectral sequences. At this point the book of Cartan and Eilenberg (1956) crystallized and redirected the field completely. Their systematic use of derived functors, defined by projective and injective resolutions of modules, united all the previously disparate homology theories. Several new fields grew out of this: homological algebra, K-theory, Galois theory, étale cohomology of schemes and so on. Much could be said also on newer developments in homological algebra.

Concerning group cohomology, the low dimensional cohomology of a group G was already classically studied in other guises, long before the formulation of group cohomology in $1943-1945$ by Eilenberg and MacLane. For example, classical objects were

$$H^0(G,A)=A^G,\ H^1(G,\mathbb{Z})=G/[G,G]$$

and for G finite, the character group

$$H^2(G,\mathbb{Z})=H^1(G,\mathbb{C}^\times)=\mathrm{Hom}(G,\mathbb{C}^\times)$$

Also the group $H^1(G,A)$ of crossed homomorphisms of G into a G-module A is classical as well: Hilbert's Theorem 90 from 1897 is actually the calculation that $H^1(G,L^\times)=0$ when G is the Galois group of a cyclic field extension L/K. One should also mention the group $H^2(G,A)$ which classifies extensions over G with normal abelian subgroup A via factor sets. The idea of factor sets appeared already in Hölders paper in 1893 and again in Schur's paper in 1904 on projective representations $G\to PGL_n(\mathbb{C})$. Schreier's paper in 1926 was the first systematic treatment of factor sets, without the assumption that A is abelian.

In 1950 Hochschild invented the term *Galois cohomology* for the group cohomology of the Galois group $G=\mathrm{Gal}(L/K)$, where L is a (possibly infinite) Galois field extension of K, such as the separable closure of K. Here G is a profinite group. Hochschild and Tate applied Galois cohomology to class field theory. In 1964 Serre published Cohomologie galoisienne, which until today is the standard reference on Galois cohomology over number fields.

The first draft was written in 2004. This is a new version with some corrections and extensions, written in 2009.

CHAPTER 1

Group extensions

Given a group G and a normal subgroup N of G we may decompose G in a way into N and G/N. The study of group extensions is related to the converse problem. Given N and Q, try to understand what different groups G can arise containing a normal subgroup N with quotient $G/N \cong Q$. Such groups are called extensions of N by Q. If N is abelian, then there is a natural Q-action on N, making N a Q-module. In that case the cohomology group $H^2(Q, N)$ classifies the equivalence classes of such group extensions which give rise to the given Q-module structure on N.

Group homology and cohomology belongs to the field of homological algebra. This deals with category theory and in particular with the theory of derived functors. In this chapter however we will focus most of the time only on group theory.

1.1. Split extensions and semidirect products

We start with the definition of exact sequences.

Definition 1.1.1. A sequence of groups and group homomorphisms

$$\cdots \to A_{n-1} \xrightarrow{\alpha_n} A_n \xrightarrow{\alpha_{n+1}} A_{n+1} \to \cdots$$

is called exact at A_n if $\operatorname{im}\alpha_n = \ker \alpha_{n+1}$. The sequence is called *exact* if it is exact at each group.

Example 1.1.2. *The sequence* $1 \xrightarrow{\alpha_1} A \xrightarrow{\alpha_2} 1$ *is exact iff* $A = 1$ *is the trivial group. The sequence* $1 \xrightarrow{\alpha} A \xrightarrow{\beta} B \xrightarrow{\gamma} 1$ *is exact iff* A *is isomorphic to* B.

Indeed, $1 = \operatorname{im}\alpha_1 = \ker \alpha_2 = A$ in the first case, and $1 = \operatorname{im}\alpha = \ker\beta, \quad \operatorname{im}\beta = \ker\gamma = B$ in the second, so that

$$A \cong A/\ker\beta \cong \operatorname{im}\beta = B$$

Example 1.1.3. *A short exact sequence is given by*

$$1 \to A' \xrightarrow{\alpha} A \xrightarrow{\beta} A'' \to 1$$

From the exactness we conclude that α is injective, β is surjective and

$$A' \cong \alpha(A') = \ker\beta \tag{1.1}$$

hence $\alpha(A')$ being a kernel is a normal subgroup of A. Sometimes we will identify A' with its image $\alpha(A')$. Furthermore we have

$$A/\ker\beta \cong \beta(A) = A'' \tag{1.2}$$

hence A'' is isomorphic to the quotient A/A'.

Definition 1.1.4. Let N and Q be groups. An *extension of N by Q* is a group G such that

(1) G contains N as a normal subgroup.
(2) The quotient G/N is isomorphic to Q.

An extension of groups defines a short exact sequence and vice versa: if G is an extension of N by Q then

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1$$

is a short exact sequence where $\iota : N \hookrightarrow G$ is the inclusion map and $\pi : G \twoheadrightarrow G/N$ is the canonical epimorphism. If

$$1 \to A^{'} \xrightarrow{\alpha} A \xrightarrow{\beta} A^{''} \to 1$$

is a short exact sequence, then A is an extension of $\alpha(A^{'}) \cong A^{'}$ by $\beta(A) \cong A^{''}$, see example (1.1.3).

Example 1.1.5. *Given any two groups N and Q, their direct product $G = Q \times N$ is an extension of N by Q, and also an extension of Q by N.*

Example 1.1.6. *The cyclic group C_6 is an extension of C_3 by C_2. Hence we obtain the short exact sequence*

$$1 \to C_3 \to C_6 \to C_2 \to 1$$

The symmetric group respectively the dihedral group $\mathcal{S}_3 \cong \mathcal{D}_3$ is an extension of C_3 by C_2, but not of C_2 by C_3. We obtain the short exact sequence

$$1 \to C_3 \to \mathcal{D}_3 \to C_2 \to 1$$

In the first case, C_3 is a normal subgroup of C_6 with quotient isomorphic to C_2. In the second case let $C_3 = \langle(123)\rangle$. This is a normal subgroup of $\mathcal{D}_3$ since the index is $[\mathcal{D}_3 : C_3] = 2$. The quotient is isomorphic to $C_2 = \langle(12)\rangle$. Note that C_2 is not a normal subgroup of $\mathcal{D}_3$.

Let $M/L/K$ be a tower of field extensions such that the field extensions M/K and L/K are normal. Denote by

$$\begin{aligned} Q &:= \mathrm{Gal}(L/K) \\ N &:= \mathrm{Gal}(M/L) \\ G &:= \mathrm{Gal}(M/K) \end{aligned}$$

Then G is a group extension of N by Q since $N \lhd G$ and $Q \cong G/N$ by Galois theory. In this way be obtain some examples of group extensions.

Example 1.1.7. *Let $M/L/K$ be $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Then*

$$\begin{aligned} Q &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2 \\ N &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})) \cong C_2 \\ G &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong C_2 \times C_2 \end{aligned}$$

This yields the short exact sequence

$$1 \to C_2 \to C_2 \times C_2 \to C_2 \to 1$$

Let us prove that $G \cong C_2 \times C_2$. Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ the group G has four elements: the automorphisms

$$(\sqrt{2}, \sqrt{3}) \mapsto \begin{cases} (\sqrt{2}, \sqrt{3}) \\ (-\sqrt{2}, \sqrt{3}) \\ (\sqrt{2}, -\sqrt{3}) \\ (-\sqrt{2}, -\sqrt{3}) \end{cases}$$

Hence all non-trivial elements of G have order 2.

Example 1.1.8. *Let $M/L/K$ be $\mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Then*

$$\begin{aligned} Q &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2 \\ N &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})/\mathbb{Q}(\sqrt{2})) \cong C_2 \\ G &:= \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})/\mathbb{Q}) \cong C_4 \end{aligned}$$

This yields the short exact sequence

$$1 \to C_2 \to C_4 \to C_2 \to 1$$

To show that the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})$ over $\mathbb{Q}$ is cyclic of order 4, we will use the following well known result:

Lemma 1.1.9. *Let K be a field of characteristic different from 2 and assume that a is not a square in K. Let $L := K(\sqrt{a})$. Then there exists a tower of normal field extensions $M/L/K$ with $\mathrm{Gal}(M/K) \cong C_4$ if and only if $a \in K^2 + K^2$. In that case there exist $s, t \in K$, $t \neq 0$ such that $M = L(\sqrt{s + t\sqrt{a}})$.*

In our case $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ and $a = 2$. Since $2 = 1^2 + 1^2$ we have $\mathrm{Gal}(M/K) \cong C_4$ and with $s = 2, t = 1$,

$$M = L(\sqrt{2+\sqrt{2}}) = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})$$

Definition 1.1.10. Let $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ be a given group extension. Denote by $\tau : Q \cong G/\alpha(N) \to G$ the map assigning each coset $x \in G/\alpha(N)$ a representative $\tau(x) \in G$. Any such function $\tau : Q \to G$ is called a *transversal function.*

By definition we have $\beta(\tau(x)) = x$, i.e.,

$$\beta\tau = \mathrm{id}_{|Q} \tag{1.3}$$

In general a transversal function need not be a homomorphism. If it is however we obtain a special class of extensions.

Definition 1.1.11. An extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ is called *split* if there is a transversal function $\tau : Q \to G$ which is a group homomorphism. In that case τ is called a *section.*

Sometimes this is called right-split, whereas left-split means that there exists a homomorphism $\sigma\colon G \to N$ such that $\sigma\alpha = \mathrm{id}_{|N}$. For the category of groups however, the properties right-split and left-split need not be equivalent.

Example 1.1.12. *The extensions of example* (1.1.6) *are both split:*

$$1 \to C_3 \to C_6 \to C_2 \to 1$$
$$1 \to C_3 \to \mathcal{D}_3 \to C_2 \to 1$$

On the other hand the extension

$$1 \to C_2 \to C_4 \to C_2 \to 1$$

of example (1.1.8) *is not split.*

Since a transversal function τ in these examples is given by its values on [0] and [1] in C_2, it is easily seen that we can find a section for the first two examples. As to the last extension it is clear that C_2 does not have a complement in C_4. But this implies that the extension is not splitting as we will see in the following.

Definition 1.1.13. Two subgroups $N, Q \le G$ are called *complementary* if

$$N \cap Q = 1 \tag{1.4}$$
$$G = NQ \tag{1.5}$$

In general, $NQ = \{nq \mid n \in N,\ q \in Q\}$ is not a subgroup of G. In fact, it is a subgroup if and only if $NQ = QN$. Hence in particular it is a subgroup if $N \lhd G$ or $Q \lhd G$.

Example 1.1.14. *The subgroups $N = \langle(123)\rangle$ and $Q = \langle(12)\rangle$ are complementary subgroups in $G = \mathcal{S}_3$. The subgroups $N = \langle(12)\rangle$ and $Q = \langle(234)\rangle$ of $G = \mathcal{S}_4$ are not complementary.*

The first case is clear, for the second note that $|NQ| = |N| \cdot |Q| \cdot |N \cap Q|^{-1} = 6$, hence $NQ \neq \mathcal{S}_4$.

Lemma 1.1.15. *Let $N, Q \le G$ be subgroups. Then N and Q are complementary if and only if each element $g \in G$ has a unique representation $g = nq$ with $n \in N$, $q \in Q$.*

Proof. If N and Q are complementary then $G = NQ$, hence each element $g \in G$ has a representation $g = nq$. To show the uniqueness assume that $g = nq = mp$ with $n, m \in N$ and $p, q \in Q$. Then $n^{-1}gp^{-1} = qp^{-1} = n^{-1}m \in N \cap Q = 1$ and hence $m = n$ and $p = q$. Conversely the unique representation implies $G = NQ$ and $N \cap Q = 1$. □

Definition 1.1.16. A group G is called *inner semidirect product* of N by Q if

(1) N is a normal subgroup of G.
(2) N and Q are complementary in G.

In that case we will write $G = Q \ltimes N$.

Example 1.1.17. *Both $\mathcal{S}_3$ and C_6 are inner semidirect products of C_3 by C_2.*

This says that in contrast to direct products, an inner semidirect product G of N by Q is not determined up to isomorphism by the two subgroups. It will also depend on how N is normal in G.

Example 1.1.18. *Let $\mathcal{S}_n$ denote the symmetric group on n letters and $\mathcal{D}_n$ the dihedral group of order $2n$. Both are inner semidirect products as follows:*

$$\mathcal{S}_n = C_2 \ltimes \mathcal{A}_n$$
$$\mathcal{D}_n = C_2 \ltimes C_n$$

Clearly $\mathcal{A}_n \lhd \mathcal{S}_n$ and $C_2, \mathcal{A}_n$ are complementary subgroups in $\mathcal{S}_n$. Let $\mathcal{D}_n = \langle s, t \mid s^n = t^2 = 1,\, tst = s^{-1}\rangle$ and $C_n = \langle s\rangle, C_2 = \langle t\rangle$. Then $C_n \lhd \mathcal{D}_n$ and C_n and C_2 are complementary in $\mathcal{D}_n$.

An inner semidirect product of N by Q is also an extension of N by Q since $Q \cong G/N$. More precisely we have:

Proposition 1.1.19. *For a group extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ the following assertions are equivalent:*

1. *There is a group homomorphism $\tau : Q \to G$ with $\beta\tau = \mathrm{id}_{|Q}$.*
2. *$\alpha(N) \cong N$ has a complement in G, i.e., $G \cong Q \ltimes N$.*

Corollary 1.1.20. *G is an inner semidirect product of N by Q if and only if G is a split extension of N by Q.*

Proof. Let τ be a section. We will show that $\tau(Q)$ then is a complement of $\alpha(N) = \ker\beta$ in G. So let $g \in \ker\beta \cap \tau(Q)$. With $g = \tau(q)$ for some $q \in Q$ it follows

$$1 = \beta(g) = \beta(\tau(q)) = q$$

Since τ is a homomorphism $g = \tau(q) = \tau(1) = 1$. So we have

$$\alpha(N) \cap \tau(Q) = 1 \tag{1.6}$$

Now let $g \in G$ and define $x := \beta(g) \in Q$. Then $\tau(x) \in G$ and

$$\beta(g\tau(x^{-1})) = \beta(g) \cdot \beta(\tau(x^{-1})) = xx^{-1} = 1$$

so that $g\tau(x^{-1}) = \alpha(n)$ for some $n \in N$ since it lies in $\ker\beta = \alpha(N)$. Using $\tau(x)^{-1} = \tau(x^{-1})$ we obtain $g = \alpha(n)\tau(x)$, i.e.,

$$G = \alpha(N)\tau(Q) \tag{1.7}$$

Since α and τ are monomorphisms we have $G \cong Q \ltimes N$, $Q \cong \tau(Q)$ and $N \cong \alpha(N)$.

For the converse direction let C be a complement of $\alpha(N)$ in G, i.e.,

$$C \cap \alpha(N) = 1 \tag{1.8}$$

$$C \cdot \alpha(N) = G \tag{1.9}$$

The homomorphism lemma now says that $\alpha(N) \subset \ker\beta$ implies the existence of a unique homomorphism $\gamma : G/\alpha(N) \to Q$ such that the following diagram commutes:

$$\begin{tikzcd} G \arrow[r, "\beta"] \arrow[d, "\varphi"'] & Q \\ G/\alpha(N) \arrow[ur, "\gamma"'] & \end{tikzcd}$$

In fact, γ is defined by $\gamma(g\alpha(N)) = \beta(g)$. Let us now restrict φ to the complement C. We still denote this map by φ. By assumption it is an isomorphism, given by $c \mapsto c\alpha(N)$ for $c \in C$. Hence there exists a unique homomorphism $\gamma : G/\alpha(N) \to Q$ satisfying

$$\gamma(\varphi(c)) = \gamma(c\alpha(N)) = \beta(c)$$

for all $c \in C$, i.e., $\gamma \circ \varphi = \beta$. Note that γ is an isomorphism. Hence the map

$$\tau : Q \to C \subset G,\ q \mapsto \varphi^{-1}(\gamma^{-1}(q))$$

is a homomorphism with

$$\beta(\tau(q)) = (\gamma \circ \varphi)(\varphi^{-1}(\gamma^{-1}(q))) = q$$

hence with $\beta\tau = \mathrm{id}_{|Q}$. □

EXAMPLE 1.1.21. *The following exact sequences are both split:*

$$1 \to \mathcal{A}_n \xrightarrow{\iota} S_n \xrightarrow{sign} \{\pm 1\} \to 1$$
$$1 \to SL_n(k) \xrightarrow{\iota} GL_n(k) \xrightarrow{det} k^\times \to 1$$

It follows that $\mathcal{S}_n \cong C_2 \ltimes \mathcal{A}_n$ and $GL_n(k) \cong k^\times \ltimes SL_n(k)$.

Since $\ker \mathrm{sign} = \mathcal{A}_n$ we see that the first sequence is exact. It also splits. Let $\pi \in \mathcal{S}_n$ be a transposition and define $\tau : \{\pm 1\} \to \mathcal{S}_n$ by $\tau(1) = \mathrm{id}$ and $\tau(-1) = \pi$. Then τ is a section. For the second sequence define $\tau : k^\times \to GL_n(k)$ by

$$a \mapsto \begin{pmatrix} 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 0 & a \end{pmatrix}$$

This is a section since $\tau(ab) = \tau(a)\tau(b)$ and $(\beta \circ \tau)(a) = \det \tau(a) = a$.

DEFINITION 1.1.22. Let N, Q be two groups and $\varphi : Q \to \mathrm{Aut}(N)$ be a homomorphism. Define a multiplication on $Q \times N$ as follows:

$$(x, a)(y, b) = (xy, \varphi(y)(a) \cdot b) \tag{1.10}$$

for $x, y \in Q$ and $a, b \in N$. Then $Q \times N$ together with this multiplication becomes a group which is denoted by $G = Q \ltimes_\varphi N$. It is called the *outer semidirect product* of N by Q with respect to φ.

Note that $\varphi(xy) = \varphi(y) \circ \varphi(x)$ for all $x, y \in Q$. The product on the RHS denotes the composition of automorphisms in $\mathrm{Aut}(N)$. Let us verify the group axioms. The element $(1, 1)$ is a left unit element in G:

$$(1, 1)(x, a) = (x, \varphi(x)(1) \cdot a) = (x, a)$$

A left inverse element to (x, a) is given by (x^{-1}, b^{-1}) where $b = \varphi(x^{-1})(a)$:

$$\begin{aligned}(x^{-1}, b^{-1})(x, a) &= (x^{-1}x, \varphi(x)(b^{-1}) \cdot a) = (1, \varphi(x)(\varphi(x^{-1})(a^{-1})) \cdot a) \\ &= (1, a^{-1}a) = (1, 1)\end{aligned}$$

since $b^{-1} = (\varphi(x^{-1})(a))^{-1} = \varphi(x^{-1})(a^{-1})$. Finally the multiplication is associative.

$$\begin{aligned}[(x,a)(y,b)](z,c) &= (xy, \varphi(y)(a)\cdot b)(z,c) = (xyz, \varphi(z)(\varphi(y)(a)\cdot b)\cdot c)\\ &= (xyz, ((\varphi(z)\circ\varphi(y))(a)\cdot \varphi(z)(b)\cdot c)\\ (x,a)[(y,b)(z,c)] &= (x,a)(yz,\varphi(z)b\cdot c) = (xyz, \varphi(yz)(a)\cdot\varphi(z)(b)\cdot c)\end{aligned}$$

Since φ is a homomorphism both sides coincide.
We want to explain the relation between an inner and outer semidirect product. If

$$1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$$

is a short exact sequence, then G acts on the normal subgroup $\alpha(N) \lhd G$ by conjugation:

$$G\times\alpha(N)\to\alpha(N), \quad (g,\alpha(a))\mapsto g^{-1}\alpha(a)g$$

Definition 1.1.23. The assignment $\gamma(g) = g^{-1}\alpha(a)g$ defines a homomorphism $\gamma : G \to \mathrm{Aut}(\alpha(N))$. The restriction on the quotient $G/\alpha(N) \cong Q$ is also denoted by $\gamma : Q \to \mathrm{Aut}(N)$.

Proposition 1.1.24. *Let $G = Q \ltimes_\varphi N$ be an outer semidirect product of N by Q. Then G defines a split short exact sequence*

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\alpha"] & G \arrow[r, shift right, "\beta"'] & Q \arrow[l, shift right, "\tau"'] \arrow[r] & 1 \end{tikzcd}$$

where the maps α, β, τ are given by

$$\alpha(a) = (1,a), \quad \beta((x,a)) = x, \quad \tau(x) = (x,1)$$

such that

$$\alpha\circ\varphi(x) = \gamma(\tau(x))\circ\alpha \tag{1.11}$$

Proof. We show first that $\alpha(N)$ is normal in G so that $\gamma : Q \to \mathrm{Aut}(N)$ is well defined. Let $(x,a)\in G$ and $(1,c)\in\alpha(N)$.

$$\begin{aligned}(x,a)^{-1}(1,c)(x,a) &= (x^{-1},\varphi(x^{-1})(a^{-1}))\cdot(x,\varphi(x)(c)\cdot a)\\ &= (1,\ a^{-1}\cdot\varphi(x)(c)\cdot a)\in\alpha(N)\end{aligned}$$

Applying this computation we obtain for all $a\in N$

$$\begin{aligned}\gamma(\tau(x))[\alpha(a)] &= \tau(x)^{-1}\alpha(a)\tau(x) = (x,1)^{-1}(1,a)(x,1)\\ &= (1,\varphi(x)(a)) = \alpha[\varphi(x)(a)]\end{aligned}$$

which gives (1.11). Since obviously α is a monomorphism and β is an epimorphism with $\beta\tau = \mathrm{id}$ we obtain a split short exact sequence. The group G is also an inner semidirect product of $\alpha(N)$ by $\tau(Q)$. □

Conversely the following result holds.

Proposition 1.1.25. *Each split short exact sequence $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ defines via* (1.11) *an outer semidirect product $Q\ltimes_\varphi N$ which is isomorphic to G.*

PROOF. Since α is a monomorphism (1.11) defines a homomorphism $\varphi : Q \to \operatorname{Aut}(N)$. Define the map $\psi : Q \ltimes_\varphi N \to G$ by

$$\psi[(x,a)] = \tau(x) \cdot \alpha(a) \tag{1.12}$$

By Lemma (1.1.15) the map ψ is bijective. Moreover it is a homomorphism. We have

$$\begin{aligned}\psi[(x,a)(y,b)] &= \psi[(xy, \varphi(y)(a) \cdot b)] = \tau(xy) \cdot \alpha(\varphi(y)(a)) \cdot \alpha(b)\\ &= \tau(x)\tau(y) \cdot \alpha(\varphi(y)(a)) \cdot \alpha(b)\end{aligned}$$

by (1.10) and the fact that τ is a homomorphism. On the other hand

$$\begin{aligned}\psi[(x,a)]\psi[(y,b)] &= \tau(x)\alpha(a) \cdot \tau(y)\alpha(b) = \tau(x)\tau(y) \cdot \big(\tau(y)^{-1}\alpha(a)\tau(y)\big) \cdot \alpha(b)\\ &= \tau(x)\tau(y) \cdot \gamma(\tau(y))(\alpha(a)) \cdot \alpha(b) = \tau(x)\tau(y) \cdot \alpha(\varphi(y)(a)) \cdot \alpha(b)\end{aligned}$$

□

EXAMPLE 1.1.26. *Let C_2 act on C_n by the automorphism $x \mapsto x^{-1}$. Then $\mathcal{D}_n \cong C_2 \ltimes_\varphi C_n$*

The homomorphism $\varphi : C_2 \to \operatorname{Aut}(C_n)$ is defined by $\varphi(1) = \mathrm{id}$ and $\varphi(-1)(x) = x^{-1}$.

The following well known result shows that certain group extensions are always semidirect products.

SCHUR-ZASSENHAUS 1.1.27. *Let N and Q be finite groups of coprime order. Then every short exact sequence $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ splits. Hence each extension of N by Q is a semidirect product.*

We will prove this theorem later, see proposition 2.5.6. There is a very elegant proof for the case that N is abelian using the second cohomology group $H^2(Q,N)$. The general case can be proved with an induction over the order of N reducing the problem to a central extension. An above extension is called *central* if $\alpha(N) \subset Z(G)$ is satisfied. In that case N is abelian. In fact, the above result has first been proved by Schur in 1902 for central extensions.
Note that the result need not be true if the orders are not coprime. A short exact sequence $1 \to C_2 \to G \to C_2 \to 1$ may split or may not. Take $G = C_2 \times C_2$ or $G = C_4$ respectively.

Exercises

(1) *Exact sequences.* Let $1 \to G_1 \to G_2 \to G_3 \to \ldots \to G_n \to 1$ be an exact sequence of finite groups. Let $|G|$ denote the cardinality of a group G. Prove the following equation:

$$\prod_{i=1}^{n} |G_i|^{(-1)^i} = 1$$

(2) *Splitting extensions.* Show that the extension

$$1 \to C_2 \to C_4 \to C_2 \to 1$$

is not split. Which extensions of C_3 by C_2 are splitting ?

(3) *Semidirect products.* Let p be a prime. Show that none of the groups C_{p^n} is a semidirect product of non-trivial subgroups.

(4) *The quaternion group.* Let $Q = \{1, -1, i, -i, j, -j, k, -k\}$ be the quaternion group. Is Q a semidirect product of non-trivial subgroups ?

1.2. Equivalent extensions and factor systems

How can we describe all possible extensions G of a group N by another group Q ? We will view extensions as short exact sequences $1 \to N \overset{\alpha}{\to} G \overset{\beta}{\to} Q \to 1$. There will be a natural equivalence relation on the set of such extensions. As a preparation we will need the following lemma.

Lemma 1.2.1. *Suppose that we have the following commutative diagram of groups and homomorphisms with exact rows:*

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "f"] & B \arrow[r, "\beta"] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & 1 \\
1 \arrow[r] & A' \arrow[r, "\gamma"] & B' \arrow[r, "\delta"] & C' \arrow[r] & 1
\end{tikzcd}$$

If f and h are both injective, respectively surjective, then so is g. In particular, if f and h are isomorphisms, so is g.

Proof. By assumption we know that α, γ are injective, β, δ are surjective and $\operatorname{im} \alpha = \ker \beta$, $\operatorname{im} \gamma = \ker \delta$. Since the diagram commutes we have

$$\gamma f = g\alpha, \quad h\beta = \delta g \tag{1.13}$$

Assume first that f and h are injective. We will show that g then is also injective. Let $g(b) = 1$ for some $b \in B$. Then by (1.13)

$$1 = \delta(g(b)) = h(\beta(b)) \quad \Longrightarrow \quad \beta(b) = 1$$

since h is injective. It follows $b \in \ker \beta = \operatorname{im} \alpha$, hence $\alpha(a) = b$ for some $a \in A$. Then again by (1.13)

$$1 = g(b) = g(\alpha(a)) = \gamma(f(a)) \quad \Longrightarrow \quad f(a) = 1$$

since γ is injective. But f is also injective hence $a = 1$ and $b = \alpha(1) = 1$. This proves the injectivity of g.

