Cohomology of Groups and Algebras

Dietrich Burde

Lecture Notes 2023

Contents

CHAPTER 1

Introduction

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

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

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.

Lie algebra cohomology was invented by Elie Cartan, Claude Chevalley und Samuel Eilenberg around 1950 to compute the de Rham cohomology of a compact Lie group. Cartan had shown that the computation of the cohomology of Lie groups can be reduced to the cohomology of compact Lie groups. Chevalley and Eilenberg defined in [**7**] first the Lie algebra cohomology $H^n(\mathfrak{g},\mathbb{R})$ with the trivial $\mathfrak{g}$-module $\mathbb{R}$, by transfering the de Rham cohomology $H^n_{dR}(G,\mathbb{R})$ of a connected compact Lie group to its Lie algebra. This yields an isomorphism $H^n_{dR}(G,\mathbb{R}) \cong H^n(\mathfrak{g},\mathbb{R})$, where $\mathfrak{g}$ is the Lie algebra of G. To study the cohomology $H^n(G/H,\mathbb{R})$ of homogeneous spaces G/H of G, Chevalley und Eilenberg defined the Lie algebra cohomology

$H^n(\mathfrak{g}, M)$ for a general $\mathfrak{g}$-Modul M. Furthermore the article [**7**] already contains the interpretation of $H^2(\mathfrak{g}, M)$ by Lie algebra extensions of $\mathfrak{g}$ by M, as well as the Whitehead Lemmas in the form $H^1(\mathfrak{g}, M) = H^2(\mathfrak{g}, M) = 0$ for finite-dimensional semisimple Lie algebras over a field of characteristic zero and finite-dimensional $\mathfrak{g}$-modules M.

CHAPTER 2

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.

2.1. Split extensions and semidirect products

We start with the definition of exact sequences.

Definition 2.1.1. 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 2.1.2. *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 2.1.3. *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

$$A' \cong \alpha(A') = \ker\beta \tag{2.1}$$

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

$$A/\ker\beta \cong \beta(A) = A'' \tag{2.2}$$

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

Definition 2.1.4. 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 2.1.3.

Example 2.1.5. *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 2.1.6. *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 $S_3 \cong D_3$ is an extension of C_3 by C_2, but not of C_2 by C_3. We obtain the short exact sequence

$$1 \to C_3 \to D_3 \to C_2 \to 1$$

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 D_3 since the index is $[D_3 : C_3] = 2$. The quotient is isomorphic to $C_2 = \langle (12) \rangle$. Note that C_2 is not a normal subgroup of 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

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

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

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

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 2.1.8. *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 2.1.9. *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 2.1.10. 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.,

$$\beta\tau = \mathrm{id}_{|Q} \tag{2.3}$$

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

Definition 2.1.11. 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 2.1.12. *The extensions of Example* 2.1.6 *are both split:*

$$1 \to C_3 \to C_6 \to C_2 \to 1$$
$$1 \to C_3 \to D_3 \to C_2 \to 1$$

On the other hand the extension

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

of Example 2.1.8 *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 2.1.13. Two subgroups $N, Q \leq G$ are called *complementary* if

$$N \cap Q = 1 \tag{2.4}$$
$$G = NQ \tag{2.5}$$

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 2.1.14. *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* $G = S_4$ *are not complementary.*

The first case is clear, for the second note that $|NQ| = |N| \cdot |Q| \cdot |N \cap Q|^{-1} = 6$, hence $NQ \neq S_4$.

Lemma 2.1.15. *Let* $N, Q \leq G$ *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 2.1.16. A group G is called *inner semidirect product* of N by Q if the followuing conditions hold.

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 2.1.17. *Both* 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 2.1.18. *Let S_n denote the symmetric group on n letters and D_n the dihedral group of order $2n$. Both are inner semidirect products as follows:*

$$S_n = C_2 \ltimes A_n$$
$$D_n = C_2 \ltimes C_n$$

Clearly $A_n \lhd S_n$ and C_2, A_n are complementary subgroups in S_n. Let $D_n = \langle s, t \mid s^n = t^2 = 1,\ tst = s^{-1}\rangle$ 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 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 2.1.19. *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 2.1.20. *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

$$\alpha(N) \cap \tau(Q) = 1 \tag{2.6}$$

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.,

$$G = \alpha(N)\tau(Q) \tag{2.7}$$

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.,

$$C \cap \alpha(N) = 1 \tag{2.8}$$

$$C \cdot \alpha(N) = G \tag{2.9}$$

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 2.1.21. *The following exact sequences are both split:*

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

It follows that $S_n \cong C_2 \ltimes A_n$ and $GL_n(k) \cong k^\times \ltimes SL_n(k)$.

Since $\ker \mathrm{sign} = A_n$ we see that the first sequence is exact. It also splits. Let $\pi \in S_n$ be a transposition and define $\tau \colon \{\pm 1\} \to S_n$ 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 2.1.22. 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:

$$(x, a)(y, b) = (xy, \varphi(y)(a) \cdot b) \tag{2.10}$$

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

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

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

Proposition 2.1.24. *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

$$\alpha\circ\varphi(x) = \gamma(\tau(x))\circ\alpha \tag{2.11}$$

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 (2.11). 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 2.1.25. *Each split short exact sequence* $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ *defines via* (2.11) *an outer semidirect product* $Q \ltimes_\varphi N$ *which is isomorphic to* G.

Proof. Since α is a monomorphism (2.11) defines a homomorphism $\varphi : Q \to \mathrm{Aut}(N)$. Define the map $\psi : Q \ltimes_\varphi N \to G$ by

$$\psi[(x,a)] = \tau(x) \cdot \alpha(a) \tag{2.12}$$

By Lemma 2.1.15 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 (2.10) and the fact that τ is a homomorphism. On the other hand

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

□

Example 2.1.26. *Let* C_2 *act on* C_n *by the automorphism* $x \mapsto x^{-1}$. *Then* $D_n \cong C_2 \ltimes_\varphi C_n$

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

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

Schur-Zassenhaus 2.1.27. *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 3.5.6. 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.

2.2. 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 2.2.1. *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

$$\gamma f = g\alpha, \quad h\beta = \delta g \tag{2.13}$$

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 (2.13)

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

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 (2.13)

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

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 (2.13)

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

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 2.2.2. *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 2.2.3. 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 2.2.2. 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 2.2.4. *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 2.2.5. 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 2.2.6. Let N and Q be two groups. A pair of functions (f, T)

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

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

$$f(xy,z)T(z)(f(x,y)) = f(x,yz)f(y,z) \tag{2.14}$$

$$T(y)\circ T(x) = \gamma\left(f(x,y)\right)\circ T(xy) \tag{2.15}$$

$$f(1,1) = 1 \tag{2.16}$$

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

The second condition (2.15) 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 2.2.7. 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 (2.15) and (2.14) reduces to $1 = 1$.

Condition (2.16) corresponds to a normalization. The first two conditions already imply the following conditions:

Lemma 2.2.8. *Let (f,T) be a pair of functions as above where only conditions* (2.14) *and* (2.15) *are satisfied. Then it follows*

$$T(1) = \gamma(f(1,1)) \tag{2.17}$$

$$f(x,1) = f(1,1) \tag{2.18}$$

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

for all $x, y \in Q$.

Proof. By (2.15) 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 (2.14) with $z = y = 1$ for the last equation. This shows (2.18).
Setting $x = y = 1$ in (2.14) 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 (2.19). □

Corollary 2.2.9. *Let (f,T) be a factor system to N and Q. Then*

$$f(x,1) = f(1,y) = 1 \tag{2.20}$$

$$T(1) = \mathrm{id}_{|N} \tag{2.21}$$

for all $x, y \in Q$.

Proof. By (2.16) 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 2.2.10. *Each group extension $1 \to N \overset{\alpha}{\to} G \overset{\beta}{\to} Q \to 1$ 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

$$\alpha(T_\tau(x)(n)) = \tau(x)^{-1}\alpha(n)\tau(x) \tag{2.22}$$

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

$$\tau(x)\tau(y) = \tau(xy)\alpha(f_\tau(x,y)) \tag{2.23}$$

Now we have to verify the conditions (2.14),(2.15),(2.16) for the pair (f_τ, T_τ) which we will denote by (f,T). We set

$$\tau(1) = 1 \tag{2.24}$$

This condition is not essential, but it helps simplify some of the computations. By (2.23) we have

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

hence $\alpha(f(1,1)) = 1$ and $f(1,1) = 1$. Hence (2.16) is satisfied. By using (2.22) and (2.23) 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 (2.15). Using (2.23) we have

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

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

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 (2.14). □

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 2.2.11. *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.

$$(x,a)\circ(y,b) = (xy, f(x,y)T(y)(a)b) \tag{2.25}$$

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.

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

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

In the second computation we have first used that $T(z)$ is an automorphism of N, then (2.15) and (2.14). 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 (2.25) 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 $\alpha : N\to G$ defined by $a\mapsto (1,a)$ is a monomorphism. We obtain a short exact sequence $1\to N\xrightarrow{\alpha} G\xrightarrow{\beta} Q\to 1$ and hence an extension G of N by Q.

The next step is to choose a transversal function $\tau : Q\to G$. 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 (2.23), where $f_\tau(x,y)$ was uniquely determined, it follows $f_\tau = f$. Using (2.14) 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

$$T(x)(f(x,x^{-1})^{-1}) = f(x^{-1},x)^{-1} \tag{2.26}$$

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 (2.22) shows $T_\tau = T$. □

EXAMPLE 2.2.12. *Consider the extension* $1\to C_2\xrightarrow{\alpha} C_4\xrightarrow{\beta} C_2\to 1$ *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* $\tau(1) = 1$, $\tau(x) = g$.

$T_\tau : C_2\to \mathrm{Aut}(C_2)$ 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 $f_\tau : C_2\times C_2\to C_2$ 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 2.2.13. *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 2.2.14. *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*

$$T'(x) = \gamma(h(x)) \circ T(x) \tag{2.27}$$

$$f'(x,y) = h(xy)^{-1} f(x,y) \cdot T(y)(h(x)) \cdot h(y) \tag{2.28}$$

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

$$\tau'(x) = \tau(x)\ell(x) \tag{2.29}$$

with a map $\ell : Q \to \alpha(N)$. Define $h : Q \to N$ by $\alpha(h(x)) = \ell(x)$. Using (2.22) 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 (2.27) follows. Using (2.23) 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 (2.28). □

The lemma tells us how to define the equivalence relation.

Definition 2.2.15. 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 (2.27) and (2.28) 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 2.2.16. *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 $1 \to N \xrightarrow{\gamma} G' \xrightarrow{\delta} Q \to 1$ and the following $\tau' : Q \to G'$:

$$\tau'(x) = \varphi(\tau(x)) \tag{2.30}$$

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 (2.22) 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 (2.23) 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 2.2.17. *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 (2.27) and (2.28). Let G, G' be the group extensions of N by Q as constructed in proposition 2.2.11. 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 2.2.16 commutes. We define φ by

$$(x,a) \mapsto (x, h(x)^{-1}a) \tag{2.31}$$

Clearly this map is bijective. It is also a homomorphism with respect to the composition (2.25).

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

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

In the second computation we have used also (2.27) and (2.28). 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 2.2.18 (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 a *trivial* factor set, i.e., with $f \equiv 1$, 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 3

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.

3.1. 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 3.1.1. 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 $m, n \in M$,

$$g(m+n) = gm + gn \tag{3.1}$$

$$(gh)m = g(hm) \tag{3.2}$$

$$1m = m \tag{3.3}$$

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

$$T(g)(m) = gm \quad \forall\, m \in M \tag{3.4}$$

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

$$\left(\sum_g n_g g\right)\left(\sum_h m_h h\right) = \sum_{g,h} n_g m_h (gh) \tag{3.5}$$

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

$$\left(\sum_g n_g g\right) m = \sum_g n_g (gm) \tag{3.6}$$

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

Example 3.1.2. *Let M be any abelian group and define*

$$gm = m \tag{3.7}$$

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

$$h\left(\sum_g n_g g\right) = \sum_g n_g hg \tag{3.8}$$

is called the regular G-module.

Definition 3.1.4. Let M be a G-module. Define

$$M^G = \{m \in M \mid gm = m \text{ for all } g \in G\} \tag{3.9}$$

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

$$\varphi(m + m') = \varphi(m) + \varphi(m') \tag{3.10}$$

$$\varphi(gm) = g\varphi(m) \tag{3.11}$$

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

3.2. 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 $C^0(G, A) = \operatorname{Hom}(1, A) \cong A$. 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 3.2.1. If $f \in C^n(G, A)$ then define $\delta_n(f)$ by

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

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

$$(\delta_0 f)(x_1) = x_1 f - f \tag{3.12}$$

$$(\delta_1 f)(x_1, x_2) = x_1 f(x_2) - f(x_1 x_2) + f(x_1) \tag{3.13}$$

$$(\delta_2 f)(x_1, x_2, x_3) = x_1 f(x_2, x_3) - f(x_1 x_2, x_3) + f(x_1, x_2 x_3) - f(x_1, x_2) \tag{3.14}$$

$$\begin{aligned}(\delta_3 f)(x_1, x_2, x_3, x_4) &= x_1 f(x_2, x_3, x_4) - f(x_1 x_2, x_3, x_4) + f(x_1, x_2 x_3, x_4) \\ &- f(x_1, x_2, x_3 x_4) + f(x_1, x_2, x_3)\end{aligned} \tag{3.15}$$

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 3.2.2. *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 $\delta^2(f)(x_1, \ldots, x_{n+2}) = 0$. Define $g_j \in C^{n+1}(G, A)$ for $0 \le j \le n+1$ by

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

This means

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

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

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

This means

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

It follows

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

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

$$(g_{ji} + g_{i-1,j})(x_1,\ldots,x_{n+2}) = 0 \tag{3.16}$$

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 $i=1,\ldots,n+2$, then $j=1$ and $i=2,\ldots n+2$, 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 (3.16). Assume first $1 \le j \le n$. If $i > j+1$ then

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

with

$$(\tau_1,\ldots,\tau_j,\tau_{j+1},\ldots,\tau_i,\tau_{i+1},\ldots,\tau_{n+1}) = \\ (x_1,\ldots,x_j,x_{j+1},\ldots,x_ix_{i+1},x_{i+2},\ldots,x_{n+2}).$$

On the other hand we have

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

with

$$(\sigma_1,\ldots,\sigma_{j-1},\sigma_j,\ldots,\sigma_{i-1},\sigma_i,\ldots,\sigma_{n+1}) = \\ (x_1,\ldots,x_{j-1},x_jx_{j+1},\ldots,x_i,x_{i+1},\ldots,x_{n+2}).$$

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

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

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

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

3.3. 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 3.3.1. *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 3.3.2. *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 $\mathbb{Z}$. □

3.4. 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 3.4.1. 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

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

Proposition 3.4.2. *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 (2.10), 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 3.4.3. *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 3.4.4. *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 3.4.5. *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 3.4.6. 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 3.4.7. *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 3.4.8. We have $H^n(G,L)=0$ for all $n\in\mathbb{N}$, but not $H^n(G,L^\times)=1$ in general.

3.5. 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 $T:G\to\operatorname{Aut}(A)$ is called factor system to A and G if

$$f(xy,z)+f(x,y)z=f(x,yz)+f(y,z) \tag{3.17}$$

$$T(xy)=T(y)T(x) \tag{3.18}$$

$$f(1,1)=0 \tag{3.19}$$

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

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

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 $T_\tau : G\to \mathrm{Aut}(A)$ 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 (3.17) 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 (3.2.1) for a right G-module according to remark (3.4.1). 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 3.5.1. *Let G be a group and A be an abelian group, and let M denote the set of group extensions*

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

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 2.2.18 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 (2.28) 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 3.5.2. *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

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

Example 3.5.3. *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 3.4.4.

Proposition 3.5.4. *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 3.5.5. *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 (2.1.27). We will sketch the proof of the general case.

Schur-Zassenhaus 3.5.6. *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 $G' \cong G$. □

3.6. 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 3.6.1. 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

$$ {}^{\alpha(m)}n = m\,n\,m^{-1} \tag{3.20}$$

$$ \alpha({}^e n) = e\,\alpha(n)\,e^{-1} \tag{3.21}$$

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

Example 3.6.2. *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 3.6.3. *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 (3.21) $G = \operatorname{coker}(\alpha)$ is a group. This means that the sequence $N \overset{\alpha}{\to} E \overset{\pi}{\to} G \to 1$ is exact. Since A is central in N by (3.20), and since the action of E on N induces an action of G on A, we obtain a 4-term exact sequence

$$0 \to A \overset{i}{\to} N \overset{\alpha}{\to} E \overset{\pi}{\to} G \to 1 \tag{3.22}$$

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 (3.22), 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 3.6.4. *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 [**29**], Theorem 6.6.13.

3.7. Categories and functors

We will briefly discuss the language of category theory.

Definition 3.7.1. A *category* $\mathcal{C}$ consists of a class $ob(\mathcal{C})$ of objects and a class $mor(\mathcal{C})$ of morphisms, together with the following structural maps:

(i) An identity map $i\colon ob(\mathcal{C}) \to mor(\mathcal{C})$, which asigns to each object A a morphism id_A, the *identity morphism* of A.

(ii) Two functions $s, t\colon mor(\mathcal{C}) \to ob(\mathcal{C})$, which assign to every morphism its *source* (or domain) and *target* (or codomain),

(iii) A composition map $\circ\colon mor(\mathcal{C}) \times mor(\mathcal{C}) \to mor(\mathcal{C})$, which assigns to any pair of morphisms f, g such that $t(f) = s(g)$ their composite morphism $g \circ f$,

such that the following axioms are satisfied:

(1) $s(g\circ f) = s(f)$ and $t(g\circ f) = t(g)$, i.e., source and target are respected by composition.

(2) $s(\mathrm{id}_A) = A$ and $t(\mathrm{id}_A) = A$, i.e, source and target are respected by identities.

(3) $(h \circ g) \circ f = h \circ (g \circ f)$ whenever $t(f) = s(g)$ and $t(g) = s(h)$, i.e., composition is associative whenever defined.

(4) If $s(f) = A$ and $t(f) = B$, then $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$, i.e., composition satisfies the left and right unit laws.

The sets

$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}(A, B) &= \{f \in mor(\mathcal{C}) \mid s(f) = A,\, t(f) = B\}\\ &= \{f\colon A \to B\}\end{aligned}$$

are called *homsets*.

Example 3.7.2. *1. The category $\mathcal{S}et$, with sets as objects and functions as morphisms.*

2. The category $\mathcal{G}rp$, with groups as objects and group homomorphisms as morphisms.

3. The category $\mathcal{V}ect$, with vector spaces as objects and linear maps as morphisms.

4. The category $\mathcal{T}op$, with topological spaces as objects and continuous functions as morphisms.

5. The category $\mathcal{D}iff$, with smooth manifolds as objects and smooth maps as morphisms.

6. The category $\mathcal{R}ing$, with rings as objects and ring homomorphisms as morphisms.

7. The category $\mathcal{M}od_R$, with R-modules over a ring R as objects and R-module homomorphisms as morphisms.

8. The category $\mathcal{A}lg_R$, with R-algebras as objects and R-algebra homomorphisms as morphisms.

9. The category $\mathscr{CRing}$, with commutative rings as objects and ring homomorphisms as morphisms.

10. The category $\mathscr{Aff}$, with affine schemes as objects and morphism of locally ringed spaces as morphisms.

Definition 3.7.3. Let $\mathscr{C}$ be a category. A *subcategory* $\mathscr{D}$ consists of a subcollection of the collection of objects of $\mathscr{C}$ and a subcollection of the collection of morphisms of $\mathscr{D}$ such that

(1) If the morphism $f\colon A \to B$ is in $\mathscr{D}$, then so are A and B.

(2) If $f\colon A \to B$ and $g\colon B \to C$ are in $\mathscr{D}$, then so is the composite $g \circ f\colon A \to C$.

(3) If A is in $\mathscr{D}$ then so is the identity morphism id_A.

In addition $\mathscr{D}$ is a *full subcategory* if for any A and B in $\mathscr{D}$, every morphism $f\colon A \to B$ in $\mathscr{C}$ is also in $\mathscr{D}$.

These conditions ensure that $\mathscr{D}$ is a category in its own right and the inclusion $D \hookrightarrow C$ is a *functor*. For example, the category $\mathscr{Ab}$ of abelian groups is a full subcategory of $\mathscr{Grp}$. Here is a table of some categories related to groups:

$\mathscr{C}$	Name
$\mathscr{Grp}$	Groups
$\mathscr{Ab}$	Abelian groups
$\mathscr{Ab}_d$	Divisible abelian groups
$\mathscr{Ab}_f$	Free abelian groups
$\mathscr{Cyc}$	Cyclic groups
$\mathscr{Ab}_{tf}$	Torsion-free abelian groups
$\mathscr{Ab}_{fg}$	Finitely generated abelian groups
$\mathscr{Ab}_{ffg}$	Finitely generated free abelian groups
$\mathscr{grp}$	Finite groups
$\mathscr{ab}$	Finite abelian groups
$\mathscr{Ab}_t$	Torsion abelian groups
$\mathscr{Ab}_p$	Profinite abelian groups

Definition 3.7.4. A *functor* F from a category $\mathscr{C}$ to a category $\mathscr{D}$ is a map sending each object $A \in \mathscr{C}$ to an object $F(A) \in \mathscr{D}$ and each morphism $f\colon A \to B$ in $\mathscr{C}$ to a morphism $F(f) : F(A) \to F(B)$ in $\mathscr{D}$, such that

(1) $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for each $A \in ob(\mathscr{C})$.
(2) $F(g \circ f) = F(g) \circ F(f)$, i.e., F is *covariant*, or
(3) $F(g \circ f) = F(f) \circ F(g)$, i.e., F is *contravariant*.

