Cohomology of Groups

Jun.-Prof. Dr. Caroline Lassueur
TU Kaiserslautern

Lecture Notes, SS 2021
(4SWS Lecture + 2SWS Exercises)

Version: 19th of July 2021

Contents

Foreword

This text constitutes a faithful transcript of the lecture **Cohomology of Groups** held at the TU Kaiserslautern during the Summer Semester 2021 (14 Weeks, 4SWS).

Together with the necessary theoretical foundations the main aims of this lecture are to:

- provide students with a modern approach to **group theory**;
- learn about **homological algebra** and a specific **cohomology theory**;
- consistently work with **universal properties** and get acquainted with the **language of category theory**;
- establish connections between the cohomology of groups and the theory of central extensions of groups as developed by Schur at the beginning of the 1900's.

We assume as pre-requisites bachelor-level algebra courses dealing with linear algebra and elementary group theory, such as the standard lectures *Grundlagen der Mathematik*, *Algebraische Strukturen*, *Einführung in die Algebra*, and *Kommutative Algebra* at the TU Kaiserslautern. In order to complement these pre-requisites, the first chapter will deal formally with more advanced background material on group theory, namely semi-direct products and presentation of groups, while the second chapter will provide a short introduction to the theory of modules, where we will emphasise in particular definitions using universal properties but omit proofs.

I am grateful to Prof. Jacques Thévenaz who provided me with his lecture "Groupes & Cohomologie" (14 weeks, 2SWS) hold at the EPFL in the Autumn Semester 2011, which I used as a basis for the development of this text, and I am grateful to Rafaël Gugliellmetti who provided me with the .tex files of his lecture notes from 2011.

Finally, I am also grateful to the students who mention typos in the preliminary versions of these notes. Further comments, corrections and suggestions are of course more than welcome.

Kaiserslautern, 4th April 2021

Chapter 1. Background Material: Group Theory

The aim of this chapter is to introduce formally two constructions of the theory of groups: *semi-direct products* and *presentations of groups*. Later on in the lecture we will relate semi-direct products with a *1st* and a *2nd cohomology group*. Presentations describe groups by generators and relations in a concise way, they will be useful when considering concrete groups, for instance in examples and in the study of the Schur multiplier.

References:

[Hum96] J. F. Humphreys, *A course in group theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1996.

[Joh90] D. L. Johnson, *Presentations of groups*, London Mathematical Society Student Texts, vol. 15, Cambridge University Press, Cambridge, 1990.

1 Semi-direct Products

The semi-direct product is a construction of the theory of groups, which allows us to build new groups from old ones. It is a natural generalisation of the direct product.

Definition 1.1 (*Semi-direct product*)

A group G is said to be the (internal or inner) **semi-direct product** of a normal subgroup $N \trianglelefteq G$ by a subgroup $H \leqslant G$ if the following conditions hold:

(a) $G = NH$;

(b) $N \cap H = \{1\}$.

Notation: $G = N \rtimes H$.

Example 1

(1) A direct product $G_1 \times G_2$ of two groups is the semi-direct product of $N := G_1 \times \{1\}$ by $H := \{1\} \times G_2$.

(2) $G = S_3$ is the semi-direct product of $N = \langle (1\ 2\ 3) \rangle \trianglelefteq S_3$ and $H = \langle (1\ 2) \rangle \leqslant S_3$.
Since $N \cong C_3$ and $H \cong C_2$, we see that a semi-direct product of an abelian subgroup by an abelian subgroup need not be abelian.

(3) More generally $G = S_n$ ($n \geqslant 3$) is a semi-direct product of $N = A_n \trianglelefteq S_n$ by $H = C_2 = \langle (1\ 2) \rangle$.

Remark 1.2

(a) If G is a semi-direct product of N by H, then the 2nd Isomorphism Theorem yields

$$G/N = HN/N \cong H/H \cap N = H/\{1\} \cong H$$

and this gives rise to a short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1\,.$$

Hence a semi-direct product of N by H is a special case of an **extension of N by H**.

(b) In a semi-direct product $G = N \rtimes H$ of N by H, the subgroup H acts by conjugation on N, namely $\forall h \in H$,

$$\begin{array}{rccc} \theta_h : & N & \longrightarrow & N \\ & n & \mapsto & hnh^{-1} \end{array}$$

is an automorphism of N. In addition $\theta_{hh'} = \theta_h \circ \theta_{h'}$ for every $h, h' \in H$, so that we have a group homomorphism

$$\begin{array}{rccc} \theta : & H & \longrightarrow & \mathrm{Aut}(N) \\ & h & \mapsto & \theta_h\,. \end{array}$$

Proposition 1.3

With the above notation, N, H and θ are sufficient to reconstruct the group law on G.

Proof:
Step 1. Each $g \in G$ can be written in a unique way as $g = nh$ where $n \in N$, $h \in H$.

Condition (a) of the definition proves the existence of such expressions, whereas Condition (b) shows that if $g = nh = n'h'$ with $n, n' \in N$, $h, h' \in H$, then

$$n^{-1}n' = h(h')^{-1} \in N \cap H = \{1\}\,,$$

hence $n = n'$ and $h = h'$.

Step 2. Group law. Let $g_1 = n_1h_1, g_2 = n_2h_2 \in G$ with $n_1, n_2 \in N$, $h_1, h_2 \in H$ as above. Then

$$g_1g_2 = n_1h_1n_2h_2 = n_1\underbrace{h_1n_2(h_1^{-1}}_{\theta_{h_1}(n_2)}h_1)h_2 = [n_1\theta_{h_1}(n_2)] \cdot [h_1h_2]\,.$$

■

With the construction of the group law in the latter proof in mind, we now consider the problem of constructing an "external" (or outer) semi-direct product of groups.