For the second part assume now that f and h are surjective. We will show that g is also surjective. Let $b' \in B'$ be given. Since h is surjective there is a $c \in C$ such that $h(c) = \delta(b') \in C'$. Since β is surjective there is a $b \in B$ such that $\beta(b) = c$. It follows

$$\delta(g(b)) = h(\beta(b)) = h(c) = \delta(b')$$

so that $\delta\left(g(b)^{-1}b'\right) = 1$ and $g(b)^{-1}b' \in \ker \delta = \operatorname{im} \gamma$. it follows $g(b)^{-1}b' = \gamma(a')$ for some $a' \in A'$. Since f is surjective there is an $a \in A$ such that $f(a) = a'$ so that, using (1.13)

$$g(\alpha(a)) = \gamma(f(a)) = \gamma(a') = g(b)^{-1}b'$$

which implies $b' = g(b) \cdot g(\alpha(a)) = g(b \cdot \alpha(a))$. Hence g is surjective. □

The following result involving 10 groups and 13 group homomorphisms generalizes the above lemma.

Lemma 1.2.2. *Consider the following commutative diagram of groups and homomorphisms with exact rows.*

$$\begin{tikzcd}
A_1 \arrow[r, "\alpha_1"] \arrow[d, "f_1"] & A_2 \arrow[r, "\alpha_2"] \arrow[d, "f_2"] & A_3 \arrow[r, "\alpha_3"] \arrow[d, "f_3"] & A_4 \arrow[r, "\alpha_4"] \arrow[d, "f_4"] & A_5 \arrow[d, "f_5"] \\
B_1 \arrow[r, "\beta_1"] & B_2 \arrow[r, "\beta_2"] & B_3 \arrow[r, "\beta_3"] & B_4 \arrow[r, "\beta_4"] & B_5
\end{tikzcd}$$

Then the following holds.

(a) *If f_2, f_4 are onto and f_5 is one-to-one, then f_3 is onto.*
(b) *If f_2, f_4 are one-to-one and f_1 is onto, then f_3 is one-to-one.*
(c) *In particular, if f_1, f_2 and f_4, f_5 are isomorphisms, so is f_3.*

The proof is done in a completely analogous way and is left to the reader.

Definition 1.2.3. Let N and Q be groups. Two extensions G and G' of N by Q are called *equivalent* if there exists a homomorphism $\varphi : G \to G'$ such that the following diagram with exact rows becomes commutative:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\alpha"] \arrow[d, "\mathrm{id}"] & G \arrow[r, "\beta"] \arrow[d, "\varphi"] & Q \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & N \arrow[r, "\gamma"] & G' \arrow[r, "\delta"] & Q \arrow[r] & 1
\end{tikzcd}$$

If the extensions G and G' are equivalent then they are automatically isomorphic as groups since φ is then an isomorphism by lemma 1.2.2. The converse however need not be true. There exist inequivalent extensions G and G' which are isomorphic as groups. Classifying inequivalent group extensions is in general much finer than classifying non-isomorphic groups. We will see that in the next example. Formaly we will write

$$(G, \alpha, \beta) \simeq (G', \gamma, \delta)$$

for two equivalent group extensions. In that case there exists a homomorphism $\varphi : G \to G'$ such that $\gamma = \varphi\alpha$ and $\beta = \delta\varphi$. This defines an equivalence relation. Clearly the relation is reflexive since $(G, \alpha, \beta) \simeq (G, \alpha, \beta)$ with $\varphi = \mathrm{id}$. It is symmetric since $(G, \alpha, \beta) \simeq (G', \gamma, \delta)$ implies $(G', \gamma, \delta) \simeq (G, \alpha, \beta)$ with $\varphi^{-1} : G' \to G$. To show transitivity consider the following diagram:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\alpha"] \arrow[d, "\mathrm{id}"] & G \arrow[r, "\beta"] \arrow[d, "\varphi"] & Q \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & N \arrow[r, "\gamma"] \arrow[d, "\mathrm{id}"] & G' \arrow[r, "\delta"] \arrow[d, "\varphi'"] & Q \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & N \arrow[r, "\varepsilon"] & G'' \arrow[r, "\kappa"] & Q \arrow[r] & 1
\end{tikzcd}$$

Assume that $(G, \alpha, \beta) \simeq (G', \gamma, \delta)$ and $(G', \gamma, \delta) \simeq (G'', \varepsilon, \kappa)$. It follows that there are homomorphisms $\varphi : G \to G'$ and $\varphi' : G' \to G''$ such that

$$\gamma = \varphi\alpha, \ \beta = \delta\varphi, \ \varepsilon = \varphi'\gamma, \ \delta = \kappa\varphi'$$

Defining $\varphi'' := \varphi'\varphi : G \to G''$ it follows

$$\begin{aligned}
\varepsilon &= \varphi'\gamma = \varphi'\varphi\alpha = \varphi''\alpha \\
\beta &= \delta\varphi = \kappa\varphi'\varphi = \kappa\varphi''
\end{aligned}$$

Hence we have $(G, \alpha, \beta) \simeq (G'', \varepsilon, \kappa)$.

Example 1.2.4. *Let p be a prime. Then there are p inequivalent extensions G of C_p by C_p. Since G has order p^2 it is either isomorphic to $C_p \times C_p$ or to C_{p^2}.*

Besides the split exact sequence $1 \to C_p \to C_p \times C_p \to C_p \to 1$ consider the following $p-1$ short exact sequences

$$1 \to C_p \xrightarrow{\alpha} C_{p^2} \xrightarrow{\beta_i} C_p \to 1$$

where $C_p = \langle a \rangle = \{1, a, a^2, \dots, a^{p-1}\}$ and $C_{p^2} = \langle g \rangle = \{1, g, g^2, \dots, g^{p^2-1}\}$ and the homomorphisms α and β are given by

$$\begin{aligned} \alpha : C_p \to C_{p^2}, \quad & a \mapsto g^p \\ \beta_i : C_{p^2} \to C_p, \quad & g \mapsto a^i, \quad i = 1, 2, \dots, p-1 \end{aligned}$$

The sequences are exact since $\beta_i(\alpha(a)) = \beta_i(g^p) = a^{pi} = 1$ in C_p, hence $\operatorname{im} \alpha = \ker \beta_i$. We claim that any two extensions β_i and β_j for $i \neq j$ are inequivalent. Suppose $(C_p, \alpha, \beta_i) \simeq (C_p, \alpha, \beta_j)$, i.e.,

$$\begin{tikzcd} 1 \arrow[r] & C_p \arrow[r, "\alpha"] \arrow[d, "\mathrm{id}"] & C_{p^2} \arrow[r, "\beta_i"] \arrow[d, "\varphi"] & C_p \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\ 1 \arrow[r] & C_p \arrow[r, "\alpha"] & C_{p^2} \arrow[r, "\beta_j"] & C_p \arrow[r] & 1 \end{tikzcd}$$

and $\alpha = \varphi\alpha$, $\beta_i = \beta_j\varphi$. It follows

$$g^p = \alpha(a) = \varphi(\alpha(a)) = \varphi(g^p) = \varphi(g)^p$$

Now $\varphi(g) = g^r$ generates C_{p^2} since φ is an isomorphism. Hence $p \nmid r$ and $g^p = \varphi(g^p) = g^{pr}$ in C_{p^2}. This implies $r \equiv 1(p)$. On the other hand we have

$$a^i = \beta_i(g) = \beta_j(\varphi(g)) = \beta_j(g^r) = a^{jr}$$

in C_p. It follows $i \equiv jr(p)$. Together with $r \equiv 1(p)$ we have $i \equiv j(p)$ or $i = j$ and $\beta_i = \beta_j$. So we have proved the claim.

Remark 1.2.5. There are exactly p equivalence classes of extensions of C_p by C_p. We will see later that they are in bijection with the elements in the group $H^2(C_p, C_p) \cong C_p$ where C_p acts trivially on C_p.

We will now reduce the classification of group extensions to so called factor systems. Schreier's theorem yields a bijection between the equivalence classes of group extensions and the equivalence classes of the associated parameter systems.

Definition 1.2.6. Let N and Q be two groups. A pair of functions (f, T)

$$\begin{aligned} f : & Q \times Q \to N \\ T : & Q \to \mathrm{Aut}(N) \end{aligned}$$

is called a *factor system* to N and Q if

$$f(xy,z)T(z)(f(x,y)) = f(x,yz)f(y,z) \tag{1.14}$$

$$T(y)\circ T(x) = \gamma\left(f(x,y)\right)\circ T(xy) \tag{1.15}$$

$$f(1,1) = 1 \tag{1.16}$$

for all $x, y, z \in Q$.

The second condition (1.15) means, using the definition of γ

$$T(y)\left(T(x)(n)\right) = f(x,y)^{-1}T(xy)(n)f(x,y)$$

for all $n \in N$. Sometimes T is referred to as the automorphism system.

Remark 1.2.7. If we choose $f(x,y) \equiv 1$ then (f,T) is called the *trivial* factor system. In that case T is a homomorphism by (1.15) and (1.14) reduces to $1 = 1$.

Condition (1.16) corresponds to a normalization. The first two conditions already imply the following conditions:

Lemma 1.2.8. *Let (f,T) be a pair of functions as above where only conditions* (1.14) *and* (1.15) *are satisfied. Then it follows*

$$T(1) = \gamma(f(1,1)) \tag{1.17}$$

$$f(x,1) = f(1,1) \tag{1.18}$$

$$f(1,y) = T(y)(f(1,1)) \tag{1.19}$$

for all $x, y \in Q$.

Proof. By (1.15) we have $T(1)\circ T(1) = \gamma(f(1,1))T(1)$ so that $T(1) = \gamma(f(1,1))$. It follows $f(1,1)^{-1}f(x,1)f(1,1) = T(1)(f(x,1))$ and hence

$$\begin{aligned} f(x,1)f(1,1) &= f(1,1)T(1)(f(x,1)) \\ &= f(x,1)T(1)(f(x,1)) \end{aligned}$$

where we have used (1.14) with $z = y = 1$ for the last equation. This shows (1.18).
Setting $x = y = 1$ in (1.14) we obtain

$$f(1,z)T(z)(f(1,1)) = f(1,z)f(1,z)$$

Multiplying $f(1,z)^{-1}$ from the left yields (1.19). □

Corollary 1.2.9. *Let (f,T) be a factor system to N and Q. Then*

$$f(x,1) = f(1,y) = 1 \tag{1.20}$$

$$T(1) = \mathrm{id}_{|N} \tag{1.21}$$

for all $x, y \in Q$.

Proof. By (1.16) it follows $T(1) = \gamma(f(1,1)) = \gamma(1) = \mathrm{id}_{|N}$. Furthermore $f(x,1) = f(1,1) = 1$ and $f(1,y) = T(y)(1) = 1$ since $T(y)$ is an automorphism of N. □

We can associate a factor system with each group extension as follows.

Proposition 1.2.10. *Each group extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ together with a transversal function $\tau : Q \to G$ defines a factor system (f_τ, T_τ).*

This associated factor system depends not only on the extension, but also on the choice of a transversal function τ.

Proof. Let $x \in Q \simeq G/\alpha(N)$ be a coset of $\alpha(N)$ in G and τ a fixed transversal function $x \mapsto \tau(x)$. It satisfies $\beta\tau = \mathrm{id}$ on Q. Since $\alpha(N)$ is normal in G, the element $\tau(x)^{-1}\alpha(n)\tau(x)$ is in $\alpha(N)$. We will denote it by

$$\alpha(T_\tau(x)(n)) = \tau(x)^{-1}\alpha(n)\tau(x) \tag{1.22}$$

where $T_\tau(x)(n) \in N$. This defines automorphisms $T_\tau(x)$ of N and a map $T_\tau : Q \to \mathrm{Aut}(N)$. Since β is a homomorphism we have

$$\beta(\tau(xy)^{-1}\tau(x)\tau(y)) = (\beta\tau)((xy)^{-1}) \cdot (\beta\tau)(x)(\beta\tau)(y) = (xy)^{-1}xy = 1$$

and hence $\tau(xy)^{-1}\tau(x)\tau(y) \in \ker\beta = \alpha(N)$. It follows that there exists a unique element $f_\tau(x,y) \in N$ such that

$$\tau(x)\tau(y) = \tau(xy)\alpha(f_\tau(x,y)) \tag{1.23}$$

Now we have to verify the conditions (1.14),(1.15),(1.16) for the pair (f_τ, T_τ) which we will denote by (f,T). We set

$$\tau(1) = 1 \tag{1.24}$$

This condition is not essential, but it helps simplify some of the computations. By (1.23) we have

$$\tau(1)\tau(1) = \tau(1)\alpha(f(1,1))$$

hence $\alpha(f(1,1)) = 1$ and $f(1,1) = 1$. Hence (1.16) is satisfied. By using (1.22) and (1.23) we obtain

$$\begin{aligned}
(\alpha T(y)T(x))\,(n) &= \tau(y)^{-1}\tau(x)^{-1}\alpha(n)\tau(x)\tau(y) \\
&= (\alpha(f(x,y))^{-1} \cdot \tau(xy)^{-1}\alpha(n)\tau(xy) \cdot \alpha(f(x,y)) \\
&= (\alpha(f(x,y))^{-1} \cdot \alpha(T(xy)(n)) \cdot \alpha(f(x,y))
\end{aligned}$$

This implies (1.15). Using (1.23) we have

$$\begin{aligned}
\tau((xy)z) &= \tau(xy)\tau(z)\left(\alpha(f(xy,z)\right)^{-1} \\
&= \tau(x)\tau(y)\left(\alpha(f(x,y))\right)^{-1} \cdot \tau(z)\left(\alpha(f(xy,z)\right)^{-1} \\
\tau(x(yz)) &= \tau(x)\tau(yz)\left(\alpha(f(x,yz)\right)^{-1} \\
&= \tau(x)\tau(y)\tau(z)\left(\alpha(f(y,z))\right)^{-1}\left(\alpha(f(x,yz)\right)^{-1}
\end{aligned}$$

Using the associativity in G both terms must be equal, i.e.,

$$\begin{aligned}\alpha(f(x,yz))\alpha(f(y,z)) &= \alpha(f(xy,z))\cdot\tau(z)^{-1}\alpha(f(x,y))\tau(z)\\ &= \alpha(f(xy,z)\cdot\alpha(T(z)(f(x,y))\end{aligned}$$

Since α is a monomorphism we obtain (1.14). □

Now we have associated a factor system (T_τ, f_τ) to a group extension and a transversal function τ. Does every factor system (f, T) arise in such a way ? The answer is given by the following proposition.

Proposition 1.2.11. *For each factor system (f,T) to N and Q there is a group extension G of N by Q such that $(f,T) = (f_\tau, T_\tau)$ for a suitable choice of a transversal function τ.*

Proof. Given (f,T) we define a group structure on $G = Q \times N$ as follows.

$$(x,a)\circ(y,b) = (xy, f(x,y)T(y)(a)b) \tag{1.25}$$

for $x, y \in Q$ and $a, b \in N$. This generalizes the construction of the outer semidirect product. If we choose the trivial factor system $f(x,y) = 1$ for all $x, y \in Q$, then $T : Q \to \mathrm{Aut}(N)$ is a homomorphism and the above definition coincides with the outer semidirect product $Q \ltimes_T N$. We need to show that the group laws are satisfied, that G is a group extension of N by Q and that (f_τ, T_τ) is exactly (f,T) with a suitable choice of τ. We start with the associativity.

$$\begin{aligned}(x,a)\circ[(y,b)\circ(z,c)] &= (x,a)\circ[yz, f(y,z)T(z)(b)c]\\ &= (xyz, f(x,yz)T(yz)(a)f(y,z)T(z)(b)c)\\ [(x,a)\circ(y,b)]\circ(z,c) &= [xy, f(x,y)T(y)(a)b]\circ(z,c)\\ &= (xyz, f(xy,z)T(z)\big(f(x,y)T(y)(a)b\big)c)\\ &= (xyz, f(xy,z)T(z)(f(x,y))\cdot T(z)(T(y)(a)b)c)\\ &= (xyz, f(xy,z)T(z)(f(x,y))\cdot\gamma(f(y,z))(T(yz)(a))\cdot T(z)(b)c)\\ &= (xyz, f(x,yz)\cdot f(y,z)\gamma(f(y,z))(T(yz)(a))\cdot T(z)(b)c)\\ &= (xyz, f(x,yz)T(yz)(a)f(y,z)T(z)(b)c)\end{aligned}$$

In the second computation we have first used that $T(z)$ is an automorphism of N, then (1.15) and (1.14). Let $b := f(x,x^{-1})T(x^{-1})(a)$. Then (x^{-1}, b^{-1}) is the inverse of (x,a).

$$(x,a)\circ(x^{-1},b^{-1}) = (xx^{-1}, f(x,x^{-1})T(x^{-1})(a)\cdot b^{-1}) = (1,1)$$

Clearly $(1,1)$ is the unit element

$$(1,1)\circ(y,b) = (y, f(1,y)T(y)(1)b) = (y,b)$$

Now define $\beta : G \to Q$ by $(x,a) \mapsto x$. This map is a surjective homomorphism:

$$\beta((x,a))\circ\beta((y,b)) = xy = \beta\big((xy, f(x,y)T(y)(a)b\big) = \beta((x,a)\circ(y,b))$$

where we have used (1.25) in the last step. The map $(1,a)\mapsto a$ is an isomorphism from $\ker\beta = \{(1,a)\mid a\in N\}$ to N:

$$(1,a)\circ(1,b) = (1, f(1,1)T(1)(a)b) = (1,ab)$$

The map $\alpha : N\longrightarrow G$ defined by $a\mapsto(1,a)$ is a monomorphism. We obtain a short exact sequence $1\longrightarrow N\xrightarrow{\alpha} G\xrightarrow{\beta} Q\longrightarrow 1$ and hence an extension G of N by Q.

The next step is to choose a transversal function $\tau : Q\longrightarrow G$. The most natural choice is $\tau(x) = (x,1)$. Since

$$\begin{aligned}\tau(x)\circ\tau(y) &= (x,1)\circ(y,1) = (xy, f(x,y)),\\ \tau(xy)\alpha(f(x,y)) &= (xy,1)\circ(1,f(x,y)) = (xy, f(xy,1)T(1)(1)f(x,y)\\ &= (xy, f(x,y))\end{aligned}$$

we have $\tau(x)\tau(y) = \tau(xy)\alpha(f(x,y))$. Comparing with (1.23), where $f_\tau(x,y)$ was uniquely determined, it follows $f_\tau = f$. Using (1.14) with $y = x^{-1}$ and $f(1,x) = f(x,1) = 1$ we obtain $T(x)(f(x,x^{-1}) = f(x^{-1},x)$. Since $T(x)$ is an automorphism it follows

$$T(x)(f(x,x^{-1})^{-1}) = f(x^{-1},x)^{-1} \tag{1.26}$$

so that, using the formula for the composition of three elements from above

$$\begin{aligned}(x,1)^{-1}\circ(1,a)\circ(x,1) &= (x^{-1}, f(x^{-1},x)^{-1})\circ(1,a)\circ(x,1)\\ &= (x\cdot 1\cdot x^{-1}, f(x^{-1},x)T(x)\left(f(x^{-1},x)^{-1}\right)f(1,x)T(x)(a)\cdot 1)\\ &= (1, T(x)(a))\end{aligned}$$

This is just $\tau(x)^{-1}\alpha(a)\tau(x) = \alpha(T(x)(a))$ and a comparison with (1.22) shows $T_\tau = T$. □

Example 1.2.12. *Consider the extension* $1\longrightarrow C_2\xrightarrow{\alpha} C_4\xrightarrow{\beta} C_2\longrightarrow 1$ *where* $N = C_2 = \langle a\rangle$, $C_4 = \langle g\rangle$, $Q = C_2 = \langle x\rangle$ *and* $\alpha(a) = g^2$, $\beta(g) = x$. *Determine the associated factor system* (f_τ, T_τ) *where* τ *is given by* $\tau(1) = 1$, $\tau(x) = g$.

$T_\tau : C_2\longrightarrow \mathrm{Aut}(C_2)$ is given by $T_\tau(1) = T_\tau(x) = \mathrm{id}$ since $\alpha(T_\tau(x)(a)) = \tau(x)^{-1}\alpha(a)\tau(x) = g^{-1}g^2g = g^2$ and hence $T_\tau(x)(a) = a$. The map $f_\tau : C_2\times C_2\longrightarrow C_2$ is given by

$$f(1,1) = f(1,x) = f(x,1) = 1,\ f(x,x) = a$$

We have to show only the last condition. It is $g\cdot g = \tau(x)\tau(x) = \alpha(f(x,x))$ so that $f(x,x) = a$.

EXAMPLE 1.2.13. *Determine the group extension* $1 \to C_2 \xrightarrow{\alpha} G \xrightarrow{\beta} C_2 \to 1$ *to the above factor system* (f_τ, T_τ).

The group $G = \{(1,1),(1,a),(x,1),(x,a)\}$ has the following multiplication

$$(x,a) \circ (y,b) = (xy, f(x,y)ab)$$

Using $x^2 = a^2 = 1$ we obtain

$$\begin{aligned}(x,a)^4 &= ((x,a)\circ(x,a))^2 = (x^2, f(x,x)a^2)^2 = ((1,a))^2 \\ &= (1,a)\circ(1,a) = (1, f(1,1)a^2) = (1,1)\end{aligned}$$

Since $(x,a)^2 = (1,a) \neq (1,1)$ the group G is isomorphic to C_4.

So far we have constructed a correspondence between factor systems (f,T) to N and Q and group extensions G of N by Q. However, the correspondence is not yet one-to-one. There are many factor systems (f_τ, T_τ) associated with one group extension. We will introduce an equivalence relation on the set of factor systems.

LEMMA 1.2.14. *Let* $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ *be a group extension and* (f,T), (f',T') *two associated factor systems. Then there is a map* $h : Q \to N$ *such that*

$$T'(x) = \gamma(h(x)) \circ T(x) \tag{1.27}$$

$$f'(x,y) = h(xy)^{-1} f(x,y) \cdot T(y)(h(x)) \cdot h(y) \tag{1.28}$$

PROOF. The associated factor systems (f,T) and $f',T')$ arise by two transversal functions $\tau : Q \to G$ and $\tau' : Q \to G$. They just assign a given coset two representatives. Hence

$$\tau'(x) = \tau(x)\ell(x) \tag{1.29}$$

with a map $\ell : Q \to \alpha(N)$. Define $h : Q \to N$ by $\alpha(h(x)) = \ell(x)$. Using (1.22) we obtain

$$\begin{aligned}\alpha(T'(x)(n)) &= \tau'(x)^{-1}\alpha(n)\tau'(x) = \ell(x)^{-1} \cdot \tau(x)^{-1}\alpha(n)\tau(x) \cdot \ell(x) \\ &= \alpha\left(h(x)^{-1}\right) \cdot \alpha\left(T(x)(n)\right) \cdot \alpha(h(x))\end{aligned}$$

so that $\alpha \circ T'(x) = \alpha \circ \gamma(h(x)) \circ T(x)$ and (1.27) follows. Using (1.23) we obtain

$$\begin{aligned}\alpha\left(f'(x,y)\right) &= \tau'(xy)^{-1}\tau'(x)\tau'(y) = \ell(xy)^{-1} \cdot \tau(xy)^{-1} \cdot \tau(x)\ell(x)\tau(y)\ell(y) \\ &= \ell(xy)^{-1}\alpha(f(x,y)) \cdot \tau(y)^{-1}\alpha(h(x))\tau(y) \cdot \ell(y) \\ &= \ell(xy)^{-1}\alpha(f(x,y)) \cdot \alpha(T(y))(h(x)) \cdot \ell(y) \\ &= \alpha\left(h(xy)^{-1}\right) \cdot \alpha(f(x,y)) \cdot \alpha(T(y)(h(x)) \cdot \alpha(h(y))\end{aligned}$$

This implies (1.28). □

The lemma tells us how to define the equivalence relation.

Definition 1.2.15. Let (f,T) and (f',T') be two factor systems to N and Q. They are called *equivalent* if there is a map $h : Q \to N$ such that (1.27) and (1.28) are satisfied, and $h(1) = 1$.

If we take $h(x) = 1$ for all $x \in Q$ then it follows immediately $(f,T) = (f',T')$. Different choices of the transversal function τ lead to equivalent factor systems in our correspondence. Next we show that the equivalence relation is compatible with equivalent group extensions.

Proposition 1.2.16. *Equivalent group extensions*

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\alpha"] \arrow[d, "\mathrm{id}"] & G \arrow[r, "\beta"] \arrow[d, "\varphi"] & Q \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & N \arrow[r, "\gamma"] & G' \arrow[r, "\delta"] & Q \arrow[r] & 1
\end{tikzcd}$$

define equivalent factor systems.