Example 3.7.5. *1.* $F\colon \mathcal{M}od_R \to \mathcal{A}b$, $N \mapsto \operatorname{Hom}_R(M,N)$ *is a functor, denoted by* $F = \operatorname{Hom}_R(M,\cdot)$ *for a given* R*-module* M*.*

2. $F\colon \mathcal{M}od_R \to \mathcal{M}od_R$, $N \mapsto M \otimes_R N$ *is a functor, denoted by* $F = M \otimes_R \cdot$ *for a given* R*-module* M *over a commutative ring* R*.*

3. $U\colon \mathcal{M}od_R \to \mathcal{A}b$, $N \mapsto (N,+)$ *is a functor, mapping* N *to its underlying abelian group. Functors of this kind a called forgetful functors.*

Proposition 3.7.6. *Let* R *be a ring and* M *be a left* R*-module. Then* $F = \operatorname{Hom}_R(M,\cdot)$ *is a covariant functor from* $\mathcal{M}od_R$ *to* $\mathcal{A}b$*, und* $F = \operatorname{Hom}_R(\cdot,M)$ *is a contravariant functor from* $\mathcal{M}od_R$ *to* $\mathcal{A}b$*.*

Proof. Let $\beta\colon A \to B$ be a morphism in $\mathcal{M}od_R$. We need to define $F(\beta)$. Let M be a fixed R-module. Consider the sequence $M \xrightarrow{\alpha} A \xrightarrow{\beta} B$ in $\mathcal{M}od_R$. Then define a homomorphism $\tilde{\beta} = F(\beta)$ of abelian groups

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

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

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

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

$$F(\gamma \circ \beta)(\alpha) = (\gamma \circ \beta)(\alpha) = \gamma \circ (\beta \circ \alpha) \tag{3.23}$$

$$= F(\gamma)(F(\beta)(\alpha)). \tag{3.24}$$

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

Proposition 3.7.7. *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* $\mathcal{M}od_R$ *to* $\mathcal{M}od_R$*.*

Proof. Given $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ in $\mathcal{M}od_R$ 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

$$F(\beta \circ \alpha) = 1_M \otimes (\beta \circ \alpha) = (1_M \otimes \beta) \circ (1_M \otimes \alpha) \tag{3.25}$$

$$= F(\beta)F(\alpha). \tag{3.26}$$

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

Definition 3.7.8. Given categories $\mathcal{C}$ and $\mathcal{D}$, and a pair of functors $F, G\colon\ \mathcal{C} \to \mathcal{D}$, a *natural transformation* N from F to G is an assigment N, which gives for every object C in $\mathcal{C}$ a morphism $N(C)\colon F(C) \to G(C)$, so that for every morphism $f \in \operatorname{Hom}_{\mathcal{C}}(C, C')$ the following diagram commutes.

$$\begin{tikzcd}
F(C) \arrow[r, "N(C)"] \arrow[d, "F(f)"'] & G(C) \arrow[d, "G(f)"] \\
F(C') \arrow[r, "N(C')"] & G(C')
\end{tikzcd}$$

Definition 3.7.9. An *equivalence* between two categories $\mathcal{C}$ and $\mathcal{D}$ is a pair of functors $F\colon \mathcal{C} \to \mathcal{D}$ and $G\colon \mathcal{D} \to \mathcal{C}$ together with natural isomorphisms $F \circ G \equiv \mathrm{id}_{\mathcal{D}}$ and $G \circ F \equiv \mathrm{id}_{\mathcal{C}}$. Here a natural isomorphism is a a natural transformation with a two-sided inverse.

Definition 3.7.10. For a category $\mathcal{C}$, the *opposite category* $\mathcal{C}^{op}$ has the same objects as $\mathcal{C}$, but a morphism $f : A \to B$ in $\mathcal{C}^{op}$ is the same as a morphism $f : B \to A$ in $\mathcal{C}$, and a composite of morphisms $g \circ f$ in $\mathcal{C}^{op}$ is defined to be the composite $f \circ g$ in $\mathcal{C}$.

In general, the categories $\mathcal{C}$ and $\mathcal{C}^{op}$ need not be equivalent. However, the opposite of an opposite category is the original category, i.e., $(\mathcal{C}^{op})^{op} = \mathcal{C}$.

Example 3.7.11. *1. The category of affine schemes is equivalent to the opposite of the category of commutative rings, i.e., $\mathcal{A}ff \cong \mathcal{CR}ing^{op}$.*

2. The Pontryagin duality restricts to an equivalence between the category of compact Hausdorff abelian topological groups and the opposite of the category of abelian groups.

3. The category of profinite abelian groups is equivalent to the opposite of the category of torsion abelian groups.

4. The category of vector spaces is self-dual, i.e., $\mathcal{V}ect \cong \mathcal{V}ect^{op}$. The same is true for the category of finite-dimensional representations of a group (or of a Lie algebra).

Definition 3.7.12. Let $\mathcal{C}$ be a category, and X_1, X_2 two objects in $\mathcal{C}$. A *product* of X_1 and X_2 is an object X, denoted $X_1 \times X_2$, together with a pair of morphisms $\pi_1 : X \to X_1$, $\pi_2\colon X \to X_2$ that satisfy the following universal property. For every object Y and every pair of morphisms $f_1 : Y \to X_1$, $f_2 : Y \to X_2$ there exists a *unique* morphism $f : Y \to X_1 \times X_2$ such that the following diagram commutes:

$$\begin{tikzcd}
 & Y \arrow[ld, "f_1"'] \arrow[d, dashed, "f"'] \arrow[rd, "f_2"] & \\
X_1 & X_1 \times X_2 \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & X_2
\end{tikzcd}$$

Example 3.7.13. *1. In the category of groups, the cartesian product $X_1 \times X_2$ with componentwise multiplication together with the canonical projections $\pi_1 : X_1 \times X_2 \to X_1$, $\pi_2\colon X_1 \times X_2 \to X_2$ is a categorial product for X_1 and X_2.*

2. The category of cyclic groups does not have a product.

A coproduct in $\mathcal{C}$ is the same as a product in the opposite category $\mathcal{C}^{op}$.

Definition 3.7.14. Let $\mathcal{C}$ be a category, and X_1, X_2 two objects in $\mathcal{C}$. A *coproduct* of X_1 and X_2 is an object X, denoted $X_1 \amalg X_2$, together with a pair of morphisms $i_1 : X_1 \to X_1 \amalg X_2$, $i_2\colon X_2 \to X_1 \amalg X_2$ that satisfy the following universal property. For every object Y and every pair of morphisms $f_1 : X_1 \to Y$, $f_2 : X_2 \to Y$ there exists a *unique* morphism $f : X_1 \amalg X_2 \to Y$ such that the following diagram commutes:

$$\begin{tikzcd}
 & Y & \\
X_1 \arrow[ru, "f_1"] \arrow[r, "i_1"'] & X_1 \amalg X_2 \arrow[u, dashed, "f"] & X_2 \arrow[lu, "f_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

Example 3.7.15. *1. The coproduct in the category of groups is the free product. It is infinite in general. For example, $C_2 * C_3 \cong PSL_2(\mathbb{Z})$.*

2. The coproduct in the category of commutative rings is the tensor product.

3. The category of cyclic groups does not have a coproduct.

Definition 3.7.16. Let $\mathcal{C}$ be a category. An *initial object* in $\mathcal{C}$ is an object X such that for every object Y there is a unique morphism $i\colon X \to Y$.

Example 3.7.17. *1. In the category of sets, the empty set is initial.*

2. In the category of groups, the trivial group is initial.

3. In the category of R-modules, the zero module is initial.

Definition 3.7.18. Let $\mathcal{C}$ be a category. An *terminal object* in $\mathcal{C}$ is an object Y such that for every object X there is a unique morphism $t\colon X \to Y$.

Example 3.7.19. *1. In the category of sets, any set containg one element is terminal.*

2. In the category of groups, the trivial group is terminal.

3. In the category of R-modules, the zero module is terminal.

Definition 3.7.20. Let $\mathcal{C}$ be a category. A *zero object* in $\mathcal{C}$ is an object which is both initial and terminal.

Example 3.7.21. *1. In the category of sets, there is no zero object.*

2. In the category of groups, the trivial group is a zero object.

3. In the category of R-modules, the zero module is a zero object.

4. In the category of rings with unity, there is no zero object.

Definition 3.7.22. A category $\mathcal{C}$ is called *pre-additive*, if each homset is an additive abelian group and composition is bilinear with respect to this addition:

$$(g+g')\circ(f+f') = g\circ f + g\circ f' + g'\circ f + g'\circ f'$$

for all morphisms $f, f'\colon A \to B$, $g, g'\colon B \to C$.

Example 3.7.23. *1. The category of groups is not pre-additive (exercise).*

2. The category of R-modules is pre-additive. In particular, for $R = \mathbb{Z}$, the category of abelian groups is pre-additive.

Definition 3.7.24. An *additive category* $\mathcal{C}$ is a pre-additive category with a zero object and a product $A \times B$ for each pair of objects A, B from $\mathcal{C}$.

One can show that this product is also a coproduct for finitely many objects, i.e., product and coproduct are isomorphic.

Example 3.7.25. *The category $\mathcal{Mod}_R$ ist additive with product and coproduct $A_1 \oplus A_2$.*

Here is a table with some examples and non-examples. For the definition of an abelian category see below.

$\mathcal{C}$	Additive	Abelian
$\mathcal{Set}$	–	–
$\mathcal{Ring}$	–	–
$\mathcal{Alg}_R$	–	–
$\mathcal{Hilb}$	✓	–
$\mathcal{Sh}(X)$	✓	✓
$\mathcal{Mod}_R$	✓	✓
$\mathcal{Grp}$	–	–
$\mathcal{Ab}$	✓	✓
$\mathcal{Ab}_d$	✓	–
$\mathcal{Ab}_f$	✓	–
$\mathcal{Cyc}$	–	–
$\mathcal{Ab}_{tf}$	✓	–
$\mathcal{Ab}_{fg}$	✓	✓
$\mathcal{Ab}_{ffg}$	✓	–
$\mathcal{grp}$	–	–
$\mathcal{ab}$	✓	✓
$\mathcal{Ab}_t$	✓	✓
$\mathcal{Ab}_p$	✓	✓

Definition 3.7.26. A morphism $i\colon A \to B$ in an additive category $\mathcal{C}$ is called *monic*, if, whenever $g\colon A' \to A$ is a morphism satisfying $i \circ g = 0$, then $g = 0$.

Monics can be cancelled from the left In $\mathcal{Set}$, $\mathcal{Grp}$ and $\mathcal{Mod}_R$, monics are just injective maps.

Definition 3.7.27. A morphism $e\colon C \to D$ in an additive category $\mathcal{C}$ is called *epi*, if, whenever $h\colon D \to D'$ is a morphism satisfying $h \circ e = 0$, then $h = 0$.

Epis can be cancelled from the right. In $\mathcal{Set}$, $\mathcal{Grp}$ and $\mathcal{Mod}_R$, epis are just surjective maps. We define the kernel and the cokernel of a morphism as follows:

Definition 3.7.28. 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 3.7.29. 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).

Example 3.7.30. *1. In $\mathscr{Grp}$, the usual definition of a kernel, with the inclusion map into A satisfies the above universal property. So kernels always exist in $\mathscr{Grp}$. A cokernel of a morphism $f\colon G \to H$ in $\mathscr{Grp}$ is the quotient of H by the normal closure of the image of f. So cokernels always exist.*

2. In $\mathscr{Ring}$, there is no zero object, so the kernel and the cokernel do not exist.

3. In $\mathscr{Mod}_R$, kernels and cokernels always exist.

Definition 3.7.31. An *abelian category* is an additive category $\mathcal{C}$ satisfying the following three conditions:

(AB1) Every morphism in $\mathcal{C}$ has a kernel and a cokernel.

(AB2) Every monic morphism in $\mathcal{C}$ is the kernel of its cokernel, i.e.,

$$i = \ker(\operatorname{coker}(i)).$$

(AB3) Every epic morphism in $\mathcal{C}$ is the cokernel of its kernel, i.e.,

$$e = \operatorname{coker}(\ker(e)).$$

The notion of abelian category is self-dual, i.e., the opposite category of any abelian category is abelian.

EXAMPLE 3.7.32. *1. $\mathcal{Mod}_R$ is an abelian category. In particular, $\mathcal{Ab}_R$ is an abelian category.*

2. The category $\mathcal{Ab}_f$ of free abelian groups is additive, but not abelian (exercise). In fact, not every monic morphism is the kernel of its cokernel.

REMARK 3.7.33. Not every abelian category is a concrete category such as $\mathcal{Mod}_R$ or $\mathcal{Ab}$. But for many proofs in homological algebra it is very convenient to have a concrete abelian category, for that allows one to check the behaviour of morphisms on actual elements of the sets underlying the objects. However, under good conditions an abelian category can be embedded into $\mathcal{Ab}$ as a full subcategory by an exact functor, and generally can be embedded this way into $\mathcal{Mod}_R$, for some ring R. This is the *Freyd-Mitchell embedding theorem.*

DEFINITION 3.7.34. Let $\mathcal{C}$ be an additive category. A sequence $0 \to A \to B \xrightarrow{\alpha} C$ is called *left-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 *right-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.

DEFINITION 3.7.35. A covariant functor $F\colon \mathcal{C} \to \mathcal{D}$ of additive categories is called *exact*, if it takes short exact sequences in $\mathcal{C}$ to short exact sequences in $\mathcal{D}$. That means, given a short exact sequence

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

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

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

in $\mathcal{D}$.
The functor is called *left-exact*, if

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

is exact. It is called *right-exact*, if

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

is exact.

The definition for contravariant functors is analogous. One has to reverse the arrows in $\mathcal{D}$. 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 3.7.36. *The contravariant functor* $\operatorname{Hom}_R(\cdot, V)$ *from* $\mathcal{M}od_R$ *to* $\mathcal{A}b$ *is left-exact, as well as the covariant functor* $\operatorname{Hom}_R(V, \cdot)$.

Proof. We only show that $\operatorname{Hom}_R(V, \cdot)$ 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

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

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 3.7.37. Let R be a commutative ring. The covariant functors $F = M \otimes_R \cdot$ and $G = \cdot \otimes_R N$ are right-exact, but not exact in general.

3.8. Functorial definition of cohomology groups

Let us first mention the definition of adjoint functors for later.

Definition 3.8.1. 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

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

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:

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

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

For the definition of homology and cohomology of groups we are not using the category of groups. Rather we use the category $\mathcal{M}od_R$ for the *group ring* $R = \mathbb{Z}[G]$.

Definition 3.8.2. Let G be a group. Denote by $\mathcal{M}_G$ the category of G-modules, i.e., of $\mathbb{Z}[G]$-modules. This is an abelian category.

For the trivial group $G = 1$ we obtain the category $\mathcal{A}b$ of $\mathbb{Z}$-modules. We recall the following result:

Proposition 3.8.3. *Let* $0 \to I \xrightarrow{\alpha} N \xrightarrow{\beta} M \to 0$ *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 $\sigma\alpha = \mathrm{id}_{|I}$.*

In this case, N is isomorphic to the direct sum of I and M, with

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

Definition 3.8.4. Let $\mathcal{C}$ be an abelian category. An object I of $\mathcal{C}$ 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 $\mathcal{C}$ 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 3.8.5. *Let I be an R-module in the category $\mathcal{Mod}_R$. 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 3.8.3 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 [**21**],

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

where $N = I \oplus_{M'} M$. Since α is a monomorphism, so is α'. By (2) the sequence $0 \to I \stackrel{\alpha}{\to} N$ 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 3.8.6. Let $\mathcal{C}$ be an abelian category. We say that $\mathcal{C}$ has *enough injectives* if for every object A in $\mathcal{C}$ there is an injection $A \to I$ where I is injective.

We have the following important theorem.

Theorem 3.8.7. *Every R-module can be embedded into an injective R-module. Hence the category $\mathcal{M}od_R$, respectively $\mathcal{M}_G$, has enough injectives.*

Proof. Here is a very rough outline of the proof. For details see [**21**]. 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 $\operatorname{Hom}_{\mathbb{Z}}(R, T)$ 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 $\operatorname{Hom}_{\mathbb{Z}}(R, T)$. □

Let $\mathcal{C}$ be an abelian category. Then $\mathcal{C}^{op}$ is also abelian and injective objects in $\mathcal{C}$ correspond to so called projective objects in $\mathcal{C}^{op}$. We have the following dual definition.

Definition 3.8.8. Let $\mathcal{C}$ be an abelian category. An object P of $\mathcal{C}$ is *projective* if $\operatorname{Hom}(P, \cdot)$ is an exact functor, i.e., if $0 \to A \to B \to C \to 0$ is exact in $\mathcal{C}$ then also

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

is exact.

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

Example 3.8.9. *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. Also, every short exact sequence splits.

Example 3.8.10. *The category of finite abelian groups $\mathcal{ab}$ is an example of an abelian category that has no (nonzero) projective objects. Since $\mathcal{ab}$ is equivalent to $\mathcal{ab}^{op}$ it has also no (nonzero) injective objects.*

Proposition 3.8.11. *Let P be an R-module in the category $\mathcal{M}od_R$. Then the following conditions are equivalent:*

(1) *P is projective, i.e., the functor $\operatorname{Hom}_R(P, \cdot)$ 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 3.8.12. Let $\mathcal{C}$ be an abelian category. We say that $\mathcal{C}$ has *enough projectives* if for every object A in $\mathcal{C}$ there is a surjection $P \to A$ where P is projective.

Proposition 3.8.13. *The category $\mathcal{M}od_R$ 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 3.8.14. Let M be an object of a category $\mathcal{C}$. 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 $\mathcal{C}$, then it is called an *injective resolution.*

Proposition 3.8.15. *If the abelian category $\mathcal{C}$ has enough injectives, then every object in $\mathcal{C}$ 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 3.8.16. The above functors R^rF are called the *right derived functors* of F.

Example 3.8.17. *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 3.8.18. *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 3.8.19. *The functor $F\colon \mathcal{M}_G \to \mathcal{A}b$, $F(M) = M^G$ 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 (3.3.2). 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 3.8.20. 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

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

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 4

Cohomology of Lie algebras

Lie algebra cohomology was first defined in [**7**] by an explicit formula for the coboundary operator. For a textbook reference see also the books of A. Knapp [**19**] and Weibel [**29**]. As in the group case, there is the general definition, which defines Lie algebra cohomology as right derived functor of the left exact invariant funtor $M \to M^{\mathfrak{g}}$. Here M is a $\mathfrak{g}$-module and $M^{\mathfrak{g}}$ is the module of invariants, see below.

4.1. The n-th cohomology group

Given a Lie algebra $\mathfrak{g}$ we define a $\mathfrak{g}$-*module* to be a vector space V equipped with a bilinear function $\mathfrak{g} \times V \to V$, often written $(x, v) \mapsto x \cdot v$, satisfying the relation

$$[x, y] \cdot v = x \cdot (y \cdot v) - y \cdot (x \cdot v)$$

A $\mathfrak{g}$-module V is just the same as a representation $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$. Indeed, given a representation φ we can define $x \cdot v = [\varphi(x)](v)$. Given an action we can define a representation $\varphi(x) \in \mathfrak{gl}(V)$ by $[\varphi(x)](v) = x \cdot v$. The above relation is exactly the statement that the bracket in $\mathfrak{g}$ corresponds to the bracket in $\mathfrak{gl}(V)$.

Modules of a Lie algebra form a category. A homomorphism of $\mathfrak{g}$-modules is a linear map $\psi : V \to W$ satisfying

$$\psi(x \cdot v) = x \cdot \varphi(v).$$

Definition 4.1.1. Let M be a $\mathfrak{g}$-Modul. Then

$$\begin{aligned} M^{\mathfrak{g}} &= \{m \in M \mid x \bullet m = 0 \, \forall \, x \in \mathfrak{g}\} \\ &= H^0(\mathfrak{g}, M) \end{aligned}$$

is called the *module of invariants* of M, or $H^0(\mathfrak{g}, M)$, the zeroth cohomology group of $\mathfrak{g}$ with coefficients in M.