Proposition-Definition 1.4

Let N and H be two arbitrary groups, and let $\theta : H \longrightarrow \mathrm{Aut}(N), h \mapsto \theta_h$ be a group homomorphism. Define $G := N \times H$ as a set. Then the binary operation

$$\begin{array}{cccl} \cdot: & G \times G & \longrightarrow & G \\ & ((n_1, h_1), (n_2, h_2)) & \mapsto & (n_1, h_1) \cdot (n_2, h_2) := (n_1\theta_{h_1}(n_2), h_1h_2) \end{array}$$

defines a group law on G, the neutral element of which is $1_G = (1_N, 1_H)$ and the inverse of $(n, h) \in N \times H$ is $(n, h)^{-1} = (\theta_{h^{-1}}(n^{-1}), h^{-1})$. The group $(G, \cdot)$ is then said to be the **external (or outer) semi-direct product** of N by H with respect to θ, and we write $G = N \rtimes_\theta H$.
Furthermore, G is an internal semi-direct product of $N_0 := N \times \{1\} \cong N$ by $H_0 := \{1\} \times H \cong H$.

Proof: Exercise 2. ■

Example 2

Here are a few examples of very intuitive semi-direct products of groups, which you have very probably already encountered in other lectures, without knowing that they were semi-direct products:

(1) If H acts trivially on N (i.e. $\theta_h = \mathrm{Id}_N \ \forall\, h \in H$), then $N \rtimes_\theta H = N \times H$.

(2) Let $C_m = \langle g \rangle$ and $C_n = \langle h \rangle$ ($m, n \in \mathbb{Z}_{\geqslant 1}$) be finite cyclic groups.
Assume moreover that $k \in \mathbb{Z}$ is such that $k^n \equiv 1 \pmod m$ and set

$$\begin{array}{cccc} \theta\colon & C_n & \longrightarrow & \mathrm{Aut}(C_m) \\ & h^i & \mapsto & (\theta_h)^i, \end{array}$$

where $\theta_h : C_m \longrightarrow C_m, g \mapsto g^k$. Then

$$(\theta_h)^n(g) = (\theta_h)^{n-1}(g^k) = (\theta_h)^{n-2}(g^{k^2}) = \ldots = g^{k^n} = g$$

since $o(g) = m$ and $k^n \equiv 1 \pmod m$. Thus $(\theta_h)^n = \mathrm{Id}_{C_m}$ and θ is a group homomorphism. It follows that under these hypotheses there exists a semi-direct product of C_m by C_n w.r.t. to θ.

Particular case: $m \geqslant 1$, $n = 2$ and $k = -1$ yield the dihedral group D_{2m} of order $2m$ with generators g (of order m) and h (of order 2) and the relation $\theta_h(g) = hgh^{-1} = g^{-1}$.

(3) See also the groups in Exercise 1, Exercise 3, and Exercise 5.

2 Presentations of Groups

Idea: describe a group using a set of generators and a set of relations between these generators, which are sufficient to characterise the group up to isomorphism.

Examples: (1) $C_m = \langle g \rangle = \langle g \mid g^m = 1 \rangle$ 1 generator: g
1 relation: $g^m = 1$

(2) $D_{2m} = C_m \rtimes_\theta C_2$ (see Ex. 2(2)) 2 generators: g, h
3 relations: $g^m = 1, h^2 = 1, hgh^{-1} = g^{-1}$

(3) $\mathbb{Z} = \langle 1_{\mathbb{Z}} \rangle$ 1 generator: $1_{\mathbb{Z}}$
no relation ($\rightsquigarrow$ "free group")

To begin with we examine free groups and generators.

Definition 2.1 (*Free group / Universal property of free groups*)

Let X be a set. A **free group of basis** X (or **free group on** X) is a group F containing X as a subset and satisfying the following universal property. For any group G and for any (set-theoretic) map $f : X \longrightarrow G$, there exists a unique group homomorphism $\tilde{f} : F \longrightarrow G$ such that $\tilde{f}|_X = \tilde{f} \circ i = f$, where $i : X \hookrightarrow F$ denotes the canonical inclusion of X in F. In other words, $\tilde{f}$ is sucht that the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, hook, "i"'] \arrow[dr, phantom, "\circlearrowleft"] & G \\
F \arrow[ur, dashed, "\exists ! \tilde{f}"'] &
\end{tikzcd}$$

Moreover, $|X|$ is called the **rank** of F.

Proposition 2.2

If F exists, then F is the unique free group of basis X up to a unique isomorphism.

Proof: Assume F' is another free group of basis X.
Let $i : X \hookrightarrow F$ be the canonical inclusion of X in F and let $i' : X \hookrightarrow F'$ be the canonical inclusion of X in F'.

$$\begin{tikzcd}
X \arrow[r, hook, "i'"] \arrow[d, hook, "i"'] & F' \arrow[dl, dashed, shift left, "\exists ! \tilde{i}"] \\
F \arrow[ur, dashed, shift left, "\exists ! \tilde{i'}"] &
\end{tikzcd}$$

By the universal property of Definition 2.1, there exists:
- a unique group homomorphism $\tilde{i'} : F \longrightarrow F'$ s.t. $i' = \tilde{i'} \circ i$; and
- a unique group homomorphism $\tilde{i} : F' \longrightarrow F$ s.t. $i = \tilde{i} \circ i'$.

$$\begin{tikzcd}
X \arrow[r, hook, "i"] \arrow[d, hook, "i"'] & F \\
F \arrow[ur, dashed, shift left, "\mathrm{Id}_F"] \arrow[ur, dashed, shift right, "\tilde{i} \circ \tilde{i'}"'] &
\end{tikzcd}$$

Then $(\tilde{i} \circ \tilde{i'})|_X = i$, but obviously we also have $\mathrm{Id}_F|_X = i$. Therefore, by uniqueness, we have $\tilde{i} \circ \tilde{i'} = \mathrm{Id}_F$.

A similar argument yields $\tilde{i'} \circ \tilde{i} = \mathrm{Id}_{F'}$, hence F and F' are isomorphic, up to a unique isomorphism, namely $\tilde{i}$ with inverse $\tilde{i'}$. ■

Proposition 2.3

If F is a free group of basis X, then X generates F.