Proof. Choose any transversal function τ to the extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ and let (f,T) denote the associated factor system. Let (f',T') the factor system associated with the extension $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ and the following $\tau' : Q \to G$:

$$\tau'(x) = \varphi(\tau(x)) \tag{1.30}$$

Since $\gamma = \varphi\alpha$ and $\beta = \delta\varphi$ we have $\delta\tau' = \delta\varphi\tau = \beta\tau = \mathrm{id}$. So τ' is really a transversal function. Its choice is such that (f',T') coincides with (f,T). Hence the two factor systems are euqivalent. In fact, by (1.22) we have

$$\begin{aligned}
\gamma\left(T'(x)(a)\right) &= \tau'(x)^{-1}\gamma(a)\tau'(x) = \tau'(x)^{-1}\varphi(\alpha(a))\tau'(x) \\
&= \varphi(\tau(x)^{-1}) \cdot \varphi(\alpha(a)) \cdot \varphi(\tau(x)) = \varphi\big(\tau(x)^{-1}\alpha(a)\tau(x)\big) \\
&= (\varphi \circ \alpha)(T(x)(a)) = \gamma(T(x)(a))
\end{aligned}$$

Since γ is injective we have $T' = T$. Using (1.23) we have

$$\begin{aligned}
\tau'(xy)\gamma(f'(x,y)) &= \tau'(x)\tau'(y) = \varphi(\tau(x)) \cdot \varphi(\tau(y)) \\
&= \varphi(\tau(x)\tau(y)) = \varphi[\tau(xy) \cdot \alpha(f(x,y))] \\
&= (\varphi\tau)(xy) \cdot (\varphi\alpha)(f(x,y)) = \tau'(xy)\gamma(f(x,y))
\end{aligned}$$

This implies $f'(x,y) = f(x,y)$ or $f' = f$. □

Proposition 1.2.17. *Let N, Q be groups and (f,T), (f',T') be two factor systems to N and Q. If the factor systems are equivalent, so are the associated group extensions.*

Proof. Assume that (f,T) and (f',T') are equivalent, so that there is a map $h : Q \to N$ satisfying (1.27) and (1.28). Let G, G' be the group extensions of N by Q as constructed in proposition 1.2.11. As a set, $G = G' = Q \times N$. We need to show that both extensions are equivalent, i.e., that there is a homomorphism $\varphi : G \to G'$ such that the diagram of proposition 1.2.16 commutes. We define φ by

$$(x,a) \mapsto (x, h(x)^{-1}a) \tag{1.31}$$

Clearly this map is bijective. It is also a homomorphism with respect to the composition (1.25).

$$\begin{aligned}
\varphi(g \circ h) &= \varphi((x,a) \circ (y,b)) = \varphi\big((xy, f(x,y)T(y)(a)b)\big) \\
&= (xy, h(xy)^{-1} f(x,y) T(y)(a)b)
\end{aligned}$$

$$\begin{aligned}
\varphi(g) \circ \varphi(h) &= (x, h(x)^{-1}a) \circ (y, h(y)^{-1}b) \\
&= (xy, f'(x,y) \cdot T'(y)(h(x)^{-1}a) \cdot h(y)^{-1}b) \\
&= (xy, f'(x,y) \cdot [\gamma(h(y)) \circ T(y)]((h(x)^{-1}a)h(y)^{-1}b)) \\
&= (xy, h(xy)^{-1} f(x,y) T(y)(h(x)) h(y) \cdot \\
&\qquad [\gamma(h(y)) \circ T(y)]((h(x)^{-1}a)h(y)^{-1}b)) \\
&= (xy, h(xy)^{-1} f(x,y) T(y)(h(x)) \cdot T(y)(h(x)^{-1}a) h(y) h(y)^{-1} b) \\
&= (xy, h(xy)^{-1} f(x,y) T(y)(a)b)
\end{aligned}$$

In the second computation we have used also (1.27) and (1.28). It remains to show that the diagram commutes. Since $h(1) = 1$ we have $h(1)^{-1} = 1$, so that we obtain

$$\begin{aligned}
(\varphi\alpha)(a) &= \varphi((1,a)) = (1, h(1)^{-1}a) = (1,a) = \gamma(a) \\
(\delta\varphi)((x,a)) &= \delta((x, h(x)^{-1}a)) = x = \beta((x,a))
\end{aligned}$$

It follows $\gamma = \varphi\alpha$ and $\beta = \delta\varphi$. □

Now we can formulate the main result of this section.

Theorem 1.2.18 (Schreier). *Let N and Q be two groups. By associating every extension of N by Q a factor system one obtains a one-to-one correspondence between the set of equivalence classes of extensions of N by Q and the set of equivalence classes of factor systems to N and Q.*

In particular, if the factor set associated with the extension G of N by Q is equivalent to the *trivial* factor set then the extension G is equivalent to some semidirect product of N by Q. Conversely, the factor set associated with a semidirect product is equivalent to the trivial factor set.

CHAPTER 2

Cohomology of groups

We shall first give the original definition of the cohomology groups which is, unlike the definition of the derived functors, quite concrete.

2.1. G-modules

If G is a group, we define a G-module M to be an abelian group, written additively, on which G acts as endomorphisms. That means the following:

DEFINITION 2.1.1. Let G be a group. A *left G-module* is an abelian group M together with a map

$$G \times M \to M, \quad (g, m) \mapsto gm$$

such that, for all $g, h \in G$ and $m, n \in M$,

$$g(m+n) = gm + gn \tag{2.1}$$

$$(gh)m = g(hm) \tag{2.2}$$

$$1m = m \tag{2.3}$$

Equivalently a left G-module is an abelian group M together with a group homomorphism

$$T : G \to \operatorname{Aut}(M)$$

where the correspondence is given by

$$T(g)(m) = gm \quad \forall\, m \in M \tag{2.4}$$

As in representation theory, we can transform this to a more familiar concept. Let $\mathbb{Z}[G]$ denote the group ring of G. This is the free $\mathbb{Z}$-module with the elements of G as base and in which multiplication is defined by

$$\left(\sum_g n_g g\right)\left(\sum_h m_h h\right) = \sum_{g,h} n_g m_h (gh) \tag{2.5}$$

where $n_g, m_h \in \mathbb{Z}$ and the sums are finite. For example, let $G = \mathbb{Z} = \langle t \rangle$. Then $\{t^i\}_{i \in \mathbb{Z}}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[G]$. Hence $\mathbb{Z}[G] = \mathbb{Z}[t, t^{-1}]$ is the ring of Laurent polynomials.

If M is a G-module, then M becomes a $\mathbb{Z}[G]$-module if we define

$$\left(\sum_g n_g g\right) m = \sum_g n_g (gm) \tag{2.6}$$

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

Example 2.1.2. *Let M be any abelian group and define*

$$gm = m \tag{2.7}$$

for all $g \in G$, $m \in M$. This action of G is called the trivial action, and M is called a trivial G-module.

Example 2.1.3. *The module $M = \mathbb{Z}[G]$ with the action*

$$h\left(\sum_g n_g g\right) = \sum_g n_g hg \tag{2.8}$$

is called the regular G-module.

Definition 2.1.4. Let M be a G-module. Define

$$M^G = \{m \in M \mid gm = m \text{ for all } g \in G\} \tag{2.9}$$

Then M^G is a submodule of M which is called the *module of invariants.*

If M is a trivial G-module then $M^G = M$.

Definition 2.1.5. Let M, N be two G-modules. A homomorphism of G-modules is a map $\varphi\colon M \to N$ such that

$$\varphi(m + m') = \varphi(m) + \varphi(m') \tag{2.10}$$

$$\varphi(gm) = g\varphi(m) \tag{2.11}$$

for all $g \in G$ and $m, m' \in M$. We write $\mathrm{Hom}_G(M, N)$ for the set of all G-module homomorphisms $\varphi\colon M \to N$.

2.2. The n-th cohomology group

Let A be a G-module and let $C^n(G, A)$ denote the set of functions of n variables

$$f : G \times G \times \cdots \times G \to A$$

into A. For $n = 0$ let $C^0(G, A) = \mathrm{Hom}(1, A) \cong A$. The elements of $C^n(G, A)$ are called *n-cochains.* The set $C^n(G, A)$ is an abelian group with the usual definitions of addition and the element 0:

$$\begin{aligned}(f + g)(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)\\ 0(x_1, \ldots, x_n) &= 0\end{aligned}$$

We now define homomorphisms $\delta = \delta_n : C^n(G, A) \to C^{n+1}(G, A)$.

Definition 2.2.1. If $f \in C^n(G, A)$ then define $\delta_n(f)$ by

$$\begin{aligned}\delta_n(f)(x_1, \dots, x_{n+1}) &= x_1 f(x_2, \dots, x_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(x_1, \dots, x_{i-1}, x_i x_{i+1}, \dots, x_{n+1}) \\ &\quad + (-1)^{n+1} f(x_1, \dots, x_n)\end{aligned}$$

For $n = 0, 1, 2, 3$ we obtain

$$(\delta_0 f)(x_1) = x_1 f - f \tag{2.12}$$

$$(\delta_1 f)(x_1, x_2) = x_1 f(x_2) - f(x_1 x_2) + f(x_1) \tag{2.13}$$

$$(\delta_2 f)(x_1, x_2, x_3) = x_1 f(x_2, x_3) - f(x_1 x_2, x_3) + f(x_1, x_2 x_3) - f(x_1, x_2) \tag{2.14}$$

$$\begin{aligned}(\delta_3 f)(x_1, x_2, x_3, x_4) &= x_1 f(x_2, x_3, x_4) - f(x_1 x_2, x_3, x_4) + f(x_1, x_2 x_3, x_4) \\ &\quad - f(x_1, x_2, x_3 x_4) + f(x_1, x_2, x_3)\end{aligned} \tag{2.15}$$

For $n = 0$, f is considered as an element of A so that $x_1 f$ makes sense.

We will show that $\delta^2(f) = 0$ for every $f \in C^n(G, A)$, i.e., $\delta_{n+1}\delta_n = 0$ for all $n \in \mathbb{N}$ and hence $\operatorname{im} \delta_n \subseteq \ker \delta_{n+1}$.

Lemma 2.2.2. *It holds $\delta_{n+1}\delta_n(C^n(G, A)) = 0$ for all $n \in \mathbb{N}$. Hence the following sequence is a complex.*

$$A \xrightarrow{\delta_0} C^1(G, A) \xrightarrow{\delta_1} \cdots \xrightarrow{\delta_{n-1}} C^n(G, A) \xrightarrow{\delta_n} C^{n+1}(G, A) \xrightarrow{\delta_{n+1}} \cdots$$

Proof. Let $f \in C^n(G, A)$. We want to show $\delta^2(f)(x_1, \dots, x_{n+2}) = 0$. Define $g_j \in C^{n+1}(G, A)$ for $0 \le j \le n+1$ by

$$g_j(x_1, \dots, x_{n+1}) = \begin{cases} x_1 f(x_2, \dots, x_{n+1}), & j = 0 \\ (-1)^j f(x_1, \dots, x_j x_{j+1}, \dots, x_{n+1}), & 1 \le j \le n \\ (-1)^{n+1} f(x_1, \dots, x_n), & j = n+1 \end{cases}$$

This means

$$(\delta f)(x_1, \dots, x_{n+1}) = \sum_{j=0}^{n+1} g_j(x_1, \dots, x_{n+1})$$

Then define $g_{ji} \in C^{n+2}(G, A)$ for $0 \le i \le n+2$ by

$$g_{ji}(x_1, \dots, x_{n+2}) = \begin{cases} x_1 g_j(x_2, \dots, x_{n+2}), & i = 0 \\ (-1)^i g_j(x_1, \dots, x_i x_{i+1}, \dots, x_{n+2}), & 1 \le i \le n+1 \\ (-1)^{n+2} g_j(x_1, \dots, x_{n+1}), & i = n+2 \end{cases}$$

This means

$$(\delta g_j)(x_1, \dots, x_{n+2}) = \sum_{i=0}^{n+2} g_{ij}(x_1, \dots, x_{n+2})$$

It follows

$$\delta^2(f)(x_1,\dots,x_{n+2}) = \sum_{j=0}^{n+1}(\delta g_j)(x_1,\dots,x_{n+2}) = \sum_{j=0}^{n+1}\sum_{i=0}^{n+2} g_{ij}(x_1,\dots,x_{n+2})$$

We will show that for all $0 \le j \le n+1$ and all $j+1 \le i \le n+2$

$$(g_{ji} + g_{i-1,j})(x_1,\dots,x_{n+2}) = 0 \tag{2.16}$$

This will imply our result as follows. Write down all g_{ji} as an $(n+2)\times(n+3)$ array and cancel out each pair $(g_{ji}, g_{i-1,j})$ starting with $j=0$ and $i=1,\dots,n+2$, then $j=1$ and $i=2,\dots n+2$, until $j=n+1$ and $i=n+2$. Then all entries of the array are cancelled out and we obtain $\delta^2(f) = \sum_{j=0}^{n+1}\sum_{i=0}^{n+2} g_{ij} = 0$.
It remains to show (2.16). Assume first $1 \le j \le n$. If $i > j+1$ then

$$\begin{aligned} g_{ji}(x_1,\dots,x_{n+2}) &= (-1)^i g_j(x_1,\dots,x_i x_{i+1},\dots,x_{n+2}) \\ &= (-1)^i g_j(\tau_1,\dots,\tau_{n+1}) \\ &= (-1)^{i+j} f(\tau_1,\dots,\tau_j\tau_{j+1},\dots,\tau_{n+1}) \\ &= (-1)^{i+j} f(x_1,\dots,x_j x_{j+1},\dots,x_i x_{i+1},\dots,x_{n+2}) \end{aligned}$$

with

$$\begin{gathered}(\tau_1,\dots,\tau_j,\tau_{j+1},\dots,\tau_i,\tau_{i+1},\dots,\tau_{n+1}) = \\ (x_1,\dots,x_j,x_{j+1},\dots,x_i x_{i+1},x_{i+2},\dots,x_{n+2}).\end{gathered}$$

On the other hand we have

$$\begin{aligned} g_{i-1,j}(x_1,\dots,x_{n+2}) &= (-1)^j g_{i-1}(x_1,\dots,x_j x_{j+1},\dots,x_{n+2}) \\ &= (-1)^j g_{i-1}(\sigma_1,\dots,\sigma_j,\dots,\sigma_{n+1}) \\ &= (-1)^{i-1+j} f(\sigma_1,\dots,\sigma_{i-1}\sigma_i,\dots,\sigma_{n+1}) \\ &= (-1)^{i+j-1} f(x_1,\dots,x_j x_{j+1},\dots,x_i x_{i+1},\dots,x_{n+2}) \end{aligned}$$

with

$$\begin{gathered}(\sigma_1,\dots,\sigma_{j-1},\sigma_j,\dots,\sigma_{i-1},\sigma_i,\dots,\sigma_{n+1}) = \\ (x_1,\dots,x_{j-1},x_j x_{j+1},\dots,x_i,x_{i+1},\dots,x_{n+2}).\end{gathered}$$

It follows $g_{ij} + g_{i-1,j} = 0$. If $i = j+1$ we obtain in the same way

$$\begin{aligned} g_{ji}(x_1,\dots,x_{n+2}) &= (-1)^{i+j} f(x_1,\dots,x_{i-1}x_i x_{i+1},\dots,x_{n+2}) \\ &= -g_{i-1,j}(x_1,\dots,x_{n+2}) \end{aligned}$$

The remaining cases $j=0$ and $j=n+1$ follow similarly. □

Define the subgroups $Z^n(G,A) = \ker\delta_n$ and $B^n(G,A) = \operatorname{im}\delta_{n-1}$. For $n=0$ let $B^0(G,A) = 0$. Since $B^n(G,A) \subseteq Z^n(G,A)$ we can form the factor group:

Definition 2.2.3. The *n-th cohomology group* of G with coefficients in A is given by the factor group

$$H^n(G,A) = Z^n(G,A)/B^n(G,A) = \ker\delta_n/\operatorname{im}\delta_{n-1}$$

2.3. The zeroth cohomology group

For $n = 0$ we have

$$H^0(G, A) = Z^0(G, A) = \{a \in A \mid xa = a \,\forall\, x \in G\} = A^G$$

Hence $H^0(G, A) = A^G$ is the module of invariants. Let L/K be a finite Galois extension with Galois group $G = Gal(L/K)$. Then L and $L^\times$ are G-modules. Here L is regarded as a group under addition and $L^\times$ is the multiplicative group of units in L. We have

$$H^0(G, L^\times) = (L^\times)^G = K^\times$$

Let p be a prime and C_p the cyclic group of order p.

Example 2.3.1. *Let $A = C_p$ be a $G = C_p$-module. Then $xa = a$ for all $x \in C_p$, i.e., A is a trivial C_p-module. We have*

$$H^0(C_p, C_p) = C_p$$

Denote by xa the action of G on A. Let $T : C_p \to \mathrm{Aut}(C_p) \cong C_{p-1}$ be the homomorphism defined by $xa = T(x)a$. Now $\ker T$ being a subgroup of C_p must be trivial or equal to C_p, since p is prime. However $\ker T = 1$ is impossible since T is not injective. In fact, C_p is not contained in $\mathrm{Aut}(C_p)$. Hence it follows $\ker T = C_p$ and $T(C_p) = \{id\}$. This means $xa = T(x)a = a$. Since A is a trivial C_p-module it follows $A^G = A$.

Lemma 2.3.2. *Let M be a G-module, and regard $\mathbb{Z}$ as a trivial G-module. Then*

$$H^0(G, M) = M^G \cong \mathrm{Hom}_G(\mathbb{Z}, M)$$

Proof. A G-module homomorphism $\varphi : \mathbb{Z} \to M$ is uniquely determined by $\varphi(1)$, and $m \in M$ is the image of 1 under φ if and only if it is fixed by G, i.e., if $m \in M^G$.

$$gm = g(\varphi(1)) = \varphi(g \cdot 1) = \varphi(1) = m$$

Here $g \cdot 1 = 1$ since G acts trivially on $\mathbb{Z}$. □

2.4. The first cohomology group

If A is a G-module then

$$Z^1(G, A) = \{f : G \to A \mid f(xy) = xf(y) + f(x)\}$$
$$B^1(G, A) = \{f : G \to A \mid f(x) = xa - a \text{ for some } a \in A\}$$

The 1-cocycles are also called crossed homomorphisms of G into A. A 1-coboundary is a crossed homomorphism, i.e., $\delta_1\delta_0 = 0$. For the convenience of the reader we repeat the calculation. Let $f = \delta_0(a)(x_1) = x_1 a - a$ and compute

$$\begin{aligned}(\delta_1\delta_0)(a)(x, y) &= \delta_1(f)(x, y) = xf(y) - f(xy) + f(x)\\ &= x(ya - a) - (xy)a + a + xa - a\\ &= 0\end{aligned}$$

Hence $(\delta_1\delta_0)(a) = 0$. Let A be a trivial G-module. Then a crossed homomorphism is just a group homomorphism, i.e., $Z^1(G, A) = \mathrm{Hom}(G, A)$, $B^1(G, A) = 0$ and

$$H^1(G, A) = \mathrm{Hom}(G, A)$$

is the set of group homomorphisms from G into A.

Remark 2.4.1. We want to consider sometimes right G-modules instead of left G-modules. If A is a left $\mathbb{Z}[G]$-module with action $(x,a)\mapsto xa$, then $a*x=xa$ defines a right module action with multiplication $y*x=xy$ in G: $a*(x*y)=(yx)a=y(xa)=(a*x)*y$. Then the definition of 1-cocycles and 1-coboundaries becomes

$$Z^1(G,A)=\{f:G\to A\mid f(x*y)=f(x)*y+f(y)\}$$
$$B^1(G,A)=\{f:G\to A\mid f(x)=a*x-a \text{ for some } a\in A\}$$

Proposition 2.4.2. *Let A be a G-module. There exists a bijection between $H^1(G,A)$ and the set of conjugacy classes of subgroups $H\le G\ltimes A$ complementary to A in which the conjugacy class of G maps to zero.*

Proof. There is a bijection between subgroups $H\le G\ltimes A$ complementary to A and 1-cocycles $h\in Z^1(G,A)$. If H is complementary to A then $H=\tau(G)$ for a section $\tau:G\to G\ltimes A$ for $\pi:G\ltimes A\to G$. Writing $\tau(x)=(x,h(x))$ with $h:G\to A$ we have $H=\{(x,h(x))\mid x\in G\}$. We want to show that $h\in Z^1(G,A)$. The multiplication in $G\ltimes A$ is given by (1.10), with $\varphi(y)a=ay$ for $y\in G$ and $a\in A$. Note that this is a right action. Since we write A additively, the formula becomes

$$(x,a)(y,b)=(xy,ay+b)$$

Since $\tau(xy)=\tau(x)\tau(y)$ we have

$$(xy,h(xy))=(x,h(x))(y,h(y))=(xy,h(x)y+h(y))$$

so that $h(xy)=h(x)y+h(y)$. The converse is also clear. Moreover two complements are conjugate precisely when their 1-cocycles differ by a 1-coboundary: for $a\in A\le G\ltimes A$ the set aHa^{-1} consists of all elements of the form

$$(1,a)(x,h(x))(1,-a)=(x,ax-a-h(x))$$

Hence the cosets of $B^1(G,A)$ in $Z^1(G,A)$ correspond to the A-conjugacy classes of complements H in A, or in $G\ltimes A$ since $G\ltimes A=HA$. □

Corollary 2.4.3. *All the complements of A in $G\ltimes A$ are conjugate iff $H^1(G,A)=0$.*

We have the following result on cohomology groups of *finite* groups.

Proposition 2.4.4. *Let G be a finite group and A be a G-module. Then every element of $H^1(G,A)$ has a finite order which divides $|G|$.*

Proof. Let $f\in Z^1(G,A)$ and $a=\sum_{y\in G}f(y)$. Then $xf(y)-f(xy)+f(x)=0$. Summing over this formula we obtain

$$\begin{aligned}0&=x\sum_{y\in G}f(y)-\sum_{y\in G}f(xy)+f(x)\sum_{y\in G}1\\&=xa-a+|G|f(x)\end{aligned}$$

It follows that $|G|f(x)\in B^1(G,A)$, which implies $|G|Z^1(G,A)\subseteq B^1(G,A)$. Hence $|G|H^1(G,A)=0$. □

Corollary 2.4.5. *Let G be a finite group and A be a finite G-module such that $(|G|,|A|)=1$. Then $H^1(G,A)=0$.*

Proof. We have $|A|f=0$ for all $f\in C^1(G,A)$. Then the order of $[f]\in H^1(G,A)$ divides $(|G|,|A|)=1$. Hence the class $[f]$ is trivial. □

REMARK 2.4.6. We will show later that $H^n(G, A) = 0$ for all $n \in \mathbb{N}$ if the conditions of the corollary are satisfied.

We shall conclude this section by proving the following result which can be found already in Hilberts book *Die Theorie der algebraischen Zahlkörper* of 1895. It is called Hilbert's Satz 90 and we present a generalization of it due to Emmy Noether.

PROPOSITION 2.4.7. *Let L/K be a finite Galois extension with Galois group $G = Gal(L/K)$. Then we have $H^1(G, L^\times) = 1$ and $H^1(G, L) = 0$.*

PROOF. We have to show $Z^1 = B^1$ in both cases. Let $f \in Z^1(G, L^\times)$. This implies $f(\sigma) \neq 0$ for all $\sigma \in G$ since $f : G \to L^\times$. The 1-cocycle condition is, written multiplicatively, $f(\sigma\tau) = f(\sigma)\sigma f(\tau)$ or $\sigma f(\tau) = f(\sigma)^{-1} f(\sigma\tau)$. The 1-coboundary condition is $g(\sigma) = \sigma(a)/a$ for a constant a. By a well known result on the linear independence of automorphisms it follows that there exists a $\beta \in L^\times$ such that

$$\alpha := \sum_{\tau \in G} f(\tau)\tau(\beta) \neq 0$$

It follows that for all $\sigma \in G$

$$\begin{aligned}\sigma(\alpha) &= \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\beta)) = \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(\beta) = f(\sigma)^{-1} \sum_{\tau \in G} f(\tau)\tau(\beta) \\ &= f(\sigma)^{-1}\alpha\end{aligned}$$

It follows $f(\sigma) = \frac{\alpha}{\sigma(\alpha)} = \frac{\sigma(\alpha^{-1})}{\alpha^{-1}}$, hence $f \in B^1(G, L^\times)$.
For the second part, let $f \in Z^1(G, L)$. Since L/K is separable there exists a $\beta \in L$ such that

$$a := \sum_{\tau \in G} \tau(\beta) = Tr_{L/K}(\beta) \neq 0$$

Setting $\gamma = a^{-1}\beta$ we obtain $\sum_{\tau \in G} \tau(\gamma) = 1$ since $\tau(a) = a$ and $\tau(a^{-1}) = a^{-1}$. Let

$$x := \sum_{\tau \in G} f(\tau)\tau(\gamma)$$

Hence we obtain for all $\sigma \in G$

$$\begin{aligned}\sigma(x) &= \sum_{\tau \in G} \sigma(f(\tau))\sigma\tau(\gamma) = \sum_{\tau \in G} f(\sigma\tau)\sigma\tau(\gamma) - f(\sigma)\sigma\tau(\gamma) \\ &= x - f(\sigma)\end{aligned}$$

It follows $f(\sigma) = x - \sigma(x) = \sigma(-x) - (-x)$, hence $f \in B^1(G, L)$. □

REMARK 2.4.8. We have $H^n(G, L) = 0$ for all $n \in \mathbb{N}$, but not $H^n(G, L^\times) = 1$ in general.

2.5. The second cohomology group

Let G be a group and A be an abelian group. We recall the definition of a factor system, written additively for A. A pair of functions (f, T), $f : G \times G \to A$ and $T : G \to \mathrm{Aut}(A)$ is called factor system to A and G if

$$f(xy,z)+f(x,y)z=f(x,yz)+f(y,z) \tag{2.17}$$

$$T(xy)=T(y)T(x) \tag{2.18}$$

$$f(1,1)=0 \tag{2.19}$$

where $f(x,y)z=T(z)(f(x,y))$. Now let

$$0\to A\xrightarrow{\alpha}E\xrightarrow{\beta}G\to 1$$

be an abelian group extension of A by G. This equippes A with a natural G-module structure. We obtain $T(x)(a)=xa$, or $T(x)(a)=ax$, for $x\in G$ and $a\in A$, which is independent of a transversal function. In fact, the extension induces an (anti)homomorphism $T_\tau : G\to \operatorname{Aut}(A)$ with a transversal function $\tau : G\to E$, see chapter 1. Since A is abelian it follows $\gamma_{h(x)}=\mathrm{id}_{|A}$ so that $T_{\tau'}(x)=\gamma_{h(x)}T_\tau(x)=T_\tau(x)$. If we fix T and hence the G-module structure on A, then the set of factor systems $f=(f,T)$ to A and G forms an abelian group with respect to addition: $(f+g)(x,y)=f(x,y)+g(x,y)$. It follows from (2.17) that this group is contained in the group

$$Z^2(G,A)=\{f:G\times G\to A\mid f(y,z)-f(xy,z)+f(x,yz)-f(x,y)z=0\}$$

where we have considered A as a right G-module. One has to rewrite the 2-cocycle condition from definition (2.2.1) for a right G-module according to remark (2.4.1). Recall that

$$B^2(G,A)=\{f:G\times G\to A\mid f(x,y)=h(y)-h(xy)+h(x)y\}$$

is a subgroup of $Z^2(G,A)$ and the factor group is $H^2(G,A)$. Indeed, a 2-coboundary is a 2-cocycle. The sum of the following terms equals zero.

$$\begin{aligned}f(y,z)&=h(z)-h(yz)+h(y)z\\-f(xy,z)&=-h(z)+h(xyz)-h(xy)z\\f(x,yz)&=h(yz)-h(xyz)+h(x)yz\\-f(x,y)z&=-h(y)z+h(xy)z-h(x)yz\end{aligned}$$

Theorem 2.5.1. *Let G be a group and A be an abelian group, and let M denote the set of group extensions*

$$0\to A\xrightarrow{\alpha}E\xrightarrow{\beta}G\to 1$$

with a given G-module structure on A. Then there is a $1-1$ correspondence between the set of equivalence classes of extensions of A by G contained in M with the elements of $H^2(G,A)$. The class of split extensions in M corresponds to the class $[0]\in H^2(G,A)$. This class corresponds to the trivial class represented by the trivial factor system $f(x,y)=0$.