Let V and W be vector spaces. A multilinear map $f\colon V^p \to W$ is called *alternating* if $f(v_1, \dots v_p) = 0$ as soon as $v_i = v_j$ for an index pair (i, j) with $i < j$. For $\sigma \in S_p$ we have

$$f(v_{\sigma_1}, \dots, v_{\sigma_p}) = \operatorname{sgn}(\sigma) \cdot f(v_1, \dots, v_p)$$

Let $\operatorname{Alt}(V^n, W)$ denote the vector space of all alternating maps $f\colon V^n \to W$. We have

$$\operatorname{Hom}(\Lambda^n(V), W) \cong \operatorname{Alt}(V^n, W).$$

Definition 4.1.2. Let $\mathfrak{g}$ be a Lie algebra of dimension n over a field K. Let M be a $\mathfrak{g}$-module with the action $\mathfrak{g} \times M \to M$, $(x, m) \mapsto x \bullet m$. The the space of *p-cochains* is defined by

$$C^p(\mathfrak{g}, M) = \begin{cases} \operatorname{Hom}_K(\Lambda^p \mathfrak{g}, M) & \text{if } p > 0, \\ 0 & \text{if } p < 0. \end{cases}$$

Moreover we define

$$\begin{aligned} C^0(\mathfrak{g}, M) &= M, \\ C(\mathfrak{g}, M) &= \bigoplus_{k=0}^{\infty} C^k(\mathfrak{g}, M). \end{aligned}$$

We also may view the space of p-cochains as $\operatorname{Alt}(\mathfrak{g}^p, M)$.

Definition 4.1.3. The *coboundary operators* $d_p : C^p(\mathfrak{g}, M) \to C^{p+1}(\mathfrak{g}, M)$ are linear maps given by

$$\begin{aligned} (d_p\omega)(x_0 \wedge \cdots \wedge x_p) = &\sum_{0 \le r < s \le p} (-1)^{r+s} \omega([x_r, x_s] \wedge x_0 \wedge \cdots \wedge \widehat{x_r} \wedge \cdots \wedge \widehat{x_s} \wedge \cdots \wedge x_p) \\ &+ \sum_{t=0}^{p} (-1)^t x_t \bullet \omega(x_0 \wedge \cdots \wedge \widehat{x_t} \wedge \cdots \wedge x_p), \end{aligned}$$

for $p \ge 0$ and $\omega \in C^p(\mathfrak{g}, M)$. For $p < 0$ we set $d_p = 0$. The maps d_p also induce a linear map

$$d \colon C(\mathfrak{g}, M) \to C(\mathfrak{g}, M).$$

Note that $d_p(\omega)$ is indeed an element of $C^{p+1}(\mathfrak{g}, M)$.

Definition 4.1.4. The elements of the subspace $Z^p(\mathfrak{g}, M) = \ker d_p$ are called *p-cocycles*, and the elements of the subspace $B^p(\mathfrak{g}, M) = \operatorname{im} d_{p-1}$ are called *p-coboundaries*.

We will show later that $d_p \circ d_{p-1} = 0$, i.e., that we have $B^p(\mathfrak{g}, M) \subseteq Z^p(\mathfrak{g}, M)$. Hence the following definition makes sense.

Definition 4.1.5. The quotient space

$$H^p(\mathfrak{g}, M) = Z^p(\mathfrak{g}, M)/B^p(\mathfrak{g}, M)$$

is called the *p-th cohomology group* of $\mathfrak{g}$ with coefficients in the $\mathfrak{g}$-module M.

Remark 4.1.6. The sequence

$$0 \to C^0(\mathfrak{g}, M) \xrightarrow{d_0} C^1(\mathfrak{g}, M) \xrightarrow{d_1} C^2(\mathfrak{g}, M) \to \cdots$$

forms a complex since $d^2 = 0$. It is called the *standard cochain complex* and is denoted by $\{C^\bullet(\mathfrak{g}, M), d\}$, see [**19**].

Let us state the coboundary formulas explicitly for $n = 0, 1, 2, 3$, in terms of alternating maps:

$$\begin{aligned}(d_0\omega)(x_0) &= x_0 \bullet \omega \\ (d_1\omega)(x_0,x_1) &= x_0 \bullet \omega(x_1) - x_1 \bullet \omega(x_0) - \omega([x_0,x_1]) \\ (d_2\omega)(x_0,x_1,x_2) &= x_0 \bullet \omega(x_1,x_2) - x_1 \bullet \omega(x_0,x_2) + x_2 \bullet \omega(x_0,x_1) \\ &\quad - \omega([x_0,x_1],x_2) + \omega([x_0,x_2],x_1) - \omega([x_1,x_2],x_0) \\ (d_3\omega)(x_0,x_1,x_2,x_3) &= x_0 \bullet \omega(x_1,x_2,x_3) - x_1 \bullet \omega(x_0,x_2,x_3) \\ &\quad + x_2 \bullet \omega(x_0,x_1,x_3) - x_3 \bullet \omega(x_0,x_1,x_2) \\ &\quad - \omega([x_0,x_1],x_2,x_3) + \omega([x_0,x_2],x_1,x_3) \\ &\quad - \omega([x_0,x_3],x_1,x_2) - \omega([x_1,x_2],x_0,x_3) \\ &\quad + \omega([x_1,x_3],x_0,x_2) - \omega([x_2,x_3],x_0,x_1)\end{aligned}$$

We can write down the definition of $H^n(\mathfrak{g},M)$ then in explicit terms. Let us do this for $n=0,1,2$.

Case 1: $n=0$. We have $B^0(\mathfrak{g},M)=0$. Hence

$$\begin{aligned}H^0(\mathfrak{g},M) = Z^0(\mathfrak{g},M) &= \{m \in M \mid x \bullet m = 0 \;\forall x \in \mathfrak{g}\} \\ &= M^{\mathfrak{g}}\end{aligned}$$

is indeed the module of invariants, as said earlier.

Case 2: $n=1$. The space of 1-cocycles and 1-coboundaries is given by

$$\begin{aligned}Z^1(\mathfrak{g},M) &= \{\omega \in \operatorname{Hom}(\mathfrak{g},M) \mid \omega([x,y]) = x \bullet \omega(y) - y \bullet \omega(x)\} \\ B^1(\mathfrak{g},M) &= \{\omega \in \operatorname{Hom}(\mathfrak{g},M) \mid \omega(x) = x \bullet m \text{ für ein } m \in M\}\end{aligned}$$

Suppose that M is the trivial $\mathfrak{g}$-module K. Then $d_0 = 0$ and $(d_1\omega)(x,y) = \omega([y,x])$. This yields

$$\begin{aligned}H^1(\mathfrak{g},K) &= \{\omega \in \mathfrak{g}^* \mid \omega([\mathfrak{g},\mathfrak{g}]) = 0\} \\ &\cong (\mathfrak{g}/[\mathfrak{g},\mathfrak{g}])^*\end{aligned}$$

More generally, for a trivial $\mathfrak{g}$-module M, we have

$$H^1(\mathfrak{g},M) \cong \operatorname{Hom}(\mathfrak{g}/[\mathfrak{g},\mathfrak{g}]),M).$$

In case that $M=\mathfrak{g}$ is the *adjoint* $\mathfrak{g}$-module we have $H^1(\mathfrak{g},\mathfrak{g}) = \operatorname{Der}(\mathfrak{g})/\operatorname{ad}(\mathfrak{g})$. This equals the space of *outer* derivations of $\mathfrak{g}$. The space of *inner* derivations of $\mathfrak{g}$ is given by $\operatorname{ad}(\mathfrak{g}) = \{\operatorname{ad} x \mid x \in \mathfrak{g}\}$.

Case 3: $n=2$. The space of 2-cocycles and 2-coboundaries is given by

$$\begin{aligned}Z^2(\mathfrak{g},M) = \{\omega \in \operatorname{Alt}(\mathfrak{g}^2,M) \mid\, & x_1 \bullet \omega(x_2,x_3) - x_2 \bullet \omega(x_1,x_3) + x_3 \bullet \omega(x_1,x_2) \\ & - \omega([x_1,x_2],x_3) + \omega([x_1,x_3],x_2) - \omega([x_2,x_3],x_1) = 0\} \\ B^2(\mathfrak{g},M) = \{\omega \in \operatorname{Alt}(\mathfrak{g}^2,M) \mid\, & \omega(x_1,x_2) = x_1 \bullet f(x_2) - x_2 \bullet f(x_1) - f([x_1,x_2]) \\ & \text{for some } f \in \operatorname{Hom}(\mathfrak{g},M)\}.\end{aligned}$$

For $M = K$ the trivial $\mathfrak{g}$-module we obtain

$$\begin{aligned} Z^2(\mathfrak{g}, K) &= \{\omega \in \mathrm{Alt}(\mathfrak{g}^2, K) \mid \omega([x_1, x_2], x_3) - \omega([x_1, x_3], x_2) \\ &\qquad + \omega([x_2, x_3], x_1) = 0\} \\ B^2(\mathfrak{g}, K) &= \{\omega \in \mathrm{Alt}(\mathfrak{g}^2, K) \mid \omega(x_1, x_2) = f([x_1, x_2]) \\ &\qquad \text{for some } f \in \mathrm{Hom}(\mathfrak{g}, K)\}. \end{aligned}$$

Definition 4.1.7. Let $i(x)\colon C^p(\mathfrak{g}, M) \to C^{p-1}(\mathfrak{g}, M)$ be the linear map, which is defined for $x \in \mathfrak{g}$ by

$$(i(x)\omega)(x_1, \ldots, x_{p-1}) = \omega(x, x_1, \ldots, x_{p-1}).$$

This map is called the *insertion map*. We define $i(x)$ as zero on $C^0(\mathfrak{g}, M)$.

Definition 4.1.8. Let $\rho\colon \mathfrak{g} \to \mathfrak{gl}(C^p(\mathfrak{g}, M))$, $x \mapsto \rho(x)$ be the linear map, which is defined for $x \in \mathfrak{g}$ by

$$\begin{aligned} (\rho(x)\omega)(x_1, \ldots, x_p) &= -\sum_{i=1}^{p} \omega(x_1, \ldots, [x, x_i], \ldots, x_p) \\ &\quad + x \bullet \omega(x_1, \ldots, x_p) \\ &= \sum_{i=1}^{p} (-1)^i \omega([x, x_i], x_1, \ldots, \widehat{x_i}, \ldots, x_p) \\ &\quad + x \bullet \omega(x_1, \ldots, x_p) \end{aligned}$$

These two maps satisfy the so-called *Cartan formula*:

Proposition 4.1.9. *The map $\rho\colon \mathfrak{g} \to \mathfrak{gl}(C(\mathfrak{g}, M))$ is a Lie algebra representation, which satifies the Cartan formula*

$$\rho(x) = d_{p-1} \circ i(x) + i(x) \circ d_p. \tag{4.1}$$

Remark 4.1.10. It is sometimes convenient to drop the indices for the maps d_p. So we just write $\rho(x) = d \circ i(x) + i(x) \circ d$.

Proof. We first show that ρ is a representation, i.e., that we have

$$\rho([x, y]) = [\rho(x), \rho(y)].$$

For this we compute

$$\begin{aligned} \rho(x)\rho(y)\omega(x_1, \ldots, x_p) &= x \bullet (y \bullet \omega(x_1, \ldots, x_p)) \\ &\quad - \sum_{i=1}^{p} y \bullet \omega(x_1, \ldots, [x, x_i], \ldots, x_p) \\ &\quad - \sum_{i=1}^{p} x \bullet \omega(x_1, \ldots, [y, x_i], \ldots, x_p) \\ &\quad + \sum_{i,j=1,\, i \neq j}^{p} \omega(x_1, \ldots, [y, x_i], \ldots, [x, x_j], \ldots, x_p) \\ &\quad + \sum_{i=1}^{p} \omega(x_1, \ldots, [y, [x, x_i]], \ldots, x_p) \end{aligned}$$

This implies, together with the Jacobi identity,

$$\begin{aligned}[\rho(x),\rho(y)]\omega(x_1,\dots,x_p) &= [x,y]\bullet\omega(x_1,\dots,x_p)\\ &\quad -\sum_{i=1}^{p}\omega(x_1,\dots,[[x,y],x_i],\dots,x_p)\\ &= \rho([x,y])\omega(x_1,\dots,x_p).\end{aligned}$$

Secondly, we show the Cartan formula. For this we rewrite the formula for the coboundary operator using the map $i(x_0)$ as follows:

$$\begin{aligned}d(i(x_0)\omega)(x_1,\dots,x_p) &= \sum_{\ell=0}^{p-1} x_\ell\bullet(i(x_0)\omega)(x_1,\dots,\widehat{x_\ell},\dots,x_p)\\ &\quad+\sum_{0\le\ell<k\le p-1}(-1)^{\ell+k}(i(x_0)\omega)([x_\ell,x_k],x_1,\dots,\widehat{x_\ell},\dots,\widehat{x_k},\dots,x_p).\end{aligned}$$

With $\omega(x_0,[x_i,x_j],\dots,x_p)=-\omega([x_i,x_j],x_0,\dots x_p)$ we obtain

$$\begin{aligned}(i(x_0)d\omega)(x_1,\dots,x_p) &= (d\omega)(x_0,x_1,\dots,x_p)\\ &= (-1)^0 x_0\bullet\omega(x_1,\dots,x_p)\\ &\quad+\sum_{j=1}^{p}(-1)^j x_j\bullet\omega(x_0,\dots,\widehat{x_j},\dots,x_p)\\ &\quad+(-1)^{0+j}\omega([x_0,x_j],x_1,\dots,\widehat{x_j},\dots,x_p)\\ &\quad+\sum_{1\le i<j\le p}(-1)^{i+j}\omega([x_i,x_j],x_0,\dots,\widehat{x_i},\dots,\widehat{x_j},\dots,x_p)\\ &= (\rho(x_0)\omega)(x_1,\dots,x_p)\\ &\quad-\sum_{j=1}^{p}(-1)^{j-1}x_j\bullet(i(x_0)\omega)(x_0,\dots,\widehat{x_j},\dots,x_p)\\ &\quad-\sum_{1\le i<j\le p}(-1)^{i+j}(i(x_0)\omega)([x_i,x_j],x_1,\dots,\widehat{x_i},\dots,\widehat{x_j},\dots,x_p)\\ &= (\rho(x_0)\omega)(x_1,\dots,x_p)-d(i(x_0)\omega)(x_1,\dots,x_p),\end{aligned}$$

and this finishes the proof. □

Proposition 4.1.11. *We have the following formulas, for all $x,y\in\mathfrak{g}$:*

$$i([x,y])=[i(x),\rho(y)] \tag{4.2}$$

$$[\rho(x),d]=0 \tag{4.3}$$

Proof. We first show (4.2). We have

$$\begin{aligned}(i(x_1)\rho(y)\omega)(x_2,\dots,x_p) &= (\rho(y)\omega)(x_1,\dots,x_p)\\ &= y\bullet\omega(x_1,\dots,x_p)-\sum_{j=1}^{p}\omega(x_1,\dots,[y,x_j],\dots,x_p).\end{aligned}$$

On the other hand we have

$$\begin{aligned}\rho(y)(i(x_1)\omega)(x_2,\dots,x_p) &= y\bullet(i(x_1)\omega)(x_2,\dots,x_p)\\ &\quad -\sum_{j=2}^{p}(i(x_1)\omega)(x_2,\dots,[y,x_j],\dots,x_p)\\ &= y\bullet\omega(x_1,\dots,x_p)-\sum_{j=2}^{p}\omega(x_1,x_2,\dots,[y,x_j],\dots,x_p).\end{aligned}$$

The difference of these two terms, i.e., $i(x_1)\rho(y)\omega-\rho(y)i(x_1)\omega$, corresponds to the RHS of (4.2): it is equal to the summand for $j=1$ in the first sum, namely to

$$-\omega([y,x_1],x_2,\dots,x_p)=(i([x_1,y])\omega)(x_2,\dots,x_p).$$

Hence we have $i(x)\rho(y)-\rho(y)i(x)=i([x,y])$.

Secondly we show (4.3). Here we compute with (4.1) and (4.2):

$$\begin{aligned}[\rho(x),\rho(y)] &= [d\circ i(x)+i(x)\circ d,\rho(y)]\\ &= d\circ i(x)\circ\rho(y)+i(x)\circ d\circ\rho(y)-\rho(y)\circ d\circ i(x)-\rho(y)\circ i(x)\circ d\\ &= d\circ\rho(y)\circ i(x)+i(x)\circ d\circ\rho(y)+d\circ i(x)\circ\rho(y)+i(x)\circ\rho(y)\circ d\\ &-\rho(y)\circ d\circ i(x)-i(x)\circ\rho(y)\circ d-d\circ\rho(y)\circ i(x)-\rho(y)\circ i(x)\circ d\\ &= [d,\rho(y)]\circ i(x)+i(x)\circ[d,\rho(y)]+d\circ[i(x),\rho(y)]+[i(x),\rho(y)]\circ d\\ &= [d,\rho(y)]\circ i(x)+i(x)\circ[d,\rho(y)]+d\circ i([x,y])+i([x,y])\circ d\\ &= [d,\rho(y)]\circ i(x)+i(x)\circ[d,\rho(y)]+\rho([x,y])\end{aligned}$$

Since ρ is a representation, this implies

$$[d,\rho(y)]\circ i(x)+i(x)\circ[d,\rho(y)]=0. \tag{4.4}$$

Now we can use induction on the degree k of $C^k(\mathfrak{g},M)$, to show that we have $[d,\rho(y)]=0$.

Case 1: $k=0$. For $\omega\in C^0(\mathfrak{g},M)=M$ we have

$$\begin{aligned}([d,\rho(y)]\omega)(x) &= (d\rho(y)\omega)(x)-(\rho(y)d\omega)(x)\\ &= d(y\bullet\omega)(x)-(y\bullet(d\omega))(x)\\ &= x\bullet(y\bullet\omega)-y\bullet(x\bullet\omega)-d\omega([y,x])\\ &= [x,y]\bullet\omega+[y,x]\bullet\omega\\ &= 0\end{aligned}$$

Case 2: $k\mapsto k+1$: we have $[d,\rho(y)]C^k(\mathfrak{g},M)=0$ by induction hypothesis. Using (4.4) we have

$$\begin{aligned}i(x)\circ[d,\rho(y)]C^{k+1}(\mathfrak{g},M) &= -[d,\rho(y)]i(x)C^{k+1}(\mathfrak{g},M)\\ &\subseteq [d,\rho(y)]C^k(\mathfrak{g},M)\\ &= \{0\}\end{aligned}$$

for all $x\in\mathfrak{g}$. This implies $[d,\rho(y)]C^{k+1}(\mathfrak{g},M)=0$. □

Now we can finally prove the following result, which we have used for Definition 4.1.5.

Proposition 4.1.12. *The coboundary operator d_p satisfies $d_p \circ d_{p-1} = 0$ for all $p \geq 1$, i.e., we have $d^2 = 0$.*

Proof. By (4.1) and (4.3) we have

$$\begin{aligned} 0 &= [\rho(x), d] \\ &= [d \circ i(x), d] + [i(x) \circ d, d] \\ &= d^2 \circ i(x) - i(x) \circ d^2. \end{aligned}$$

With this formula we will show that $d^2 = 0$.

Case 1: $k = 0$. For $\omega \in C^0(\mathfrak{g}, M) = M$ we have $(d\omega)(x) = x \bullet \omega$. Thus we have

$$\begin{aligned} (d^2\omega)(x, y) &= x \bullet d\omega(y) - y \bullet d\omega(x) - d\omega([x, y]) \\ &= x \bullet (y \bullet \omega) - y \bullet (x \bullet \omega) - [x, y] \bullet \omega \\ &= 0. \end{aligned}$$

Case 2: $k \mapsto k+1$: Suppose that $d^2(C^k(\mathfrak{g}, M)) = \{0\}$. Then

$$\begin{aligned} i(x) \circ d^2(C^{k+1}(\mathfrak{g}, M)) &= d^2 \circ i(x)(C^{k+1}(\mathfrak{g}, M)) \\ &\subseteq d^2(C^k(\mathfrak{g}, M)) = \{0\}, \end{aligned}$$

so that $d^2(C^{k+1}(\mathfrak{g}, M)) = \{0\}$. □

The Lie algebra $\mathfrak{g}$ acts on the graded vector space $C(\mathfrak{g}, M)$ by $x \bullet \omega = \rho(x)\omega$. The coboundary operatorr d commutes with this action, as we have seen in (4.3). Hence the spaces $Z^p(\mathfrak{g}, M)$ and $B^p(\mathfrak{g}, M)$ are both $\mathfrak{g}$-invariant and we obtain an action on the quotient $H^p(\mathfrak{g}, M)$. This way $H^p(\mathfrak{g}, M)$ becomes a $\mathfrak{g}$-module, which however is trivial:

Lemma 4.1.13. *The action of $\mathfrak{g}$ on $H^p(\mathfrak{g}, M)$ is trivial, i.e., we have*

$$\mathfrak{g} \bullet Z^p(\mathfrak{g}, M) \subseteq B^p(\mathfrak{g}, M).$$

Proof. Let $\omega \in Z^p(\mathfrak{g}, M)$, so that $d_p\omega = 0$. Because of (4.1) we have

$$\begin{aligned} \rho(x)\omega &= i(x) \circ d_p\omega + d_{p-1} \circ i(x)\omega \\ &= d_{p-1} \circ i(x)\omega, \end{aligned}$$

which lies in $B^p(\mathfrak{g}, M)$. Hence the induced action on $H^p(\mathfrak{g}, M)$ is trivial. □

Let M be a trivial $\mathfrak{g}$-Modul. Then it is also possible to equip $H^p(\mathfrak{g}, M)$ with a $\mathrm{Der}(\mathfrak{g})$-module structure. We define a representation $\pi\colon \mathrm{Der}(\mathfrak{g}) \to \mathfrak{gl}(C(\mathfrak{g}, M))$ by endomorphisms $\pi(D) \in \mathrm{End}(C^p(\mathfrak{g}, M))$ for $D \in \mathrm{Der}(\mathfrak{g})$ as follows. For $\omega \in C^p(\mathfrak{g}, M)$ we put $\pi(D)(\omega) = D \bullet \omega$ with

$$(D \bullet \omega)(x_1, \ldots, x_p) = -\sum_{j=1}^{p} \omega(x_1, \ldots, D(x_j), \ldots, x_p) \tag{4.5}$$

Proposition 4.1.14. *We have the following formulas:*

$$[\pi(D), i(x)] = i(D(x)) \tag{4.6}$$

$$[\pi(D), \rho(x)] = \rho(D(x)) \tag{4.7}$$

$$[\pi(D), d] = 0 \tag{4.8}$$

Proof. Let $\omega \in C^{p+1}(\mathfrak{g}, M)$, $D \in \operatorname{Der}(\mathfrak{g})$ and $x \in \mathfrak{g}$. Then we have, using (4.5),

$$\begin{aligned} D(i(x)\omega)(x_1, \dots, x_p) &= -\sum_{j=1}^{p} (i(x)\omega)(x_1, \dots, D(x_j), \dots, x_p) \\ &= -\sum_{j=1}^{p} \omega(x, x_1, \dots, D(x_j), \dots, x_p) \\ &= (\pi(D)(\omega))(x, x_1, \dots, x_p) + \omega(D(x), x_1, \dots, x_p) \end{aligned}$$

This implies $(\pi(D)i(x))(\omega) = (i(x)\pi(D))(\omega) + (i(D(x))(\omega)$, so we have (4.6).