Proof: Let $H := \langle X \rangle$ be the subgroup of F generated by X, and let $j_H := X \hookrightarrow H$ denote the canonical inclusion of X in H. By the universal property of Definition 2.1, there exists a unique group homomorphism $\widetilde{j_H}$ such that $\widetilde{j_H} \circ i = j_H$:

$$\begin{tikzcd}
X \arrow[r, hook, "j_H"] \arrow[d, hook, "i"'] \arrow[dr, phantom, "\circlearrowleft"] & H \\
F \arrow[ur, dashed, "\exists ! \widetilde{j_H}"'] &
\end{tikzcd}$$

Therefore, letting $\kappa : H \hookrightarrow F$ denote the canonical inclusion of H in F, we have the following commutative diagram:

$$\begin{tikzcd}
X \arrow[r, hook, "j_H"] \arrow[d, hook, "i"'] & H \arrow[r, hook, "\kappa"] & F \\
F \arrow[ur, dashed, "\widetilde{j_H}"] \arrow[urr, shift left, "\mathrm{Id}_F"] \arrow[urr, shift right, "\kappa\circ\widetilde{j_H}"'] & &
\end{tikzcd}$$

Thus by uniqueness $\kappa \circ \widetilde{j_H} = \mathrm{Id}_F$ and it follows that

$$F = \mathrm{Im}(\mathrm{Id}_F) = \mathrm{Im}(\kappa \circ \widetilde{j_H}) = \mathrm{Im}(\widetilde{j_H}) \subseteq H\,,$$

so $F = H$. The claim follows. ■

Theorem 2.4

For any set X, there exists a free group F with basis X.

Proof: Set $X := \{x_\alpha \mid \alpha \in I\}$ where I is a set in bijection with X, set $Y := \{y_\alpha \mid \alpha \in I\}$ in bijection with X but disjoint from X, i.e. $X \cap Y = \emptyset$, and let $Z := X \cup Y$.
Furthermore, set $E := \bigcup_{n=0}^{\infty} Z^n$, where $Z^0 := \{(\ )\}$ (i.e. a singleton), $Z^1 := Z$, $Z^2 := Z \times Z$, ...
Then E becomes a monoid for the concatenation of sequences, that is

$$\underbrace{(z_1,\ldots,z_n)}_{\in Z^n} \cdot \underbrace{(z'_1,\ldots,z'_m)}_{\in Z^m} := \underbrace{(z_1,\ldots,z_n,z'_1,\ldots,z'_n)}_{\in Z^{n+m}}\,.$$

The law $\cdot$ is clearly associative by definition, and the neutral element is the empty sequence $(\ ) \in Z^0$.
Define the following *Elementary Operations* on the elements of E:

Type (1): add in a sequence $(z_1,\ldots,z_n)$ two consecutive elements x_α, y_α and obtain $(z_1,\ldots,z_k,x_\alpha,y_\alpha,z_{k+1},\ldots,z_n)$

Type (1bis): add in a sequence $(z_1,\ldots,z_n)$ two consecutive elements y_α, x_α and obtain $(z_1,\ldots,z_m,y_\alpha,x_\alpha,z_{m+1},\ldots,z_n)$

Type (2): remove from a sequence $(z_1,\ldots,z_n)$ two consecutive elements x_α, y_α and obtain $(z_1,\ldots,z_r,\check{x}_\alpha,\check{y}_\alpha,z_{r+3},\ldots,z_n)$

Type (2bis): remove from a sequence $(z_1,\ldots,z_n)$ two consecutive elements y_α, x_α and obtain $(z_1,\ldots,z_s,\check{y}_\alpha,\check{x}_\alpha,z_{s+3},\ldots,z_n)$

Now define an equivalence relation $\sim$ on E as follows:

two sequences in E are equivalent $:\Longleftrightarrow$ the 2nd sequence can be obtain from the 1st sequence through a succession of Elementary Operations of type (1), (1bis), (2) and (2bis).

It is indeed easily checked that this relation is:
– reflexive: simply use an empty sequence of Elementary Operations;
– symmetric: since each Elementary Operation is invertible;
– transitive: since 2 consecutive sequences of Elementary Operations is again a sequence of Elementary Operations.

Now set $F := E/\sim$, and write $[z_1,\ldots,z_n]$ for the equivalence class of $(z_1,\ldots,z_n)$ in $F = E/\sim$.

Claim 1: The above monoid law on E induces a monoid law on F.
The induced law on F is: $[z_1,\ldots,z_n] \cdot [z'_1,\ldots,z'_m] = [z_1,\ldots,z_n,z'_1,\ldots,z'_m]$.
It is well-defined: if $(z_1,\ldots,z_n) \sim (t_1,\ldots,t_k)$ and $(z'_1,\ldots,z'_m) \sim (t'_1,\ldots,t'_l)$, then

$$\begin{aligned}
(z_1,\ldots,z_n)\cdot(z'_1,\ldots,z'_m) &= (z_1,\ldots,z_n,z'_1,\ldots,z'_m) \\
&\sim (t_1,\ldots,t_k,z'_1,\ldots,z'_m) \quad \text{via Elementary Operations on the 1st part} \\
&\sim (t_1,\ldots,t_k,t'_1,\ldots,t'_l) \quad \text{via Elementary Operations on the 2nd part} \\
&= (t_1,\ldots,t_n)\cdot(t'_1,\ldots,t'_m)
\end{aligned}$$

The associativity is clear, and the neutral element is $[(\ )]$. The claim follows.

Claim 2: F endowed with the monoid law defined in Claim 1 is a group.

Inverses: the inverse of $[z_1, \dots, z_n] \in F$ is the equivalence of the sequence class obtained from $(z_1, \dots, z_n)$ by reversing the order and replacing each x_α with y_α and each y_α with x_α. (Obvious by definition of $\sim$.)

Claim 3: F is a free group on X.

Let G be a group and $f : X \longrightarrow G$ be a map. Set $f(y_\alpha) := f(x_\alpha)^{-1}$ for every $y_\alpha \in Y$ and define

$$\begin{array}{cccc} \hat{f}: & E & \longrightarrow & G \\ & (z_1, \dots, z_n) & \mapsto & f(z_1) \cdot \cdots \cdot f(z_n) . \end{array}$$

Thus, if $(z_1, \dots, z_n) \sim (t_1, \dots, t_k)$, then $\hat{f}(z_1, \dots, z_n) = \hat{f}(t_1, \dots, t_k)$ by definition of f on Y. Hence f induces a map

$$\begin{array}{cccc} \hat{\hat{f}}: & F & \longrightarrow & G \\ & [z_1, \dots, z_n] & \mapsto & f(z_1) \cdot \cdots \cdot f(z_n) , \end{array}$$

By construction $\hat{f}$ is a monoid homomorphism, therfore so is $\hat{\hat{f}}$, but since F and G are groups, $\hat{\hat{f}}$ is in fact a group homomorphism. Hence we have a commutative diagram

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, hook, "i"'] \arrow[dr, phantom, "\circlearrowleft"] & G \\ F \arrow[ur, dashed, "\hat{\hat{f}}"'] & \end{tikzcd}$$

where $i : X \longrightarrow F, x \mapsto [x]$ is the canonical inclusion.