Proof. By theorem (1.2.18) the set of equivalence classes of such extensions is in bijective correspondence with the equivalence classes of factor systems $f\in Z^2(G,A)$. Two factor systems are equivalent if and only if they differ by a 2-coboundary in $B^2(G,A)$: by (1.28) we have

$$f_{\tau'}(x,y)=f_\tau(x,y)-h(xy)+h(x)y+h(y)$$

Note that there is exactly one normalized 2-cocycle in each cohomology class, i.e., with $f(1,1)=0$. Hence two extensions of A by G contained in M are equivalent if and only if they determine the same element of $H^2(G,A)$. □

Example 2.5.2. *Let $A=\mathbb{Z}/p\mathbb{Z}$ be a trivial $G=C_p$-module. Then $H^2(G,A)\cong\mathbb{Z}/p\mathbb{Z}$.*

Here p is a prime. There are exactly p equivalence classes of extensions

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{\alpha} E \xrightarrow{\beta} C_p \to 1$$

EXAMPLE 2.5.3. *Consider the Galois extension $L/K = \mathbb{C}/\mathbb{R}$ with Galois group $G = Gal(\mathbb{C}/\mathbb{R}) \cong C_2$. Then we have*

$$H^2(G, L^\times) \cong \mathbb{Z}/2\mathbb{Z}$$

The proof is left as an exercise. In general we have $H^2(G, L^\times) \cong Br(L/K)$, where $Br(L/K)$ is the relative Brauer group. It consists of equivalence classes of central simple K-algebras S such that $S \otimes_K L \cong M_n(L)$. Two central simple K-algebras are called equivalent if their skew-symmetric components are isomorphic. For any field K the equivalence classes of finite-dimensional central simple K-algebras form an abelian group with respect to the multiplication induced by the tensor product.
The group $Br(\mathbb{C}/\mathbb{R})$ consists of two equivalence classes. The matrix algebra $M_2(\mathbb{R})$ represents the class [0] and the real quaternion algebra $\mathbb{H}$ represents the class [1].
We will now generalize proposition (2.4.4).

PROPOSITION 2.5.4. *Let G be a finite group and A be a G-module. Then every element of $H^n(G, A)$, $n \in \mathbb{N}$, has a finite order which divides $|G|$.*

PROOF. Let $f \in C^n(G, A)$ and denote

$$a(x_1, \dots, x_{n-1}) = \sum_{y \in G} f(x_1, \dots, x_{n-1}, y)$$

Summing the formula for δf and using

$$\sum_{y \in G} f(x_1, \dots, x_{n-1}, x_n y) = a(x_1, \dots, x_{n-1})$$

we obtain

$$\begin{aligned} \sum_{y \in G} (\delta f)(x_1, \dots, x_n, y) = \; & x_1 a(x_2, \dots, x_n) \\ & + \sum_{i=1}^{n-1} (-1)^i a(x_1, \dots, x_i x_{i+1}, \dots, x_n) + (-1)^n a(x_1, \dots, x_{n-1}) \\ & + (-1)^{n+1} |G| f(x_1, \dots, x_n) \\ & = (\delta a)(x_1, \dots, x_n) + (-1)^{n+1} |G| f(x_1, \dots, x_n) \end{aligned}$$

Hence if $\delta f = 0$, then $|G| f(x_1, \dots, x_n) = \pm(\delta a)(x_1, \dots, x_n)$ is an element of $B^n(G, A)$. Then $|G| Z^n(G, A) \subseteq B^n(G, A)$, so that $|G| H^n(G, A) = 0$. □

COROLLARY 2.5.5. *Let G be a finite group and A be a finite G-module such that $(|G|, |A|) = 1$. Then $H^n(G, A) = 0$ for all $n \geq 1$. In particular, $H^2(G, A) = 0$. Hence any extension of A by G is split.*

The last part is a special case of the Schur-Zassenhaus theorem, see (1.1.27). We will sketch the proof of the general case.

SCHUR-ZASSENHAUS 2.5.6. *If n and m are relatively prime, then any extension $1 \to A \xrightarrow{\alpha} E \xrightarrow{\beta} G \to 1$ of a group A of order n by a group G of order m is split.*

Proof. If A is abelian, the extensions are classified by the groups $H^2(G, A)$, one group for every G-module structure on A. These are all zero, hence any extension of A by G is split.
In the general case we use induction on n. It suffices to prove that E contains a subgroup S of order m. Such a subgroup must be isomorphic to G under $\beta : E \to G$. For, if S is such a subgroup, then $S \cap A$ is a subgroup whose order divides $|S| = m$ and $|A| = n$. Then $S \cap A = 1$. Also $AS = E$ since $\alpha(A) = A$ is normal in E so that AS is a subgroup whose order is divided by $|S| = m$ and $|A| = n$ and so is a multiple of $nm = |E|$. It follows that E is a semidirect product and hence the extension of A by G is split.
Choose a prime p dividing n and let P be a p-Sylow subgroup of A, hence of E. Let Z be the center of P. It is well known that $Z \neq 1$, see [**4**], p. 75. Let N be the normalizer of Z in E. A counting argument shows that $AN = E$ and $|N/(A \cap N)| = m$, see [**5**]. Hence there is an extension $1 \to (A \cap N) \to N \to G \to 1$. If $N \neq E$, this extension splits by induction, so there is a subgroup of N, and hence of E, isomorphic to G. If $N = E$, then $Z \lhd E$ and the extension $1 \to A/Z \to E/Z \to G \to 1$ is split by induction. Let G' be a subgroup of E/Z isomorphic to G and let E' denote the set of all $x \in E$ mapping onto G'. Then E' is a subgroup of E, and $0 \to Z \to E' \to G' \to 1$ is an extension. As Z is abelian, the extension splits and there is a subgroup of E', hence of E, isomorphic to $G' \cong G$. □

2.6. The third cohomology group

We have seen that $H^n(G, A)$ for $n = 0, 1, 2$ have concrete group-theoretic interpretations. It turns out that this is also the case for $n \geq 3$. We will briefly discuss the case $n = 3$, which is connected to so called crossed modules. Such modules arise also naturally in topology.

Definition 2.6.1. Let E and N be groups. A *crossed module* (N, α) over E is a group homomorphism $\alpha\colon N \to E$ together with an action of E on N, denoted by $(e, n) \mapsto {}^{e}n$ satisfying

$$ {}^{\alpha(m)}n = m\,n\,m^{-1} \tag{2.20}$$

$$ \alpha({}^{e}n) = e\,\alpha(n)\,e^{-1} \tag{2.21}$$

for all $n, m \in N$ and all $e \in E$.

Example 2.6.2. *Let $E = \mathrm{Aut}(N)$ and $\alpha(n)$ be the inner automorphism associated to n. Then (N, α) is a crossed module over E.*

By definition we have ${}^{\alpha(m)}n = \alpha(m)(n) = m\,n\,m^{-1}$ and

$$\begin{aligned} \alpha({}^{e}n)(m) &= \alpha(e(n))(m) = e(n)me(n)^{-1} = e(ne^{-1}(m)n^{-1}) = e(\alpha(n)(e^{-1}(m))) \\ &= (e\alpha(n)e^{-1})(m) \end{aligned}$$

Example 2.6.3. *Any normal subgroup $N \lhd E$ is a crossed module with E acting by conjugation and α being the inclusion.*

Let (N, α) be a crossed module over E and $A := \ker \alpha$. Then the sequence $0 \to A \xrightarrow{i} N \xrightarrow{\alpha} E$ is exact. Since $\operatorname{im}\alpha$ is normal in E by (2.21) $G = \operatorname{coker}(\alpha)$ is a group. This means that the sequence $N \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1$ is exact. Since A is central in N by (2.20), and since the action of E on N induces an action of G on A, we obtain a 4-term exact sequence

$$0 \to A \xrightarrow{i} N \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1 \tag{2.22}$$

where A is a G-module. It turns out that equivalence classes of exact sequences of this form are classified by the group $H^3(G, A)$. Let us explain the equivalence relation. Let G be an arbitrary group and A be an arbitrary G-module. Consider all possible exact sequences of the form (2.22), where N is a crossed module over E such that the action of E on N induces the given action of G on A. We take on these exact sequences the smallest equivalence relation such that two exact sequences as shown below are equivalent whenever their diagram is commutative:

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "\mathrm{id}"] & N \arrow[r, "\alpha"] \arrow[d, "f"] & E \arrow[r] \arrow[d, "g"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A \arrow[r] & N' \arrow[r, "\alpha'"] & E' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Note that f and g need not be isomorphisms. We then have:

Theorem 2.6.4. *There is a* $1-1$ *correspondence between equivalence classes of crossed modules represented by sequences as above and elements of* $H^3(G,A)$.

We omit the proof, which can be found in [**12**], theorem 6.6.13.

2.7. Functorial definition of cohomology groups

We will briefly discuss the language of category theory.

DEFINITION 2.7.1. A *category* $\mathcal{C}$ consists of a nonempty class $ob(\mathcal{C})$ of objects, a set $\mathrm{Hom}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$ for each pair of objects A, B, called the set of morphisms from A to B, and a map

$$(\alpha, \beta) \mapsto \beta \circ \alpha \colon \mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$$

for each triple of objects A, B, C satisfying the following conditions:

(1) composition of morphisms is associative;
(2) for each object A, $\mathrm{Hom}(A, A)$ has an element id_A that is left and right identity for composition.

A fundamental category is the category $\mathcal{AB}$ of abelian groups. The objects are abelian groups , and the morphisms are group homomorphisms. Another important category is the category $\mathcal{M}_R$ of R-modules for a given arbitrary ring R.

DEFINITION 2.7.2. A *covariant functor* $F \colon \mathcal{C} \to \mathcal{D}$ is a map that associates with each object A of $\mathcal{C}$ an object $F(A)$ of $\mathcal{D}$, and with each morphism $\alpha \colon A \to B$ a morphism $F(\alpha) \colon F(A) \to F(B)$ such that $F(\alpha \circ \beta) = F(\alpha) \circ F(\beta)$ and $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$. The functor is called *contravariant* if $F(\alpha \circ \beta) = F(\beta) \circ F(\alpha)$.

DEFINITION 2.7.3. A pair of functors $F \colon \mathcal{A} \to \mathcal{B}$ and $G \colon \mathcal{B} \to \mathcal{A}$ is called *adjoint*, if for every pair of objects (A, B) with $A \in \mathcal{A}$ and $B \in \mathcal{B}$ there is a functorial bijection

$$\tau = \tau_{A,B} \colon \mathrm{Hom}_{\mathcal{B}}(F(A), B) \to \mathrm{Hom}_{\mathcal{A}}(A, G(B)).$$

This means, there is a bijection such that for all $f \colon A \to A'$ in $\mathcal{A}$ and all $g \colon B \to B'$ in $\mathcal{B}$ the following diagram of induced mappings commutes:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{B}}(F(A'), B) \arrow[r] \arrow[d] & \mathrm{Hom}_{\mathcal{B}}(F(A), B) \arrow[r] \arrow[d] & \mathrm{Hom}_{\mathcal{B}}(F(A), B') \arrow[d] \\
\mathrm{Hom}_{\mathcal{A}}(A', G(B)) \arrow[r] & \mathrm{Hom}_{\mathcal{A}}(A, G(B)) \arrow[r] & \mathrm{Hom}_{\mathcal{A}}(A, G(B'))
\end{tikzcd}$$

In this case, F is called the *left adjoint* of this pair, and G is called the *right adjoint* of this pair.

For example, $F = \mathrm{Hom}_R(M, \cdot)$ is a functor from $\mathcal{M}_R$ to $\mathcal{AB}$. The symbol $F = \mathrm{Hom}_R(M, \cdot)$ means that $F(N) = \mathrm{Hom}_R(M, N)$ for all N in $\mathcal{M}_R$.

PROPOSITION 2.7.4. *Let R be a ring and M be a left R-module. Then $F = \mathrm{Hom}_R(M, \cdot)$ is a covariant functor from $\mathcal{M}_R$ to $\mathcal{AB}$, und $F = \mathrm{Hom}_R(\cdot, M)$ is a contravariant functor from $\mathcal{M}_R$ to $\mathcal{AB}$.*

PROOF. Let $\beta \colon A \to B$ be a morphism in $\mathcal{M}_R$. How do we define $F(\beta)$? Let M be a fixed R-module. Consider the sequence $M \xrightarrow{\alpha} A \xrightarrow{\beta} B$ in $\mathcal{M}_R$. Then define a homomorphism $\tilde{\beta} = F(\beta)$ of abelian groups

$$F(\beta) \colon \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B)$$

by $F(\beta)(\alpha) = \tilde{\beta}(\alpha) = \beta \circ \alpha$. Obviously $\beta = \mathrm{id}$ in $\mathcal{M}_R$ implies $F(\beta) = \mathrm{id}$ in $\mathcal{AB}$. Given a sequence

$$M \xrightarrow{\alpha} A \xrightarrow{\beta} B \xrightarrow{\gamma} C$$

in $\mathcal{M}_R$, we obtain

$$F(\gamma \circ \beta)(\alpha) = (\gamma \circ \beta)(\alpha) = \gamma \circ (\beta \circ \alpha) \tag{2.23}$$

$$= F(\gamma)(F(\beta)(\alpha)). \tag{2.24}$$

Hence the functor $F = \mathrm{Hom}_R(M, \cdot)$ is covariant. The second claim follows similarly. □

PROPOSITION 2.7.5. *Let R be a commutative ring and M, N be two R-modules. Then both $F = M \otimes_R \cdot$ and $G = \cdot \otimes_R N$ are covariant functors from $\mathcal{M}_R$ to $\mathcal{M}_R$.*

PROOF. Given $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ in $\mathcal{M}_R$ we put

$$F(\alpha) = 1_M \otimes \alpha \colon M \otimes_R A \to M \otimes_R B,$$

where $(1_M \otimes \alpha)(x \otimes y) = x \otimes \alpha(y)$. Then

$$F(\beta \circ \alpha) = 1_M \otimes (\beta \circ \alpha) = (1_M \otimes \beta) \circ (1_M \otimes \alpha) \tag{2.25}$$

$$= F(\beta)F(\alpha). \tag{2.26}$$

Hence F is covariant. The second claim follows similarly. □

DEFINITION 2.7.6. A covariant functor $F \colon \mathcal{A} \to \mathcal{B}$ is called *exact*, if it takes short exact sequences in $\mathcal{A}$ to short exact sequences in $\mathcal{B}$. That means, given a short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

in $\mathcal{A}$ yields a short exact sequence

$$0 \to F(M_1) \to F(M_2) \to F(M_3) \to 0$$

in $\mathcal{B}$.
The functor is called *left-exact*, if only follows that

$$0 \to F(M_1) \to F(M_2) \to F(M_3)$$

is exact. It is called *right-exact*, if only follows that

$$F(M_1) \to F(M_2) \to F(M_3) \to 0$$

is exact.

The definition for contravariant functors is analogous. One has to reverse the arrows in $\mathcal{B}$. Hence a contravariant functor F is left-exact if every exact sequence

$$0 \to M_1 \to M_2 \to M_3$$

is taken to an exact sequence

$$0 \to F(M_3) \to F(M_2) \to F(M_1).$$

PROPOSITION 2.7.7. *The contravariant functor* $\mathrm{Hom}_R(\cdot, V)$ *from $\mathcal{M}_R$ to $\mathcal{AB}$ is left-exact, as well as the covariant functor* $\mathrm{Hom}_R(V, \cdot)$.

PROOF. We only show that $\mathrm{Hom}_R(V, \cdot)$ is a left-exact functor. In general, it is not an exact functor. So let

$$0 \to M_1 \xrightarrow{\psi} M_2 \xrightarrow{\varphi} M_3$$

be a short exact sequence of R-modules. We have to show that the sequence

$$0 \to \mathrm{Hom}_R(V, M_1) \xrightarrow{\tilde{\psi}} \mathrm{Hom}_R(V, M_2) \xrightarrow{\tilde{\varphi}} \mathrm{Hom}_R(V, M_3)$$

is exact. Let $\tilde{\psi}\sigma = 0$ for $\sigma \in \operatorname{Hom}_R(V, M_1)$. This means $\psi(\sigma(v)) = 0$ for all $v \in V$. We have $\sigma(v) = 0$, because ψ is injective, and hence $\sigma = 0$. This implies that also $\tilde{\psi}$ is injective.
Now let $\tilde{\varphi}\tau = 0$ with $\tau \in \operatorname{Hom}_R(V, M_2)$. Then $\varphi(\tau(v)) = 0$ for all $v \in V$, and $\tau(v) = \psi(v')$ with some $v' \in M_1$, depending on v. Since ψ is injective, v' is unique. Define $\tau' \in \operatorname{Hom}_R(V, M_1)$ by this v', i.e., let $\tau'(v) = v'$. Then it follows that

$$\tau(v) = \psi(v') = \psi(\tau'(v)) = (\tilde{\psi}\tau')(v).$$

Hence τ is contained in the image of $\tilde{\psi}$. □

Remark 2.7.8. The covariant functors $F = M \otimes_R \cdot$ and $G = \cdot \otimes_R N$ are right-exact, but not exact in general.

Definition 2.7.9. A category $\mathcal{C}$ is called *additive* if the sets $\operatorname{Hom}(A, B)$ are endowed with the structure of abelian groups for all objects A and B in $\mathcal{C}$, such that the following conditions hold:

(1) The law of composition of morphisms is bilinear, and there exists a zero object 0, i.e., such that $\operatorname{Hom}(0, A)$ and $\operatorname{Hom}(A, 0)$ have precisely one element for each object A.
(2) Finite products and finite coproducts exist in $\mathcal{C}$.

The second property can be replaced by the requirement, that every finite collection of objects in $\mathcal{C}$ has a direct sum. To say that objects A and B admit a *direct sum* means that there is an object $A \oplus B$ in the category and maps $i_A \colon A \to A \oplus B$, $i_B \colon B \to A \oplus B$, $p_A \colon A \oplus B \to A$, $p_B \colon A \oplus B \to B$ such that $p_A \circ i_A = \mathrm{id}_A$, $p_B \circ i_B = \mathrm{id}_B$, $p_A \circ i_B = 0$, $p_B \circ i_A = 0$ and $i_A p_A + i_B p_B = \mathrm{id}_{A \oplus B}$.
Some authors also use the following definition (using proposition 2.7.4 as a motivation):

Definition 2.7.10. Let $\mathcal{C}$ be an additive category. A sequence $0 \to A \to B \xrightarrow{\alpha} C$ is called *exact* if the sequence of abelian groups

$$0 \to \operatorname{Hom}(T, A) \to \operatorname{Hom}(T, B) \to \operatorname{Hom}(T, C)$$

is exact for all objects T in $\mathcal{C}$. A sequence $A \xrightarrow{\beta} B \to C \to 0$ is exact if the sequence of abelian groups

$$0 \to \operatorname{Hom}(C, T) \to \operatorname{Hom}(B, T) \to \operatorname{Hom}(A, T)$$

is exact for all objects T.

We define the kernel and the cokernel of a morphism as follows:

Definition 2.7.11. Let $\mathcal{C}$ be an additive category. Suppose that $f \colon A \to B$ is an arbitrary morphism in $\mathcal{C}$. A *kernel of f* is a morphism $\kappa \colon C \to A$ such that

(a) $f \circ \kappa \colon C \to B$ is the zero morphism:

$$\begin{tikzcd}
A \arrow[dr, "f"] & \\
C \arrow[u, "\kappa"] \arrow[r, "0"'] & B
\end{tikzcd}$$

(b) Given any morphism $\kappa' \colon D \to A$ such that $f \circ \kappa'$ is the zero morphism, there is a unique morphism $g \colon D \to C$ such that $\kappa \circ g = \kappa'$:

$$\begin{tikzcd}
 & A \arrow[dr, "f"] & \\
 & C \arrow[u, "\kappa"'] \arrow[r, "0"] & B \\
D \arrow[uur, "\kappa'"] \arrow[ur, dotted, "g"] \arrow[urr, "0"'] & &
\end{tikzcd}$$

Definition 2.7.12. Let $\mathcal{C}$ be an additive category. Suppose that $f \colon A \to B$ is an arbitrary morphism in $\mathcal{C}$. A *cokernel of* f is a morphism $\lambda \colon B \to C$ such that

(a) $\lambda \circ f \colon A \to C$ is the zero morphism:

$$\begin{tikzcd}
 & B \arrow[d, "\lambda"] \\
A \arrow[ur, "f"] \arrow[r, "0"'] & C
\end{tikzcd}$$

(b) Given any morphism $\lambda' \colon B \to D$ such that $\lambda' \circ f$ is the zero morphism, there is a unique morphism $g \colon C \to D$ such that $\lambda \circ g = \lambda'$:

$$\begin{tikzcd}
 & B \arrow[d, "\lambda"] \arrow[ddr, "\lambda'"] & \\
A \arrow[ur, "f"] \arrow[r, "0"] \arrow[drr, "0"'] & C \arrow[dr, dotted, "g"] & \\
 & & D
\end{tikzcd}$$

It is easy to see that kernels and cokernels are universal and hence uniquely determined if they exist (they need not exist in general).

Definition 2.7.13. An *abelian category* is an additive category $\mathcal{A}$ in which the following two conditions hold:

(3) Kernels and cokernels exist in $\mathcal{C}$.

(4) If $f \colon A \to B$ is a morphism whose kernel is 0, then f is the kernel of its cokernel, i.e., $\ker(\operatorname{coker}(f)) = f$.
If $f \colon A \to B$ is a morphism whose cokernel is 0, then f is the cokernel of its kernel, i.e., $\operatorname{coker}(\ker(f))) = f$.
A morphism whose kernel and cokernel are 0 is an isomorphism.

In other words, every morphism has both a kernel and a cokernel, every monomorphism is a kernel of a morphism and every epimorphism is a cokernel of a morphism.

We list some examples (and one counter-example) of abelian categories.

(a) The category $\mathcal{M}_R$ of R-modules, for any ring R.
(b) The category of finitely generated R-modules, for a Noetherian ring R.
(c) The category of complexes of R-modules.
(d) The category of vector bundles over a topological space.
(e) The category of sheaves of abelian groups over a topological space.

(f) The category of all groups is *not* an abelian category.

We need also special cases of the category $\mathcal{M}_R$. Taking the group ring $R = \mathbb{Z}[G]$ we obtain the category $\mathcal{M}_G$ of G-modules. For the trivial group $G = \{1\}$ we have the category of abelian groups ($\mathbb{Z}$-modules). We recall the following result:

Proposition 2.7.14. *Let* $1 \to I \xrightarrow{\alpha} N \xrightarrow{\beta} M \to 1$ *be a short exact sequence of R-modules. Then the following conditions are equivalent:*

(1) *There exists a module homomorphism* $\tau\colon M \to N$ *such that* $\beta\tau = \mathrm{id}_{|M}$.
(2) *There exists a module homomorphism* $\sigma\colon N \to I$ *such that* $\sigma\alpha = \mathrm{id}_{|I}$.
(3) *N is isomorphic to the direct sum of I and M, i.e.,*

$$N \simeq \mathrm{im}(\alpha) \oplus \ker(\sigma) \simeq \ker(\beta) \oplus \mathrm{im}(\tau)$$

Definition 2.7.15. Let $\mathcal{A}$ be an abelian category. An object I of $\mathcal{A}$ is *injective* if $\mathrm{Hom}(\cdot, I)$ is an exact functor, i.e., if $0 \to A \to B \to C \to 0$ is exact in $\mathcal{A}$ then also

$$0 \to \mathrm{Hom}(C, I) \to \mathrm{Hom}(B, I) \to \mathrm{Hom}(A, I) \to 0$$

is exact.

This sequence is automatically exact except at $\mathrm{Hom}(A, I)$. Hence to say that I is injective means that every homomorphism $A \to I$ extends to B, i.e., for each injection $f\colon A \to B$ and each $\alpha\colon A \to I$ there exists at least one map $\beta\colon B \to I$ such that $\alpha = \beta \circ f$.

Proposition 2.7.16. *Let I be an R-module in the category $\mathcal{M}_R$. Then the following conditions are equivalent:*

(1) *I is injective, i.e., the functor* $\mathrm{Hom}_R(\cdot, I)$ *is exact.*
(2) *Each short exact sequence of R-modules* $0 \to I \to N \to M \to 0$ *is split.*
(3) *Each R-module homomorphism f of a submodule M' of M to I can be extended to a R-module homomorphism $h\colon M \to I$. In other words, the following diagram is commutative, $h \circ \alpha = f$:*

$$\begin{tikzcd}
& I & \\
0 \arrow[r] & M' \arrow[u, "f"] \arrow[r, "\alpha"] & M \arrow[ul, dotted, "h"']
\end{tikzcd}$$

Proof. We just gave a short reasoning why (1) and (3) are equivalent. Now assume (3) and consider the following diagram:

$$\begin{tikzcd}
& I & \\
0 \arrow[r] & I \arrow[u, "\mathrm{id}"] \arrow[r, "\alpha"] & N \arrow[ul, dotted, "h"']
\end{tikzcd}$$

Then (3) yields a homomorphism $h\colon N \to I$ such that $h \circ \alpha = \mathrm{id}_{|N}$. Using proposition 2.7.14 it follows (2), i.e., the short exact sequence there splits. Conversely, assume (2). To show (3), let

$$\begin{tikzcd}
& I \\
0 \arrow[r] & M' \arrow[u, "f"] \arrow[r, "\alpha"] & M
\end{tikzcd}$$

be an exact diagram. We form the so-called push-out, see [**8**],

$$\begin{tikzcd}
M' \arrow[r, "\alpha"] \arrow[d] & M \arrow[d] \\
I \arrow[r, "\alpha'"] & N
\end{tikzcd}$$

where $N = I \oplus_{M'} M$. Since α is a monomorphism, so is α'. By (2) the sequence $0 \to I \xrightarrow{\alpha} N$ splits, and composing the splitting map $\sigma\colon N \to I$ with the push-out map $M \to N$ we obtain the desired homomorphism $h\colon M \to I$ satisfying $h \circ \alpha = f$, proving (3). □

Definition 2.7.17. Let $\mathcal{A}$ be an abelian category. We say that $\mathcal{A}$ has *enough injectives* if for every object A in $\mathcal{A}$ there is an injection $A \to I$ where I is injective.

We have the following important theorem.

Theorem 2.7.18. *Every R-module can be embedded into an injective R-module, i.e., the category $\mathcal{M}_R$ respectively $\mathcal{M}_G$ has enough injectives.*

Proof. Here is a very rough outline of the proof. For details see [**8**]. Let T be a *divisible abelian group*. This means, the homomorphism $x \mapsto mx$ from T to T is surjective for all $m \in \mathbb{Z}$. The first step in the proof is to show that then $\mathrm{Hom}_{\mathbb{Z}}(R,T)$ is an injective R-module. If M is an arbitrary R-module then it is possible to embedd M into some divisible abelian group T. This will induce an embedding of M into the injective R-module $\mathrm{Hom}_{\mathbb{Z}}(R,T)$. □

Every category $\mathcal{C}$ has an opposite category $\mathcal{C}^{op}$ where the objects are the same as the objects in $\mathcal{C}$, but the morphisms and compositions are reversed, so that there is a $1-1$ correspondence $f \mapsto f^{op}$ between morphisms $f\colon B \to C$ in $\mathcal{C}$ and morphisms $f^{op}\colon C \to B$ in $\mathcal{C}^{op}$. The categories $\mathcal{C}$ and $\mathcal{C}^{op}$ need not be isomorphic: for example, let $\mathcal{T}$ be the category of torsion abelian groups. Then $\mathcal{T}^{op}$ is the category of profinite abelian groups.
Let $\mathcal{A}$ be an abelian category. Then $\mathcal{A}^{op}$ is also abelian and injective objects in $\mathcal{A}$ correspond to so called projective objects in $\mathcal{A}^{op}$. We have the following dual definition.