It is easy to see that the relation

$$[D, \operatorname{ad} x] = \operatorname{ad} D(x)$$

on $\mathfrak{g}$ implies (4.7) for the representation ρ on $C(\mathfrak{g}, M)$. Now we can apply the Cartan formula (4.1), as well as (4.6) and (4.7), to conclude the relation

$$i(x)[\pi(D), d] + [\pi(D), d]i(x) = 0 \tag{4.9}$$

We have

$$\begin{aligned} i(D(x))d + di(D(x)) &= \rho(D(x)) \\ &= [\pi(D), i(x)d + di(x)] \\ &= \pi(D)i(x)d - di(x)\pi(D) + \pi(D)di(x) - i(x)d\pi(D) \\ &= (i(D(x))d + i(x)\pi(D)d) + (di(D(x)) - d\pi(D)i(x)) \\ &\quad + \pi(D)di(x) - i(x)d\pi(D) \\ &= i(D(x))d + i(x)[\pi(D), d] + [\pi(D), d]i(x) + di(D(x)) \end{aligned}$$

The relation (4.9) is used, to show (4.8) by induction. For $\omega \in C^0(\mathfrak{g}, M) = M$ we have $d\omega = 0$ and $\pi(D)\omega = D \bullet \omega = 0$, hence also $[\pi(D), d]\omega = 0$. Assuming $[\pi(D), d]C^k(\mathfrak{g}, M) = \{0\}$, it follows by (4.9) then $[\pi(D), d]C^{k+1}(\mathfrak{g}, M) = \{0\}$. □

Hence the action of $\pi(D)$ on $C^p(\mathfrak{g}, M)$ preserves the spaces $Z^p(\mathfrak{g}, M)$ and $B^p(\mathfrak{g}, M)$, since it commutes with d. So we obtain the following result.

Proposition 4.1.15. *Let M be a trivial $\mathfrak{g}$-module. Then the representation $\pi\colon \operatorname{Der}(\mathfrak{g}) \to \mathfrak{gl}(C(\mathfrak{g}, M))$ induces a module action of* $\operatorname{Der}(\mathfrak{g})$ *on $H^p(\mathfrak{g}, M)$.*

4.2. The first cohomology group

In this section we will show that the first cohomology group describes equivalence classes of certain extensions of $\mathfrak{g}$-modules.

Definition 4.2.1. Let V, W be $\mathfrak{g}$-modules. A $\mathfrak{g}$-module U is called an *extension of V by W*, if

$$0 \to W \xrightarrow{\alpha} U \xrightarrow{\beta} V \to 0 \tag{4.10}$$

is a short exact sequence of $\mathfrak{g}$-modules.

Definition 4.2.2. An extension U of V by W is called *trivial*, or *split*, if in (4.10) there exists a $\mathfrak{g}$-module homomorphism $\tau\colon V \to U$ with $\beta \circ \tau = \mathrm{id}_{|V}$.

If the extension (4.10) is split, then the map $V \oplus W \to U$, $(x, a) \mapsto a + \tau(x)$ is a $\mathfrak{g}$-module isomorphism.

Definition 4.2.3. Let U_1, U_2 be extensions of V by W. They are called *equivalent*, if there exists a $\mathfrak{g}$-module homomorphism $\varphi\colon U_1 \to U_2$, such that the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & W \arrow[r, "\alpha"] \arrow[d, "\mathrm{id}"] & U_1 \arrow[r, "\beta"] \arrow[d, "\varphi"] & V \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & W \arrow[r, "\gamma"] & U_2 \arrow[r, "\delta"] & V \arrow[r] & 0
\end{tikzcd}$$

Denote by $\mathrm{Ext}(V, W)$ dthe set of equivalence classes of all $\mathfrak{g}$-module extensions (4.10) of V by W.

Every two equivalent extensions U_1 and U_2 are isomorphic as $\mathfrak{g}$-modules by the five-lemma. The converse is not true in general.

The aim of this section is to show that the equivalence classes of extensions

$$0 \to W \xrightarrow{\alpha} U \xrightarrow{\beta} K \to 0,$$

where K is the 1-dimensional trivial $\mathfrak{g}$-module, are classified by $H^1(\mathfrak{g}, W)$. First we show that every $\omega \in Z^1(\mathfrak{g}, W)$ induces an extension of K by W.

Lemma 4.2.4. *Let W be a $\mathfrak{g}$-module and $\omega \in Z^1(\mathfrak{g}, W)$. Define on $W_\omega := K \times W$ an action of $\mathfrak{g}$ by*

$$x \bullet (t, w) = (0, x.w + t\omega(x)) \tag{4.11}$$

for $x \in \mathfrak{g}, w \in W$ and $t \in K$. Then W_ω becomes a $\mathfrak{g}$-module of dimension $\dim W + 1$.

Proof. We have

$$\begin{aligned}
x \bullet (y \bullet (t, w)) - y \bullet (x \bullet (t, w)) &= x \bullet (0, y.w + t\omega(y)) - y \bullet (0, x.w + t\omega(x)) \\
&= (0, x.(y.w) + tx.\omega(y)) - (0, y.(x.w) + ty.\omega(x)) \\
&= (0, [x, y].w + t(x.\omega(y) - y.\omega(x))) \\
&= (0, [x, y].w + t\omega([x, y]) \\
&= [x, y] \bullet (t, w)
\end{aligned}$$

□

Clearly W_ω is an extension of K by W. So we have the following corollary.

Corollary 4.2.5. $0 \to W \xrightarrow{\alpha} W_\omega \xrightarrow{\beta} K \to 0$ *is a short exact sequence of $\mathfrak{g}$-modules.*

Given two $\mathfrak{g}$-modules A and B, with actions $x.a$ and $x \circ b$ for $x \in \mathfrak{g}, a \in A, b \in B$, we can equip $\mathrm{Hom}(B, A)$ with a $\mathfrak{g}$-module structure by

$$(x \bullet \varphi)(b) = x.\varphi(b) - \varphi(x \circ b) \tag{4.12}$$

for $x \in \mathfrak{g}$ und $\varphi \in \mathrm{Hom}(B, A)$. Then we have the following result.

Theorem 4.2.6. *Let A and B be $\mathfrak{g}$-modules. Then we have the isomorphism*

$$\mathrm{Ext}(B, A) \cong H^1(\mathfrak{g}, \mathrm{Hom}(B, A)). \tag{4.13}$$

In particular we have $\mathrm{Ext}(K, A) \cong H^1(\mathfrak{g}, A)$ for the trivial module $B = K$.

Proof. The last part follows from the first part. Indeed, let

$$0 \to A \to C \overset{\beta}{\to} B \to 0$$

be an extension of B by A. For $B = K$ the $\mathfrak{g}$-modules A and $\mathrm{Hom}(K, A)$ are isomorphic. Hence we have $\mathrm{Ext}(K, A) \cong H^1(\mathfrak{g}, A)$ by (4.13). In other words, $H^1(\mathfrak{g}, A)$ *classifies the equivalence classes of extensions* $0 \to A \to C \to K \to 0$.

Let C be an extension of A by B. We may write C as $B \times A$, together with the action

$$x \bullet (b, a) = (x.b, x.a + \omega(x)(b)), \tag{4.14}$$

for $x \in \mathfrak{g}, a \in A, b \in B$ and $\omega \in \mathrm{Hom}(\mathfrak{g}, \mathrm{Hom}(B, A)) = C^1(\mathfrak{g}, \mathrm{Hom}(B, A))$. To see this, choose a transversal function τ, that is, a linear map $\tau \colon B \to C$ with $\tau \circ \beta = \mathrm{id}_{|B}$ and define

$$\omega_\tau(x)(b) = \omega(x)(b) := x.\tau(b) - \tau(x.b).$$

Then the map

$$\psi \colon B \times A \to C, \quad (b, a) \mapsto \tau(b) + a$$

is a $\mathfrak{g}$-module isomorphism. Note that (4.14) defines a $\mathfrak{g}$-module structure on $B \times A$, if and only if $\omega \in Z^1(\mathfrak{g}, \mathrm{Hom}(B, A))$: on one hand we have

$$[y, x] \bullet (b, a) = ([y, x].b,\ [y, x].a + \omega([y, x])(b)),$$

and on the other hand we have

$$\begin{aligned} y \bullet (x \bullet (b, a)) - x \bullet (y \bullet (b, a)) &= (y.(x.b),\ y.(x.a) + y.\omega(x)(b) + \omega(y)(x.b)) \\ &\quad - (x.(y.b),\ x.(y.a) + x.\omega(y)(b) + \omega(x)(y.b)) \\ &= ([y, x].b,\ [y, x].a + y.\omega(x)(b) + \omega(y)(x.b) \\ &\quad - x.\omega(y)(b) - \omega(x)(y.b)) \\ &= ([y, x].b,\ [y, x].a + (y \cdot \omega(x))(b) - (x \cdot \omega(y))(b)) \end{aligned}$$

So these terms are equal if and only if we have

$$\omega([y, x]) = y.\omega(x) - x.\omega(y),$$

i.e., if $\omega \in Z^1(\mathfrak{g}, \mathrm{Hom}(B, A))$. This gives us a correspondence between extensions of B by A and the space $Z^1(\mathfrak{g}, \mathrm{Hom}(B, A))$.

However, we still have different parametrizations of C as $B \times A$, by choosing different transversal functions τ. For a linear map $\gamma \in \mathrm{Hom}(B, A)$ we have

$$\begin{aligned} \omega_{\tau+\gamma}(x)(b) &= x.((\tau + \gamma)(b)) - (\tau + \gamma)(x.b) \\ &= x.\tau(b) - \tau(x.b) + x.\gamma(b) - \gamma(x.b) \\ &= \omega_\tau(x)(b) + (x.\gamma)(b). \end{aligned}$$

Hence we have $\omega_{\tau+\gamma} = \omega_\tau + d\gamma$, and $\omega_{\tau+\gamma}$ and ω_τ just differ by a 1-coboundary. Hence different choices of τ lead to cohomologous cocycles. Consequently equivalent extensions of B by A correspond to classes $[\omega_\tau]$ in $H^1(\mathfrak{g}, \mathrm{Hom}(B, A))$. This yields the desired bijection between $\mathrm{Ext}(B, A)$ and $H^1(\mathfrak{g}, \mathrm{Hom}(B, A))$. □

We also want to state an important result concerning the first cohomology group of semisimple Lie algebras. It is called the *first Whitehead Lemma*. If we assume Weyl's theorem, which is a standard result in a course on Lie algebras and its representations, then we can give a rather short proof of it.

THEOREM 4.2.7 (First Whitehead Lemma). *Let $\mathfrak{g}$ be a finite-dimensional semisimple Lie algebra over a field K of characteristic zero, and let M be a finite-dimensional $\mathfrak{g}$-module. Then we have $H^1(\mathfrak{g}, M) = 0$.*

PROOF. By Weyl's Theorem, every finite-dimensional $\mathfrak{g}$-module of $\mathfrak{g}$ is semisimple. This says that every submodule has a module complement. Therefore all module extensions are trivial, and by Theorem 4.2.6 we obtain

$$0 = \operatorname{Ext}(B, A) = H^1(\mathfrak{g}, \operatorname{Hom}(B, A))$$

for each pair of finite-dimensional $\mathfrak{g}$-modules A, B. For $B = K$ we obtain $H^1(\mathfrak{g}, A) = 0$ for all finite-dimensional $\mathfrak{g}$-modules A. □

REMARK 4.2.8. There are several different proofs of Whitehead's First Lemma. For a proof using Casimir operators see [**15**]. Conversely Weyl's theorem has a short proof using the First Whitehead Lemma. Note that the First Whitehead Lemma does not hold for characteristic $p > 0$. There are even simple Lie algebras $\mathfrak{g}$ in characteristic p having non-trivial outer derivations, i.e., with $H^1(\mathfrak{g}, \mathfrak{g}) \neq 0$.

We note that the converse of the First Whitehead Lemma is also true.

PROPOSITION 4.2.9. *A finite-dimensional Lie algebra $\mathfrak{g}$ over a field of characteristic zero is semisimple if and only if $H^1(\mathfrak{g}, M) = 0$ for all finite-dimensional $\mathfrak{g}$-modules M.*

The case of the adjoint $\mathfrak{g}$-module $\mathfrak{g}$ is of particular interest. We have

$$H^1(\mathfrak{g}, \mathfrak{g}) = \operatorname{Der}(\mathfrak{g})/\operatorname{ad}(\mathfrak{g}),$$

because we have

$$\begin{aligned} Z^1(\mathfrak{g}, \mathfrak{g}) &= \{D \in \operatorname{End}(\mathfrak{g}) \mid D([x, y]) = [x, D(y)] + [D(x), y]\} = \operatorname{Der}(\mathfrak{g}), \\ B^1(\mathfrak{g}, \mathfrak{g}) &= \{D \in \operatorname{End}(\mathfrak{g}) \mid D = \operatorname{ad}(x)\} = \operatorname{ad}(\mathfrak{g}). \end{aligned}$$

Let us do an explicit computation for some easy examples.

EXAMPLE 4.2.10. *Sei $\mathfrak{g} = \mathfrak{sl}_2(K)$. Then we have*

$$\dim H^1(\mathfrak{g}, \mathfrak{g}) = \begin{cases} 0 & \textit{for char}(K) \neq 2, \\ 4 & \textit{otherwise} \end{cases}$$

Here is the proof. For $\operatorname{char}(K) = 0$ we do not need to do a calculation, because it follows from the First Whitehead Lemma, or even from the fact that semisimple Lie algebras in characteristic zero only have inner derivations, i.e., that $\operatorname{Der}(\mathfrak{g}) = \operatorname{ad}(\mathfrak{g})$. Note that in characteristic 2, the Lie algebra $\mathfrak{sl}_2(K)$ is no longer semisimple, but rather coincides with the Heisenberg Lie algebra $\mathfrak{n}_3(K)$.

Let (e_1, e_2, e_3) be a basis of $\mathfrak{sl}_2(K)$ with

$$\begin{aligned} [e_1, e_2] &= e_3 \\ [e_1, e_3] &= -2e_1 \\ [e_2, e_3] &= 2e_2 \end{aligned}$$

Represent $D \in \operatorname{End}(\mathfrak{g})$ by

$$D = \begin{pmatrix} \alpha_1 & \alpha_4 & \alpha_7 \\ \alpha_2 & \alpha_5 & \alpha_8 \\ \alpha_3 & \alpha_6 & \alpha_9 \end{pmatrix}$$

The condition

$$D(e_3) = D([e_1,e_2]) = [e_1, D(e_2)] + [D(e_1), e_2]$$

means

$$\begin{aligned} \alpha_7 e_1 + \alpha_8 e_2 + \alpha_9 e_3 &= [e_1, \alpha_4 e_1 + \alpha_5 e_2 + \alpha_6 e_3] + [\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3, e_2] \\ &= (\alpha_5 e_3 - 2\alpha_6 e_1) + (\alpha_1 e_3 - 2\alpha_3 e_2). \end{aligned}$$

We obtain the linear equations

$$\begin{aligned} \alpha_7 + 2\alpha_6 &= 0, \\ \alpha_8 + 2\alpha_3 &= 0, \\ \alpha_9 - \alpha_5 - \alpha_1 &= 0. \end{aligned}$$

In the same way the derivation conditions for $D([e_1,e_3])$ and $D([e_2,e_3])$ imply

$$\begin{aligned} 2\alpha_9 &= 0, \\ -4\alpha_2 &= 0, \\ 4\alpha_4 &= 0. \end{aligned}$$

Hence for $2 \neq 0$ every derivation is of the form

$$D = \begin{pmatrix} \alpha_1 & 0 & -2\alpha_6 \\ 0 & -\alpha_1 & -2\alpha_3 \\ \alpha_3 & \alpha_6 & 0 \end{pmatrix} = \alpha_6 \operatorname{ad} e_1 - \alpha_3 \operatorname{ad} e_2 + \frac{1}{2} \operatorname{ad} e_3$$

So we have $Z^1(\mathfrak{g},\mathfrak{g}) = \operatorname{Der}(\mathfrak{g}) = \operatorname{ad}(\mathfrak{g})$ und $H^1(\mathfrak{g},\mathfrak{g}) = 0$.

However, for $2 = 0$ we have

$$D = \begin{pmatrix} \alpha_1 & \alpha_4 & 0 \\ \alpha_2 & \alpha_5 & 0 \\ \alpha_3 & \alpha_6 & \alpha_1 + \alpha_5 \end{pmatrix}$$

Then $\dim Z^1(\mathfrak{g},\mathfrak{g}) = 6$ and $\dim B^1(\mathfrak{g},\mathfrak{g}) = \dim \operatorname{ad}(\mathfrak{g}) = 2$. This says

$$\dim H^1(\mathfrak{g},\mathfrak{g}) = 4.$$

Example 4.2.11. *Let $\mathfrak{g} = \mathfrak{n}_4(K)$ be the filiform nilpotent Lie algebra of dimension 4 over an arbitrary field K. Then we have* $\dim H^1(\mathfrak{g},\mathfrak{g}) = 4$.

Let (e_1, e_2, e_3, e_4) be a basis of $\mathfrak{n}_4(K)$ with

$$\begin{aligned} [e_1,e_2] &= e_3 \\ [e_1,e_3] &= e_4 \end{aligned}$$

Now let

$$D = \begin{pmatrix} \alpha_1 & \cdots & \alpha_{13} \\ \vdots & \ddots & \vdots \\ \alpha_4 & \cdots & \alpha_{16} \end{pmatrix}$$

Evaluating the derivation conditions gives us linear equations. For example,

$$D(e_3) = D([e_1,e_2]) = [e_1, D(e_2)] + [D(e_1), e_2]$$

yields

$$\begin{aligned}\alpha_9 e_1 + \dots \alpha_{12} e_4 &= [e_1, \alpha_5 e_1 + \dots + \alpha_8 e_4] + [\alpha_1 e_1 + \dots + \alpha_4 e_4, e_2] \\ &= (\alpha_6 e_3 + \alpha_7 e_4) - (\alpha_1 e_3),\end{aligned}$$

so that $\alpha_9 = \alpha_{10} = 0$, $\alpha_{11} = \alpha_6 - \alpha_1$ and $\alpha_{12} = \alpha_7$. Altogether we see that D has the form

$$D = \begin{pmatrix} \xi_1 & 0 & 0 & 0 \\ \xi_2 & \xi_5 & 0 & 0 \\ \xi_3 & \xi_6 & \xi_1 + \xi_5 & 0 \\ \xi_4 & \xi_7 & \xi_6 & 2\xi_1 + \xi_5 \end{pmatrix}.$$

The space of such derivations is 7-dimensional with basis $D_1, \dots D_7$. So we have

$$D = \sum_{i=1}^{7} \xi_i D_i.$$

This implies $\dim Z^1(\mathfrak{g}, \mathfrak{g}) = 7$. Moreover we have $\dim B^1(\mathfrak{g}, \mathfrak{g}) = 3$, so that $\dim H^1(\mathfrak{g}, \mathfrak{g}) = 4$. In fact,

$$H^1(\mathfrak{g}, \mathfrak{g}) = \operatorname{span}\{[D_1], [D_2], [D_5], [D_7]\},$$

because $D_6 = \operatorname{ad} e_1$, $D_3 = -\operatorname{ad} e_2$ and $D_4 = -\operatorname{ad} e_3$ are inner derivations.