Finally, notice that the definition of $\hat{\hat{f}}$ is forced if we want $\hat{\hat{f}}$ to be a group homorphism, hence we have uniqueness of $\hat{\hat{f}}$, and the universal property of Definition 2.1 is satisfied. ■

Notation and Terminology

- To lighten notation, we identify $[x_\alpha] \in F$ with x_α, hence $[y_\alpha]$ with x_α^{-1}, and $[z_1, \dots, z_n]$ with $z_1 \cdots z_n$ in F.
- A sequence $(z_1, \dots, z_n) \in E$ with each letter z_i ($1 \leqslant i \leqslant n$) equal to an element $x_{\alpha_i} \in X$ or $x_{\alpha_i}^{-1}$ is called a **word** in the generators $\{x_\alpha \mid \alpha \in I\}$. Each word defines an element of F via: $(z_1, \dots, z_n) \mapsto z_1 \cdots z_n \in F$. By abuse of language, we then often also call $z_1 \cdots z_n \in F$ a *word*.
- Two words are called **equivalent** $:\Longleftrightarrow$ they define the same element of F.
- If $(z_1, \dots, z_n) \in Z_n \subseteq E$ ($n \in \mathbb{Z}_{\geqslant 0}$), then n is called the **length** of the word $(z_1, \dots, z_n)$.
- A word is said to be **reduced** if it has minimal length amongst all the words which are equivalent to this word.

Proposition 2.5

Every group G is isomorphic to a factor group of a free group.

Proof: Let $S := \{g_\alpha \in G \mid \alpha \in I\}$ be a set of generators for G (in the worst case, take $I = G$). Let $X := \{x_\alpha \mid \alpha \in I\}$ be a set in bijection with S, and let F be the free group on X. Let $i : X \hookrightarrow F$ denote the canonical inclusion.

$$\begin{tikzcd}
X \arrow[rr, hook, "f"] \arrow[d, hook, "i"'] & & G \\
F \arrow[urr, dashed, "\exists!\tilde{f}"] \arrow[d, two heads, "can.proj."'] \arrow[r, phantom, "\circlearrowleft"] & & \\
F/\ker(\tilde{f}) \arrow[uurr, dashed, "\exists!\hat{\tilde{f}}"'] & &
\end{tikzcd}$$

By the universal property of free groups the map $f : X \hookrightarrow G, x_\alpha \mapsto g_\alpha$ induces a unique group homomorphism $\tilde{f} : F \longrightarrow G$ such that $\tilde{f} \circ i = f$. Clearly $\tilde{f}$ is surjective since the generators of G are all $\mathrm{Im}(\tilde{f})$. Therefore the 1st Isomorphism Theorem yields $G \cong F/\ker(\tilde{f})$.

$\blacksquare$

We can now consider relations between the generators of groups:

Notation and Terminology

Let $S := \{g_\alpha \in G \mid \alpha \in I\}$ be a set of generators for the group G, let $X := \{x_\alpha \mid \alpha \in I\}$ be in bijection with S, and let F be the free group on X.

By the previous proof, $G \cong F/N$, where $N := \ker(\tilde{f})$ ($g_\alpha \leftrightarrow \overline{x_\alpha} := x_\alpha N$ via the homomorphism $\hat{\tilde{f}}$).

Any word $(z_1, \dots, z_n)$ in the x_α's which defines an element of F in N is mapped in G to an expression of the form

$$\overline{z_1} \cdots \overline{z_n} = 1_G \ , \qquad \text{where } \overline{z_i} := \text{image of } z_i \text{ in } G \text{ under the canonical homomorphism.}$$

In this case, the word $(z_1, \dots, z_n)$ is called a **relation in the group G for the set of generators S**.

Now let $R := \{r_\beta \mid \beta \in J\}$ be a set of generators of N as normal subgroup of F (this means that N is generated by the set of all conjugates of R). Such a set R is called a **set of defining relations of G with respect to S**.

Then the ordered pair (X, R) is called a **presentation** of G, and we write

$$G = \langle X \mid R \rangle = \langle \{x_\alpha\}_{\alpha \in I} \mid \{r_\beta\}_{\beta \in J} \rangle .$$

The group G is said to be **finitely presented** if it admits a presentation $G = \langle X \mid R \rangle$, where both $|X|, |R| < \infty$. In this case, by abuse of notation, we shall write presentations under the form

$$G = \langle \overline{x_1}, \dots, \overline{x_{|X|}} \mid \overline{r_1} = 1, \dots, \overline{r_{|R|}} = 1 \rangle$$

or even under the simplified form

$$G = \langle x_1, \dots, x_{|X|} \mid r_1 = 1, \dots, r_{|R|} = 1 \rangle .$$

Example 3

The cyclic group $C_n = \{1, g, \dots, g^{n-1}\}$ of order $n \in \mathbb{Z}_{\geqslant 1}$ generated by $S := \{g\}$. In this case, we have:

$X = \{x\}$
$R = \{x^n\}$
$F = \langle x \rangle \cong (C_\infty, \cdot)$
$\tilde{f} : C_\infty \longrightarrow C_n, x \mapsto g$ has a kernel generated by x^n as a normal subgroup.

Then $C_n = \langle \{x\} \,|\, \{x^n\} \rangle$.
However, by abuse of notation, we one rather writes $C_n = \langle x \mid x^n = 1 \rangle$.

Proposition 2.6 (*Universal property of presentations*)

Let G be a group generated by $S = \{s_\alpha \mid \alpha \in I\}$, isomorphic to a quotient of a free group F on $X = \{x_\alpha \mid \alpha \in I\}$ in bijection with S. Let $R := \{r_\beta \mid \beta \in J\}$ be a set of relations in G.
Then G admits the presentation (X, R), i.e. $G = \langle X \mid R\rangle$, if and only if G satisfies the following universal property:

$$\begin{tikzcd} X \arrow[r, "h"] \arrow[d, "j"'] & H \\ G \arrow[ur, dashed, "\circlearrowleft", "\exists!\overline{h}"'] & \end{tikzcd}$$

For every group H, and for every set-theoretic map $h : X \longrightarrow H$ such that $\tilde{h}(r_\beta) = 1_H \ \forall\, r_\beta \in R$, there exists a unique group homomorphism $\overline{h} : G \longrightarrow H$ such that $\overline{h} \circ j = h$, where $j : X \longrightarrow G, x_\alpha \mapsto s_\alpha$, and $\tilde{h}$ is the unique extension of h to the free group F on X given by Definition 2.1.