Definition 2.7.19. Let $\mathcal{A}$ be an abelian category. An object P of $\mathcal{A}$ is *projective* if $\mathrm{Hom}(P,\cdot)$ is an exact functor, i.e., if $0 \to A \to B \to C \to 0$ is exact in $\mathcal{A}$ then also

$$0 \to \mathrm{Hom}(P,A) \to \mathrm{Hom}(P,B) \to \mathrm{Hom}(P,C) \to 0$$

is exact.

Indeed, A is injective in $\mathcal{A}$ if and only if A is projective in $\mathcal{A}^{op}$.

Example 2.7.20. *Consider the category of all complex vector spaces. Then each object is projective and injective.*

Indeed, every module in this category is free, since it has a basis, and hence projective.

Example 2.7.21. *The category of finite abelian groups $\mathcal{F}$ is an example of an abelian category that has no projective objects. Since $\mathcal{F}$ is equivalent to $\mathcal{F}^{op}$ it has also no injective objects.*

Proposition 2.7.22. *Let P be an R-module in the category $\mathcal{M}_R$. Then the following conditions are equivalent:*

(1) *P is projective, i.e., the functor $\mathrm{Hom}_R(P,\cdot)$ is exact.*
(2) *Each short exact sequence of R-modules $0 \to N \to M \to P \to 0$ is split.*

(3) *For each surjective R-module homomorphism $g\colon B \to C$ and an R-module homomorphism $\gamma\colon P \to C$ there is at least one R-module homomorphism $\beta\colon P \to B$ such that $\gamma = g \circ \beta$:*

$$\begin{tikzcd}
 & P \arrow[d, "\gamma"'] \arrow[dr, dotted, "\beta"] & \\
0 & C \arrow[l] & B \arrow[l, "g"']
\end{tikzcd}$$

Definition 2.7.23. Let $\mathcal{A}$ be an abelian category. We say that $\mathcal{A}$ has *enough projectives* if for every object A in $\mathcal{A}$ there is a surjection $P \to A$ where P is projective.

Proposition 2.7.24. *The category $\mathcal{M}_R$ respectively $\mathcal{M}_G$ has enough projectives.*

Indeed, every R-module is the homomorphic image of a free, hence projective R-module.

We could also use projectives for the definition of cohomology, but we will do it with injectives.

Definition 2.7.25. Let M be an object of a category $\mathcal{A}$. A *resolution* of M is a long exact sequence

$$0 \to M \to I^0 \to I^1 \to \cdots \to I^r \to \cdots$$

We sometimes write this $M \to I^\bullet$. If all the I^r are injective objects of $\mathcal{A}$, then it is called an *injective resolution.*

Proposition 2.7.26. *If the abelian category $\mathcal{A}$ has enough injectives, then every object in $\mathcal{A}$ has an injective resolution.*

Let $F\colon \mathcal{C} \to \mathcal{D}$ be a left exact functor from one abelian category to a second one. Let $M \to I^\bullet$ be an injective resolution of M. On applying the functor F, we obtain a complex

$$F(I)\colon 0 \xrightarrow{d^{-1}} F(I^0) \to F(I^1) \to \cdots \to F(I^r) \xrightarrow{d^r} F(I^{r+1}) \to \cdots$$

which may be no longer exact. Define

$$(R^rF)(M) = H^r(F(I)) := \ker(d^r)/\operatorname{im}(d^{r-1})$$

for all $r \geq 0$. One can show that the objects $(R^rF)(M)$ are well-defined up to a canonical isomorphism. Moreover, a morphism $\alpha : M \to N$ gives rise to a well-defined morphism $(R^rF)(M) \to (R^rF)(N)$. In fact, the R^rF are functors.

Definition 2.7.27. The above functors R^rF are called the *right derived functors* of F.

Example 2.7.28. *We have $R^0F = F$.*

Because F is left exact, $0 \to F(M) \to F(I^0) \xrightarrow{d^0} F(I^1)$ is exact. Therefore

$$(R^0F)(M) = \ker(d^0) = F(M)$$

Theorem 2.7.29. *A short exact sequence* $0 \to A \to B \to C \to 0$ *gives rise to a long exact sequence*

$$\begin{aligned} 0 &\to F(A) \to F(B) \to F(C) \to R^1F(A) \to R^1F(B) \to R^1F(C) \to \cdots \\ &\to R^rF(A) \to R^rF(B) \to R^rF(C) \to \cdots \end{aligned}$$

and the association of the long exact sequence to the short exact sequence is functorial.

The last condition means that a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

gives rise to a commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r] & R^{r-1}F(C) \arrow[r] \arrow[d] & R^rF(A) \arrow[r] \arrow[d] & R^rF(B) \arrow[r] \arrow[d] & R^rF(C) \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & R^{r-1}F(C') \arrow[r] & R^rF(A') \arrow[r] & R^rF(B') \arrow[r] & R^rF(C') \arrow[r] & \cdots
\end{tikzcd}$$

Now we turn to the functorial definition of cohomology groups.

LEMMA 2.7.30. *The functor $F\colon \mathcal{M}_G \to \mathcal{AB}$, $F(M) = M^G$ from the category of G-modules to the category of abelian groups is left exact.*

PROOF. This follows from the fact that $M^G = \mathrm{Hom}_G(\mathbb{Z}, M)$ for any G-module, see (2.3.2). Here $\mathbb{Z}$ is regarded as trivial G-module. □

Hence, if $0 \to N \to M \to V \to 0$ is exact then $0 \to N^G \to M^G \to V^G$ is exact. Since the category of G-modules has enough injectives, every G-module has an injective resolution and we can form the right derived functors of F.

DEFINITION 2.7.31. Let G be a group and M be a G-module. Define the r^{th} cohomology group of G with coefficients in M to be

$$H^r(G, M) = R^rF(M)$$

That means, if we choose an injective resolution

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$

of M, then the complex

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \to \cdots \xrightarrow{d^{r-1}} (I^r)^G \xrightarrow{d^r} (I^{r+1})^G \to \cdots$$

need no longer be exact, and we have $H^r(G, M) \cong \ker(d^r)/\operatorname{im}(d^{r-1})$. For any homomorphism $\alpha\colon M \to N$ of G-modules and any injective resolutions $M \to I^\bullet$ and $N \to J^\bullet$, α extends to a map of complexes $\widetilde{\alpha}\colon I^\bullet \to J^\bullet$,

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "\alpha"] & I^0 \arrow[r] \arrow[d] & I^1 \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & N \arrow[r] & J^0 \arrow[r] & J^1 \arrow[r] & \cdots
\end{tikzcd}$$

and the homomorphisms $H^r(\widetilde{\alpha})\colon H^r(I^{\bullet G}) \to H^r(J^{\bullet G})$ are independent of the choice of $\widetilde{\alpha}$. On applying this statement to the identity map $\mathrm{id}\colon M \to M$, we see that the groups $H^r(G, M)$ are well defined up to a canonical isomorphism. These groups have the following basic properties.

(1) We have $H^0(G, M) = F(M) = M^G$.

(2) If I is an injective G-module, then $H^r(G, I) = 0$ for all $r > 0$, because $0 \to I \to I \to 0 \to 0 \to \cdots$ is an injective resolution of I.

(3) A short exact sequence $0 \to N \to M \to V \to 0$ of G-modules gives rise to a long exact sequence

$$\begin{aligned} 0 &\to H^0(G,N) \to H^0(G,M) \to H^0(G,V) \to H^1(G,N) \to H^1(G,M) \to \cdots \\ &\to H^r(G,N) \to H^r(G,M) \to H^r(G,V) \to H^{r+1}(G,N) \to \cdots \end{aligned}$$

We have finally obtained two different definitions of cohomology groups. One by means of cochains and explicit formulas of the coboundary operators, the other by means of derived functors. One can show that there is a canonical isomorphism between the two cohomology groups.

CHAPTER 3

Galois cohomology

3.1. Profinite groups

Profinite groups G are compact topological groups for which the open normal subgroups form a fundamental system of neighbourhoods of $e = 1_G$. Following Bourbaki we require compact spaces to be Hausdorff.

Definition 3.1.1. A group G equipped with a topology is called a *topologic group* if

(1) the map $x \mapsto x^{-1}$, $G \to G$ is continuous.
(2) the map $(x, y) \mapsto xy$, $G \times G \to G$ is continuous, where $G \times G$ is equipped with the product topology.

There are numerous examples of topological groups. Any finite group equipped with the discrete topology is a topological group. The groups

$$(\mathbb{Q}, +), \ (\mathbb{R}, +), \ (\mathbb{C}, +)$$

with the usual topology induced by the Eudlidean metric are topological groups. Furthermore $(\mathbb{Q}, +)$ is also a topological group with respect to the p-adic topologies. Important examples of topological groups are given by the Lie groups (topological groups that are also differentiable manifolds), for instance by the group $GL(n, \mathbb{R})$. The topology on $GL(n, \mathbb{R})$ is defined by viewing $GL(n, \mathbb{R})$ as a subset of Euclidean space $\mathbb{R}^{n^2}$.
An isomorphism between two topological groups is an isomorphism of abstract groups and a homeomorphism of their topological spaces. There is a large literature on topological groups. We only need a few results.

Lemma 3.1.2. *Let G be a topological group and L_a be the left multiplication by $a \in G$. Then L_a is a homeomorphism. In particular, a subset $A \subseteq G$ is open if and only if aA is open.*

Proof. Of course, L_a is a homomorphism. Since L_a is the composition of the continuous maps $G \to G \times G$, $g \mapsto (a, g)$ and $G \times G \to G$, $(a, g) \mapsto ag$, it is also continuous. The inverse mapping $L_{a^{-1}}$ is continuous for the same reason. □

Lemma 3.1.3. *Let G be a topological group, $A, B \subseteq G$ be subsets and $\overline{A}, \overline{B}$ the topological closure of A resp. B. Then we have*

(1) $\overline{A} \cdot \overline{B} \subseteq \overline{AB}$.
(2) $\overline{A^{-1}} = \overline{A}^{-1}$.
(3) $\overline{gA} = g\overline{A}$ *for all* $g \in G$.

Proof. (1): Let $x \in \overline{A}$, $y \in \overline{B}$, and U a neighborhood of xy. Because group multiplication is continuous there exists a neighborhood V of 1 such that $xV \cdot yV \subset xyU$. Then xV is a neighborhood of x, and by assumption there is an $a \in xV \cap A$. Similarly there is a $b \in yV \cap B$. This implies $ab \in AB \cap xyU$, so that each neighborhood of xy intersects AB. Thus we have $xy \in \overline{AB}$.

(2): Denote by I the homeomorphism $G \to$, $g \mapsto g^{-1}$. Since $A^{-1} \subseteq \overline{A}^{-1} = I(\overline{A})$ the RHS is closed, so that $\overline{A^{-1}} \subseteq \overline{A}^{-1}$. On the other hand, $A^{-1} \subseteq \overline{A^{-1}}$, i.e.,

$$A \subseteq (\overline{A^{-1}})^{-1} = I(\overline{A^{-1}}).$$

Again the RHS is closed, so that $\overline{A} \subseteq (\overline{A^{-1}})^{-1}$, and hence $\overline{A}^{-1} \subseteq \overline{A^{-1}}$.

(3): We have $gA \subseteq g\overline{A}$, implying $\overline{gA} \subseteq g\overline{A}$ by the same argument as in (2), using the homeomorphism L_g instead of I. Conversely we have $A \subseteq g^{-1}\overline{gA}$, implying again $\overline{A} \subseteq g^{-1}\overline{gA}$. This means $g\overline{A} \subseteq \overline{gA}$. □

Lemma 3.1.4. *Let G be a topological group and H be a subgroup of G. Then H is a topological group with respect to the relative topology and the embedding $H \hookrightarrow G$ is continuous. The topological closure $\overline{H}$ is a subgroup of G as well.*

Proof. The multiplication $H \times H \to H$ is a restriction of a continuous map, hence continuous. The same is true for the Inverse $I \colon H \to H$. It remains to show that $\overline{H}$ is a group. By lemma 3.1.3 we have $\overline{H} \cdot \overline{H} \subseteq \overline{H \cdot H} = \overline{H}$ and $\overline{H}^{-1} = \overline{H^{-1}} = \overline{H}$. Hence $\overline{H}$ is a group. □

Lemma 3.1.5. *Every open subgroup H of a topological group G is closed at the same time.*

Proof. We have $G \setminus H = \bigcup_{g \notin H} gH$. Together with H all gH are open as well. Hence $G \setminus H$ is open, that is, H is closed. □

Lemma 3.1.6. *Let G be a topological group. If H is a normal subgroup then G/H is a topological group with respect to the quotient topology and the canonical projection $\pi \colon G \to G/H$ is open and continuous.*

Proof. Let $\mathcal{O}$ be the topology on G and $\pi \colon G \to G/H$ be the canonical projection. Then $\mathcal{O}' := \{U \subseteq G/H \mid \pi^{-1}(U) \in \mathcal{O}\}$ defines a topology on G/H such that π is continuous and open with respect to this topology. Indeed, $\emptyset$ and G/H are open sets, since $\emptyset = \pi^{-1}(\emptyset)$ and $G = \pi^{-1}(G/H)$. Furthermore, if $A_i \in \mathcal{O}'$, i.e., $\pi^{-1}(A_i) \in \mathcal{O}$, then

$$\pi^{-1}(\bigcup_i A_i) = \bigcup_i \pi^{-1}(A_i) \in \mathcal{O}$$

so that $\cup_i A_i \in \mathcal{O}'$. Similarly, the intersection of finitely many open sets A_i is again open. The map π is continuous by definition. It maps open sets to open sets: if $U \in \mathcal{O}$ then $\pi^{-1}(\pi(U)) = UH$. However, if U is open then UH is open as well. Now $(G/H, \mathcal{O}')$ is a topological group. To see that the multiplication is continuous, let W be a neighborhood of $g_1g_2H \in G/H$. Then $\pi^{-1}(W)$ is an open neighborhood of g_1g_2. Since multiplication in G is continuous, there exist neighborhoods U_j of g_j with $U_1U_2 \subseteq \pi^{-1}(W)$. Since π is open, the sets $\pi(U_j)$ are neigborhoods of g_jH, and $\pi(U_1)\pi(U_2) = \pi(U_1U_2) \subseteq W$. Similarly we see that the inverse taking is continuous. □

Let L/K be a Galois extension, possibly infinite. This means that L/K is algebraic, normal and separable. We want to give a topology on the group $G = Gal(L/K)$. Define a fundamental system of open neighbourhoods of $1_G \in G$ by the collection of subgroups of the form $H = Gal(L/F)$ for a finite extension F/K. Then the Galois closure M of F is still a finite Galois extension of K. Hence we always find a normal open subgroup $Gal(L/M) \subseteq H$. Thus we may actually define the system of neighbourhoods of 1_G to be the set of all normal subgroups $N = Gal(L/F)$ where F/K is a finite Galois extension. Let

$$\mathcal{O}' = \{N = Gal(L/F) \mid F/K \text{ is a finite Galois extension}\}$$

For each $\sigma \in G$, we define the system of neighbourhoods of σ to be $\sigma\mathcal{O}' = \{\sigma N \mid N \in \mathcal{O}'\}$. We will show that this defines a topology $\mathcal{O}$ on G, the so called *Krull topology.*

Proposition 3.1.7. *Let L/K be a Galois extension. Then $(Gal(L/K), \mathcal{O})$ is a Hausdorff topological group.*

Proof. We first show that $\mathcal{O}$ defines a topology. Let $G = Gal(L/K)$. Clearly $G \in \mathcal{O}$. Just take $F = K$. Also $\emptyset \in \mathcal{O}$. If $N_i = Gal(L/F_i) \in \mathcal{O}$ for $i = 1, 2$, then so is $N_1 \cap N_2 = Gal(L/F_1F_2) \in \mathcal{O}$ since the composite F_1F_2 of two finite Galois extensions is again a finite Galois extension. This shows that each intersection of finitely many sets in $\mathcal{O}$ is again contained in $\mathcal{O}$. Finally each union of sets in $\mathcal{O}$ belongs again to $\mathcal{O}$. If $\{N_i\}$ is a family of sets in $\mathcal{O}$ then $\cup_i N_i = Gal(L/\cap_i F_i) \in \mathcal{O}$ since the intersection $\cap_i F_i$ of arbitrarily many finite Galois extensions is again a finite Galois extension. Hence G is a topological space. It is also a topological group. The map $i\colon x \mapsto x^{-1}$ is continuous since the preimage of an open set $N = Gal(L/F) \in \mathcal{O}$ contains again an open set, i.e., a set contained in $\mathcal{O}$: because H is a group we have $i^{-1}(N) = N$. The map $(x, y) \mapsto xy$ is also continuous: let $N = \sigma\tau Gal(L/F) \in \mathcal{O}$ be an open neighbourhood of $\sigma\tau$. Then σN and τN are open neighbourhoods of σ respectively τ, and we have

$$\sigma N \cdot \tau N = \sigma\tau N \cdot N = \sigma\tau N$$

The first equality follows since N is a normal subgroup, and the second one since N is a group, i.e., $N = N \cdot N$. Finally we show that G is a Hausdorff group. Let $\sigma, \tau \in G$ such that $\sigma \neq \tau$. We have to find $U, V \in \mathcal{O}$ such that $\sigma U \cap \tau V = \emptyset$. Choose $\alpha \in L$ such that $\sigma(\alpha) \neq \tau(\alpha)$. Let F be the normal closure of $K(\alpha)$. This is a finite Galois extension of K so that $N = Gal(L/F) \in \mathcal{O}$. We claim that $\sigma N \cap \tau N = \emptyset$. Hence taking $U = V = N$ finishes the proof. Assume that the intersection would be non-empty. Then we would have $\sigma \in \tau N$. But then $\sigma(\alpha) = \tau(\alpha)$ since $\alpha \in F$ and N fixes F elementwise. This is a contradiction. □

Proposition 3.1.8. *Let L/K be a Galois extension. Then $(Gal(L/K), \mathcal{O})$ is totally disconnected and compact.*

Proof. A topological space is called totally disconnected if its connected components are the one-points sets. Let $G = Gal(L/K)$. We first show that $(Gal(L/K), \mathcal{O})$ is totally disconnected. For any finite subset S of L let

$$G(S) = \{\sigma \in G \mid \sigma(s) = s \;\forall\; s \in S\}.$$

The sets $G(S)$ with S being G-stable form a neighborhood base of 1 consisting of open normal subgroups. These $G(S)$ are open subgroups, hence also closed. Since $\bigcap G(S) = \{1_G\}$, this shows that the connected component of G containing 1_G is just $\{1_G\}$. By homogeneity (for each x, y in a topological group G there is a homeomorphism $f\colon G \to G$ such that $f(x) = y$), the analogue statement is true for every element of G.

To show that $(Gal(L/K), \mathcal{O})$ is compact is more difficult. We just give a rough idea, for a detailed and direct proof see Artin [**1**]. Also recall that we follow Bourbaki by requiring compact spaces to be Hausdorff. This property, however, we have just proved above. Let S be a finite subset of L stable under G. Then $G(S)$ is a normal subgroup of G of finite index because it is the kernel of the associated map $G \to \mathrm{Sym}(S)$. Since every finite set is contained in a stable finite set, one can show that the map

$$G \to \prod G/G(S)$$

is injective, where the product runs over these finite sets S which are stable under G. We endow $\prod G/G(S)$ with the product topology, so that the induced topology on G is that for which the $G(S)$ form an open neighborhodd base of 1_G, i.e., it is the Krull topology. According to the *Tychonoff theorem*, $\prod G/G(S)$ is compact. The proof is finished by showing that G is closed in the product. □

Remark 3.1.9. A good deal of number theory of this century can be interpreted as the study of the absolute Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. To obtain information on this group one lets it act on K-vector spaces. In other words, one is considering continuous homomorphisms $\varphi\colon Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(K)$ where $GL_n(K)$ is equipped with the discrete topology (even if it carries a natural topology, e.g., if $K = \mathbb{C}$). For $n = 1$ such continuous representations correspond to finite cyclic extensions of $\mathbb{Q}$. They have been studied already by Gauß and the results include, for example, the theorem of Kronecker-Weber and the prime number theorem of Dirichlet. The Kronecker-Weber Theorem is as follows: let $K/\mathbb{Q}$ be a finite abelian Galois extension, i.e, $Gal(K/\mathbb{Q})$ is abelian, then K is contained in a cyclotomic extension, i.e., there is a root of unity ζ such that $K \subseteq \mathbb{Q}(\zeta)$. The study of 2-dimensional continuous representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is among other things connected with the results of Wiles on the Taniyama-Shimura conjecture. This conjecture roughly says that any elliptic curve over $\mathbb{Q}$ is a modular form in disguise. It has been proved in 1999 by Wiles, Taylor, Ribet and the work of many more.

We want to explain briefly how the Krull topology can be used to extend the fundamental theorem of E. Galois to infinite Galois extensions. We recall a part of Galois' fundamental theorem when L/K is finite.

Theorem 3.1.10. *Let L/K be a finite Galois extension. Suppose that M is an intermediate field, i.e., $L/M/K$. Then L/M is a Galois extension and there is a one-to-one correspondence*

$$\{M \mid L/M/K \textit{ is an intermediate field}\} \leftrightarrow \{H \mid H \textit{ is a subgroup of } Gal(L/K)\}$$

given by $M \mapsto Gal(L/M)$ and $H \mapsto L^H$. For two intermediate fields M, M' we have $M \supset M'$ if and only if $Gal(L/M) \subset Gal(L/M')$, and $Gal(L/MM') = Gal(L/M) \cap Gal(L/M')$. Furthermore M/K is a Galois extension if and only if $Gal(L/M) \lhd Gal(L/K)$. In that case we have $Gal(L/K)/Gal(L/M) \cong Gal(M/K)$, induced by $\sigma \mapsto \sigma|_M$.

The fixed field is defined by $L^H = \{x \in L \mid \sigma(x) = x \;\forall \sigma \in H\}$.
It was already Dedekind who noted that the fundamental theorem fails in general for infinite Galois extensions. Here is an example. Let $K = \mathbb{F}_p$ be the field with p elements and let

$$\mathbb{F} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$$

its algebraic closure. The extension $\mathbb{F}/\mathbb{F}_p$ is normal and separabel since algebaic extensions of a finite field are separabel. Let $G = Gal(\mathbb{F}/\mathbb{F}_p)$ be its Galois group. Denote by $\varphi\colon \alpha \mapsto \alpha^p$ the Frobenius automorphism. We have $\varphi \in G$. Let $H = \langle \varphi \rangle$ be the subgroup of G generated by φ.

Example 3.1.11. *The fundamental theorem of Galois fails for the infinite Galois extension $L/K = \mathbb{F}/\mathbb{F}_p$. We have $L^H = L^G = \mathbb{F}_p$ and $H \neq G$. Hence there are two different subgroups of G with the same fixed field.*

Let us give a proof. Clearly $L^G = \mathbb{F}_p$. Let $x \in L^H$. Then we have $\varphi(x) = x$, hence x is a root of $X^p - X \in \mathbb{F}_p[X]$. All p elements of $\mathbb{F}_p$ are roots of this polynomial. Since $\mathbb{F}_p$ is a field, there cannot be more roots. Hence $x \in \mathbb{F}_p$ and $L^H = \mathbb{F}_p$. To show that H is a proper subgroup of G we have to construct a $\tau \in Gal(\mathbb{F}/\mathbb{F}_p)$ which is not a power of φ. It suffices to construct an infinite subfield M with $\mathbb{F}_p \subsetneqq M \subsetneqq \mathbb{F}$. The extension $\mathbb{F}/M$ will be also a Galois extension. Choose a $\tau \in Gal(\mathbb{F}/M) \setminus \{1\}$ and assume that $H = G$. Then $\tau = \varphi^n$ for some $n \in \mathbb{N}$. One may replace τ by τ^{-1} if necessary. Then φ^n fixes M elementwise and M is contained in the fixed field of φ^n, i.e., $M \subset \mathbb{F}_{p^n}$. This is a contradiction because M is infinite. Hence we have $H \neq G$. We claim that $M = \cup_{n \geq 0} \mathbb{F}_{p^{2^n}}$ is such an intermediate field. It is infinite but different from $\mathbb{F}$. To see this let F be a cubic extension of $\mathbb{F}_p$. Of course $F \subset \mathbb{F}$, but $F \nsubseteq M$. Write $F = \mathbb{F}_p(\alpha)$ and assume $\alpha \in M$. Then $\alpha \in \mathbb{F}_{p^{2^n}}$ for some n and $[\mathbb{F}_{p^{2^n}} : \mathbb{F}_p] = [\mathbb{F}_{p^{2^n}} : F][F : \mathbb{F}_p]$. However $3 = [F : \mathbb{F}_p]$ is not a divisor of $2^n = [\mathbb{F}_{p^{2^n}} : \mathbb{F}_p]$, a contradiction.

Remark 3.1.12. Let $\mathbb{F}_q$ be a finite field. Then $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}}$ is the profinite completion of the additive group $\mathbb{Z}$. It consists of sequences $(s_n)_{n=1}^{\infty}$ with $s_n \in \mathbb{Z}/n\mathbb{Z}$ such that if $m \mid n$, then $s_m \equiv s_n \mod m$. The set of such sequences forms a group by componentwise addition. The group $\widehat{\mathbb{Z}}$ is uncountable.

The question of how to modify the fundamental theorem so that it will apply also for infinite Galois extensions was solved by Krull. One has to equipp the Galois group with the Krull topology. Then there will be a bijection between *closed* subgroups of Galois groups and intermediate fields of the extension. In our example we would obtain $\overline{H} = G$, so that the above problem dissolves.

Theorem 3.1.13. *Let L/K be a Galois extension. We have the following canonical one-to-one correspondence*

$$\{M \mid L/M/K \text{ is an intermediate field}\} \leftrightarrow$$
$$\{H \mid H \text{ is a closed subgroup of } Gal(L/K)\}$$

given by $M \mapsto Gal(L/M)$ and $H \mapsto L^H$. Every open subgroup of $Gal(L/K)$ is closed, and open subgroups correspond to finite extensions L^H/K. For two intermediate fields M, M' we have $M \supset M'$ if and only if $Gal(L/M) \subset Gal(L/M')$, and $Gal(L/MM') = Gal(L/M) \cap Gal(L/M')$. Furthermore M/K is a Galois extension if and only if $Gal(L/M) \lhd Gal(L/K)$. In this case $\sigma \mapsto \sigma|_M$ induces an isomorphism of topological groups

$$Gal(L/K)/Gal(L/M) \cong Gal(M/K),$$

where the factor group is equipped with the quotient topology.