Note that for characteristic different from 2 and 3 there exist *invertibe* derivations. For example, $D_1 + D_5 = \operatorname{diag}\{1, 1, 2, 3\}$ is an imvertible derivation, or $D_1 + 2D_6 = \operatorname{diag}\{1, 2, 3, 4\}$. In this context Jacobson proved in 1955 the following interesting result [**17**]:

Proposition 4.2.12 (Jacobson). *Let $\mathfrak{g}$ be a finite-dimensional Lie algebra of characteristic zero admitting an invertible derivation $D \in \operatorname{Der}(\mathfrak{g})$. Then $\mathfrak{g}$ is nilpotent.*

We also mention the result by Dixmier [**11**] from 1955:

Proposition 4.2.13 (Dixmier). *Let $\mathfrak{g}$ be a finite-dimensional nilpotent Lie algebra of charakteristic zero. Then there exists an outer derivation $D \in \operatorname{Der}(\mathfrak{g})$. So we have $H^1(\mathfrak{g}, \mathfrak{g}) \neq 0$.*

The following result by Zassenhaus holds for arbitrary characteristic.

Proposition 4.2.14 (Zassenhaus). *Let $\mathfrak{g}$ be a finite-dimensional Lie algebra of arbitrary characteristic, having a non-degenerate Killing form. Then all derivations $D \in \operatorname{Der}(\mathfrak{g})$ are inner and we have $H^1(\mathfrak{g}, \mathfrak{g}) = 0$.*

Proof. Let $f(x, y) = \operatorname{tr}(\operatorname{ad} x \circ \operatorname{ad} y)$ be the Killing form on $\mathfrak{g}$, and let $D \in \operatorname{Der}(\mathfrak{g})$. Consider the linear form $x \mapsto \operatorname{tr}(\operatorname{ad} x \circ D)$ on $\mathfrak{g}$. Since f is non-degenerate, there eixsts a $z \in \mathfrak{g}$ such that $f(x, z) = \operatorname{tr}(\operatorname{ad} x \circ D)$ for all $x \in \mathfrak{g}$. Let $E := D - \operatorname{ad} z \in \operatorname{Der}(\mathfrak{g})$. Then we have

$$\begin{aligned}\operatorname{tr}(\operatorname{ad} x \circ E) &= \operatorname{tr}(\operatorname{ad} x \circ D) - \operatorname{tr}(\operatorname{ad} x \circ \operatorname{ad} z) \\ &= \operatorname{tr}(\operatorname{ad} x \circ D) - f(x, z) \\ &= 0\end{aligned}$$

This implies

$$\begin{aligned} f(E(x),y) &= \operatorname{tr}(\operatorname{ad} E(x) \circ \operatorname{ad} y) \\ &= \operatorname{tr}([\operatorname{ad} x, E] \circ \operatorname{ad} y) \\ &= \operatorname{tr}(\operatorname{ad} x \circ E \circ \operatorname{ad} y - E \circ \operatorname{ad} x \circ \operatorname{ad} y) \\ &= \operatorname{tr}(E \circ \operatorname{ad} y \circ \operatorname{ad} x - E \circ \operatorname{ad} x \circ \operatorname{ad} y) \\ &= \operatorname{tr}(E \circ [\operatorname{ad} y, \operatorname{ad} x]) \\ &= \operatorname{tr}(E \circ \operatorname{ad}[y,x]) \\ &= 0 \end{aligned}$$

since $\operatorname{tr}(E \circ \operatorname{ad} w) = 0$ for all $w \in \mathfrak{g}$, see above. Since f is non-degenerate, we obtain $E = 0$ and thus $D = \operatorname{ad} z$. □

4.3. The second cohomology group

The main result of this section is the interpretation of the second cohomology group as the set of equivalence classes of abelian extensions of Lie algebras.

Definition 4.3.1. Let $\mathfrak{q}$ and $\mathfrak{n}$ be two Lie algebras. A short exact sequence

$$0 \to \mathfrak{n} \xrightarrow{\alpha} \mathfrak{g} \xrightarrow{\beta} \mathfrak{q} \to 0 \tag{4.15}$$

is called an *extension of* $\mathfrak{q}$ *by* $\mathfrak{n}$.

Identifying $\mathfrak{n}$ with $\alpha(\mathfrak{n})$ we see that $\mathfrak{g}$ contains $\mathfrak{n}$ as an ideal with quotient $\mathfrak{g}/\mathfrak{n} \cong \mathfrak{q}$.

Definition 4.3.2. An extension (4.15) is called *split*, if there exists a Lie algebra homomorphism $\tau\colon \mathfrak{q} \to \mathfrak{g}$ with $\beta \circ \tau = \mathrm{id}_{|\mathfrak{q}}$.

Definition 4.3.3. Let $\mathfrak{a}$ and $\mathfrak{b}$ two Lie algebras, together with a Lie algebra homomorphism $\varphi\colon \mathfrak{a} \to \operatorname{Der}(\mathfrak{b})$. Let $\mathfrak{g} = \mathfrak{a} \ltimes_\varphi \mathfrak{b}$ be the direct vector space sum $\mathfrak{a} \oplus \mathfrak{b}$, equipped with the following Lie bracket

$$[(x,a),(y,b)] = ([x,y],[a,b] + \varphi(x)(b) - \varphi(y)(a))), \tag{4.16}$$

for all $x, y \in \mathfrak{a}$ and $a, b \in \mathfrak{b}$. Then $\mathfrak{g}$ is a Lie algebra, which is called the *semidirect product*, or the semidirect sum of $\mathfrak{a}$ and $\mathfrak{b}$.

We have the following result.

Proposition 4.3.4. *Every semidirect product* $\mathfrak{g} = \mathfrak{q} \ltimes_\varphi \mathfrak{n}$ *defines a split short exact sequence* (4.15) *with respect to* τ*, such that* $\varphi(x)(n) = [\tau(x), n]$ *for* $x \in \mathfrak{q}, n \in \mathfrak{n}$*. Conversely, every split short exact sequence* (4.15) *together with a Lie algebra homomorphims* $\tau\colon \mathfrak{q} \to \mathfrak{g}$ *defines a semidirect product* $\mathfrak{q} \ltimes_\varphi \mathfrak{n}$ *by*

$$\varphi\colon \mathfrak{q} \to \operatorname{Der}(\mathfrak{n}) \tag{4.17}$$

$$\varphi(x)(n) = [\tau(x), n], \tag{4.18}$$

which is isomorphic as a Lie algebra to $\mathfrak{g}$.

Proof. The proof is analogous to the group case. We only show here that the map

$$\psi\colon \mathfrak{q} \ltimes_\varphi \mathfrak{n} \to \mathfrak{g}, \quad (x,a) \mapsto \tau(x) + a \tag{4.19}$$

is a Lie algebra isomorphism. First, let us indetify $a \in \mathfrak{n}$ with $0al(a) \in \mathfrak{g}$. Since $\mathfrak{g} = \mathfrak{q} \oplus \mathfrak{n}$ is a direct vector space sum, the representation $\tau(x) + a$ is unique. Hence ψ is bijektive. Furthermore, by (4.16) and (4.17) we have

$$\begin{aligned} \psi([(x,a),(y,b)]) &= \psi([x,y],\ [a,b] + \varphi(x)(b) - \varphi(y)(a)) \\ &= \psi([x,y],\ [a,b] + [\tau(x),b] - [\tau(y),a]) \\ &= \tau([x,y]) + [a,b] + [\tau(x),b] - [\tau(y),a]. \end{aligned}$$

On the other hand we have

$$\begin{aligned} [\psi(x,a),\psi(y,b)] &= [\tau(x)+a, \tau(y)+b] \\ &= [\tau(x),\tau(y)] + [a,\tau(y)] + [\tau(x),b] + [a,b] \\ &= \tau([x,y]) + [a,b] + [\tau(x),b] - [\tau(y),a], \end{aligned}$$

because τ is a Lie algebra homomorphism. Hence ψ is a Lie algebra isomorphism. □

Definition 4.3.5. Let $\mathfrak{g}$ and $\mathfrak{g}'$ be two extensions of $\mathfrak{q}$ by $\mathfrak{n}$. The extensions are called *equivalent*, if there is a Lie algebra homomorphism $\varphi\colon \mathfrak{g} \to \mathfrak{g}'$, such that the following diagram commutes:

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{n} \arrow[r, "\alpha"] \arrow[d, "\mathrm{id}"] & \mathfrak{g} \arrow[r, "\beta"] \arrow[d, "\varphi"] & \mathfrak{q} \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ 0 \arrow[r] & \mathfrak{n} \arrow[r, "\gamma"] & \mathfrak{g}' \arrow[r, "\delta"] & \mathfrak{q} \arrow[r] & 0 \end{tikzcd}$$

Denote by $\mathrm{Ext}(\mathfrak{q},\mathfrak{n})$ the set of equivalence classes of all Lie algebra extensions (4.15) of $\mathfrak{q}$ by $\mathfrak{n}$.

As in the group case, equivalent extensions $\mathfrak{g}$ and $\mathfrak{g}'$ of $\mathfrak{q}$ by $\mathfrak{n}$ are isomorphic as Lie algebras by the Five Lemma, but the converse is not true.

Let V be a $\mathfrak{g}$-module. We may consider V as an abelian Lie algebra. We have the following result.

Proposition 4.3.6. *Let V be a $\mathfrak{g}$-module, $\omega \in C^2(\mathfrak{g},V)$ and $\mathfrak{g}_\omega = \mathfrak{g} \oplus V$. Then the following bracket on $\mathfrak{g} \oplus V$ given by*

$$[(x,a),(y,b)]_{\mathfrak{g}_\omega} = ([x,y], x.b - y.a + \omega(x,y)) \tag{4.20}$$

defines a Lie algebra if and only if $\omega \in Z^2(\mathfrak{g},V)$. Then we obtain a short exact sequence

$$0 \to V \xrightarrow{\iota} \mathfrak{g}_\omega \xrightarrow{\pi} \mathfrak{g} \to 0,$$

which splits if and only if $\omega \in B^2(\mathfrak{g},V)$.

Proof. The Jacobi identity for the bracket (4.20) says

$$\begin{aligned} 0 = [(x,a),[(y,b),(z,c)]] &+ [(y,b),[(z,c),(x,a)]] \\ &+ [(z,c),[(x,a),(y,b)]] \end{aligned}$$

The second component yields

$$0 = x.\omega(y,z) - y.\omega(x,z) + z.\omega(x,y) - \omega([x,y],z) + \omega([x,z],y) - \omega([y,z],x).$$

But this means $\omega \in Z^2(\mathfrak{g},V)$. In this case $\mathfrak{g}_\omega$ is a Lie algebra with bracket (4.20), such that $\iota(a) = (0,a)$ for $a \in V$ and $\pi(x,a) = x$ for $x \in \mathfrak{g}$ and the above sequence is exact.

Now every homomorphism $\tau\colon \mathfrak{g} \to \mathfrak{g}_\omega$ with $\pi \circ \tau = \mathrm{id}$ is of the form $\tau(x) = (x, f(x))$ with $f \in \operatorname{Hom}(\mathfrak{g}, V)$. We have

$$\begin{aligned} \tau([x,y]) &= ([x,y], f([x,y])) \\ [\tau(x), \tau(y)] &= [(x, f(x)), (y, f(y))] \\ &= ([x,y],\, x.f(y) - y.f(x) + \omega(x,y)). \end{aligned}$$

So τ is a homomorphism if and only if

$$\omega(x,y) = f([x,y]) - x.f(y) + y.f(x) \in B^2(\mathfrak{g}, V).$$

□

An extension of Lie algebras

$$0 \to \mathfrak{a} \xrightarrow{\alpha} \mathfrak{g} \xrightarrow{\beta} \mathfrak{q} \to 0, \tag{4.21}$$

is called *abelian* if $\mathfrak{a}$ is abelian. Then $\mathfrak{a}$ beomes a $\mathfrak{g}$-module by

$$x.a = \alpha^{-1}([\beta^{-1}(x), \alpha(a)]_{\mathfrak{g}}) \tag{4.22}$$

for $x \in \mathfrak{q}$ and $a \in \mathfrak{a}$. Here $\beta^{-1}(x)$ is an arbitrary preimage of x under β. Since $\alpha(\mathfrak{a})$ is an ideal in $\mathfrak{g}$, α^{-1} is defined on $[\beta^{-1}(x), \alpha(a)]$. The action is well-defined since $\mathfrak{a}$ is abelian. We obtain the following interpretation of $H^2(\mathfrak{q}, \mathfrak{a})$:

Theorem 4.3.7. *Let $\mathfrak{a}$ be an abelian Lie-Algebra and $\mathfrak{q}$ be a Lie algebra. Then there is a bijective correspondence between the equivalence classes of abelian extensions $\mathfrak{g}$ of $\mathfrak{q}$ by $\mathfrak{a}$ and $H^2(\mathfrak{q}, \mathfrak{a})$, together with the action* (4.22).

Proof. Let $\mathfrak{g}$ be an abelian extension (4.21) of $\mathfrak{q}$ by $\mathfrak{a}$. Then choose a linear map $\tau\colon \mathfrak{q} \to \mathfrak{g}$ with $\beta \circ \tau = \mathrm{id}$ and define $\omega = \omega_\tau \in \operatorname{Alt}(\mathfrak{g}^2, \mathfrak{a})$ by

$$\omega(x,y) = \alpha^{-1}([\tau(x), \tau(y)] - \tau([x,y])). \tag{4.23}$$

Note that this makes sense, because we have by

$$\begin{aligned} \beta([\tau(x), \tau(y)] - \tau([x,y]) &= [(\beta \circ \tau)(x), (\beta \circ \tau)(y)] - (\beta \circ \tau)([x,y]) \\ &= 0 \end{aligned}$$

that $[\tau(x), \tau(y)] - \tau([x,y]) \in \ker \beta = \operatorname{im} \alpha$. Hence we can indeed apply the map α^{-1}. First we show that $\omega \in Z^2(\mathfrak{q}, \mathfrak{a})$. We may choose $\tau(x)$ as preimage $\beta^{-1}(x)$ in (4.22), i.e.,

$$x.a = \alpha^{-1}([\tau(x), \alpha(a)]) \tag{4.24}$$

Then we obtain by (4.23),

$$\begin{aligned} (d_2\omega)(x_1, x_2, x_3) &= x_1.\omega(x_2, x_3) - x_2.\omega(x_1, x_3) + x_3.\omega(x_1, x_2) \\ &\quad - \omega([x_1, x_2], x_3) + \omega([x_1, x_3], x_2) - \omega([x_2, x_3], x_1) \\ &= \alpha^{-1}([\tau(x_1), [\tau(x_2), \tau(x_3)]]) - \alpha^{-1}([\tau(x_1), \tau[x_2, x_3])]) \\ &\quad - \alpha^{-1}([\tau(x_2), [\tau(x_1), \tau(x_3)]]) + \alpha^{-1}([\tau(x_2), \tau[x_1, x_3])]) \\ &\quad + \alpha^{-1}([\tau(x_3), [\tau(x_1), \tau(x_2)]]) - \alpha^{-1}([\tau(x_3), \tau[x_1, x_2])]) \\ &\quad - \alpha^{-1}([\tau([x_1, x_2]), \tau(x_3)]) + \alpha^{-1}(\tau([[x_1, x_2], x_3])) \\ &\quad + \alpha^{-1}([\tau([x_1, x_3]), \tau(x_2)]) - \alpha^{-1}(\tau([[x_1, x_3], x_2])) \\ &\quad - \alpha^{-1}([\tau([x_2, x_3]), \tau(x_1)]) + \alpha^{-1}(\tau([[x_2, x_3], x_1])). \end{aligned}$$

This equals zero as follows. View the terms as four equal-sized blocks. The two diagonal blocks are zero by the Jacobi identity in $\mathfrak{g}$ and in $\mathfrak{q}$. The other two blocks cancel each other. So we have $\omega \in \ker d_2 = Z^2(\mathfrak{q}, \mathfrak{a})$. Replacing τ by τ', it follows that $\omega_\tau - \omega_{\tau'} \in B^2(\mathfrak{q}, \mathfrak{a})$. Indeed, let $\sigma = \tau - \tau'$. Then $\beta(\sigma) = 0$, so that $\sigma(\mathfrak{q}) \subset \alpha(\mathfrak{a})$ and $\alpha^{-1}\sigma \in \operatorname{Hom}(\mathfrak{q}, \mathfrak{a})$. We have

$$d(\alpha^{-1}\sigma)(x, y) = x.(\alpha^{-1}\sigma(y)) - y.(\alpha^{-1}\sigma(x)) - (\alpha^{-1}\sigma)([x, y]).$$

This together with (4.24) yields

$$\begin{aligned}\omega_\tau(x, y) - \omega_{\tau'}(x, y) &= \alpha^{-1}([\tau(x), \tau(y)] - \tau([x, y])) \\ &\quad - \alpha^{-1}([\tau'(x), \tau'(y)] - \tau'([x, y])) \\ &= \alpha^{-1}([\sigma(x), \tau(y)] + [\tau(x), \sigma(y)] - \sigma([x, y]) \\ &= x.(\alpha^{-1}\sigma(y)) - y.(\alpha^{-1}\sigma(x)) - (\alpha^{-1}\sigma)([x, y]) \\ &= d(\alpha^{-1}\sigma)(x, y).\end{aligned}$$

Thus the cohomology class $[\omega] \in H^2(\mathfrak{q}, \mathfrak{a})$ does not depend on the choice of τ.

Finally we will show that two equivalent abelian extensions define the same cohomology class with respect to a given $\mathfrak{q}$-action on $\mathfrak{a}$. Let $\mathfrak{g}_\omega$ and $\mathfrak{g}_{\omega'}$ be two equivalent extension of $\mathfrak{q}$ by $\mathfrak{a}$. Then there exists a linear map $\widetilde{\varphi}\colon \mathfrak{q} \to \mathfrak{a}$ such that the map

$$\varphi\colon \mathfrak{g}_\omega \to \mathfrak{g}_{\omega'}, \quad (x, a) \mapsto (x, a + \widetilde{\varphi}(x)),\ x \in \mathfrak{q}, a \in \mathfrak{a}$$

is a Lie algebra homomorphism. But this means that

$$\begin{aligned}\varphi([(x, a), (y, b)]) &= \varphi([x, y],\, x.b - y.a + \omega(x, y)) \\ &= ([x, y],\, x.b - y.a + \omega(x, y) + \widetilde{\varphi}([x, y]))\end{aligned}$$

coincides with

$$\begin{aligned}[\varphi(x, a), \varphi(y, b)] &= [(x, a + \widetilde{\varphi}(x)), (y, b + \widetilde{\varphi}(y))] \\ &= ([x, y],\, x.(b + \widetilde{\varphi}(y)) - y.(a + \widetilde{\varphi}(x)) + \omega'([x, y]))\end{aligned}$$

This means that

$$\begin{aligned}\omega_{\tau'}(x, y) - \omega_\tau(x, y) &= \widetilde{\varphi}([x, y]) - x.\widetilde{\varphi}(y) + y.\widetilde{\varphi}(x) \\ &= -(d\widetilde{\varphi})(x, y) \in B^2(\mathfrak{q}, \mathfrak{a}).\end{aligned}$$

Conversely consider a fixed $\omega \in Z^2(\mathfrak{q}, \mathfrak{a})$. It defines an extension by (4.20), given by Erweiterung

$$0 \to \mathfrak{a} \to \mathfrak{g}_\omega \to \mathfrak{q} \to 0,$$

as we have seen in Proposition (4.3.6). It is easy to see that different representatives of the class $[\omega] \in H^2(\mathfrak{g}, \mathfrak{a})$ lead to equivalent extensions. □

We will note two corollaries of this theorem.

Corollary 4.3.8. *The map $Z^2(\mathfrak{q}, \mathfrak{a}) \to \operatorname{Ext}(\mathfrak{q}, \mathfrak{a})$, $\omega \to [\mathfrak{g}_\omega]$ induces a bijection $H^2(\mathfrak{q}, \mathfrak{a}) \to \operatorname{Ext}(\mathfrak{q}, \mathfrak{a})$, where the zero class $[0] \in H^2(\mathfrak{q}, \mathfrak{a})$ corresponds to the class of splitting extensions of $\mathfrak{q}$ by $\mathfrak{a}$.*

Corollary 4.3.9. *The elements of $H^2(\mathfrak{q}, K)$ classify the equivalence classes of central extensions of $\mathfrak{q}$ by K.*

Here K is the trivial 1-dimensional $\mathfrak{q}$-module. The Lie bracket (4.20) then becomes

$$[(x,t),(y,t')] = ([x,y],\omega(x,y)), \quad t,t' \in K,\ x,y \in \mathfrak{g},$$

so that $\alpha(K)$ lies in the center of $\mathfrak{g}$.