Proof: "$\Rightarrow$": Suppose that $G = \langle X \mid R\rangle$. Therefore $G \cong F/N$, where N is generated by R as normal subgroup. Thus the condition $\tilde{h}(r_\beta) = 1_H \ \forall\, r_\beta \in R$ implies that $N \subseteq \ker(\tilde{h})$, since

$$\tilde{h}(zr_\beta z^{-1}) = \tilde{h}(z)\, \underbrace{\tilde{h}(r_\beta)}_{=1_H}\, \tilde{h}(z)^{-1} = 1_H \qquad \forall\, r_\beta \in R, \forall\, z \in F.$$

Therefore, by the universal property of the quotient, $\tilde{h}$ induces a unique group homomorphism $\overline{h} : G \cong F/N \longrightarrow H$ such that $\overline{h} \circ \pi = \tilde{h}$, where $\pi : F \longrightarrow F/N$ is the quotient morphism. Now, if $i : X \longrightarrow F$ denotes the canonical inclusion, then $j = \pi \circ i$, and as a consequence we have $\overline{h} \circ j = h$.

"$\Leftarrow$": Conversely, assume that G satisfies the universal property of the statement (i.e. relatively to X, F, R). Set $N := \overline{R}$ for the normal closure of R. Then we have two group homomorphisms:

$$\begin{array}{rccc} \varphi: & F/N & \longrightarrow & G \\ & \overline{x_\alpha} & \mapsto & s_\alpha \end{array}$$

induced by $\tilde{h} : F \longrightarrow G$ (by the universal property of the quotient), and

$$\begin{array}{rccc} \psi: & G & \longrightarrow & F/N \\ & s_\alpha & \mapsto & \overline{x_\alpha} \end{array}$$

given by the universal property of the assumption. Then clearly $\varphi \circ \psi(s_\alpha) = \varphi(\overline{x_\alpha}) = s_\alpha$ for each $\alpha \in I$, so that $\varphi \circ \psi = \mathrm{Id}_G$ and similarly $\psi \circ \varphi = \mathrm{Id}_{F/N}$, hence $G \cong F/N$ and the claim follows. ■

Example 4 (*The dihedral groups*)

Consider the finite dihedral group D_{2m} of order $2m$ with $2 \leqslant m < \infty$, that is, the isometry group of the regular m-gone. We can assume that D_{2m} is generated by

$$r := \text{ rotation of angle } \frac{2\pi}{m} \quad \text{ and } \quad s := \text{ symmetry through the origin in } \mathbb{R}^2 .$$

Then $\langle r\rangle \cong C_m$, $\langle s\rangle \cong C_2$ and we have seen that $D_{2m} = \langle r\rangle \rtimes \langle s\rangle$ with three obvious relations $r^m = 1$, $s^2 = 1$, and $srs^{-1} = r^{-1}$.

Claim: D_{2m} admits the presentation $\langle r, s \mid r^m = 1, s^2 = 1, srs^{-1} = r^{-1}\rangle$.

In order to prove the Claim, we let F be the free group on $X := \{x, y\}$, $R := \{x^m, y^2, yxy^{-1}x\}$, $N \trianglelefteq F$ be the normal subgroup generated by R, and $G := F/N$ so that

$$G = \langle \overline{x}, \overline{y} \mid \overline{x}^m = 1, \overline{y}^2 = 1, \overline{y}\,\overline{x}\,\overline{y}^{-1}\overline{x} = 1\rangle .$$

By the universal property of presentations the map

$$\begin{array}{rccc} h: & \{x, y\} & \longrightarrow & D_{2m} \\ & x & \mapsto & r \\ & y & \mapsto & s \end{array}$$

induces a group homomorphism

$$\begin{array}{rccl} \overline{h}\colon & G & \longrightarrow & D_{2m} \\ & \overline{x} & \mapsto & r \\ & \overline{y} & \mapsto & s\,, \end{array}$$

because

$$\tilde{h}(x^m) = h(x)^m = r^m = 1_{D_{2m}}\,,$$
$$\tilde{h}(y^2) = h(y)^2 = s^2 = 1_{D_{2m}}\,,$$
$$\tilde{h}(yxy^{-1}x) = h(y)h(x)h(y)^{-1}h(x) = srs^{-1}r = 1_{D_{2m}}\,.$$

Clearly $\overline{h}$ is surjective since $D_{2m} = \langle r, s\rangle$. In order to prove that $\overline{h}$ is injective, we prove that G is a group of order at most $2m$. Recall that each element of G is an expression in $\overline{x}, \overline{y}, \overline{x}^{-1}, \overline{y}^{-1}$, hence actually an expression in $\overline{x}, \overline{y}$, since $\overline{x}^{-1} = \overline{x}^{m-1}$ and $\overline{y}^{-1} = \overline{y}$. Moreover, $\overline{yxy}^{-1} = \overline{x}^{-1}$ implies $\overline{yx} = \overline{x}^{-1}\overline{y}$, hence we are left with expressions of the form

$$\overline{x}^a\overline{y}^b \qquad \text{with } 0 \leqslant a \leqslant m-1 \text{ and } 0 \leqslant b \leqslant 1\,.$$

Thus we have $|G| \leqslant 2m$, and it follows that $\overline{h}$ is an isomorphism.

Notice that if we remove the relation $r^m = 1$, we can also formally define an *infinite dihedral group* D_∞ via the following presentation

$$D_\infty := \langle r, s \mid s^2 = 1, srs^{-1} = r^{-1}\rangle\,.$$

Theorem 2.7

Let G be a group generated by two distinct elements, s and t, both of order 2. Then $G \cong D_{2m}$, where $2 \leqslant m \leqslant \infty$ is the order of st in G, and

$$G = \langle s, t \mid s^2 = 1, t^2 = 1, (st)^m = 1\rangle\,.$$

(Here $m = \infty$ simply means "no relation".)