Galois groups will be our motivating example of profinite groups.

Definition 3.1.14. A partially ordered set $(I, \leq)$ is said to be *directed* if for any two elements i and j of I, there exists a $k \in I$ such that $i, j \leq k$. Suppose that for every element i of a directed set $(I, \leq)$ we have a group G_i, and for every inequality $i \leq j$ we have a group homomorphism $\pi_{ji} \colon G_j \to G_i$. If

(1) $\pi_{ii} = \mathrm{id}$ for all $i \in I$,
(2) $\pi_{ji} \circ \pi_{kj} = \pi_{ki}$ for all $i \leq j \leq k$,

then the family (G_i, π_{ji}) is called a *projective system* of groups (some authors write $(I, \leq, G_i, \pi_{ji})$). Given any such projective system, one defines a *projective limit* of it by

$$\varprojlim G_i = \{(g_i)_{i \in I} \in \prod_{i \in I} G_i \mid \pi_{ji}(g_j) = g_i \text{ whenever } i \leq j\}$$

This is indeed a group, being a subgroup of the direct product $\prod G_i$. The neutral element is $(1, 1, 1, \ldots)$. It is in $\varprojlim G_i$. If $g, h \in \varprojlim G_i$ with $g = (\cdots, g_i, \cdots)$ and $h = (\cdots, h_i, \cdots)$ then we have also $gh = (\cdots, g_ih_i, \cdots) \in \varprojlim G_i$. In fact $\pi_{ji}(g_jh_j) = \pi_{ji}(g_j)\pi_{ji}(h_j) = g_ih_i$. The group $\varprojlim G_i$ comes together with projections $\varprojlim G_i \to G_j$, induced by the projections $\pi_j \colon \prod G_i \to G_j$. Furthermore $\varprojlim G_i$ is a topological group as well. We give each G_i the discrete topology, the product $\prod G_i$ the product topology and the projective limit the restriction topology.

Proposition 3.1.15. *Let (G_i, π_{ji}) be a projective system of groups such that all G_i are compact Hausdorff topological groups. Then $\varprojlim G_i$ is a compact (Hausdorff) topological group.*

Proof. By the theorem of Tychonoff the product $\prod G_i$ together with the product topology is compact since all G_i are compact. The product topology is the most coarse topology such that all projections $\pi_j \colon \prod G_i \to G_j$ are continuous. It suffices to show that $\varprojlim G_i$ is closed in $\prod G_i$ with respect to the relative topology, because this will imply that $\varprojlim G_i$ is a compact topological group. If $g = (\ldots, g_i, \ldots)$ is in $\prod G_i \setminus \varprojlim G_i$ then there is an index pair (i, j) with $j \geq i$ and $\pi_{ji}(g_j) \neq g_i$. Since all G_i are Hausdorff there are open neighbourhoods V_j of $\pi_{ji}(g_j) \in G_i$ and U_i of $g_i \in G_i$ such that $V_j \cap U_i = \emptyset$. Since π_{ji} is continuous $U_j = \pi_{ji}^{-1}(V_j)$ is an open neighbourhood of $g_j \in G_j$. Then

$$U = U_i \times U_j \times \prod_{k \neq i,j} G_k$$

is an open neighbourhood of $g \in G$ which does not intersect $\varprojlim G_i$. In fact $U \cap \varprojlim G_i = \emptyset$ since $\pi_{ji}(U_j) \subset V_j$ and U_i have empty intersection. It follows that $\prod G_i \setminus \varprojlim G_i$ is open since every $g \in \prod G_i \setminus \varprojlim G_i$ has an open neighbourhood not intersecting $\varprojlim G_i$. But then $\varprojlim G_i$ is closed. □

Definition 3.1.16. A topological group which is isomorphic (as a topological group) to a projective limit of finite groups is called a *profinite group.*

One defines topological ring and profinite ring similarly. Before giving examples let us say that profinite groups can be described topologically as follows:

Proposition 3.1.17. *Let G be a topological group. The following assertions are equivalent.*

(1) *G is a profinite group.*
(2) *G is a compact (Hausdorff) totally disconnected group.*

Example 3.1.18. *Any finite group G is profinite.*

Let $I = \{1\}$, $G_i = G$ and $\pi_{11} = \mathrm{id}$. Equipp the finite groups G_i with the discrete topology. Then (G_i, π_{ji}) is a projective system with limit G. Hence G is profinite. Conversely every discrete profinite group is finite.

Example 3.1.19. *The group $\mathbb{Z}$ is not profinite.*

Indeed, $\mathbb{Z}$ is not compact. But we may form its profinite completion $\widehat{\mathbb{Z}}$, see below.

Example 3.1.20. *The p-adic numbers $\mathbb{Z}_p$ form a profinite ring.*

Let $R_i = \mathbb{Z}/p^i\mathbb{Z}$ and $\pi_{ji} \colon \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ the natural projections. The projective limit of these rings will be again a ring, namely the ring of p-adic integers

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

We can express the expansion of elements in $\mathbb{Z}_p$ as

$$\mathbb{Z}_p = \{(x_n)_{n=0}^{\infty} \in \prod_{n\geq 0} \mathbb{Z}/p^n\mathbb{Z} \mid x_{n+1} \equiv x_n \mod p^n\}$$

Definition 3.1.21. Let G be a group. The *profinite completion* of G is the profinite group $\widehat{G}$ defined by $\widehat{G} = \varprojlim G/N$, with N ranging over the set of normal subgroups of G of finite index, ordered by containment, the maps π_{ji} being the natural ones.

There is a natural group homomorphism $G \to \widehat{G}$ with dense image, which need not be injective in general.

Example 3.1.22. *The projective completion of $\mathbb{Z}$ is given by*

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \prod_{p\in\mathbb{P}} \mathbb{Z}_p$$

This is the absolute Galois group of a finite field $\mathbb{F}_q$, see remark 3.1.12.

Let I be the set of positive integers, partially ordered by $n \leq m$ iff $n \mid m$. Then $(I, \leq)$ is directed and $(I, \leq, \mathbb{Z}/nZ, \pi_{mn})$ forms a projective system with projective limit $\widehat{\mathbb{Z}}$. The π_{mn} are again the usual surjections.

Example 3.1.23. *Let L/K be a Galois extension. Then $Gal(L/K)$ is a profinite group and the profinite topology coincides with the Krull topology on $Gal(L/K)$.*

Let I be the set of intermediate fields F_i inside L/K such that F_i/K is a finite Galois extension. The set I is partially ordered by inclusion. We may take the composed field of two subfields, which is again a finite Galois extension, so the set I is directed. For $F_j \supset F_i$ we have restriction maps $\pi_{ji}\colon Gal(F_j/K) \to Gal(F_i/K)$. So we have a projective system and

$$Gal(L/K) = \varprojlim Gal(F_i/K)$$

where now each $Gal(F_i/K)$ is a finite group. We have now equipped $Gal(L/K)$ with the profinite topology. It coincides with the Krull topology. To see this we use the following lemma.

Lemma 3.1.24. *Let $(I, \leq, G_i, \pi_{ij})$ be a projective system of finite groups and $G = \varprojlim G_i$ the associated profinite group. Let $\pi_i\colon G \to G_i$ be the projections induced by the projections $\prod G_j \to G_i$. Then the sets $\{\ker(\pi_i) \mid i \in I\}$ form a fundamental system of open neighbourhoods of 1 in G.*

Proof. Since all G_i are finite, equipped with the discrete topology, we know that $\{1\}$ is a fundamental system of open neighbourhoods of 1 in G_i. According to the definition of the product topology of $\prod G_i$ and the relative topology of $G \subseteq \prod G_i$ the sets

$$G \cap \left(\prod_{j\in J} \{1\} \times \prod_{i\in I\setminus J} G_i \right) = \bigcap_{J\subseteq I} \ker(\pi_i)$$

form a fundamental system of open neighbourhoods of 1 in G, where J runs through the *finite* subsets of I. Since I is directed, and all J are finite there exists a $k \in I$ such that $j \leq k$ for all $j \in J$. This implies that

$$\ker(\pi_k) \subseteq \bigcap_{J\subseteq I} \ker(\pi_i),$$

so that the kernels of the projections π_i form a fundamental system of open neighbourhoods of 1 in G. □

Now we can identify the profinite topology and the Krull topology on $G = Gal(L/K)$. A fundamental system of open neighbourhoods of 1 in the Krull topology on $G = Gal(L/K)$ consists of the groups $G_i = Gal(L/F_i)$, where F_i/K is finite and normal. We have $G = \varprojlim G_i$ and $\ker(\pi_i) = Gal(L/F_i)$, since $\ker(\pi_i)$ consists of all automorphisms of L which are trivial on F_i.

Remark 3.1.25. The fact that $Gal(L/K)$ is a profinite group also follows from propositions 3.1.8 and 3.1.17.

We mention some properties of profinite groups.

Proposition 3.1.26. *Let H be a closed subgroup of a profinite group G. Then H is profinite as well.*

Note that the condition that H is closed is necessary. If we consider the profinite group $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ and its subgroup H, generated by the Frobenius automorphism, then $H \simeq \mathbb{Z}$, which is not a profinite group.

Proposition 3.1.27. *Let N be a closed normal subgroup of a profinite group G. Then G/N is profinite with the quotient topology.*

If H is an open subgroup of G, then the index $(G : H)$ is finite: G is compact and $\cup_{g\in G}\, gH$ is an open covering of G. On the other hand, subgroups of profinite groups of finite index need not be open in general:

Lemma 3.1.28. *Let V be an infinite dimensional vector space. For all $n \geq 1$, there exists a subspace V_n of V such that V/V_n has dimension n.*

Proof. It follows form Zorn's lemma that V contains maximal linearly independent subsets, which are indeed a basis of V. Choose such a basis and take V_n to be the subspace spanned by the set obtained by omitting exactly n elements from this basis. □

Proposition 3.1.29. *The profinite group $Gal(\mathbb{Q}^{al}/\mathbb{Q})$ has nonopen normal subgroups of finite index 2^n for all $n \geq 1$.*

Proof. Let E be the subfield

$$\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \ldots]$$

of the field $\mathbb{C}$. For each prime $p \in \mathbb{P}$ we have

$$Gal(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}]/\mathbb{Q}) \simeq \prod_{\substack{\ell\in\mathbb{P},\ell\leq p \\ \ell=\infty}} \mathbb{Z}/2\mathbb{Z}$$

This implies that

$$G := Gal(E/\mathbb{Q}) = \varprojlim_n Gal(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}]/\mathbb{Q})$$

is a direct product of coplies of $\mathbb{Z}/2\mathbb{Z}$ indexed by the primes ℓ of $\mathbb{Q}$ including $\ell = \infty$. Consider the following subgroup H of G:

$$H = \{(a_\ell) \in G \mid a_\ell = 0 \text{ for all but finitely many } \ell\}.$$

This subgroup is dense in G because, given a point $(a_\ell) \in G$, there is a sequence in H converging to (a_ℓ), given by

$$(a_\infty, 0, 0, 0, \ldots),\ (a_\infty, a_2, 0, 0, \ldots),\ (a_\infty, a_2, a_3, 0, \ldots),\ \ldots$$

We can regard G/H as a vector space over $\mathbb{F}_2$ and apply lemma 3.1.28 to obtain subgroups G_n of index 2^n in G containing H. Now G_n cannot be open. Otherwise it would be also closed, which contradicts the fact that H is dense. It follows that the inverse inverse of G_n in $Gal(\mathbb{Q}^{al}/\mathbb{Q})$ is a normal nonopen subgroup of finite index. □

A profinite group is called *topologically finitely-generated*, if it has a dense finitely-generated subgroup.

THEOREM 3.1.30 (Nikolov, Segal 2003). *Let G be a topologically finitely-generated profinite group. Then all subgroups of finite index are open.*

This generalizes an earlier analogous result of Jean-Pierre Serre for topologically finitely-generated pro-p groups. The proof uses the classification of finite simple groups.

PROPOSITION 3.1.31. *Every profinite group occurs as a Galois group of an appropriate Galois extension L/K.*

PROOF. A proof can be found in [**9**], Theorem 2.11.5. Here is a brief outline of the idea of the proof. Let G be a profinite group, and let F be any field. Denote by T the disjoint union of all the sets G/U, where U runs through the collection of all open normal subgroups of G. One may interpret the elements of T as indeterminates, and consider the field

$$L = F(T)$$

of all rational functions on the indeterminates in T with coefficients in F. The group G acts on T in a natural way: if $g \in G$ and $g'U \in G/U$, then $g(g'U) = gg'U$. This induces an action of G on L as a group of F-automorphisms of L. Now define $K = L^G$, the fixed field. One can show that L/K is a Galois extension with Galois group G. □

REMARK 3.1.32. In contrast to the above theorem it is not true that every profinite group occurs as an absolute Galois group.

In fact, it follows from a result of Artin and Schreier that the only *finite* absolute Galois groups are $Gal(\mathbb{C}/\mathbb{C}) = 1$ and $Gal(\mathbb{C}/\mathbb{R}) = C_2$.

THEOREM 3.1.33 (Artin-Schreier, 1927). *Let K be an algebraically closed field, and F be a subfield such that $1 < [K : F] < \infty$. Then K/F is a Galois extension, $K = F(i)$ with $i^2 = -1$, and F has characteristic zero. Furthermore, any finite sum of nonzero squares in F is again a nonzero square in F.*

There is a lot of very modern research now on the characterization of absolute Galois groups among all profinite groups.

DEFINITION 3.1.34. Denote by K_s the separable closure of K. If K is perfect (for example, all fields of characteristic zero), then it coincides with the algebraic closure $\overline{K}$. The *absolute Galois group* of K is $Gal(K_s/K)$.

DEFINITION 3.1.35. A field K is called *pseudo algebraically closed*, or a PAC field, if each nonempty absolutely irreducible variety V defined over K has a K-rational point.

Suppose that $\overline{K}$ is an algebraically closed field and consider the ideal I generated by polynomials $f_1, \dots, f_m \in \overline{K}[x_1, \dots, x_n]$. Assume that I is not the whole ring. Then Hilbert's Nullstellensatz says that $f_1, \dots, f_m$ have a common $\overline{K}$-zero. This implies that $\overline{K}$ is a PAC field, i.e., algebraically closed fields are PAC fields. So are separably closed fields. We have the following results:

Proposition 3.1.36. *Let K be a PAC field and V be a variety defined over K. Then the set $V(K)$ is dense in V in the Zariski K-topology. In particular, K is infinite.*

Hence a finite field $\mathbb{F}_q$, $q = p^k$ is not a PAC field.

Proposition 3.1.37. *Infinite algebraic extensions of finite fields are PAC-fields.*

Proposition 3.1.38 (Ax,Roquette). *Every algebraic extension of a PAC-field is a PAC field.*

Both results follow from the following theorem, see [**6**], Theorem 11.2.3.

Theorem 3.1.39. *Let L be an algebraic extension of an infinite field K. Suppose every plane algebraic curve defined over K has an L-rational point. Then L is a PAC field.*

Recently, Kollár solved an open problem of [**6**] on PAC fields.

Theorem 3.1.40 (Kollár). *A field K is a PAC field if and only if every absolutely irreducible homogeneous polynomial $f(x, y, z) \in K[x, y, z]$ has a nontrivial zero in K^3.*

It is interesting to look at the finite field $K = \mathbb{F}_q$. Since it is not a PAC field, there must be a plane projective curve $C\colon f(x, y, z) = 0$ defined over $\mathbb{F}_q$ with no K-rational point, defined by an homogeneous absolutely irreducible polynomial. In fact, for $p > 3$ we may take

$$f(x, y, z) = x^{q-1} + y^{q-1} + z^{q-1}$$

The absolute irreducibility of f reduces to the absolute irreducibility of the polynomial $1 + X^{q-1} + Y^{q-1}$. For the latter observe that $1 + X^{q-1}$ has simple roots in $\mathbb{F}_p$ and apply Eisenstein's criterion over the ring $\overline{\mathbb{F}_p}[X]$. Since we have $a^{q-1} = 1$ for all $a \in \mathbb{F}_q^\times$ it follows that $a^{q-1} + b^{q-1} + c^{q-1}$ is 1, 2 or 3 for all $(a, b, c) \in \mathbb{F}_q^3 \setminus \{(0, 0, 0)\}$. Since $p > 3$, this value is not 0 in $\mathbb{F}_q$.
For $p = 3$ and $q = p^1$ we take

$$f(x, y, z) = x^6 + y^6 + z^6 + x^2y^2z^2.$$

It takes some effort to show that f is abolutely irreducible. Since $a^2 = 1$ for each $\mathbb{F}_3^\times$ it follows that f takes only the nonzero values 1 and 2 on $\mathbb{F}_3^3 \setminus \{(0, 0, 0)\}$.
For $q = 3^k$ and $k \geq 2$ choose $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_3$ and let

$$f(x, y, z) = \alpha x^{q-1} + y^{q-1} + z^{q-1}$$

Then f is abolutely irreducible, and the values of f on $\mathbb{F}_q^3 \setminus \{(0, 0, 0)\}$ are $1, 2, \alpha, \alpha + 1$ or $\alpha + 2$. None of them is 0.
For $q = 2^k$ and $k \geq 3$ choose $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_4$ and let

$$f(x, y, z) = \alpha^2 x^{q-1} + \alpha y^{q-1} + z^{q-1}.$$

Then α is a root of no quadratic polynomial with coefficients in $\mathbb{F}_2$. Hence $f(x, y, z) = 0$ has no nontrivial solution in $\mathbb{F}_q$.

Finally for $q = 4$ and $q = 2$ let

$$f(x, y, z) = x^6 + y^6 + z^6 + x^3y^3 + x^3z^3 + y^3z^3 + x^2y^2z^2.$$

Using that $a^3 = 1$ for each $a \in \mathbb{F}_4^\times$, we may check that $f(a, b, c) = 1$ for all $(a, b, c) \in \mathbb{F}_4^3 \setminus \{(0, 0, 0)\}$ such that one of the coordinates is zero. Otherwise, $f(a, b, c) = 6 \cdot 1 + a^2b^2c^2 \neq 0$. One can prove that f is absolutely irreducible.

Definition 3.1.41. A profinite group G is called *projective*, if every finite embedding problem

$$\begin{tikzcd}
 & G \arrow[d, "\varphi"'] \arrow[dr, dotted, "\gamma"] & \\
0 & A \arrow[l] & B \arrow[l, "\alpha"']
\end{tikzcd}$$

is solvable. This means, for all finite groups A and B, and a homomorphism $\varphi\colon G \to A$, and an epimorphism $\alpha\colon B \to A$ there is a solution, i.e., a homomorphism $\gamma\colon G \to B$ with $\alpha \circ \gamma = \varphi$.

The absolute Galois group of a PAC field is projective, and conversely, every projective profinite group can be realized as an absolute Galois group of a PAC field.

Theorem 3.1.42 (J. Ax). *If K is a PAC field, then $Gal(K_s/K)$ is a projective profinite group.*

Proof. See Theorem 11.6.2 in [**6**]. □

Theorem 3.1.43 (Lubotzky, van den Dries). *Every projective profinite group can be realized as an absolute Galois group of a PAC field.*

Proof. See Corollary 23.1.2 in [**6**]. □

However, not every field with projective absolute Galois group is a PAC field.

Example 3.1.44. *For each prime number p, $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \widehat{\mathbb{Z}}$ is a projective group, but $\mathbb{F}_p$, being a finite field, is not a PAC field.*

The projectivity of the absolute Galois group of a field K is closely related to the vanishing of the Brauer group $Br(K)$ of K, although it is not equivalent to it.

Definition 3.1.45. A *central simple K-algebra* is a K-algebra A whose center is K and which has no two sided ideals except 0 and A.

For example, if D is a division ring with center K, then the ring $M_n(D)$ of all $n \times n$ matrices with entries in D is a central simple K-algebra. Conversely, if A is a finite dimensional cantral simple K-algebra, then by a theorem of Wedderburn, there exists a unique division ring D with center K and some $n \geq 1$ such that $A \simeq_K M_n(D)$. Suppose B is another finite dimensional central simple K-algebra. B is called *equivalent* to A if there exists a positive integer n with $B \simeq M_n(D)$. In particular, A is equivalent to D. We denote the equivalence class of A by $[A]$.

Definition 3.1.46. Denote by $Br(K)$ the set of all equivalence classes of finite dimensional central simple K-algebras. This forms an abelian group under the tensor product, called the *Brauer group of K*.

Indeed, the tensor product of two finite dimensional central simple K-algebras is again a finite dimensional central simple K-algebra. Moreover, the tensor product respects the euqivalence relation between finite dimensional central simple K-algebras. Hence,

$$[A] \cdot [B] = [A \otimes_K B]$$

is an associative multiplication rule on $Br(K)$. This rule is commutative since $A \otimes_K B \simeq B \otimes_K A$. The equivalence class $[K]$ is a unit in $Br(K)$, because $A \otimes_K K \simeq A$. An inverse to $[A]$ is given by $[A^{op}]$, where A^{op} is the opposite algebra of A. It consists of all elements a°, with $a \in A$, and addition and multiplication defined by the rules

$$\begin{aligned} a^\circ + b^\circ &= (a+b)^\circ, \\ a^\circ b^\circ &= (ba)^\circ. \end{aligned}$$

One proves that $A \otimes_K A^{op} \simeq M_n(K)$, where $n = \dim_K(A)$. This shows $[A^{op}] = [A]^{-1}$.

Proposition 3.1.47. *Let K be a PAC field. Then its Brauer group $Br(K)$ is trivial.*

The connection between projectivity of the absolute Galois group of a field K and its Brauer group $Br(K)$ is based on the following canonical isomorphism

$$H^2(Gal(K_s/K), K_s^\times) \simeq Br(K).$$

It is known that every element of $Br(K)$ has finite order.

Let K be a field and L a finite extension. Multiplication by $a \in L$ is a K-linear transformation $\ell_a \colon L \to L$. The norm $N_{L/K}(a)$ is defined as the determinant of ℓ_a. Properties of the determinant imply that the norm belongs to K and $N_{L/K}(ab) = N_{L/K}(a)N_{L/K}(b)$. Hence the norm is a group homomorphism $N \colon L^\times \to K^\times$ on the multiplicative groups of non-zero elements. If L/K is a Galois extension, the norm $N = N_{L/K}$ of an element $a \in L$ is the product of all the conjugates $\sigma(a)$ of a, for $\sigma \in Gal(L/K)$.

Proposition 3.1.48. *The following conditions on a field K are equivalent:*

(a) *The Brauer group $Br(L)$ is trivial for every finite separable extension L of K.*
(b) *The norm map $N \colon M^\times \to L^\times$ is surjective for every finite separable extension L of K and for every finite Galois extension M/L.*

For PAC fields we summarize the following consequences:

Proposition 3.1.49. *Let K be a PAC field. Then the following assertions hold:*

(a) *The absolute Galois group $Gal(K_s/K)$ is projective.*
(b) *The Brauer group $Br(K)$ is trivial.*
(c) *The norm map $N \colon M^\times \to K^\times$ is surjective for every finite Galois extension M/L.*

3.2. The cohomology of profinite groups

One can define cohomology groups for profinite groups, if one carries along the profinite topology.

Definition 3.2.1. Let G be a profinite group. An abelian group M is called a *discrete* G-module, if M is a G-module such that the action $G \times M \to M$ is *continuous* when M is endowed with the discrete topology, and $G \times M$ with the product topology.

In the discrete topology every subset is open.

Lemma 3.2.2. *Let G be a profinite group and M be a G-module. Then the following assertions are equivalent.*

(1) *M is a discrete G-module.*
(2) *The stabilizer $G_m = \{\sigma \in G \mid \sigma(m) = m\}$ of every $m \in M$ is open in G.*
(3) *$M = \cup_H M^H$, where H runs through the open subgroups of G.*

Proof. Suppose that (1) holds, i.e., that $G \times M \to M$ is continuous. Then also the restriction $\varphi\colon G \times \{m\} \to M$ is continuous. Hence $G_m \times \{m\} = \varphi^{-1}(m)$ is open in $G \times \{m\}$, so that G_m is open in G. Hence (2) follows.
Now assume that (2) holds and let $m \in M$. Since G_m is open it contains an open subgroup H so that $m \in M^{G_m} \subseteq M^H$. Hence (3) follows.
Assume that (3) holds. Let $(\sigma, m) \in G \times \{m\}$ and $n = \sigma(m)$. By assumption $n \in M^H$ for some open subgroup H. Then $M\sigma \times \{m\}$ is an open neighbourhood of (σ, m) which is mapped to n under the G-action $G \times M \to M$. Hence this action is continuous and (1) follows. □

Submodules and quotient modules of discrete modules are again discrete.

Example 3.2.3. *Consider the Galois extension $\mathbb{Q}(\sqrt{\mathbb{N}})/\mathbb{Q}$ with*

$$\mathbb{Q}(\sqrt{\mathbb{N}}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots),$$

and $G = Gal(\mathbb{Q}(\sqrt{\mathbb{N}})/\mathbb{Q})$. Then $M = \prod_p \mathbb{Q}(\sqrt{p})$ is a G-module which is not discrete.

If G is profinite and M is a discrete topological space, a map $G \to M$ is continuous iff there is an open normal subgroup N of G such that f is constant on the cosets of G/N. Since N has finite index in G, continuous maps $G \to M$ have only finitely many values. In the above example, assume that $G \times M \to M$ is continuous. Then $G \times \{m\} \to M$ is continuous and any m has only finitely many images under the action of G. However, this is not true since e.g. $m = (\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$ has infinitely many images.

Proposition 3.2.4. *The discrete G-modules form an abelian category $\mathcal{C}_G$. This category has enough injectives.*

This enables us to define cohomology groups $H^n_c(G, M)$ for profinite groups G and discrete G-modules M by taking injective resolutions, just as before. The groups can also be calculated using *continuous* cocycles. Let $C^n_c(G, M)$ be the group of continuous maps $G^{\times n} \to M$, and define the coboundary operators $\delta_n : C^n_c(G, M) \to C^{n+1}_c(G, M)$ as before. Then we obtain

$$H^n_c(G, M) \cong Z^n_c(G, M)/B^n_c(G, M) = \ker(\delta_n)/\operatorname{im}(\delta_{n-1})$$

Most of the theory concerning the cohomology groups $H^n(G, M)$ continues to hold for the groups defined by continuous cochains. Sometimes the subscript c will be dropped. It will be clear from the context which cohomology is used.

Remark 3.2.5. It follows from the definition that $H^0_c(G,M) = H^0(G,M)$ for all discrete G-modules M, and that $H^i_c(G,M) = H^i(G,M)$ for all $i \geq 0$ if G is finite. However, for $i > 0$ and G infinite the two groups are different in general.