Remark 4.3.10. The interpretation of non-abelian extensions of $\mathfrak{q}$ by $\mathfrak{n}$ is much more complicated to describe. Each extension

$$0 \to \mathfrak{n} \to \mathfrak{g} \to \mathfrak{q} \to 0$$

of $\mathfrak{q}$ by $\mathfrak{n}$ defines a factor system $(\mathfrak{n}, T)$, with a Lie algebra homomorphism $T\colon \mathfrak{q} \to \operatorname{Der}(\mathfrak{n})/\operatorname{ad}\mathfrak{n}$. However, not all such homomorphisms arise by a Lie algebra extension. The obstruction of such a homomorphism T lies in the cohomology group $H^3(\mathfrak{q}, Z(\mathfrak{n}))$. Note that $Z(\mathfrak{n})$ becomes a $\mathfrak{q}$-module via the action of $\operatorname{Der}(\mathfrak{n})/\operatorname{ad}\mathfrak{n}$ on $Z(\mathfrak{n})$, by $[D].z = D(z)$ for $D \in \operatorname{Der}(\mathfrak{g})$ and $z \in Z(\mathfrak{n})$. The equivalence classes of Lie algebra extensions corresponding to a factor system $(\mathfrak{n}, T)$ are classified by $H^2(\mathfrak{g}, Z(\mathfrak{n}))$.

As for the first cohomology group there is a Whitehead Lemma for the second cohomology group. Again we are able to give a rather short proof.

Theorem 4.3.11 (Second Whitehead Lemma). *Let $\mathfrak{g}$ be a finite-dimensional semisimple Lie algebra of characteristic zero and M be a finite-dimensional $\mathfrak{g}$-module. Then we have $H^2(\mathfrak{g}, M) = 0$.*

Proof. Let $\omega \in Z^2(\mathfrak{g}, M)$ and $\mathfrak{g}_\omega = \mathfrak{g} \oplus_\omega M$ be the corresponding abelian extension of $\mathfrak{g}$ by M, given by the short exaxct sequence

$$0 \to M \to \mathfrak{g}_\omega \to \mathfrak{g} \to 0.$$

Then $M = \operatorname{rad}(\mathfrak{g}_\omega)$ equals the solvable radical of $\mathfrak{g}_\omega$, because M is an abelian ideal of $\mathfrak{g}_\omega$ with semisimple quotient $\mathfrak{g} \cong \mathfrak{g}_\omega/M$. By Levi's Theorem there exists a Levi complement to M in $\mathfrak{g}_\omega$. Thus the above short exact sequence splits. By Proposition 4.3.6 this means that $\omega \in B^2(\mathfrak{g}, M)$. □

Remark 4.3.12. There is no Third Whitehead Lemma, at least not without further assumptions. This is seen from the next result.

Proposition 4.3.13. *Let $\mathfrak{g}$ be a semisimple Lie algebra over a field of characteristic zero. Then $H^3(\mathfrak{g}, K)$ is nonzero.*

Proof. See Exercise 27. □

For example, let $\mathfrak{g}$ be a complex simple Lie algebra. Then we have

$$H^3(\mathfrak{g}, \mathbb{C}) \cong \mathbb{C}.$$

Still, there is a way to generalize the Whitehead Lemmas. Note that we have for $M = M_1 \oplus M_2$, that

$$H^q(\mathfrak{g}, M) = H^q(\mathfrak{g}, M_1) \oplus H^q(\mathfrak{g}, M_2).$$

By Weyl's Theorem we see that the computation of $H^q(\mathfrak{g}, M)$ for semisimple Lie algebras $\mathfrak{g}$ can be reduced to coefficients in simple $\mathfrak{g}$-modules M. Indeed, M is the direct sum of finitely many simple $\mathfrak{g}$-modules. So we may assume that M is simple. If $\mathfrak{g}.M = 0$, then $\dim M = 1$ and $M = K$. Then $H^q(\mathfrak{g}, \mathbb{C})$ need not be trivial for $q \geq 3$. On the other hand, if $\mathfrak{g}.M \neq 0$, and therefore $\mathfrak{g}.M = M$ and $M^{\mathfrak{g}} = 0$, we have the following result.

THEOREM 4.3.14 (Whitehead). *Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over a field K of characteristic zero and M be a finite-dimensional simple $\mathfrak{g}$-module with $M^{\mathfrak{g}} = 0$. Then we have $H^q(\mathfrak{g}, M) = 0$ für alle $q \geq 0$.*

We obtain also the following result.

PROPOSITION 4.3.15. *Let $\mathfrak{g}$ be a finite-dimensional reductive Lie-Algebra over a field K of characteristic zero, and let M be a finite-dimensional semisimple $\mathfrak{g}$-module. Then we have*

$$H^n(\mathfrak{g}, M) \cong H^n(\mathfrak{g}, M^{\mathfrak{g}}) \cong H^n(\mathfrak{g}, K) \otimes M^{\mathfrak{g}}.$$

We can again compute the second cohomology group for some easy examples.

EXAMPLE 4.3.16. *Let $\mathfrak{g} = \mathfrak{sl}_2(K)$ and K be a field of characteristic not 2. Then we have $H^2(\mathfrak{g}, K) = 0$.*

Indeed, this follows for characteristic zero already from the Second Whitehead Lemma. Let (e_1, e_2, e_3) be a basis of $\mathfrak{g}$ as in Example 4.2.10, and let $\omega \in C^2(\mathfrak{g}, K)$. Then $\omega \in Z^2(\mathfrak{g}, K)$ if and only if

$$\omega([e_i, e_j], e_k) - \omega([e_i, e_k], e_j) + \omega([e_j, e_k], e_i) = 0$$

for all i, j, k. However, this is an empty condition. For example, let $(i, j, k) = (1, 2, 3)$. Then it means

$$\omega(e_3, e_3) + 2\omega(e_1, e_2) + 2\omega(e_2, e_1) = 0,$$

which says that $0 = 0$. It is also obvious that $\omega(e_i, e_j) = f([e_i, e_j])$ for some $f \in \operatorname{Hom}(\mathfrak{g}, K)$, because $[e_1, e_2], [e_1, e_3], [e_2, e_3]$ is again a basis for $\mathfrak{g}$. So we have $Z^2(\mathfrak{g}, K) = C^2(\mathfrak{g}, M) = B^2(\mathfrak{g}, M)$.

EXAMPLE 4.3.17. *Let $\mathfrak{g} = \mathfrak{n}_4(K)$. Tehn we have* $\dim H^2(\mathfrak{g}, K) = 2$.

Let (e_1, e_2, e_3, e_4) be a basis of $\mathfrak{n}_4(K)$ as in Example 4.2.11. The condition

$$\omega([e_1, e_2], e_3) - \omega([e_1, e_3], e_2) + \omega([e_2, e_3], e_1) = 0$$

yields $\omega(e_2, e_4) = 0$. For $(i, j, k) = (1, 2, 3)$ we obtain $\omega(e_3, e_4) = 0$. We have $Z^2(\mathfrak{g}, K) = \operatorname{span}\{\omega_{12}, \omega_{13}, \omega_{14}, \omega_{23}\}$, where $\omega_{ij}(e_i, e_j) = 1$, $\omega_{ij}(e_j, e_i) = -1$ and zero otherwise. It is easy to see that $B^2(\mathfrak{g}, K) = \operatorname{span}\{\omega_{12}, \omega_{13}\}$, because of

$$\begin{aligned} 1 &= \omega_{12}(e_1, e_2) = f([e_1, e_2]) = f(e_3) \\ 1 &= \omega_{13}(e_1, e_3) = f([e_1, e_3]) = f(e_4) \\ 1 &= \omega_{14}(e_1, e_4) \neq f([e_1, e_4]) = 0 \\ 1 &= \omega_{23}(e_2, e_3) \neq f([e_2, e_3]) = 0. \end{aligned}$$

Thus $H^2(\mathfrak{g}, K) = \operatorname{span}\{[\omega_{14}], [\omega_{23}]\}$.

The second cohomology group $H^2(\mathfrak{g}, \mathfrak{g})$ with adjoint coefficients has another special interpretation. It describes all infinitesimal deformations of $\mathfrak{g}$. For references see, among others, the papers by Gerstenhaber. He introduced defomations of associative algebras and rings in [**13**]. For deformations of Lie algebras see Nijenhuis and Richardson [**23**].

Definition 4.3.18. Let $(\mathfrak{g}, [\ ,\ ])$ be a Lie algebra over a field K, and $g, h \in \mathfrak{g}$, $\varphi_k \in \operatorname{Hom}(\Lambda^2\mathfrak{g}, \mathfrak{g}) = C^2(\mathfrak{g}, \mathfrak{g})$. A *formal one-parameter defomation* of $\mathfrak{g}$ is a power series

$$[g,h]_t := [g,h] + \sum_{k\geq 1} \varphi_k(g,h)t^k,$$

so that the Jacobi identity is satisfied for $[\ ,\ ]_t$.

Actually, the Jacobi identity is equivalent to infinitely many conditions over $k \in \mathbb{N}$. For $k=1$ we see that it implies $\varphi_1 \in Z^2(\mathfrak{g}, \mathfrak{g})$. One can summarize all conditions in the following differentially graded Lie algebra structure of the complex $\{C^\bullet(\mathfrak{g}, \mathfrak{g}), d\}$ as follows. For $\alpha \in C^p(\mathfrak{g}, \mathfrak{g})$ and $\beta \in C^q(\mathfrak{g}, \mathfrak{g})$ is the product $[\alpha, \beta] \in C^{p+q-1}(\mathfrak{g}, \mathfrak{g})$ defined by

$$\begin{aligned}
&[\alpha, \beta](g_1, \dots, g_{p+q-1}) \\
&= \sum_{i_1 < \cdots < i_q} (-1)^{\sum_s (i_s - s)} \alpha(\beta(g_{i_1}, \dots, g_{i_q}), g_1, \dots, \widehat{g_{i_1}}, \dots, \widehat{g_{i_q}}, \dots, g_{p+q-1}) \\
&- (-1)^{(p-1)(q-1)} \sum_{j_1 < \cdots < j_q} (-1)^{\sum_t (j_t - t)} \beta(\alpha(g_{j_1}, \dots, g_{j_p}), g_1, \dots, \\
&\widehat{g_{j_1}}, \dots, \widehat{g_{j_p}}, \dots, g_{p+q-1}),
\end{aligned}$$

where the summation goes over all indices i_r, j_r with $1 \leq i_r, j_r \leq p+q-1$.

The Jacobi identity for $[\ ,\ ]_t$ is equivalent to the sequence of relations Relationen

$$d\varphi_k = -\frac{1}{2}\sum_{i=1}^{k-1} [\varphi_i, \varphi_{k-i}], \quad k = 1, 2, 3, \dots$$

For $k=1$ we obtain $d\varphi_1 = 0$, hence $\varphi_1 \in Z^2(\mathfrak{g}, \mathfrak{g})$.

Two deformations of $\mathfrak{g}$ are called equivalent if the corresponding Lie algebras are isomorphic. The cohomology class of φ_1 is called the *differential* of the formal deformation $[\ ,\ ]_t$ and only depends on the equivalence class of the deformation. A cohomology class $[\varphi]$ in $H^2(\mathfrak{g}, \mathfrak{g})$ is called an *infinitesimal deformation* of $\mathfrak{g}$. Note that an infinitesimal deformation $[\varphi] \in H^2(\mathfrak{g}, \mathfrak{g})$ need not be the differential of a formal derivation. For this, the above equations for $k = 2, 3, 4, \dots$ are necessary and sufficient conditions. If they are satisfied, the deformation is called *integrable*. We have the following resultat, see [**25**]:

Theorem 4.3.19 (Rauch). *Let $\mathfrak{g}$ be an finite-dimensional real or complex Lie algebra. If $H^3(\mathfrak{g}, \mathfrak{g}) = 0$, then every infinitesimal deformation of $\mathfrak{g}$ is integrable.*

Definition 4.3.20. A n-dimensional Lie algebra $\mathfrak{g}$ is called (geometrically) *rigid*, if its Lie algebra law μ in the variety $\mathcal{L}_n(k)$ of all Lie algebra structures has open orbit $O(\mu)$ in the Zariski topology.

This means intuitively that all Lie algebra structures $\lambda \in \mathcal{L}_n(k)$ nearby μ are already isomorphic to μ. Then μ has only trivial infinitesimal deformations, i.e., is also *formally rigid*.

Theorem 4.3.21 (Richardson 1967). *Let $\mathfrak{g}$ be a Lie algebra over an algebraically closed field k of characteristic zero, or over $k = \mathbb{R}$. If $H^2(\mathfrak{g}, \mathfrak{g}) = 0$, then $\mathfrak{g}$ is rigid.*

The converse is not true. There are infinitely many rigid Lie algebras $\mathfrak{g}$ with nonzero $H^2(\mathfrak{g}, \mathfrak{g})$.

EXAMPLE 4.3.22. *Let $\varphi\colon \mathfrak{sl}_2(\mathbb{C}) \to \mathfrak{gl}_n(\mathbb{C})$ be the standard n-dimensional irreducible representation of $\mathfrak{sl}_2(\mathbb{C})$. We denote this module by $V(n)$. Suppose that $n \equiv 1(4)$ and $n \geq 13$. Then the Lie algebras*

$$\mathfrak{g}_n = \mathfrak{sl}_2(\mathbb{C}) \ltimes_\varphi V(n)$$

are rigid and have nonzero second cohomology $H^2(\mathfrak{g}_n, \mathfrak{g}_n)$.

Note that every semisimple Lie algebra of characteristic is rigid by the Second Whitehead Lemma. This can be generalized to parabolic subalgebras of semisimple Lie algebras, see [**27**], or [**22**], page 1.

THEOREM 4.3.23. *Let $\mathfrak{p}$ be a parabolic subalgebra of a semisimple Lie algebra in characteristic zero. Then we have $H^n(\mathfrak{p}, \mathfrak{p}) = 0$ for all $n \geq 0$.*

REMARK 4.3.24. The number of nonisomorphic rigid Lie algebra laws $\mu \in \mathcal{L}_n(k)$ is finite for a given n, because $\overline{O(\mu)}$ then is an irreducible component of the algebraic set $\mathcal{L}_n(k)$, which has only finitely many component for a given $n \geq 1$. One can show that the number grows at least with

$$\exp\left(\frac{\log^2(2)n}{2\log(n)}\right)$$

for n big.

REMARK 4.3.25. Note that there is also a converse to the Second Whitehead Lemma, see [**30**]. Let $\mathfrak{g}$ be a finite-dimensional Lie algebra in characteristic zero satisfying $H^2(\mathfrak{g}, M) = 0$ for all finite-dimensional $\mathfrak{g}$-modules M. Then $\mathfrak{g}$ is either semisimple, or 1-dimensional, or the direct sum of a semisimple algebra and a one-dimensional algebra.

In positive characteristic there is no such Lie algebra at all, see [**12**]: Let $\mathfrak{g}$ be a finite-dimensional Lie algebra in characteristic $p > 0$. Then there exists a finite-dimensional $\mathfrak{g}$-module M such that

$$H^n(\mathfrak{g}, M) \neq 0$$

für alle $n = 0, 1, \ldots, \dim(\mathfrak{g})$.

We also want to mention a result by Dixmier [**11**] on the cohomology of *nilpotent* Lie algebras. We say that a $\mathfrak{g}$-module contains a $\mathfrak{g}$-module N, if N is a quotient module of a submodule of M.

THEOREM 4.3.26 (Dixmier). *Let $\mathfrak{g}$ be a nilpotent Lie algebra over an infinite field K and M be a finite-dimensional $\mathfrak{g}$-module. Then we have:*

(1) $H^p(\mathfrak{g}, M) = 0$ *for all* $p \geq 0$*, if* M *does not contain a trivial module.*
(2) $\dim H^p(\mathfrak{g}, M) \geq 2$ *for* $0 < p < \dim \mathfrak{g}$*, if* M *contains a trivial module.*

4.4. The third cohomology group

In this section we present the interpretation of the third Lie algebra cohomology $H^3(\mathfrak{g}, M)$ as equivalence classes of *crossed modules*, and as equivalence classes of Lie algebra *kernels*, i.e., of homomorphisms $\varphi\colon \mathfrak{g} \to H^1(\mathfrak{m}, \mathfrak{m})$, where $\mathfrak{m}$ is a Lie algebra with $Z(\mathfrak{m}) = M$. For a reference see for example [**28**].

Definition 4.4.1. Let $\mathfrak{m}$ and $\mathfrak{n}$ be two Lie algebras. A *crossed module* $(\mu, \mathfrak{m}, \mathfrak{n})$ is a Lie algebra homomorphism $\mu\colon \mathfrak{m} \to \mathfrak{n}$ together with an action η of $\mathfrak{n}$ on $\mathfrak{m}$, $(n, m) \mapsto n \cdot m = \eta(n)(m)$, with the following conditions:

$$\eta(\mu(m))(m') = [m, m'] \quad \forall\, m, m' \in \mathfrak{m}, \tag{4.25}$$

$$\mu(\eta(n)(m)) = [\mu(m), n] \quad \forall\, n \in \mathfrak{n}, \forall\, m \in \mathfrak{m}. \tag{4.26}$$

The definition has a natural example.

Example 4.4.2. *Let $\mathfrak{m}$ be a Lie algebra and $\mathfrak{n} = \operatorname{Der}(\mathfrak{m})$. Define μ by $\mu(m) = \operatorname{ad}(m)$ and $\eta(n)(m) = n(m)$ for derivations n, then $(\mu, \mathfrak{m}, \mathfrak{n})$ is a crossed module.*

Indeed, we have

$$\begin{aligned} \eta(\mu(m))(m') &= \mu(m)(m') = [m, m'], \\ \mu(\eta(n)(m)) &= \operatorname{ad}(n(m)) = [\operatorname{ad}(m), n] = [\mu(m), n]. \end{aligned}$$

For a crossed module $(\mu, \mathfrak{m}, \mathfrak{n})$ let

$$M := \ker(\mu).$$

The the sequence

$$0 \to M \xrightarrow{i} \mathfrak{m} \xrightarrow{\mu} \mathfrak{n}$$

is exact. Because of (4.26), $\operatorname{im}(\mu)$ is a Lie algebra ideal in $\mathfrak{n}$. Also

$$\mathfrak{g} := \operatorname{coker}(\mu)$$

is a Lie algebra, and we obtain the following short exact sequence

$$\mathfrak{m} \xrightarrow{\mu} \mathfrak{n} \xrightarrow{\pi} \mathfrak{g} \to 0.$$

Now M is an abelian Lie algebra, since M is, by (4.25), a subalgebra of $Z(\mathfrak{m})$. Then, by (4.26), the action of $\mathfrak{n}$ on $\mathfrak{m}$ also induces an action of $\mathfrak{g}$ on M. So we obtain the following result.

Proposition 4.4.3. *Every crossed module $(\mu, \mathfrak{m}, \mathfrak{n})$ induces a 4-term exact sequence*

$$0 \to M \xrightarrow{i} \mathfrak{m} \xrightarrow{\mu} \mathfrak{n} \xrightarrow{\pi} \mathfrak{g} \to 0, \tag{4.27}$$

where M is a $\mathfrak{g}$-module.

Definition 4.4.4. Two crossed modules $(\mu, \mathfrak{m}, \mathfrak{n})$ and $(\mu', \mathfrak{m}', \mathfrak{n}')$ with actions η respectively η' with $\ker(\mu) = \ker(\mu') = M$ and $\operatorname{coker}(\mu) = \operatorname{coker}(\mu') = \mathfrak{g}$ are called *equivalent*, if there exists a Lie algebra homomorphism $\varphi\colon \mathfrak{m} \to \mathfrak{m}'$ and $\psi\colon \mathfrak{n} \to \mathfrak{n}'$, such that

$$\varphi(\eta(n)(m)) = \eta'(\psi(n))(\varphi(m)) \quad \forall\, m \in \mathfrak{m}, \forall\, n \in \mathfrak{n},$$

and the following diagram is commutative:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "i"] \arrow[d, "\mathrm{id}"] & \mathfrak{m} \arrow[r, "\mu"] \arrow[d, "\varphi"] & \mathfrak{n} \arrow[r, "\pi"] \arrow[d, "\psi"] & \mathfrak{g} \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & M \arrow[r, "i'"] & \mathfrak{m}' \arrow[r, "\mu'"] & \mathfrak{n}' \arrow[r, "\pi'"] & \mathfrak{g} \arrow[r] & 0
\end{tikzcd}$$

Note that φ and ψ are not necessarily isomorphisms. Denote by $\mathcal{CM}(\mathfrak{g}, M)$ the equivalence classes of crossed Lie algebra modules with fixed kernel M and cokernel $\mathfrak{g}$. The following result is due to Gerstenhaber [**14**]:

THEOREM 4.4.5. *There is a $1-1$ correspondence between equivalence classes of crossed modules with kernel M and cokernel $\mathfrak{g}$ and elements of $H^3(\mathfrak{g},M)$. We have $\mathcal{CM}(\mathfrak{g},M)\cong H^3(\mathfrak{g},M)$ as abelian groups.*

PROOF. We only give a sketch of the proof. First we explain how to obtain a 3-cocycle in $Z^3(\mathfrak{g},M)$ from a crossed module $(\mu,\mathfrak{m},\mathfrak{n})$. Consider the associated 4-term exact sequence

$$0\rightarrow M\xrightarrow{i}\mathfrak{m}\xrightarrow{\mu}\mathfrak{n}\xrightarrow{\pi}\mathfrak{g}\rightarrow 0,$$

induced by $(\mu,\mathfrak{m},\mathfrak{n})$. Choose a transversal function $\tau\colon\mathfrak{g}\rightarrow\mathfrak{n}$ with $\pi\circ\tau=\mathrm{id}_{\mathfrak{g}}$, and set, for $x_1,x_2\in\mathfrak{g}$,

$$\omega(x_1,x_2)=[\tau(x_1),\tau(x_2)]-\tau([x_1,x_2]).$$

Then ω is bilinear and skew-symmetric in x_1,x_2. We have $\pi(\omega(x_1,x_2))=0$, because π is a Lie algebra homomorphism, i.e.,

$$\omega(x_1,x_2)\in\mathrm{im}(\mu)=\ker(\pi).$$

Hence there exists a $\beta(x_1,x_2)\in\mathfrak{m}$ with

$$\mu(\beta(x_1,x_2))=\omega(x_1,x_2).$$

Now we may choose a transversal function $\sigma\colon\ \mathrm{im}(\mu)\rightarrow\mathfrak{m}$, so that we can write β as

$$\beta(x_1,x_2)=\sigma(\omega(x_1,x_2)).$$

This shows that we may assume that β is bilinear and skew-symmetric. Denote by $d^{\mathfrak{m}}$ the formal coboundary operator for $\mathfrak{g}$ with values in $\mathfrak{m}$. Note that $\mathfrak{m}$ need not be a $\mathfrak{g}$-module. Nevertheless we can formally consider the coboundary operator. It is not difficult to prove the following fact.