Proof: The theorem can be proved through the following steps. Set $r := st$ and let m be the order of r. Set $H := \langle r\rangle \cong C_m$ and $C := \langle s\rangle \cong C_2$.

1. Prove that $m \geqslant 2$ and $srs^{-1} = r^{-1}$.
2. Prove that $G = H \rtimes C = D_{2m}$.
3. By Step 2. and Example 4, G admits the presentation $\langle r, s \mid r^m = 1, s^2 = 1, srs^{-1} = 1\rangle$. Apply the universal property of presentations twice to prove that G also admits the presentation $\langle s, t \mid s^2 = 1, t^2 = 1, (st)^m = 1\rangle$.

See Exercise 8. ■

Remark 2.8

The presentation of D_{2m} ($2 \leqslant m \leqslant \infty$) is the standard presentation of the dihedral group of order $2m$ seen as a Coxeter group (the Coxeter group associated to the graph $\mathrm{I}_2(m)$).

3 Exercises for Chapter 1

Exercise 1

Let K be a field.

(a) Prove that
$$\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes \left\{\mathrm{diag}(\lambda, 1, \dots, 1) \in \mathrm{GL}_n(K) \mid \lambda \in K^\times\right\} ,$$
where $\mathrm{diag}(\lambda, 1, \dots, 1)$ is the diagonal matrix with (ordered) diagonal entries $\lambda, 1, \dots, 1$. Describe the action.

(b) Let
$$B := \left\{ \begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix} \in \mathrm{GL}_n(K) \right\} \quad (= \text{upper triangular matrices}),$$
$$U := \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathrm{GL}_n(K) \right\} \quad (= \text{upper unitriangular matrices}),$$
$$T := \left\{ \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \in \mathrm{GL}_n(K) \right\} \quad (= \text{diagonal matrices}).$$
Prove that B is a semi-direct product of U by T, that is, $B = U \rtimes T$. Describe the action.

Exercise 2

Let N and H be two arbitrary groups, and let $\theta : H \longrightarrow \mathrm{Aut}(N), h \mapsto \theta_h$ be a group homomorphism. Set $G := N \times H$ as a set. Prove that:

(a) The binary operation
$$\begin{array}{rccl} \cdot : & G \times G & \longrightarrow & G \\ & \big((n_1, h_1), (n_2, h_2)\big) & \mapsto & (n_1, h_1) \cdot (n_2, h_2) := (n_1\theta_{h_1}(n_2), h_1h_2) \end{array}$$
defines a group law on G. The neutral element is $1_G = (1_N, 1_H)$ and the inverse of $(n, h) \in N \times H$ is $(n, h)^{-1} = (\theta_{h^{-1}}(n^{-1}), h^{-1})$.

(b) The group G is an internal semi-direct product of $N_0 := N \times \{1\} \cong N$ by $H_0 := \{1\} \times H \cong H$.

Exercise 3

(a) Prove that $D_8 \cong V_4 \rtimes C_2$, where V_4 is the Klein-four group. Describe the action of C_2 on V_4.

(b) Prove that $\mathfrak{S}_4 \cong V_4 \rtimes \mathfrak{S}_3$. Deduce that a Sylow 2-subgroup of $\mathfrak{S}_4$ is isomorphic to D_8.

(c) Construct all semi-direct products of C_3 by C_3 up to isomorphism.

(d) Identify the group described in Example 1.2(2) when $m = 7$, $n = 3$ and $k = 2$. (Hint. Is it an abelian group?)

Exercise 4

Let $N \rtimes_\theta H$ be an external semi-direct product of a group N by a group H with respect to $\theta : H \longrightarrow \mathrm{Aut}(N), h \mapsto \theta_h$. Assume moreover that H acts on N by inner automorphisms of N, that is, for every $h \in H$ and every $n \in N$, we have

$$\theta_h(n) = \varphi(h)n\varphi(h)^{-1}$$

where $\varphi : H \longrightarrow N$ is a group homomorphism. Prove that

$$N \rtimes_\theta H \cong N \times H\,.$$

Exercise 5

Let $\mathrm{Aff}(\mathbb{R}^n)$ denote the group of affine transformations of $\mathbb{R}^n$, i.e. the group generated by the translations and the invertible linear transformations of $\mathbb{R}^n$. Prove that

$$\mathrm{Aff}(\mathbb{R}^n) \cong \mathbb{R}^n \rtimes_\theta \mathrm{GL}_n(\mathbb{R})\,,$$

where $\theta : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathrm{Aut}(\mathbb{R}^n)$ is the automorphism induced by the natural action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$.

Exercise 6

(a) Let X and Y be two sets with the same cardinality. Prove that $F_X \cong F_Y$.
[Notice that the converse holds as well. You can try to find a proof too, but arguments are more involved.]

(b) Prove that in a free group, every equivalence class of words contains a unique reduced word.

(c) How many reduced words of length $\ell \geqslant 1$ are there in a free group of rank $r \in \mathbb{Z}_{>0}$?

Exercise 7

Let $G = \langle x, y \mid x^2 = y^2 = (xy)^2 \rangle$. Prove that G is a finite group, determine its order and identify this group up to isomorphism.
[Hint. Draw the Cayley graph of G. Consider $Z(G)$ and $G/Z(G)$.]

Exercise 8

Prove Theorem 2.7 through the following steps. Set $r := st$ and let m be the order of r. Set $H := \langle r \rangle \cong C_m$ and $C := \langle s \rangle \cong C_2$.

1. Prove that $m \geqslant 2$ and $srs^{-1} = r^{-1}$.

2. Prove that $G = H \rtimes C = D_{2m}$.

3. By 2. and Example 4, G admits the presentation $\langle r, s \mid r^m = 1, s^2 = 1, srs^{-1} = 1 \rangle$. Apply the universal property of presentations twice to prove that G also admits the presentation $\langle s, t \mid s^2 = 1, t^2 = 1, (st)^m = 1 \rangle$.

Chapter 2. Background Material: Module Theory

The aim of this chapter is to recall the basics of the theory of modules, which we will use throughout. We review elementary constructions such as quotients, direct sum, direct products, exact sequences, free/projective/injective modules and tensor products, where we emphasise the approach via universal properties. Particularly important for the forthcoming homological algebra and cohomology of groups are the notions of free and projective modules and the snake lemma.