Example 3.2.6. *Let $G = \widehat{\mathbb{Z}}$ and $M = \mathbb{Q}$ with the trivial $\widehat{\mathbb{Z}}$-action. Then $H^1_c(\widehat{\mathbb{Z}},\mathbb{Q}) = 0$, but $H^1(\widehat{\mathbb{Z}},\mathbb{Q}) \neq 0$.*

In fact, $H^1_c(\widehat{\mathbb{Z}},\mathbb{Q}) = \varinjlim_n \operatorname{Hom}(\mathbb{Z}/n\mathbb{Z},\mathbb{Q}) = 0$, because $\mathbb{Q}$ is torsion free. On the other hand, $H^1(\widehat{\mathbb{Z}},\mathbb{Q})$ is the group of $\widehat{\mathbb{Z}}$-module homomorphisms $\varphi\colon \widehat{\mathbb{Z}} \to \mathbb{Q}$. But as $\mathbb{Q}$ is a divisible abelian group, every homomorphism $C \to \mathbb{Q}$ from a subgroup C of an abelian group B extends to a homomorphism $B \to \mathbb{Q}$. Applying this with $C = \mathbb{Z}$, $B = \widehat{\mathbb{Z}}$ and the natural inclusion $\mathbb{Z} \to \mathbb{Q}$ we obtain a nontrivial homomorphism $\widehat{\mathbb{Z}} \to \mathbb{Q}$.

Remark 3.2.7. Let G be a profinite group, $\mathcal{M}_G$ be the category of all G-modules, and $\mathcal{C}_G$ the category of discrete G-modules. Then $\mathcal{C}_G$ is a full subcategory of $\mathcal{M}_G$. Moreover there is a functor $F : \mathcal{M}_G \to \mathcal{C}_G$, $F(M) = M^{\cup}$ where

$$M^{\cup} = \bigcup_{H \text{ open in } G} M^H$$

We have $\operatorname{Hom}_G(M, N^{\cup}) = \operatorname{Hom}_G(M,N)$ if M is a discrete G-module. The functor F preserves injectives and is left exact. Hence $\mathcal{C}_G$ has enough injectives. But F is not exact and hence $H^n(G,M)$ and $H^n(G,M^{\cup})$ in general are *different*. The inclusion functor $i\colon \mathcal{C}_G \to \mathcal{M}_G$ is exact but does not preserve injectives. Hence $H^n(G,M)$ and $H^n(G,i(M))$ are also different in general.

3.3. Inflation, restriction and the Hochschild-Serre spectral sequence

We will start with induced modules in the version without continuity.

Definition 3.3.1. Let G be a group, H a subgroup and M be an H-module. Let

$$\mathrm{Ind}_H^G(M) = \{\varphi\colon G \to M \mid \varphi(hg) = h\varphi(g) \text{ for all } h \in H, g \in G\}$$

Then $\mathrm{Ind}_H^G(M)$ becomes a G-module with the operations

$$(\varphi + \varphi')(x) = \varphi(x) + \varphi'(x)$$
$$(g\varphi)(x) = \varphi(xg)$$

Indeed, $(g, \varphi) \mapsto g\varphi$ defines an action since $(g'g)\varphi = g'(g\varphi)$:

$$((g'g)\varphi)(x) = \varphi(xg'g) = (g\varphi)(xg') = (g'(g\varphi))(x)$$

A homomorphism $\alpha\colon M \to N$ of H-modules defines a homomorphism

$$\alpha_*\colon \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(N)$$

of G-modules by $\alpha_*(\varphi) = \alpha \circ \varphi$. Hence $\mathrm{Ind}_H^G\colon \mathcal{M}_H \to \mathcal{M}_G$ is a functor.

Definition 3.3.2. A G-module is said to be *induced* if it is isomorphic to $\mathrm{Ind}_1^G(A) = \{\varphi\colon G \to A\}$ for some abelian group A.

Note that the maps φ are just maps, not necessarily homomorphisms. We have $\mathrm{Ind}_H^G(M) = \mathrm{Hom}_H(\mathbb{Z}[G], M)$, where $\mathbb{Z}[G]$ is an H-module as well, with its canonical G-action, and the action of G on an H-module homomorphism $\varphi\colon \mathbb{Z}[G] \to M$ is given by $(\sigma\varphi)(g) := \varphi(g.\sigma)$ for a basis element g of $\mathbb{Z}[G]$.

Remark 3.3.3. Let G be a profinite group, H a closed subgroup and M be a discrete H-module. Then

$$\mathrm{Ind}_H^G(M) = \{\varphi\colon G \to M \text{ continuous } \mid \varphi(hg) = h\varphi(g) \text{ for all } h \in H, g \in G\}$$

becomes a *discrete* G-module.

Lemma 3.3.4. *For any G-module M and H-module N we have*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \cong \mathrm{Hom}_H(M, N)$$

Moreover the functor $\mathrm{Ind}_H^G\colon \mathcal{M}_H \to \mathcal{M}_G$ is exact.

Proof. Given a G-homomorphism $\alpha\colon M \to \mathrm{Ind}_H^G(N)$, we define $\beta\colon M \to N$ by $\beta(m) = \alpha(m)(1)$, where 1 is the identity in G. Then we have for any $g \in G$

$$\beta(gm) = (\alpha(gm))(1) = (g\alpha(m))(1) = \alpha(m)(g \cdot 1) = \alpha(m)(g)$$

because α is a G-homomorphism and $\alpha(m) \in \mathrm{Ind}_H^G(N)$. Hence for $h \in H$

$$\beta(hm) = \alpha(m)(h) = h(\alpha(m)(1) = h(\beta(m))$$

so that $\beta \in \mathrm{Hom}_H(M, N)$. Conversely, given such a β we define $\alpha\colon M \to \mathrm{Ind}_H^G(N)$ such that $\alpha(m)(g) = \beta(gm)$. It follows similarly that α is a G-homomorphism. These correspondences yield the desired isomorphism of the first part. Given an exact sequence of H-modules

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

we have to prove that the sequence of G-modules

$$0 \to \mathrm{Ind}_H^G(M) \xrightarrow{\alpha_*} \mathrm{Ind}_H^G(N) \xrightarrow{\beta_*} \mathrm{Ind}_H^G(P) \to 0$$

is exact. Let $\varphi \in \operatorname{Ind}_H^G(M)$ and $\alpha_*(\varphi) = \alpha \circ \varphi = 0$. Since α is injective we have $\varphi = 0$, so that α_* is injective. Furthermore $(\beta_*\alpha_*)(\varphi) = \beta \circ \alpha \circ \varphi = 0$ since $\beta \circ \alpha = 0$. Hence $\beta_*\alpha_* = 0$ and $\operatorname{im}\alpha_* \subset \ker\beta_*$.
Conversely let $\psi \in \ker\beta_*$, i.e., $\beta_*(\psi) = \beta \circ \psi = 0$. For all $g \in G$ there is an $m \in M$ such that $\psi(g) = \alpha(m)$, because $\psi(g) \in \ker\beta \subset \operatorname{im}\alpha$. Define a map $\varphi\colon G \to M$ by $\varphi(g) = m$. This is well defined, since α is injective. Furthermore $\psi = \alpha \circ \varphi = \alpha_*(\varphi)$. We have to show that $\varphi \in \operatorname{Ind}_H^G(M)$, and hence $\psi \in \operatorname{im}\alpha_*$. Then $\ker\beta_* \subset \operatorname{im}\alpha_*$ and it follows the exactness at $\operatorname{Ind}_H^G(N)$. Since $\psi \in \operatorname{Ind}_H^G(N)$ we have

$$\alpha(\varphi(hg)) = \psi(hg) = h\psi(g) = h\alpha(m) = \alpha(hm) = \alpha(h\varphi(g))$$

and hence $\varphi(hg) = h\varphi(g)$, because α is injective. This shows $\varphi \in \operatorname{Ind}_H^G(M)$.
Finally we have to show that β_* is surjective. Let S be a set of right coset representatives for H in G, i.e., $G = \cup_{s\in S} Hs$, and let $\varphi \in \operatorname{Ind}_H^G(P)$. For each $s \in S$, choose an $n(s) \in N$ mapping under β to $\varphi(s) \in P$, and define $\widetilde{\varphi}(hs) = h{\cdot}n(s)$. Then $\widetilde{\varphi} \in \operatorname{Ind}_H^G(N)$ and $\beta_*(\widetilde{\varphi}) = \beta\circ\widetilde{\varphi} = \varphi$. □

Remark 3.3.5. Let G be a profinite group and H a closed subgroup. Then Ind_H^G is also an exact functor from the category $\mathcal{C}_H$ of discrete H-modules to the category $\mathcal{C}_G$ of discrete G-modules.

Theorem 3.3.6 (Shapiro's Lemma). *Let G be a profinite group, H a closed subgroup of G. For any discrete H-module N and all $r \geq 0$, there is a canonical isomorphism*

$$H^r(G, \operatorname{Ind}_H^G(N)) \cong H^r(H, N)$$

Proof. Let us first mention that the result holds for any abstract group G with subgroup H and H-module N.
For $r = 0$, the isomorphism is the composite of the following isomorphisms:

$$N^H \cong \operatorname{Hom}_H(\mathbb{Z}, N) \cong \operatorname{Hom}_G(\mathbb{Z}, \operatorname{Ind}_H^G(N)) \cong \operatorname{Ind}_H^G(N)^G$$

The first and the third isomorphism follow from lemma 2.3.2, the second one from lemma 3.3.4. $\mathbb{Z}$ is regarded as a trivial module. Now choose an injective resolution $N \to I^\bullet$ of N. By applying the functor Ind_H^G, we obtain an injective resolution $\operatorname{Ind}_H^G(N) \to \operatorname{Ind}_H^G(I^\bullet)$ of the G-module $\operatorname{Ind}_H^G(N)$, because Ind_H^G is exact and preserves injectives. Hence

$$H^r(G, \operatorname{Ind}_H^G(N)) = H^r((\operatorname{Ind}_H^G(I^\bullet))^G) = H^r(I^{\bullet H}) = H^r(H, N)$$

□

Corollary 3.3.7. *If M is an induced G-module, then $H^n(G, M) = 0$ for all $n \geq 1$.*

Proof. If $M = \operatorname{Ind}_1^G(A)$, then $H^n(G, M) = H^n(\{1\}, A) = 0$. □

Corollary 3.3.8. *Let L/K be a finite Galois extension and $G = Gal(L/K)$. Then $H^n(G, L) = 0$ for all $n \geq 1$.*

This generalizes the additive part of proposition 2.4.7. Recall that $H^n(G, L^\times)$ in general need not be trivial.

Proof. By the normal basis theorem there exists an $\alpha \in L$ such that $\{\sigma\alpha \mid \sigma \in G\}$ is a basis (a "normal" basis) for L as a K-vector space. This means, L is isomorphic to $K[G]$ as a G-module. But $K[G] = \operatorname{Ind}_1^G K$, and hence $H^n(G, L) = H^n(\{1\}, K) = 0$. □

If $\alpha\colon M \to N$ is a homomorphism of G-modules, then it induces a homomorphism

$$H^n(G,M) \to H^n(G,N)$$

of cohomology groups. This can be generalized as follows.

Definition 3.3.9. Let M be a G-module and N be a G'-module. Two homomorphisms $\alpha\colon G' \to G$ and $\beta\colon M \to N$ are said to be *compatible* if

$$\beta(\alpha(g')m) = g'\beta(m) \quad \forall\, g' \in G', m \in M$$

In this case M becomes a G'-module by $g'm = \alpha(g')m$ such that $\beta\colon M \to N$ becomes a homomorphism of G'-modules. Furthermore the map

$$(\alpha,\beta)\colon C^\bullet(G,M) \to C^\bullet(G',N)$$

given by $\varphi \mapsto \beta\circ\varphi\circ\alpha^n$ defines a homomorphism of complexes. It commutes with the coboundary operators, so that it induces a homomorphism of cohomology groups

$$(\alpha,\beta)\colon H^n(G,M) \to H^n(G',N).$$

Example 3.3.10. *Let H be a subgroup of G and $\alpha\colon H \hookrightarrow G$ be the inclusion map. For any H-module N let $\beta\colon \operatorname{Ind}_H^G(N) \to N$ be the map defined by $\beta(\varphi) = \varphi(1)$. Then α and β are compatible:*

$$\beta(\alpha(h)\varphi) = \beta(h\varphi) = h\beta(\varphi)$$

The induced homomorphism

$$H^n(G, \operatorname{Ind}_H^G(N)) \to H^n(H,N)$$

is precisely the isomorphism in Shapiro's Lemma.

Similarly, if H is a subgroup of G, $\alpha\colon H \hookrightarrow G$ is the inclusion map and $\beta\colon M \to M$ is the identity, both maps are compatible:

Definition 3.3.11. The induced homomorphisms are called the *restriction homomorphisms*

$$\operatorname{Res}\colon H^n(G,M) \to H^n(H,M)$$

These homomorphisms can also be constructed as follows: let $\varphi_m(g) = gm$. Then $\varphi_m \in \operatorname{Ind}_H^G(M)$ and $\varphi\colon M \to \operatorname{Ind}_H^G(M)$, $m \mapsto \varphi_m$ is a homomorphism of G-modules. Denote by $\widetilde{\varphi}\colon H^n(G,M) \to H^n(G,\operatorname{Ind}_H^G(M))$ the induced homomorphism of cohomology groups. Let $\psi\colon H^n(G,\operatorname{Ind}_H^G(M)) \to H^n(H,M)$ be the isomorphism in Shapiro's Lemma. Then we have

$$\operatorname{Res} = \psi \circ \widetilde{\varphi}$$

Let H be a normal subgroup of G, $\alpha\colon G \to G/H$ be the quotient map and $\beta\colon M^H \hookrightarrow M$ be the inclusion. Then α and β are compatible:

Definition 3.3.12. The induced homomorphisms are called the *inflation homomorphisms*

$$\operatorname{Inf}\colon H^n(G/H, M^H) \to H^n(G,M)$$

We can extend the definition of restriction and inflation to profinite groups and discrete modules. There is the following inflation-restriction exact sequence.

Theorem 3.3.13. *Let G be a profinite group, H be a closed normal subgroup of G and M be a discrete G-module. Let $n \in \mathbb{N}$. Assume that $H^r(H,M) = 0$ for all r with $1 \leq r < n$. Then the following sequence is exact.*

$$0 \to H^n(G/H, M^H) \xrightarrow{\text{Inf}} H^n(G,M) \xrightarrow{\text{Res}} H^n(H,M)$$

For $n = 1$ the hypothesis on $H^r(H,M)$ is vacuous, so that we always have

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G,M) \xrightarrow{\text{Res}} H^1(H,M) \tag{3.1}$$

Proof. Let $n = 1$. We will show that Inf is injective and $\operatorname{im}\text{Inf} = \ker\text{Res}$. Let $\varphi\colon G/H \to M^H$ be a 1-cocycle and $\varphi' = \text{Inf}\,\varphi$. Then φ' is a 1-cocycle in $H^1(G,M)$ via $G \to G/H \xrightarrow{\varphi} M^H \to M$. Suppose that the class of φ' is trivial, i.e., φ' is a 1-coboundary. Then $\varphi'(g) = gm - m$ for some $m \in M$. Hence $gm - m = ghm - m$ for all $h \in H$, so that $m = hm$ for all $h \in H$, i.e., $m \in M^H$. But then $\varphi(gH) = gHm - m$ is a 1-coboundary in $H^1(G/H, M^H)$ and the class of φ is zero. It follows that Inf is injective. Similarly we see that $\operatorname{im}\text{Inf} = \ker\text{Res}$. For $n > 1$ the result can be proved by induction. □

Example 3.3.14. *Let Ω/K and L/K be finite Galois extension with $L \subset \Omega$. Then $H := Gal(\Omega/L)$ is a normal subgroup of $G := Gal(\Omega/K)$, and with $M = \Omega^\times$ we have $M^H = L^\times$. According to Proposition* 2.4.7, *$H^1(H, \Omega^\times) = 1$, and so there is an exact sequence*

$$1 \to H^2(G/H, L^\times) \to H^2(G, \Omega^\times) \to H^2(H, \Omega^\times)$$

Remark 3.3.15. In Theorem 3.3.13 the cohomology groups $H^n(H,M)$ can be equipped with a G-module structure, such that H acts trivially on it. Then $H^n(H,M)$ becomes a G/H-module and it is not difficult to show that the image of $H^n(G,M)$ under Res actually lies in $H^n(H,M)^{G/H}$. Then (3.1) can be extended to the following special case of of the *Hochschild-Serre spectral sequence*

$$\begin{aligned} 0 \to H^1(G/H, M^H) &\xrightarrow{\text{Inf}} H^1(G,M) \xrightarrow{\text{Res}} H^1(H,M)^{G/H} \\ &\to H^2(G/H, M^H) \xrightarrow{\text{Inf}} H^2(G,M) \end{aligned}$$

The result for $n \geq 1$ here is as follows:

Theorem 3.3.16. *Let G be a profinite group, H be a closed normal subgroup of G and M be a discrete G-module. Let $n \geq 1$ be an integer and assume that that $H^r(H,M) = 0$ for all r with $1 \leq r < n$. Then there is a natural map*

$$\tau_{n,M}\colon H^n(H,M)^{G/H} \to H^{n+1}(G/H, M^H)$$

fitting into the following exact sequence:

$$\begin{aligned} 0 \to H^n(G/H, M^H) &\xrightarrow{\text{Inf}} H^n(G,M) \xrightarrow{\text{Res}} H^n(H,M)^{G/H} \xrightarrow{\tau_{n,M}} \\ &\to H^{n+1}(G/H, M^H) \xrightarrow{\text{Inf}} H^{n+1}(G,M). \end{aligned}$$

Among many possible topics within techniques from group cohomology we want to mention the *cup-product* (see [**7**]). We will assume that G is a group and A, B are G-modules (the cup-product can also be adapted to profinite groups and discrete modules). A cup-product is an associative product operation

$$H^i(G,A)\times H^j(G,B)\to H^{i+j}(G,A\otimes B),$$
$$(a,b)\mapsto a\cup b,$$

which is graded-commutative, i.e., it satisfies

$$a\cup b=(-1)^{ij}(b\cup a).$$

Here $A\otimes B=A\otimes_{\mathbb{Z}}B$ is the tensor product of A and B over the commutative ring $\mathbb{Z}$, equipped with the G-module structure given by

$$g.(a\otimes b)=g.a\otimes g.b$$

for $g\in G$, $a\in A$ and $b\in B$. Note that in general this is different from the tensor product of A and B over the group ring $\mathbb{Z}[G]$. We begin with a construction of the cup-product with the **first step** as follows: let $A^\bullet$ and $B^\bullet$ be complexes of abelian groups, i.e.,

$$\cdots\to A^{i-1}\xrightarrow{\partial_A^{i-1}}A^i\xrightarrow{\partial_A^i}A^{i+1}\to\cdots,$$

and similarly for $B^\bullet$. Then we define the *tensor product complex* $A^\bullet\otimes B^\bullet$ by first considering the double complex

$$\begin{tikzcd}
 & \vdots & \vdots & \vdots & \\
\cdots \arrow[r] & A^{i-1}\otimes B^{j+1} \arrow[r] \arrow[u] & A^i\otimes B^{j+1} \arrow[r] \arrow[u] & A^{i+1}\otimes B^{j+1} \arrow[r] \arrow[u] & \cdots \\
\cdots \arrow[r] & A^{i-1}\otimes B^{j} \arrow[r] \arrow[u] & A^i\otimes B^{j} \arrow[r] \arrow[u] & A^{i+1}\otimes B^{j} \arrow[r] \arrow[u] & \cdots \\
\cdots \arrow[r] & A^{i-1}\otimes B^{j-1} \arrow[r] \arrow[u] & A^i\otimes B^{j-1} \arrow[r] \arrow[u] & A^{i+1}\otimes B^{j-1} \arrow[r] \arrow[u] & \cdots \\
 & \vdots \arrow[u] & \vdots \arrow[u] & \vdots \arrow[u] &
\end{tikzcd}$$

where the horizontal maps are given by

$$\partial^h_{i,j}=\partial^i_A\otimes\mathrm{id}\colon A^i\otimes B^j\to A^{i+1}\otimes B^j,$$
$$a\otimes b\mapsto\partial^i_A(a)\otimes b,$$

and the vertical maps are given by

$$\partial^v_{i,j}=\mathrm{id}\otimes(-1)^i\partial^j_B\colon A^i\otimes B^j\to A^i\otimes B^{j+1},$$
$$a\otimes b\mapsto a\otimes(-1)^i\partial^j_B(b).$$

The above squares *anticommute*, i.e., one has

$$\partial^h_{i,j+1}\circ\partial^v_{i,j}=-\partial^v_{i+1,j}\circ\partial^h_{i,j}.$$

Now take the total complex associated with this double complex. This is, by definition, the complex $T^\bullet$ with

$$T^n=\bigoplus_{i+j=n}A^i\otimes B^j$$

and $\partial^n \colon T^n \to T^{n+1}$ given on the component $A^i \otimes B^j$ by $\partial^h_{i,j} + \partial^v_{i,j}$. The above anticommutativity then implies $\partial^{n+1} \circ \partial^n = 0$, i.e., that $T^\bullet$ is really a complex. We define this $T^\bullet$ to be the *tensor product of* $A^\bullet$ *and* $B^\bullet$, and denote it as above by $A^\bullet \otimes B^\bullet$.

This enables us to proceed to the **second step** of the cup-product construction. In addition to the situation before, assume further given abelian groups A and B. Then we have the complex $\operatorname{Hom}(A^\bullet, A)$ whose degree i term is $\operatorname{Hom}(A^{-i}, A)$ and whose differentials are those induced by the differentials of $A^\bullet$. In the same way we have the complex $\operatorname{Hom}(B^\bullet, B)$. We construct a product operation

$$H^i(\operatorname{Hom}(A^\bullet, A)) \times H^j(\operatorname{Hom}(B^\bullet, B)) \to H^{i+j}(\operatorname{Hom}(A^\bullet \otimes B^\bullet, A \otimes B)) \tag{3.2}$$

as follows. Given homomorphisms of abelian groups $\alpha \colon A^{-i} \to A$ and $\beta \colon B^{-j} \to B$ with $i + j = n$, the tensor product $\alpha \otimes \beta$ is a homomorphism

$$\alpha \otimes \beta \colon A^{-i} \otimes B^{-j} \to A \otimes B,$$

and hence defines an element of the degree $(i+j)$ term in $\operatorname{Hom}(A^\bullet \otimes B^\bullet, A \otimes B)$ via the diagonal embedding

$$\operatorname{Hom}(A^{-i} \otimes B^{-j}, A \otimes B) \to \operatorname{Hom}\left(\bigoplus_{k+l=i+j} A^{-k} \otimes B^{-l}, A \otimes B \right).$$

Here if $\alpha \in Z^i(\operatorname{Hom}(A^\bullet, A))$ and $\beta \in Z^j(\operatorname{Hom}(B^\bullet, B))$, then by construction of $A^\bullet \otimes B^\bullet$ we have

$$\alpha \otimes \beta \in Z^{i+j}(\operatorname{Hom}(A^\bullet \otimes B^\bullet, A \otimes B)).$$

Moreover, if $\alpha \in B^i(\operatorname{Hom}(A^\bullet, A))$, then $\alpha \otimes \beta \in Z^{i+j}(\operatorname{Hom}(A^\bullet \otimes B^\bullet, A \otimes B))$. The same follows if $\beta \in B^j(\operatorname{Hom}(B^\bullet, B))$. This defines the required map (3.2).

If in this construction all abelian groups carry a G-module structure for some group G and G-(module)-homomorphisms α and β, then also $\alpha \otimes \beta$ is a G-homomorphism, hence by restricting to G-homomorphisms the product (3.2) induces a product

$$H^i(\operatorname{Hom}_G(A^\bullet, A)) \times H^j(\operatorname{Hom}_G(B^\bullet, B)) \to H^{i+j}(\operatorname{Hom}_G(A^\bullet \otimes B^\bullet, A \otimes B)),$$

where $A \otimes B$ and $A^\bullet \otimes B^\bullet$ are endowed with the G-module structure defined before.

For the next step we need the following proposition. Recall that the lower numbering in a projective resolution $P_\bullet$ is defined by $P_i := P^{-i}$.

Proposition 3.3.17. *Let G be a group, and let $P_\bullet$ be a complex of G-modules which is a projective resolution of the trivial G-module $\mathbb{Z}$. Then $P_\bullet \otimes P_\bullet$ is a projective resolution of the trivial $\mathbb{Z}[G \times G]$-module $\mathbb{Z}$.*

Here the terms of $P_\bullet \otimes P_\bullet$ are endowed by a $G \times G$-action coming from

$$(g_1, g_2)(p_1 \otimes p_2) = g_1.p_1 \otimes g_2.p_2$$

The proof is based on the following lemma. Recall that a complex $A^\bullet$ is called *acyclic* or *exact*, if $H^i(A^\bullet) = 0$ for all i.

Lemma 3.3.18. *Let $A^\bullet$ and $B^\bullet$ be complexes of free abelian groups. Then the following holds.*

(1) *$A^\bullet \otimes B^\bullet$ is again a complex of free abelian groups.*

(2) *If $A^\bullet$ and $B^\bullet$ are acyclic, then so is the complex $A^\bullet \otimes B^\bullet$.*

(3) *If $A^\bullet$ and $B^\bullet$ are concentrated in nonpositive degree, acyclic in negative degrees and having a free abelian group as* 0*-cohomology, then so is the complex $A^\bullet \otimes B^\bullet$, and in addition*

$$H^0(A^\bullet \otimes B^\bullet) \simeq H^0(A^\bullet) \otimes H^0(B^\bullet).$$

Proof. (1): As tensor products and direct sums of free abelian groups are again free, it follows that the terms of $A^\bullet \otimes B^\bullet$ are free abelian.

(2): The proof of acyclicity is based on the fact that a subgroup of a free abelian group is again free. This implies that for all i, the subgroups $B^i(A^\bullet)$ are free, and in particular projective. For all i we have the exact sequence

$$0 \to Z^i(A^\bullet) \to A^i \to B^{i+1}(A^\bullet) \to 0,$$

the terms being free abelian groups. Hence the sequence splits. Moreover, we have $Z^i(A^\bullet) = B^i(A^\bullet)$ by the acyclicity of $A^\bullet$. Therefore we may rewrite the above exact sequence as

$$0 \to B^i(A^\bullet) \xrightarrow{\text{id}} B^i(A^\bullet) \oplus B^{i+1}(A^\bullet) \xrightarrow{(0,\text{id})} B^{i+1}(A^\bullet) \to 0.$$

Hence the complex $A^\bullet$ decomposes as an infinite direct sum of complexes of the shape

$$\cdots \to 0 \to 0 \to A \xrightarrow{\text{id}} A \to 0 \to 0 \to \cdots$$

and similarly, the complex $B^\bullet$ decomposes as a direct sum of complexes

$$\cdots \to 0 \to 0 \to B \xrightarrow{\text{id}} B \to 0 \to 0 \to \cdots$$

The construction of tensor products of complexes commutes with arbitrary direct sums. Hence we are reduced to check acyclicity for the tensor product of complexes of the above type. But by definition, these are complexes of the form

$$\cdots \to 0 \to 0 \to A \otimes B \xrightarrow{(\text{id},\pm\,\text{id})} (A \otimes B) \oplus (A \otimes B) \xrightarrow{(0,\pm\,\text{id})} A \otimes B \to 0 \to 0 \to \cdots$$

Therefore the claim follows.