Fact 1: We have $\mu((d^{\mathfrak{m}}\beta)(x_1,x_2,x_3))=0$ for all $x_1,x_2,x_3\in\mathfrak{g}$.

It follows that $(d^{\mathfrak{m}}\beta)(x_1,x_2,x_3))\in\ker(\mu)=\mathrm{im}(i)=i(M)$. Hence there exists a

$$\gamma(x_1,x_2,x_3)\in M$$

with $(d^{\mathfrak{m}}\beta)(x_1,x_2,x_3)=i(\gamma(x_1,x_2,x_3))$. by using a transversal function ρ on $i(M)=\ker(\mu)$ we can choose γ in such a way that $\gamma=\rho\circ d^{\mathfrak{m}}\beta$. This shows that we may assume that γ is trilinear and skew-symmetric in x_1,x_2,x_3. It is easy to verify the following claim.

Fact 2: We have $\gamma\in Z^3(\mathfrak{g},M)$. Here γ is independent of the choice of the transversal functions τ,σ,ρ.

The next step is to show that two equivalent crossed modules induce the same class $[\gamma]\in H^3(\mathfrak{g},M)$. Then we have a well-defined map $\varphi\colon\mathcal{CM}(\mathfrak{g},M)\rightarrow H^3(\mathfrak{g},M)$, and we need to show that φ is injective and surjective. For a proof see [**28**]. The idea is, to view the 4-term exact sequence (4.27) as so- called *Yoneda product* of two short exact sequences, which naturally arise from (4.27), namely

$$0\rightarrow\mathfrak{m}/i(M)\xrightarrow{\mu}\mathfrak{n}\xrightarrow{\pi}\mathfrak{g}\rightarrow 0$$

and

$$0\rightarrow M\xrightarrow{i}\mathfrak{m}\xrightarrow{\mu}\mathrm{im}(\mu)\rightarrow 0.$$

The second one defines a central extension. Since π in (4.27) is surjectiv, and since $\ker(\pi)=\mathrm{im}(\mu)\cong\mathfrak{m}/ker(\mu)=\mathfrak{m}/i(M)$, we obtain the first short exact sequence.

In general the Yoneda product of short exact sequences yields *all* such crossed modules, which gives the surjectivity of φ. Indeed, to every cohomology class $[\gamma] \in H^3(\mathfrak{g}, M)$ there exists a crossed module, whose associated cohomology class equals $[\gamma]$. □

4.5. Functorial definition of Lie algebra cohomology

We will use the language of categories and functors to define Lie algebra cohomology. Recall that $\mathcal{M}od_R$ denotes the category of left R-modules. For a Lie algebra $\mathfrak{g}$ we let $R = U(\mathfrak{g})$, the universal enveloping algebra of $\mathfrak{g}$. This yields the category $\mathcal{M}_{U(\mathfrak{g})} := \mathcal{M}od_{U(\mathfrak{g})}$ of left $U(\mathfrak{g})$-modules. Denote by $\mathcal{M}_{\mathfrak{g}}$ the category of $\mathfrak{g}$-modules. Since every $\mathfrak{g}$-module is a $U(\mathfrak{g})$-module and also the converse way, the categories $\mathcal{M}_{U(\mathfrak{g})}$ and $\mathcal{M}_{\mathfrak{g}}$ are equivalent. Indeed, this follows from the universal property of $U(\mathfrak{g})$: given a unital associative K-algebra A, and a Lie algebra homomorphism $\varphi\colon \mathfrak{g} \to A$, then there exists a unique homomorphism of K-algebras $\tilde{\varphi}\colon U(\mathfrak{g}) \to A$ with $\tilde{\varphi}(1) = 1$, so that $\varphi = \tilde{\varphi} \circ \iota$:

$$\begin{tikzcd}
\mathfrak{g} \arrow[r, "\varphi"] \arrow[d, "\iota"] & A \\
U(\mathfrak{g}) \arrow[ur, dotted, "\tilde{\varphi}"'] &
\end{tikzcd}$$

For the construction of $U(\mathfrak{g})$ consider the tensor algebra

$$T(\mathfrak{g}) = \bigoplus_{n \in \mathbb{N}} T^n(\mathfrak{g}) = \bigoplus_{n \in \mathbb{N}} \mathfrak{g}^{\otimes n}$$

and defined the quotient $U(\mathfrak{g}) = T(\mathfrak{g})/I$ by the ideal I, which is generated by all $x \otimes y - y \otimes x - [x, y]$. The tensor algebra is *filtered* by

$$F_n T(\mathfrak{g}) = \bigoplus_{0 \le i \le n} T^i(\mathfrak{g}).$$

This filtration descends to the quotient, so that also $U(\mathfrak{g})$ is a filtered algebra, with

$$U_n(\mathfrak{g}) = F_n T(\mathfrak{g})/(I \cap F_n T(\mathfrak{g})).$$

For example, we have $U_0(\mathfrak{g}) \cong K$ and $U_1(\mathfrak{g}) \cong K \oplus \mathfrak{g}$.

We still need the following lemma for the functorial definition of Lie algebra cohomology.

Lemma 4.5.1. *The functor $F\colon \mathcal{M}_{\mathfrak{g}} \to \mathcal{M}_K$, $F(M) = M^{\mathfrak{g}}$ from the category of $\mathfrak{g}$-modules to the category of K-modules is left exact.*

Proof. The trivial $\mathfrak{g}$-module functor $T\colon \mathcal{M}_K \to \mathcal{M}_{\mathfrak{g}}$ is the exact functor which we obtain by considering a K-module as trivial $\mathfrak{g}$-module. Since $M^{\mathfrak{g}}$ is the maximal trivial $\mathfrak{g}$-submodule of M, F is right adjoint to T. Therefore F is left exact. □

In other words, if $0 \to N \to M \to V \to 0$ is a short exact sequence of $\mathfrak{g}$-modules, then also the sequence $0 \to N^{\mathfrak{g}} \to M^{\mathfrak{g}} \to V^{\mathfrak{g}}$ is exact. Since the category of $\mathfrak{g}$-modules has enough injectives, every $\mathfrak{g}$-module has an injective resolution, and we can form the roght derived functors $R^n F$ of F.

Definition 4.5.2. Let $\mathfrak{g}$ be a Lie algebra and M be a $\mathfrak{g}$-module. Define the n-th cohomology group of $\mathfrak{g}$ with coefficients in M by

$$H^n(\mathfrak{g}, M) = (R^n F)(M).$$

More concretely we have, for a given injective resolution

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

of M, that the complex

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

is no longer exact in general, and that we have $H^r(\mathfrak{g}, M) \cong \ker(d^r)/\operatorname{im}(d^{r-1})$.

For every homomorphism $\alpha\colon M \to N$ of $\mathfrak{g}$-modules and each pair of injective resolutions $M \to I^\bullet$ and $N \to J^\bullet$, we can lift α to a map $\widetilde{\alpha}\colon I^\bullet \to J^\bullet$ of complexes

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

Here the homomorphisms $H^r(\widetilde{\alpha})\colon H^r(I^{\bullet\mathfrak{g}}) \to H^r(J^{\bullet\mathfrak{g}})$ are independent of the choice of $\widetilde{\alpha}$. Applying this to the identity $\mathrm{id}\colon M \to M$, we see that the groups $H^r(\mathfrak{g}, M)$ are well-defined up to canonical isomorphism. Let us summarize some fundamental properties.

(1) We have $H^0(\mathfrak{g}, M) = F(M) = M^{\mathfrak{g}}$.
(2) If I is an injective $\mathfrak{g}$-module, then $H^r(\mathfrak{g}, I) = 0$ for all $r > 0$, because $0 \to I \to I \to 0 \to 0 \to \cdots$ is an injective resolution of I.
(3) Each short exact sequence $0 \to N \to M \to V \to 0$ of $\mathfrak{g}$-modules induces a long exact sequence of cohomology groups

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

The maps $\partial : H^r(\mathfrak{g}, V) \to H^{r+1}(\mathfrak{g}, N)$ are called *connecting homomorphisms*. Note that again the cohomology groups obtained by the explicit coboundary operator and by the functorial definition are isomorphic.

Remark 4.5.3. We also can define the *homology* groups of Lie algebras via functors and via an direct boundary operator. The functorial definition is just the dual one, using the covariant functor and projective resolutions. The explicit definition goes as follows. Denote by

$$C_n(\mathfrak{g}, M) = \Lambda^n(\mathfrak{g}) \otimes_K M.$$

The space of n-chains. The standard complex is given by

$$0 \leftarrow M \cong \Lambda^0(\mathfrak{g}) \otimes M \xleftarrow{\partial_0} \Lambda^1(\mathfrak{g}) \otimes M \xleftarrow{\partial_1} \Lambda^2(\mathfrak{g}) \otimes M \xleftarrow{\partial_2} \cdots$$

where the boundary operator $\partial_n\colon \Lambda^{n+1}(\mathfrak{g}) \otimes M \to \Lambda^n(\mathfrak{g}) \otimes M$ is given by

$$\begin{aligned} \partial(y_1 \wedge \cdots \wedge y_{n+1} \otimes x) &= \sum_{k=1}^{n+1} (-1)^k y_1 \wedge \cdots \widehat{y_k} \cdots \wedge y_{n+1} \otimes y_k \cdot x \\ &\quad + \sum_{1 \le r < s \le n+1} (-1)^{r+s} [y_r, y_s] \wedge y_1 \wedge \cdots \widehat{y_r} \cdots \widehat{y_s} \cdots \wedge y_{n+1} \otimes x \end{aligned}$$

Then we define

$$H_n(\mathfrak{g}, M) = \ker(\partial_n)/\operatorname{im}(\partial_{n+1}).$$

For the trivial $\mathfrak{g}$-module K we have

$$\dim H_n(\mathfrak{g}, K) = \dim H^n(\mathfrak{g}, K).$$

A connection between Lie algebra cohomology and homology with trivial coefficients is given by the so-called *Poincare duality.* Recall that a Lie algebra $\mathfrak{g}$ is called *unimodular*, if $\operatorname{tr}\operatorname{ad}(x) = 0$ for all $x \in \mathfrak{g}$.

PROPOSITION 4.5.4 (Poincare duality). *Let $\mathfrak{g}$ be a unimodular Lie algebra of dimension n. Then we have*

$$H_p(\mathfrak{g}, K) \cong H^{n-p}(\mathfrak{g}, K), \quad p = 0, 1, \dots, n.$$

4.6. Betti numbers of nilpotent Lie algebras

The Betti numbers $b_i(\mathfrak{g})$ for $i \geq 0$ of a Lie algebra $\mathfrak{g}$ are defined by

$$b_i(\mathfrak{g}) = \dim H^i(\mathfrak{g}, K).$$

There are several open questions on the Betti numbers of a finite dimensional nilpotent Lie algebra $\mathfrak{g}$. Often there is no explicit formula known and it may be impossible to obtain one. Then one tries to obtain lower and upper estimates for the Betti numbers. Some results concerning p-groups can be transfered to the Lie algebra case. A famous example for this is the *Golod-Shafarevich theorem* for p-groups. Let G be a finite p-group. Then we denote by $d(G)$ the minimal number of generators for G, and by $r(G)$ the minimal number of relations between these generators in the associated free pro-p group. We can reformulate this in terms of group cohomology:

$$d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p),$$
$$r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p).$$

Then the following result holds.

THEOREM 4.6.1 (Golod-Shafarevich). *For every finite p-group we have*

$$r(G) > \frac{d(G)^2}{4}.$$

The problem can be formulated for Lie algebras as well. For a finite dimensional nilpotent Lie algebra $\mathfrak{g}$ the cardinality of a minimal generating system is given by Erzeugendensystems gleich

$$\dim(\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}]) = \dim H_1(\mathfrak{g}, K) = \dim H^1(\mathfrak{g}, K) = b_1(\mathfrak{g}).$$

Moreover the cardinality of a minimal system of relations is given by

$$\dim H^2(\mathfrak{g}, K) = b_2(\mathfrak{g}).$$

Now we have an analogous result to Golod-Shafarevich:

THEOREM 4.6.2 (Koch). *Let $\mathfrak{g}$ be a finite dimensional nilpotent Lie algebra. Then we have*

$$b_2(\mathfrak{g}) > \frac{b_1(\mathfrak{g})^2}{4}.$$

The result was proved by Koch [**20**] in 1977, but seems to have been forgotten afterwards. In a paper by Cairns et al. in 1997 this result was called the b_2-*conjecture*, see [**10**].

There is another famous conjecture on the Betti numbers of nilpotent Lie algebras, namely the so called *toral rank conjecture*, or TRC. It says that

$$\sum_{p=0}^{n} b_p(\mathfrak{g}) \geq 2^{\dim Z(\mathfrak{g})},$$

where $Z(\mathfrak{g})$ is the center of a nilpotent Lie algebra $\mathfrak{g}$. The conjecture originates from algebraic topology. Denote by $\mathrm{rk}(M)$ the *toroidal rank* of a closed manifold M. This is the dimension of the largest torus acting freely on M. Halperin conjectured in 1985 that we have

$$\dim H^*(M) \geq 2^{rk(M)}.$$

The conjecture is still open, as far as I know.

Now suppose that N is a nilpotent Lie group, and Γ is a discrete cocompact subgroup of N. Then $M := N/\Gamma$ is a compact nilmanifold with toral rank $\mathrm{rk}(M) = \dim Z(\mathfrak{g})$. Then the Halperin conjecture implies the TRC for a certain class of nilpotent Lie algebras, namely for such which are a model of a compact nilmanifold. Unfortunately there are many nilpotent Lie algebras, which are not such a model, because they do not admit a basis with only rational structure constants. Already in dimesnion 7 over $\mathbb{C}$ we have infinitely many distict nilpotent Lie algebras, which are "non-rational". So there is no reason why the TRC should be true for general nilpotent Lie algebras. On the other hand, the TRC has been shown in many special cases, see [**8**]:

THEOREM 4.6.3. *Let $\mathfrak{g}$ be a complex finite dimensional nilpotent Lie algebra satisfying one of the following conditions:*

(1) $\dim Z(\mathfrak{g}) \leq 5$*,*
(2) $\dim \mathfrak{g}/Z(\mathfrak{g}) \leq 7$
(3) $\dim \mathfrak{g} \leq 14$
(4) $\mathfrak{g}$ *ist* 2*-stufig nilpotent.*

Then the TRC is true, i.e., we have $\sum_{p=0}^{n} b_p(\mathfrak{g}) \geq 2^{\dim Z(\mathfrak{g})}$.

Note that the estimate is often not very good. For certain classes of nilpotent Lie algebras one can obtain better estimates, see [**26**]:

THEOREM 4.6.4. *Let $\mathfrak{g}$ be a* 2*-step nilpotent Lie algebra and $\mathfrak{v}$ be a vector space complement of $Z(\mathfrak{g})$ in $\mathfrak{g}$. Then we have*

$$\sum_{p=0}^{n} b_p(\mathfrak{g}) \geq 2^t, \quad t = \dim Z(\mathfrak{g}) + \left[\frac{\dim \mathfrak{v} + 1}{2}\right]$$

There are also upper bounds for the Betti numbers of nilpotent Lie algebras. For example, we have the following result, see [**8**]:

THEOREM 4.6.5. *Let $\mathfrak{g}$ be a nilpotent nonabelian Lie algebra of dimension $n \geq 3$. Then we have, for $p = 1, \ldots, n-1$,*

$$b_p(\mathfrak{g}) \leq \binom{n}{p} - \binom{n-2}{p-1}.$$

For some Lie algebras we have equality, e.g., for $\mathfrak{n}_3(K) \oplus K^{n-3}$. And is some exceptional cases we can find an explicit formula for the Betti numbers. One case are the heisenberg algebras.

THEOREM 4.6.6 (Santharoubane). *Let $\mathfrak{h}_n$ be the $2n+1$-dimensional Heisenberg Lie algebra. Then for all $0 \leq p \leq n$ we have*

$$b_p(\mathfrak{h}_n) = \binom{2n}{p} - \binom{2n}{p-2}.$$

Note that the other half of the Betti numbers is given by the Poincaré duality. For a slighly more complicated Lie algebra we have the following formula for the Betti numbers, see [**1**]:

THEOREM 4.6.7. *Let $\mathfrak{g}_n$ be the Lie algebra of dimension $2n+1$ with basis (x_i, y_i, z), $1 \leq i \leq n$ and Lie brackets $[z, x_i] = y_i$. The for all $0 \leq p \leq 2n+1$ we have*

$$b_p(\mathfrak{g}_n) = \binom{n+1}{\left[\frac{p+1}{2}\right]}\binom{n}{\left[\frac{p}{2}\right]}.$$

For nilpotent Lie algebras $\mathfrak{g}$ admitting an *abelian ideal of codimension* 1 there exists a recursive formula for the Betti numbers $b_p(\mathfrak{g})$ in terms of partitions, see [**2**]. We want to use this for the so called *standard graded filiform nilpotent Lie algebra* $\mathfrak{f}_{n+1}$ of dimension $n+1$ for $n \geq 2$. It is defined by

$$[e_1, e_i] = e_{i+1},\ 2 \leq i \leq n$$

where $(e_1, e_2, \ldots, e_{n+1})$ is a basis of $\mathfrak{f}_{n+1}$. The result is as follows.

PROPOSITION 4.6.8. *The p-th Betti number of $\mathfrak{f}_{n+1}$ is given by*

$$b_p(\mathfrak{f}_{n+1}) = P_{p,n} + P_{p-1,n}$$

for $1 \leq p \leq n+1$, where $P_{0,n} = 1$ and

$$P_{p,n} = \#\Big\{(a_1, \ldots, a_p) \in \mathbb{Z}^p \mid 1 \leq a_1 < \cdots < a_p \leq n,\quad \sum_{j=1}^{p} a_j = \left\lceil \frac{p(n+1)}{2} \right\rceil\Big\}$$

For small p this yields explicit formulas for the Betti numbers $b_p(\mathfrak{f}_n)$:

$$\begin{aligned}
b_1(\mathfrak{f}_n) &= 2 \\
b_2(\mathfrak{f}_n) &= \left\lfloor \frac{n+1}{2} \right\rfloor, \\
b_3(\mathfrak{f}_n) &= \left\lfloor \binom{\frac{n+1}{2}}{2} + \frac{1}{8} \right\rfloor = \left\lfloor \frac{n^2}{8} \right\rfloor, \\
b_4(\mathfrak{f}_n) &= \left\lfloor \frac{4}{3}\binom{\frac{n+1}{2}}{3} + \frac{4n+13}{36} \right\rfloor = \left\lfloor \frac{(n-1)^3+18}{36} \right\rfloor
\end{aligned}$$

The formulas can be derived as follows. Define the q-binomial coefficient by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \prod_{i=0}^{k-1} \frac{1-q^{n-i}}{1-q^{i+1}}.$$

We can rewrite the definition of the sets used for the numbers $P_{p,n}$ by using restricted partitions, i.e.,

$$\begin{aligned} P_{p,n} &= \#\Big\{(b_1,\dots,b_p)\in\mathbb{Z}^p \mid 1\le b_1\le\cdots\le b_p\le n-p+1, \quad \sum_{j=1}^p b_j = s_p\Big\}, \\ s_p &:= \Big\lceil \frac{p(n+1)}{2}\Big\rceil - \frac{p(p-1)}{2}. \end{aligned}$$

Then $P_{p,n}$ is given by the coefficient of x^{s_p} in the series development of

$$\begin{bmatrix} n+1 \\ p \end{bmatrix}_x - \begin{bmatrix} n \\ p-1 \end{bmatrix}_x .$$

This is quite effective for the computation of the numbers $P_{p,n}$. For small p we also can determine the generating function. Then one can derive an explicit formula by using the partial fraction decomposition.