Notation: throughout this chapter we let R and S denote rings, and, unless otherwise specified, all rings are assumed to be *unital* and *associative*.

Most results are stated without proof, as they have been / will be studied in the B.Sc. lecture *Commutative Algebra*. As further reference we recommend for example:

Reference:

[Rot10] J. J. Rotman, *Advanced modern algebra. 2nd ed.*, Providence, RI: American Mathematical Society (AMS), 2010.

4 Modules, Submodules, Morphisms

Definition 4.1 (*Left R-module, right R-module, (R,S)-bimodule*)

(a) A **left R-module** is an ordered triple $(M,+,\cdot)$, where $(M,+)$ is an abelian group and $\cdot : R\times M \longrightarrow M, (r,m)\mapsto r\cdot m$ is a binary operation such that the map

$$\begin{array}{rccl} \lambda\colon & R & \longrightarrow & \operatorname{End}(M) \\ & r & \mapsto & \lambda(r) := \lambda_r : M \longrightarrow M, m \mapsto r\cdot m \end{array}$$

is a ring homomorphism. The operation $\cdot$ is called a **scalar multiplication** or an **external composition law**.

(b) A **right R-module** is defined analogously using a scalar multiplication $\cdot : M\times R\longrightarrow M$, $(m,r)\mapsto m\cdot r$ on the right-hand side.

(c) An **(R,S)-bimodule** is an abelian group $(M,+)$ which is both a left R-module and a right S-module, and which satisfies the axiom

$$r\cdot(m\cdot s) = (r\cdot m)\cdot s \qquad \forall\, r\in R, \forall\, s\in S, \forall\, m\in M\,.$$

Convention: Unless otherwise stated, in this lecture we always work with left modules. When no confusion is to be made, we will simply write "R-module" to mean "left R-module", denote R-modules by their underlying sets and write rm instead of $r \cdot m$. Definitions for right modules and bimodules are similar to those for left modules, hence in the sequel we omit them.

Definition 4.2 (*R-submodule*)

An R-**submodule** of an R-module M is a subgroup $U \leqslant M$ such that $r \cdot u \in U \ \forall\ r \in R, \forall\ u \in U$.

Definition 4.3 (*Morphisms*)

A **(homo)morphism** of R-modules (or an R**-linear map**, or an R**-homomorphism**) is a map of R-modules $\varphi : M \longrightarrow N$ such that:

(i) φ is a group homomorphism; and

(ii) $\varphi(r \cdot m) = r \cdot \varphi(m) \ \forall\ r \in R, \forall\ m \in M$.

Furthermore:

- An injective (resp. surjective) morphism of R-modules is sometimes called a **monomorphism** (resp. an **epimorphism**) and we often denote it with a *hook arrow* "$\hookrightarrow$" (resp. a *two-head arrow* "$\twoheadrightarrow$").
- A bijective morphism of R-modules is called an **isomorphism** (or an R**-isomorphism**), and we write $M \cong N$ if there exists an R-isomorphism between M and N.
- A morphism from an R-module to itself is called an **endomorphism** and a bijective endomorphism is called an **automorphism** .

Notation: We let **Ab** denote the category of abelian groups, we let ${}_R$**Mod** denote the category of left R-modules (with R-homomorphisms as morphisms), we let **Mod**$_R$ denote the category of right R-modules (with R-homomorphisms as morphisms), and we let ${}_R$**Mod**$_S$ denote the category of (R, S)-bimodules (with (R, S)-homomorphisms as morphisms).

Example 5

(a) Definition 4.1(a) is equivalent to requiring that $(M, +, \cdot)$ satisfies the following axioms:

(M1) $(M, +)$ is an abelian group;

(M2) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ for each $r_1, r_2 \in R$ and each $m \in M$;

(M3) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ for each $r \in R$ and all $m_1, m_2 \in M$;

(M4) $(rs) \cdot m = r \cdot (s \cdot m)$ for each $r, s \in R$ and all $m \in M$.

(M5) $1_R \cdot m = m$ for each $m \in M$.

In other words, modules over rings satisfy the same axioms as vector spaces over fields. Hence: Vector spaces over a field K are K-modules, and conversely.

(b) Abelian groups are $\mathbb{Z}$-modules, and conversely.

(c) If the ring R is commutative, then any right module can be made into a left module, and conversely.

(d) If $\varphi : M \longrightarrow N$ is a morphism of R-modules, then the kernel

$$\ker(\varphi) := \{m \in M \mid \varphi(m) = 0_N\}$$

of φ is an R-submodule of M and the image

$$\mathrm{Im}(\varphi) := \varphi(M) = \{\varphi(m) \mid m \in M\}$$

of φ is an R-submodule of N.
If $M = N$ and φ is invertible, then the inverse is the usual set-theoretic *inverse map* φ^{-1} and is also an R-homomorphism.

(e) **Change of the base ring**. If $\varphi : S \longrightarrow R$ is a ring homomorphism, then every R-module M can be endowed with the structure of an S-module with external composition law given by

$$\begin{array}{rccl} \cdot : & S \times M & \longrightarrow & M \\ & (s, m) & \mapsto & s \cdot m := \varphi(s) \cdot m\,. \end{array}$$

Notation 4.4

Given R-modules M and N, we set $\mathrm{Hom}_R(M, N) := \{\varphi : M \longrightarrow N \mid \varphi \text{ is an } R\text{-homomorphism}\}$. This is an abelian group for the pointwise addition of maps:

$$\begin{array}{rccl} + : & \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(M, N) & \longrightarrow & \mathrm{Hom}_R(M, N) \\ & (\varphi, \psi) & \mapsto & \varphi + \psi : M \longrightarrow N, m \mapsto \varphi(m) + \psi(m)\,. \end{array}$$

In case $N = M$, we write $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ for the set of endomorphisms of M and $\mathrm{Aut}_R(M)$ for the set of automorphisms of M, i.e. the set of invertible endomorphisms of M.