(3): The proof goes along the same lines as for (2), and the description of the 0-cohomology follows from the right exactness of the tensor product. □

Proof of Proposition 3.3.17: By definition, the P_i are direct summands in some free G-module, which is in particular a free abelian group, so they are also free abelian groups. Hence we can use (3) of lemma 3.3.18, and we are done if we show that the terms of $P_\bullet \otimes P_\bullet$ are projective as $\mathbb{Z}[G \times G]$-modules. For this, notice first the canonical isomorphism

$$\mathbb{Z}[G \times G] \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G]:$$

indeed, both abelian groups are free on a basis corresponding to pairs of elements in G. Taking direct sums we obtain that tensor products of free $\mathbb{Z}[G]$-modules are free $\mathbb{Z}[G\times G]$-modules with the above $G \times G$-action. If P_i resp. P_j are projective $\mathbb{Z}[G]$-modules with a direct complement Q_i resp. Q_j in some free $\mathbb{Z}[G]$-module, then the isomorphism

$$(P_i \oplus Q_i) \otimes (P_j \oplus Q_j) \simeq (P_i \otimes P_j) \oplus (P_i \otimes Q_j) \oplus (Q_i \otimes P_j) \oplus (Q_i \otimes Q_j)$$

shows that $P_i \otimes P_j$ is a direct summand in a free $\mathbb{Z}[G \times G]$-module, and hence it is projective. Then the projectivity of the terms of $P_\bullet \otimes P_\bullet$ follows. □

Putting everything together, we can finally construct the cup-product.

Third step: Let A and B be G-modules, and $P_\bullet$ be a projective resolution of the trivial G-module $\mathbb{Z}$. Applying the second step with $A^\bullet = B^\bullet = P_\bullet$ we obtain maps

$$H^i(\mathrm{Hom}(P_\bullet, A)) \times H^j(\mathrm{Hom}(P_\bullet, B)) \to H^{i+j}(P_\bullet \otimes P_\bullet, A \otimes B)).$$

By proposition 3.3.17, the complex $P_\bullet \otimes P_\bullet$ is a projective resolution of $\mathbb{Z}$ as a $G \times G$-module. Hence using the definition of cohomology via projective resolutions we may rewrite the above maps as

$$H^i(G, A) \times H^j(G, B) \to H^{i+j}(G \times G, A \otimes B).$$

On the other hand, the diagonal embedding $G \to G \times G$ induces a restriction map

$$\mathrm{Res}\colon H^{i+j}(G \times G, A \otimes B) \to H^{i+j}(G, A \otimes B).$$

Composing the two maps we finally obtain an operation

$$\begin{gathered} H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, A \otimes B), \\ (a, b) \mapsto a \cup b. \end{gathered}$$

which we call the **cup-product** map.
One may check that this construction does not depend on the chosen projective resolution $P_\bullet$.

Remark 3.3.19. The construction is functorial in the following sense. For a given morphism $A \to A'$ of G-modules the diagram

$$\begin{tikzcd} H^i(G, A) \times H^j(G, B) \arrow[r] \arrow[d] & H^{i+j}(G, A \otimes B) \arrow[d] \\ H^i(G, A') \times H^j(G, B) \arrow[r] & H^{i+j}(G, A' \otimes B) \end{tikzcd}$$

commutes. Similarly such a diagram for the second variable commutes.

Remark 3.3.20. For $i = j = 0$ the cup-product map

$$H^0(G, A) \times H^0(G, B) \to H^0(G, A \otimes B)$$

is just the natural map $A^G \otimes B^G \to (A \otimes B)^G$. This follows from the construction of the cup-product.

Remark 3.3.21. There is the following generalization of a cup-product, usually again denoted as cup-product. For a given morphism $A \times B \to C$ of G-modules we obtain pairings

$$H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, C)$$

by composing the cup-product with the natural map

$$H^{i+j}(G, A \otimes B) \to H^{i+j}(G, C).$$

Proposition 3.3.22. *The cup-product is associative and graded-commutative.*

Proof. We leave it to the reader to check associativity. One has to follow carefully the construction. It ultimately boils down to the associativity of the tensor product.

For graded-commutativity, we first work on the level of tensor products of complexes and compare the images of the obvious maps

$$A^i \otimes B^j \to \bigoplus_{k+l=i+j} A^k \otimes B^l,$$
$$B^j \otimes A^i \to \bigoplus_{k+l=i+j} B^l \otimes A^k$$

in the complexes $A^\bullet \otimes B^\bullet$ and $B^\bullet \otimes A^\bullet$ respectively. Given $a \otimes b \in A^i \otimes B^j$, the differential in $A^\bullet \otimes B^\bullet$ acts on it by

$$\partial_A^i \otimes \mathrm{id}_B + (-1)^i \, \mathrm{id}_A \otimes \partial_B^j,$$

whereas the differential in $B^\bullet \otimes A^\bullet$ acts on $b \otimes a \in B^j \otimes A^i$ by

$$\partial_B^j \otimes \mathrm{id}_A + (-1)^j \, \mathrm{id}_B \otimes \partial_A^i.$$

Therefore mapping $a \otimes b$ to $(-1)^{ij}(b \otimes a)$ induces an isomorphism of complexes $A^\bullet \otimes B^\bullet \simeq B^\bullet \otimes A^\bullet$. Applying this with $A^\bullet = B^\bullet = P_\bullet$ and performing the rest of the construction of the cup-product, we obtain that both elements $a \cup b$ and $(-1)^{ij}(b \cup a)$ are mapped, via the above isomorphism, to the same element in $H^{i+j}(G, A \otimes B)$. □

The following exactness property holds for the cup-product.

PROPOSITION 3.3.23. *Given an short exact sequence of G-modules*

$$0 \to A_1 \to A_2 \to A_3 \to 0 \tag{3.3}$$

with the property that the tensor product over $\mathbb{Z}$ with a G-module B remains exact, i.e., such that

$$0 \to A_1 \otimes B \to A_2 \otimes B \to A_3 \otimes B \to 0 \tag{3.4}$$

is again exact, we have for all elements $a \in H^i(G, A_3)$ and $b \in H^j(G, B)$ the relation

$$\delta(a) \cup b = \delta(a \cup b)$$

in $H^{i+j+1}(G, A_1 \otimes B)$, where the δ are the connecting maps in the associated long sequence of cohomology.
Similarly, if

$$0 \to B_1 \to B_2 \to B_3 \to 0$$

is a short exact sequence of G-modules such that the tensor product over $\mathbb{Z}$

$$0 \to A \otimes B_1 \to A \otimes B_2 \to A \otimes B_3 \to 0$$

with a G-module A remains exact, we have for all elements $a \in H^i(G, A)$ and $b \in H^j(G, B_3)$ the relation

$$a \cup \delta(b) = (-1)^i \delta(a \cup b)$$

in $H^{i+j+1}(G, A \otimes B_1)$.

PROOF. For the first statement, fix an element $b \in H^j(G, B)$. Take a projective resolution $P_\bullet$ of the trivial G-module $\mathbb{Z}$ and consider the sequences

$$0 \to \mathrm{Hom}(P_\bullet, A_1) \to \mathrm{Hom}(P_\bullet, A_2) \to \mathrm{Hom}(P_\bullet, A_3) \to 0 \tag{3.5}$$

and

$$(3.6)\qquad \begin{aligned} 0 &\to \mathrm{Hom}(P_\bullet \otimes P_\bullet, A_1 \otimes B) \to \mathrm{Hom}(P_\bullet \otimes P_\bullet, A_2 \otimes B) \\ &\to \mathrm{Hom}(P_\bullet \otimes P_\bullet, A_3 \otimes B) \to 0. \end{aligned}$$

These are exact sequences of complexes because of the projectivity of the P_i and the exactness of the sequences (3.3) and (3.4). Lifting b to an element $\beta \in \mathrm{Hom}(P_j, B)$ and tensor product with β yields maps

$$\mathrm{Hom}(P_j, A_k) \to \mathrm{Hom}(P_i \otimes P_j, A_k \otimes B)$$

for $k = 1, 2, 3$. Hence proceeding as in the second step of the cup-product construction we obtain maps form the terms in the sequence (3.5) to those of the sequence (3.6), increasing degrees by j, giving rise to a commutative diagram by functoriality of the cup-product construction. The connecting maps δ are obtained by applying the so called snake lemma to the above sequences - we leave out the details. Finally one obtains the first statement by following the image of an element $a \in H^i(G, A)$ by using the above mentioned commutativity. Let us say, that the proof of the second statement is similar, except that one has to replace the differentials in the complexes $\mathrm{Hom}^\bullet(P_\bullet, B_k)$ by their multiples by $(-1)^i$ in order to obtain a commutative diagram, by virtue of the sign convention we have taken in the first step of the cup-product construction. □

Let H be a subgroup of G of finite index, and let A be a G-module. We mention briefly the so called *correstriction maps*

$$\mathrm{Cor}\colon H^i(H, A) \to H^i(G, A),\ i \geq 0$$

which are given by taking cohomology and applying Shapiro's lemma. It satisfies the following property.

Proposition 3.3.24. *Let H be a subgroup of G of finite index $n \geq 1$, and let A be a G-module. Then the composite maps*

$$\mathrm{Cor} \circ \mathrm{Res}\colon H^i(G, A) \to H^i(G, A)$$

are given by multiplication by n for all $i \geq 0$.

Given a subgroup H of G, perhaps a normal subgroup, or a subgroup of finite index if needed, the cup-product satisfies the following compatibility relations with the associated restriction maps, inflation maps and corestriction maps.

Proposition 3.3.25. *For given G-modules A and B we have the following relations.*

1. *For $a \in H^i(G, A)$ and $b \in H^j(G, B)$ we have*
$$\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b).$$
2. *If H is normal in G, $a \in H^i(G/H, A^H)$ and $b \in H^j(G/H, B^H)$, then we have*
$$\mathrm{Inf}(a \cup b) = \mathrm{Inf}(a) \cup \mathrm{Inf}(b).$$
3. *Let H be a subgroup of G of finite index. Then for $a \in H^i(H, A)$ and $b \in H^j(G, B)$ we have*
$$\mathrm{Cor}(a \cup \mathrm{Res}(b)) = \mathrm{Cor}(a) \cup b.$$
This is called the "projection formula".

Proof. According to the definition of restriction maps, (1) follows by performing the cup-product construction for the modules

$$\begin{aligned}\mathrm{Ind}_H^G(A) &= \mathrm{Hom}_H(\mathbb{Z}[G], A)\\ \mathrm{Ind}_H^G(B) &= \mathrm{Hom}_H(\mathbb{Z}[G], B),\end{aligned}$$

and using the functoriality of the construction for the natural maps $A \to \mathrm{Ind}_H^G(A)$ and $B \to \mathrm{Ind}_H^G(B)$.
Similarly, (2) follows by performing the cup-product construction simultaneously for the projective resolutions $P_\bullet$ and $Q_\bullet$ considered in the definition of inflation maps (a projective resolution $P_\bullet$ of $\mathbb{Z}$ as a trivial G-module and a projective resolution $Q_\bullet$ of $\mathbb{Z}$ as a trivial G/H-module), and using functoriality.
For (3), consider the diagram

$$\begin{tikzcd}
\mathrm{Hom}_H(\mathbb{Z}[G], A) \times \mathrm{Hom}_H(\mathbb{Z}[G], B) \arrow[r] \arrow[d] & \mathrm{Hom}_{H\times H}(\mathbb{Z}[G\times G], A\otimes B) \arrow[d] \\
\mathrm{Hom}_G(\mathbb{Z}[G], A) \times \mathrm{Hom}_G(\mathbb{Z}[G], B) \arrow[r] \arrow[u] & \mathrm{Hom}_{G\times G}(\mathbb{Z}[G\times G], A\otimes B)
\end{tikzcd}$$

where the horizontal maps are induced by the tensor product, the middle vertical map upwards is the one inducing the restriction and the two others are those inducing the correstriction maps. The diagram is “commutative” in the sense that starting form elements in $\mathrm{Hom}_H(\mathbb{Z}[G], A)$ and $\mathrm{Hom}_G(\mathbb{Z}[G], B)$ we obtain the same elements in $\mathrm{Hom}_{G\times G}(\mathbb{Z}[G\times G], A\otimes B)$ by going through the diagram in the two possible ways; this follows from the definition of the maps. The claim then again follows by performing the cup-product construction for the pairings of the two rows of the diagram and using functoriality. □

3.4. Homology groups and Tate groups

The functorial definition of cohomology groups can be dualized to give us homology groups.

Definition 3.4.1. Let M be a G-module and define M_G to be the largest quotient module of M on which G acts trivially. This is called the *module of coinvariants.*

In other words, M_G is the quotient of M by the subgroup generated by

$$\{gm - m \mid g \in G, m \in M\}$$

If M is a trivial G-module then $M = M_G$. Considering $\mathbb{Z}[G]$-modules we have the following description of M_G. Let $\varepsilon \colon \mathbb{Z}[G] \to \mathbb{Z}$ be the *augmentation map*, given by

$$\sum_{g \in G} n_g g \mapsto \sum_{g \in G} n_g$$

This is a ring epimomorphism (but not a G-module homomorphism). Its kernel is called the *augmentation ideal*, denoted by $\ker \varepsilon = I_G = I$. It is a free $\mathbb{Z}$-submodule of $\mathbb{Z}[G]$ with basis $\{g - 1 \mid g \in G\}$: if $x \in I_G$ then $x = \sum_g n_g g$ such that $\sum_g n_g = 0$. Thus, $x = \sum_g n_g (g - 1)$.

Lemma 3.4.2. *Let M be a G-module. Then we have*

$$M_G \cong M/IM \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$$

Proof. By definition the quotient map $\pi \colon M \to M_G$ satisfies $\pi(gm - m) = 0$ for all $g \in G, m \in M$. Hence $I_G M \subset \ker \pi$. But M_G is maximal with this property, and hence $I_G M = \ker \pi$ and $M_G \cong M/I_G M$. For the second part consider the map $\mathbb{Z} \otimes_{\mathbb{Z}[G]} M \to M_G$ given by $n \otimes m \mapsto n[m]$, where $[m]$ denotes the natural image of an element $m \in M$ in $M_G = M/IM$. Clearly this map defines an epimorphism. We will show that it is also injective. Let $1 \otimes m$ be in the kernel. This means $[m] = [0]$. Consequently we can write $m = \lambda_1 m_1 + \ldots + \lambda_n m_n$, where $\lambda_r \in I$ and $m_r \in M$. Since for $\lambda \in I$ we have $1\lambda = 0$ it follows

$$1 \otimes m = \sum_r (1 \otimes \lambda_r m_r) = \sum_r ((1\lambda_r) \otimes m_r) = 0.$$

□

Lemma 3.4.3. *The functor $F \colon \mathcal{M}_G \to \mathcal{AB}$, $F(M) = M_G$ from the category of G-modules to the category of abelian groups is right exact.*

Proof. This follows from the fact that F is naturally equivalent to the functor $M \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$, which is clearly right exact. Recall that F being right exact means the following. If

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of G-modules, then so is

$$M'_G \to M_G \to M''_G \to 0$$

□

Recall that the category $\mathcal{M}_G$ has enough projectives, see proposition 2.7.24. Hence every G-module M has a projective resolution

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to M \to 0$$

Then the complex

$$\cdots \to (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \to M_G \to 0$$

need no longer be exact, and we define

$$H_n(G,M) = \ker(d_n)/\operatorname{im}(d_{n+1})$$

These groups have the following basic properties.

(1) We have $H_0(G,M) = F(M) = M_G$, because
$$(P_1)_G \to (P_0)_G \to M_G \to 0$$
is exact.

(2) If P is a projective G-module, then $H_n(G,P) = 0$ for all $n \geq 1$, because $\cdots 0 \to P \to P \to 0$ is a projective resolution of P.

(3) Let $P_\bullet \to M$ and $Q_\bullet \to N$ be projective resolutions of G-modules M and N. Then any homomorphism $\alpha\colon M \to N$ of G-modules extends to a morphism of complexes
$$\begin{tikzcd} P_\bullet \arrow[r] \arrow[d, "\widetilde{\alpha}"] & M \arrow[d, "\alpha"] \\ Q_\bullet \arrow[r] & N \end{tikzcd}$$
and the homomorphisms $H_n(\widetilde{\alpha})\colon H_n(P_{\bullet G}) \to H_n(Q_{\bullet G})$ are independent of the choice of α. Applying this to the identity map $\operatorname{id}\colon M \to M$, it follows that the groups are well-defined up to canonical isomorphism. Moreover $M \mapsto H_n(G,M)$ is a functor from the category of G-modules to the category of abelian groups.

(4) A short exact sequence $0 \to N \to M \to V \to 0$ of G-modules gives rise to a long exact sequence
$$\cdots \to H_n(G,N) \to H_n(G,M) \to H_n(G,V) \to H_{n-1}(G,N) \to \cdots$$
$$\to H_1(G,V) \to H_0(G,N) \to H_0(G,M) \to H_0(G,V) \to 0$$
Each morphism of short exact sequences induces a morphism of long exact sequences.

Note that these properties determine the functors $H_n(G,\bullet)$. Just as in the case of cohomology, it is possible to give an explicit description of the homology groups $H_n(G,M)$ as the quotient of a group of n-cycles by a subgroup of n-boundaries.

We will shortly discuss the low-dimensional homology groups. They also have interpretations in group theory. However, the low-dimensional cohomology groups are more important. Let us start with $n = 0$. By definition we have

$$H_0(G,M) = M_G$$

In the following we consider $\mathbb{Z}$ as a trivial G-module.

Lemma 3.4.4. *For any group G we have*

$$H_1(G,\mathbb{Z}) \cong I/I^2$$

Proof. By definition of I we have a short exact sequence of G-modules

$$0 \to I \xrightarrow{\imath} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

It induces a long exact sequence of homology groups, ending with

$$H_1(G,\mathbb{Z}[G]) \to H_1(G,\mathbb{Z}) \xrightarrow{\partial} H_0(G,I) \xrightarrow{\beta} H_0(G,\mathbb{Z}[G]) \xrightarrow{\varepsilon_*} H_0(G,\mathbb{Z}) \to 0$$

By Lemma 3.4.2 we have

$$\begin{aligned} H_0(G,\mathbb{Z}) &= \mathbb{Z}_G = \mathbb{Z} \\ H_0(G,\mathbb{Z}[G]) &= \mathbb{Z}[G]_G = \mathbb{Z}[G]/I\mathbb{Z}[G] = \mathbb{Z} \\ H_0(G,I) &= I/I^2 \end{aligned}$$

Also $H_1(G,\mathbb{Z}[G]) = 0$, because $\mathbb{Z}[G]$ is projective. In fact, it is free, hence projective as $\mathbb{Z}[G]$-module. The exactness of the sequence thus implies that ∂ is injective and ε_* is surjective. Together it shows that

$$\mathbb{Z}/\ker\varepsilon_* \cong \operatorname{im}\varepsilon_* \cong \mathbb{Z}$$

Hence ε_* must be injective as well: if $\ker\varepsilon_*$ is nonzero, then $\mathbb{Z}/\ker\varepsilon_*$ is finite, which is not the case. It follows that β is zero and ∂ is surjective, hence bijective:

$$\partial\colon H_1(G,\mathbb{Z}) \cong I/I^2$$

□

We can now interpret $H_1(G,\mathbb{Z})$ with the trivial G-action.

Proposition 3.4.5. *For any group G we have*

$$H_1(G,\mathbb{Z}) \cong G/G'$$

where G' is the commutator subgroup of G.

Proof. Because of the Lemma it suffices to prove that $G/G' \cong I/I^2$ as abelian groups. Define $\theta\colon G \to I/I^2$ by

$$x \mapsto (x-1) + I^2$$

To see that θ is a homomorphism, note that

$$xy - 1 - (x-1) - (y-1) = (x-1)(y-1) \in I^2$$

so that

$$\begin{aligned} \theta(xy) &= xy - 1 + I^2 \\ &= (x-1) + (y-1) + I^2 \\ &= (x - 1 + I^2) + (y - 1 + I^2) \\ &= \theta(x) + \theta(y) \end{aligned}$$

Since I/I^2 is abelian we have $\ker\theta \subset G'$, and so θ induces a homomorphism $\psi\colon G/G' \to I/I^2$ given by

$$xG' \mapsto x - 1 + I^2$$

We will construct the inverse of ψ, showing that ψ is a group isomorphism. Define $\varphi\colon I \to G/G'$ by

$$x - 1 \mapsto xG'$$

Because I is a free abelan group with basis all $x-1$, where $x \in G \setminus 1$, φ is a well-defined homomorphism. We have to show that I^2 is a subgroup of $\ker\varphi$. Then φ induces a map $I/I^2 \to G/G'$, which is clearly the inverse of ψ. But this follows from the identity

$$\begin{aligned} \varphi((x-1)(y-1)) &= \varphi((xy-1) - (x-1) - (y-1)) \\ &= xyG'(xG')^{-1}(yG')^{-1} \\ &= 1 \end{aligned}$$

□

Corollary 3.4.6. *For any group and any trivial G-module M we have*

$$H_1(G, M) \cong (G/G') \otimes_{\mathbb{Z}[G]} M$$

The group $H_2(G, \mathbb{Z})$ is also useful in group theory. It is called the *Schur multiplier* of G, because it has to do with universal central extensions of G. There is also a formula of Hopf: let $G = F/R$ be a presentation of a group G, where F is a free group and R is a normal subgroup of relations.

Theorem 3.4.7 (Hopf). *We have*

$$H_2(G, \mathbb{Z}) \cong (R \cap F')/[F, R]$$

so that the group on the RHS depends only on G and not upon the choice of the presentation of G.

Remark 3.4.8. For any group G, there exists a topological space BG, called the *classifying space* of G, such that $G = \pi_1(BG)$, and

$$H_n(BG, \mathbb{Z}) = H_n(G, \mathbb{Z})$$

There is also a topological space $K(G, 1)$, unique up to homotopoy type, such that $G = \pi_1(K(G, 1))$, $\pi_n(K(G, 1)) = 0$ for $n > 1$, and

$$H^n(K(G, 1), \mathbb{Z}) = H^n(G, \mathbb{Z})$$

Example 3.4.9. *Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ be the Kleinian 4-group. A presentation of G is given by*

$$G = \langle x, y \mid x^2, y^2, xyx^{-1}y^{-1} \rangle$$

Then $H_2(G, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

Here, F is the free group with basis (x, y). One shows that $(R \cap F')/[F, R] = \mathbb{Z}/2\mathbb{Z}$. The proof is left to the reader.
We will now define the so called Tate groups which combine homology and cohomology groups so that we become a doubly infinite exact sequence of homology and cohomology. For that we require G to be *finite.*

Definition 3.4.10. Let G be a finite group and M be a G-module. The map $\mathrm{Norm}_G \colon M \to M$ is defined to be

$$m \mapsto \sum_{g \in G} gm$$

It is called the *Norm map.*

Lemma 3.4.11. *The norm map induces a homomorphism*

$$\mathrm{Norm}_G \colon H_0(G, M) \to H^0(G, M)$$

Definition 3.4.12. Let G be a finite group and M be a G-module. The *Tate groups* are defined to be

$$H^k_T(G, M) = \begin{cases} H^k(G, M) & k > 0 \\ M^G/\mathrm{Norm}_G(M) & k = 0 \\ \ker(\mathrm{Norm}_G)/IM & k = -1 \\ H_{-k-1}(G, M) & k < -1 \end{cases}$$

For example, $H_T^{-2}(G,\mathbb{Z}) = H_1(G,\mathbb{Z}) \cong G/G'$. The T stands for Tate, who had a major part in introducing Galois cohomology into algebraic number theory.

PROPOSITION 3.4.13. *Any short exact sequence of G-modules*

$$0 \to M' \to M \to M'' \to 0$$

induces an exact sequence of Tate groups, for all $k \in \mathbb{Z}$,

$$\cdots \to H_T^{k-1}(G,M'') \to H_T^k(G,M') \to H_T^k(G,M) \to$$
$$H_T^k(G,M'') \to H_T^{k+1}(G,M') \to \cdots$$

which extends infinitely in both directions.

In general, for any given G and M the Tate groups exhibit very little obvious structure. This is different, if G is cyclic.

THEOREM 3.4.14. *Let G be a finite cyclic group and M be a G-module. Then, for all $k \in \mathbb{Z}$,*

$$H_T^k(G,M) \cong H_T^{k+2}(G,M)$$

We mention another result.

THEOREM 3.4.15. *Let G be a finite group and M be a G-module. If*

$$H_T^1(H,M) = H_T^2(H,M) = 0$$

for all proper subgroups H of G, then $H_T^k(G,M) = 0$ for all $k \in \mathbb{Z}$.

If G is cyclic, this follows of course from the periodicity of the Tate cohomology.

REMARK 3.4.16. We will not attempt to define homology groups or Tate groups for profinite groups. The passage from finite groups to profinite groups is only well-behaved for cohomology.

Bibliography

[1] E. Artin: *Algebraic numbers and algebraic functions.* Gordon and Breach **1967**.

[2] K. S. Brown: *Cohomology of groups.* Springer Verlag **1982**.

[3] P. M. Cohn: *Algebra.* Second Edition, John Wiley & Sons **1995**.

[4] N. Jacobson: *Basic algebra I.* San Francisco: Freeman and Co. **1974**.

[5] N. Jacobson: *Basic algebra II.* Second Edition. San Francisco: Freeman and Co. **1989**.

[6] M. D. Fried, M. Jarden: *Field arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 11, Springer-Verlag **2005**.

[7] P. Gille, T. Szamuely: *Central simple algebras and Galois cohomology.* Cambridge Studies in advanced mathematics 101 **2006**.

[8] S. Lang: *Algebra.* Revised third edition. Graduate Texts in Mathematics 211. Springer-Verlag, New York, **2002**.

[9] L. Ribes, P. Zalesskij: *Profinite groups.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 40, Springer Verlag **2000**.

[10] J. J. Rotman: *Advanced modern algebra.* Pearson Education Upper Saddle River, New York **2002**.

[11] M. Suzuki: *Group Theory I.* Grundlehren der Mathematischen Wissenschaften, Band 247, Springer Verlag **1982**.

[12] C. A. Weibel: *An introduction to homological algebra.* Cambridge University Press **1997**.