For example, the generating function of $P_{2,n}$ is given by

$$\frac{x^2}{(1-x)(1-x^2)} = x^2 + x^3 + 2x^4 + 2x^5 + 3x^6 + 3x^7 + 4x^8 + 4x^9 + \cdots +$$

of course we have $P_{1,n}=1$ and $P_{2,n}=\lfloor \frac{n}{2}\rfloor$. Furthermore we obtain

$$\begin{aligned} P_{3,n} &= \Big\lfloor \frac{(n-1)^2+4}{8}\Big\rfloor, \\ P_{4,n} &= \Big\lfloor \frac{(n-2)^3+\frac{3}{2}(n-1)^2+18}{36}\Big\rfloor. \end{aligned}$$

The generating functions of $P_{1,n},\dots,P_{7,n}$ are given by

$$
\begin{aligned}
&P_{1,n} : 1,\\
&P_{2,n} : \frac{x^2}{(1-x)(1-x^2)},\\
&P_{3,n} : \frac{x^3(1-x^6)}{(1-x)(1-x^2)(1-x^3)(1-x^4)},\\
&P_{4,n} : \frac{x^4(1+x^3)}{(1-x)(1-x^2)^2(1-x^3)},\\
&P_{5,n} : \frac{x^5(1+x)f_5(x)}{(1-x)(1-x^2)(1-x^4)(1-x^6)(1-x^8)},\\
&P_{6,n} : \frac{x^6(1+x^2+3x^3+4x^4+4x^5+3x^7+x^8+x^{10})}{(1-x)(1-x^2)^2(1-x^3)(1-x^4)(1-x^5)},\\
&P_{7,n} : \frac{x^7 f_7(x)}{g_7(x)},
\end{aligned}
$$

where

$$
\begin{aligned}
f_5(x) &= x^{14} - x^{13} + 2x^{12} + x^{11} + 2x^{10}\\
&\quad + 3x^9 + x^8 + 5x^7 + x^6 + 3x^5 + 2x^4 + x^3 + 2x^2 - x + 1,\\
f_7(x) &= 1 - x + 3x^2 + 3x^3 + 7x^4 + 12x^5 + 16x^6 + 28x^7 + 33x^8 + 46x^9 + 56x^{10} + 73x^{11}\\
&\quad + 83x^{12} + 90x^{13} + 106x^{14} + 109x^{15} + 121x^{16} + 110x^{17} + 121x^{18} + 109x^{19} + 106x^{20}\\
&\quad + 90x^{21} + 83x^{22} + 73x^{23} + 56x^{24} + 46x^{25} + 33x^{26} + 28x^{27} + 16x^{28} + 12x^{29} + 7x^{30}\\
&\quad + 3x^{31} + 3x^{32} - x^{33} + x^{34},\\
g_7(x) &= (1-x)^7(1+x)^5(1+x^2)^3(1-x+x^2)^2(1+x+x^2)^2(1+x^4)(1-x^2+x^4)\\
&\qquad (1-x+x^2-x^3+x^4)(1+x+x^2+x^3+x^4).
\end{aligned}
$$

This can be used to compute the sequence explicitly. For example, the sequence $(P_{5,n})$, $n \geq 5$ starts with

$$
\begin{aligned}
&(1, 1, 3, 6, 12, 20, 32, 49, 73, 102, 141, 190, 252, 325, 414, 521, 649,\\
&795, 967, 1165, 1394, 1651, 1944, 2275, 2649, 3061, 3523, 4035, 4604,\\
&5225, 5910, 6660, 7483, 8372, 9343, 10395, 11538, 12764, 14090, 15516,\\
&17053, 18691, 20451, 22330, 24342, 26476, 28754, 31174, 33751, 36471,\\
&39361, 42416, 45654, 49060, 52662, 56455, 60459, 64656, 69079, 73720,\\
&78602, 83705, 89064, 94671, 100551, 106681, \ldots)
\end{aligned}
$$

Consequently we also can compute the Betti numbers explictly. For example, the Betti numbers of $\mathfrak{f}_n$, for $3 \leq n \leq 15$, are given by

n	$(b_0, \dots, b_n)$
3	$(1, 2, 2, 1)$
4	$(1, 2, 2, 2, 1)$
5	$(1, 2, 3, 3, 2, 1)$
6	$(1, 2, 3, 4, 3, 2, 1)$
7	$(1, 2, 4, 6, 6, 4, 2, 1)$
8	$(1, 2, 4, 8, 10, 8, 4, 2, 1)$
9	$(1, 2, 5, 10, 14, 14, 10, 5, 2, 1)$
10	$(1, 2, 5, 12, 20, 24, 20, 12, 5, 2, 1)$
11	$(1, 2, 6, 15, 28, 38, 38, 28, 15, 6, 2, 1)$
12	$(1, 2, 6, 18, 37, 56, 64, 56, 37, 18, 6, 2, 1)$
13	$(1, 2, 7, 21, 48, 82, 107, 107, 82, 48, 21, 7, 2, 1)$
14	$(1, 2, 7, 24, 61, 116, 167, 188, 167, 116, 61, 24, 7, 2, 1)$
15	$(1, 2, 8, 28, 76, 157, 253, 320, 320, 253, 157, 76, 28, 8, 2, 1)$

However, in general we cannot expect an explicit formula for $b_p(\mathfrak{f}_n)$.

Note that the above sequence of numbers $(b_0, b_1, \dots, b_n)$ is *unimodal*.

Definition 4.6.9. A sequence $(a_0, a_1, \dots a_d)$ of real numbers is called *unimodal*, if there exists a j with $0 \leq j \leq d$, such that $a_i \leq a_{i+1}$ for all $i = 0, \dots, j-1$ and $a_i \geq a_{i+1}$ for all $i = j, \dots, d-1$. The sequence is called *log-concave*, if

$$a_i^2 \geq a_{i-1} a_{i+1}$$

for all $i = 1, \dots, d-1$.

A log-concave sequence with positive terms is unimodal. We have the following result, see [**2**]:

Theorem 4.6.10. *Let $\mathfrak{g}$ be a nilpotent Lie algebra having an abelian ideal of codimension 1. Then the sequence of its Betti numbers is unimodal. In particualr, the sequence of Betti numbers of $\mathfrak{f}_n$ is unimodal.*

For a generalization of the formula for $b_p(\mathfrak{f}_n)$, see [**2**].

It is natural to als also for which nilpotent Lie algebras the sequence of Betti numbers is log-concave. We have the following conjecture.

Conjecture 4.6.11. *The sequence of Betti numbers $(b_1(\mathfrak{f}_n), \dots, b_{n-1}(\mathfrak{f}_n))$ is log-concave, i.e., we have*

$$b_i^2 \geq b_{i-1} b_{i+1}$$

for all $2 \leq i \leq n-2$.

Note that $b_1^2 \geq b_0 b_2$ means $4 \geq \left\lfloor \frac{n+1}{2} \right\rfloor$, which cannot hold as soon as $n \geq 9$. Therefore we need to omit b_0 and b_n in the sequence. For $n \leq 50$ the conjecture is true. This follows from a computation. For the general proof one could use that the partition function $p(n)$ satisfies, for all $n > 25$,

$$p(n)^2 > p(n-1)p(n+1).$$

In other words, the sequence $(p(n))_{n\in\mathbb{N}}$ is log-concave, or satisfies PF_2, with

$$\det\begin{pmatrix} p(n) & p(n+1) \\ p(n-1) & p(n) \end{pmatrix} > 0$$

for $n > 25$. This seemed to be open, but in fact has been proved, see my mathoverflow question number 138321.

On the other hand, the sequence of Betti numbers $(b_0, b_1, \ldots, b_n)$ is not always unimodal for nilpotent Lie algebras. For example, this is *not* the case for the Heisenberg Lie algebras $\mathfrak{h}_n$ discussed above. Indeed, there is a minimum exactly in the middle.

Consider now a family $\mathfrak{t}_n$ of filiform nilpotent Lie algebras with basis $(x_1, \ldots, x_n)$ and Lie brackets

$$[x_1, x_i] = x_{i+1}, \quad 2 \le i \le n-1$$
$$[x_j, x_{n-j+1}] = (-1)^{j+1} x_n, \quad 2 \le j \le n/2$$

Here the sequence of Betti numbers $b_p(\mathfrak{t}_n)$ resembles the one for the Heisenberg Lie algebras. Here is a small list.

n	$(b_0, b_1, \ldots, b_{\frac{n}{2}})$
4	$(1, 2, 2)$
6	$(1, 2, 2, 2)$
8	$(1, 2, 3, 4, 4)$
10	$(1, 2, 4, 8, 9, 8)$
12	$(1, 2, 5, 13, 22, 23, 20)$
14	$(1, 2, 6, 19, 41, 61, 59, 50)$
16	$(1, 2, 7, 26, 68, 129, 177, 163, 134)$
18	$(1, 2, 8, 34, 105, 240, 414, 530, 466, 376)$
20	$(1, 2, 9, 43, 152, 406, 839, 1342, 1630, 1388, 1100)$
22	$(1, 2, 10, 53, 211, 643, 1541, 2929, 4410, 5129, 4243, 3320)$
24	$(1, 2, 11, 64, 284, 970, 2636, 5773, 10252, 14657, 16430, 13278, 10260)$

Hence one would believe that the sequence is not unimodal for $n \ge 10$. This seems to be open, though.

The sum of all Betti numbers is also called the *total cohomology* of $\mathfrak{g}$.

Definition 4.6.12. The *total cohomology* of $\mathfrak{g}$ is the number

$$\sigma(\mathfrak{g}) = \sum_{i=0}^{n} \dim H^i(\mathfrak{g}, K) = \sum_{i=0}^{n} b_i(\mathfrak{g}).$$

There was a claim of Deninger and Singhof in [**9**], Proposition 2.7, that $\sigma(\mathfrak{g}) \equiv 0 \bmod 4$ for nilpotent Lie algebras $\mathfrak{g}$ of dimension $n \ne 1, 3, 7$. However, it turned out to be incorrect. And indeed, our table for the Betti numbers of $\mathfrak{f}_n$ yields another counterexample. We have

$$\sigma(\mathfrak{f}_{15}) = 2 \cdot (1 + 2 + 8 + 28 + 76 + 157 + 253 + 320) = 1690 \equiv 2 \bmod 4.$$

Which Lie algebras $\mathfrak{g}$ then do satisfy $\sigma(\mathfrak{g}) \equiv 0 \mod 4$? Certainly simple Lie algebras of dimension $n > 3$ over $\mathbb{C}$, because then the trivial cohomology is given by an exterior algebra, whose dimension is a power of 2 bigger than 2. In [**6**] the following result is proved.

Theorem 4.6.13. *Let $\mathfrak{g}$ be a unimodular Lie algebra of characteristic not 2, and assume that $n = \dim \mathfrak{g} \not\equiv 3 \mod 4$. Then we have $\sigma(\mathfrak{g}) \equiv 0 \mod 4$.*

The proof uses the *Euler characteristic* $\chi(\mathfrak{g})$ of $\mathfrak{g}$, which is related to $\sigma(\mathfrak{g})$ as follows.

Definition 4.6.14. Let $\mathfrak{g}$ be a Lie algebra of dimension n and M be a finite-dimensional $\mathfrak{g}$-module. Then the number

$$\chi(\mathfrak{g}, M) = \sum_{i=0}^{n} (-1)^i \dim H^i(\mathfrak{g}, M)$$

is called the *Euler-Poincaré characteristic* of $\mathfrak{g}$. If M is the trivial $\mathfrak{g}$-module K, then we write $\chi(\mathfrak{g}) = \chi(\mathfrak{g}, K) = \sum_{i=0}^{n}(-1)^i b_i(\mathfrak{g})$.

We have the following result [**24**]:

Theorem 4.6.15. *Let $\mathfrak{g} \neq 0$ be a finite dimensional Lie algebra over a field K, and M be a finite dimensional $\mathfrak{g}$-module. Assume that we have either $\mathfrak{g} \neq [\mathfrak{g}, \mathfrak{g}]$, or $\operatorname{char}(K) = 0$. Then we have $\chi(\mathfrak{g}, M) = 0$.*

4.7. The Hochschild-Serre formula

In [**16**], Hochschild and Serre introduced a spectral sequence for the cohomology of Lie algebras. We only want to state here some applications of it, from the forth section of this paper.

Let $\mathfrak{g}$ be a Lie algebra, M be a $\mathfrak{g}$-module and $\mathfrak{k}$ be an ideal in $\mathfrak{g}$. So we have the short exact sequence of Lie algebras

$$0 \to \mathfrak{k} \to \mathfrak{g} \to \mathfrak{g}/\mathfrak{k} \to 0.$$

Denote by

$$r_n \colon H(\mathfrak{g}, M) \to H^n(\mathfrak{k}, M)$$

the homomorphism induced by the restriction map of $C^n(\mathfrak{g}, M)$ into $C^n(\mathfrak{k}, M)$ by viewing $\mathfrak{k}$ as a subalgebra of $\mathfrak{g}$. Since $\mathfrak{k}$ is also an ideal in $\mathfrak{g}$, we may regard the cochains for $\mathfrak{g}/\mathfrak{k}$ in $M^{\mathfrak{k}}$ as cochains for $\mathfrak{g}$ in M, in the natural fashion. This gives rise to a natural homomorphism

$$\ell_n \colon H^n(\mathfrak{g}/\mathfrak{k}, M^{\mathfrak{k}}) \to H^n(\mathfrak{g}, M).$$

Assume now that either $m = 1$, or that $H^n(\mathfrak{k}, M) = 0$ for all $0 < n < m$ for a given $m > 1$. Then every element of $H^m(\mathfrak{k}, M)^{\mathfrak{g}}$ has a representing cocycle which is the restriction to $\mathfrak{k}$ of an element $f \in C^m(\mathfrak{g}, M)$, which determines an element of $H^{m+1}/\mathfrak{g}/\mathfrak{k}, M^{\mathfrak{k}})$. This element depends only on the given element of $H^m(\mathfrak{k}, M)^{\mathfrak{g}}$. We denote the reysulting homomorphism by

$$t_{m+1} \colon H^m(\mathfrak{k}, M)^{\mathfrak{g}} \to H^{m+1}(\mathfrak{g}/\mathfrak{k}, M^{\mathfrak{k}}).$$

Theorem 4.7.1. *Let $m \geq 1$ and assume that $H^n(\mathfrak{k}, M) = 0$ for all $0 < n < m$. This is vacuously satisfied for $m = 1$. Then we have a long exact sequence*

$$0 \to H^m(\mathfrak{g}/\mathfrak{k}, M^{\mathfrak{k}}) \xrightarrow{\ell_m} H^m(\mathfrak{g}, M) \xrightarrow{r_m} H^m(\mathfrak{k}, M)^{\mathfrak{g}}$$

$$\xrightarrow{t_{m+1}} H^{m+1}(\mathfrak{g}/\mathfrak{k}, M^{\mathfrak{k}}) \xrightarrow{\ell_{m+1}} H^{m+1}(\mathfrak{g}, M).$$

This induces the following result.

Theorem 4.7.2. *Let $m \geq 1$. If $m > 1$, assume that $H^n(\mathfrak{k}, M) = 0$ for all $2 \leq n \leq m$. Then we have a long exact sequence*

$$\begin{aligned} \cdots \to H^m(\mathfrak{g}/\mathfrak{k}, M^{\mathfrak{k}}) &\xrightarrow{\ell_m} H^m(\mathfrak{g}, M) \xrightarrow{r'_m} H^{m-1}(\mathfrak{g}/\mathfrak{k}, H^1(\mathfrak{k}, M)) \\ &\xrightarrow{d_2} H^{m+1}(\mathfrak{g}/\mathfrak{k}, M^{\mathfrak{k}}) \xrightarrow{\ell_{m+1}} H^{m+1}(\mathfrak{g}, M). \end{aligned}$$

Here, the homomorphism r'_m results by restricting the first argument of a suitably selected cocycle, representing the given cohomology class, to $\mathfrak{k}$.

Finally, let us state the Hochschild-Serre formula, which is Theorem 13 in [**16**] on page 603.

Theorem 4.7.3. *Let $\mathfrak{g}$ be a finite dimensional Lie algebra over a field $\mathbb{F}$ of characteristic zero, $\mathfrak{r}$ be an ideal of $\mathfrak{g}$ such that $\mathfrak{s} := \mathfrak{g}/\mathfrak{r}$ is semisimple. Let M be a $\mathfrak{g}$-module. Then we have*

$$H^n(\mathfrak{g}, M) \cong \bigoplus_{i+j=n} H^i(\mathfrak{s}, \mathbb{F}) \otimes H^j(\mathfrak{g}, M)^{\mathfrak{s}}$$

for all $n \geq 0$.

Bibliography

[1] G. F. Armstrong, G. Cairns, B. Jessup: *Explicit Betti numbers for a family of nilpotent Lie algebras.* Proc. Amer. Math. Soc. **125** (1997), 381–385.

[2] G. F. Armstrong, S. Sigg. *On the cohomology of a class of nilpotent Lie algebras.* Bull. Austral. Math. Soc. **54** (1996), 517–527.

[3] K. S. Brown: *Cohomology of groups.* Springer Verlag **1982**.

[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] G. Cairns, G. Kim: *The mod 4 behaviour of total Lie algebra cohomology.* Arch. Math. **77** (2001), 177–180.

[7] C. Chevalley, S. Eilenberg: *Cohomology theory of Lie groups and Lie algebras.* Trans. AMS **63** (1948), 85–124.

[8] G. Cairns, B. Jessup: *New bounds on the Betti numbers of nilpotent Lie algebras.* Comm. Algebra **25** (1997), 415–430.

[9] C. Deninger, W. Singhof: *On the cohomology of nilpotent Lie algebras.* Bull. Soc. Math. France **116** (1988), 3–14.

[10] G. Cairns, B. Jessup, J. Pitkethly: *On the Betti numbers of nilpotent Lie algebras of small dimension.* Prog. Math. **145** (1997), 19–31.

[11] J. Dixmier: *Cohomologie des algèbres de Lie nilpotentes.* Acta Sci. Math. Szeged **16** (1955), 246–250.

[12] R. Farnsteiner, H. Strade: *Shapiro's lemma and its consequences in the cohomology theory of modular Lie algebras.* Math. Z. **206** (1991), 153–168.

[13] M. Gerstenhaber: *On the deformation of rings and algebras.* Ann. of Math. **79** (1964), 59–104.

[14] M. Gerstenhaber: *On the deformation of rings and algebras: II.* Ann. of Math. **84** (1966), 1–19.

[15] J. Hilgert, K. H. Neeb: *Lie-Gruppen und Lie-Algebren.* Braunschweig: Vieweg Verlag **1991**.

[16] G. Hochschild, J-P. Serre: *Cohomology of Lie algebras.* Ann. Math. (2) **57** (1953), no. 3, 591–603.

[17] N. Jacobson: *A note on automorphisms amd derivations of Lie algebras.* Proc. Amer. Math. Soc. **6**, (1955), 281–283.

[18] J. C. Jantzen, J. Schwermer: *Algebra.* Springer-Verlag (2006).

[19] A. W. Knapp: *Lie groups, Lie algebras, and cohomology.* Princeton University Press **1988**.

[20] H. Koch: *Generator and realtion ranks for finite-dimensional nilpotent Lie algebras.* Algebra Logic **16** (1978), 246–253.

[21] S. Lang: *Algebra.* Revised third edition. Graduate Texts in Mathematics 211. Springer-Verlag, New York, **2002**.

[22] G. Leger, E. Luks: *Cohomology and weight systems for nilpotent Lie algebras.* Bull. Amer. Math. Soc. **80** (1974), 77–80.

[23] A. Nijenhuis, R. W. Richardson: *Deformations of Lie algebra structures.* J. Math. Mech. **17** (1967), 89–105.

[24] T. Pirashvili: *The Euler-Poincaré characteristic of a Lie algebra.* J. Lie Theory. **8**, (1998), 429–431.

[25] G. Rauch: *Effacement et deformation*, Ann. Inst. Fourier **22** (1972), 239–269.

[26] P. Tirao: *A refinement of the toral rank conjecture for 2-step nilpotent Lie algebras.* Proc. Amer. Math. Soc. **128**, (2000), 2875–2878.

[27] A. K. Tolpygo: *Cohomologies of parabolic Lie algebras.* Mathematical Notes of the Academy of Sciences of the USSR **12** (1972), 585–587.

[28] F. Wagemann: *On Lie algebra crossed modules.* Comm. in Algebra **34**, (2006), 1699–1722.

[29] C. A. Weibel: *An introduction to homological algebra.* Cambridge University Press **1997**.

[30] P. Zusmanovich: *A Converse to the Second Whitehead Lemma.* Journal of Lie Theory Volume **18** (2007), 295–299.