Lemma-Definition 4.5 (*Quotients of modules*)

Let U be an R-submodule of an R-module M. The quotient group M/U can be endowed with the structure of an R-module in a natural way via the external composition law

$$\begin{aligned} R \times M/U &\longrightarrow M/U \\ \big(r, m + U\big) &\longmapsto r \cdot m + U \end{aligned}$$

The canonical map $\pi : M \longrightarrow M/U, m \mapsto m + U$ is R-linear and we call it the **canonical** (or **natural**) **homomorphism** or the **quotient homomorphism**.

Definition 4.6 (*Cokernel, coimage*)

Let $\varphi \in \mathrm{Hom}_R(M, N)$. The **cokernel** of φ is the quotient R-module $\mathrm{coker}(\varphi) := N/\mathrm{Im}\,\varphi$, and the **coimage** of φ is the quotient R-module $M/\ker\varphi$.

Theorem 4.7 (***The universal property of the quotient and the isomorphism theorems***)

Let M, N be R-modules.

(a) **Universal property of the quotient**. Let $\varphi \in \mathrm{Hom}_R(M,N)$. If U is an R-submodule of M such that $U \subseteq \ker(\varphi)$, then there exists a unique R-module homomorphism $\overline{\varphi} : M/U \longrightarrow N$ such that $\overline{\varphi} \circ \pi = \varphi$, or in other words such that the following diagram commutes:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & N \\ M/U \arrow[ur, dashed, "\exists!\,\overline{\varphi}"'] & \end{tikzcd}$$

Concretely, $\overline{\varphi}(m+U) = \varphi(m)\ \forall\ m+U \in M/U$.

(b) **1st isomorphism theorem**. With the notation of (a), if $U = \ker(\varphi)$, then

$$\overline{\varphi} : M/\ker(\varphi) \longrightarrow \mathrm{Im}(\varphi)$$

is an isomorphism of R-modules.

(c) **2nd isomorphism theorem**. If U_1, U_2 are R-submodules of M, then so are $U_1 \cap U_2$ and $U_1 + U_2$, and there is an isomorphism of R-modules

$$(U_1 + U_2)/U_2 \cong U_1/(U_1 \cap U_2)\,.$$

(d) **3rd isomorphism theorem**. If $U_1 \subseteq U_2$ are R-submodules of M, then there is an isomorphism of R-modules

$$(M/U_1)\big/(U_2/U_1) \cong M/U_2\,.$$

(e) **Correspondence theorem**. If U is an R-submodule of M, then there is a bijection

$$\begin{array}{ccc} \{R\text{-submodules } X \text{ of } M \mid U \subseteq X\} & \longleftrightarrow & \{R\text{-submodules of } M/U\} \\ X & \mapsto & X/U \\ \pi^{-1}(Z) & \leftarrow\!\shortmid & Z\,. \end{array}$$

5 Direct Products and Direct Sums

Let $\{M_i\}_{i\in I}$ be a family of R-modules. Then the abelian group $\prod_{i\in I} M_i$, that is the product of $\{M_i\}_{i\in I}$ seen as a family of abelian groups, becomes an R-module via the following external composition law:

$$\begin{aligned} R \times \prod_{i\in I} M_i &\longrightarrow \prod_{i\in I} M_i \\ (r, (m_i)_{i\in I}) &\longmapsto (r\cdot m_i)_{i\in I}\,. \end{aligned}$$

Furthermore, for each $j \in I$, we let $\pi_j : \prod_{i\in I} M_i \longrightarrow M_j, (m_i)_{i\in I} \mapsto m_j$ denotes the j-th projection from the product to the module M_j.

Proposition 5.1 (Universal property of the direct product)

If $\{\varphi_i : L \longrightarrow M_i\}_{i\in I}$ is a family of R-homomorphisms, then there exists a unique R-homomorphism $\varphi : L \longrightarrow \prod_{i\in I} M_i$ such that $\pi_j \circ \varphi = \varphi_j$ for every $j \in I$.

$$\begin{tikzcd}
 & & L \arrow[ldd, bend right, "\varphi_k"'] \arrow[d, dotted, "\varphi"] \arrow[rdd, bend left, "\varphi_j"] & & \\
\cdots & \circlearrowleft & \prod_{i\in I} M_i \arrow[ld, "\pi_k"] \arrow[rd, "\pi_j"'] & \circlearrowleft & \cdots \\
 & M_k & & M_j &
\end{tikzcd}$$

Thus,

$$\begin{aligned} \mathrm{Hom}_R\Big(L, \prod_{i\in I} M_i\Big) &\longrightarrow \prod_{i\in I} \mathrm{Hom}_R(L, M_i) \\ f &\longmapsto \big(\pi_i \circ f\big)_{i\in I} \end{aligned}$$

is an isomorphism of abelian groups.

Now let $\bigoplus_{i\in I} M_i$ be the subgroup of $\prod_{i\in I} M_i$ consisting of the elements $(m_i)_{i\in I}$ such that $m_i = 0$ almost everywhere (i.e. $m_i = 0$ exept for a finite subset of indices $i \in I$). This subgroup is called the **direct sum** of the family $\{M_i\}_{i\in I}$ and is in fact an R-submodule of the product. For each $j \in I$, we let $\eta_j : M_j \longrightarrow \bigoplus_{i\in I} M_i, m_j \mapsto$ denote the canonical injection of M_j in the direct sum.

Proposition 5.2 (Universal property of the direct sum)

If $\{f_i : M_i \longrightarrow L\}_{i\in I}$ is a family of R-homomorphisms, then there exists a unique R-homomorphism $\varphi : \bigoplus_{i\in I} M_i \longrightarrow L$ such that $f \circ \eta_j = f_j$ for every $j \in I$.

$$\begin{tikzcd}
 & & L & & \\
\cdots & \circlearrowleft & \bigoplus_{i\in I} M_i \arrow[u, dotted, "f"] & \circlearrowleft & \cdots \\
 & M_k \arrow[ruu, bend left, "f_k"] \arrow[ru, "\eta_k"'] & & M_j \arrow[luu, bend right, "f_j"'] \arrow[lu, "\eta_j"] &
\end{tikzcd}$$

Thus,

$$\begin{aligned} \mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, L\Big) &\longrightarrow \prod_{i\in I} \mathrm{Hom}_R(M_i, L) \\ f &\longmapsto \big(f \circ \eta_i\big)_{i\in I} \end{aligned}$$

is an isomorphism of abelian groups.

Remark 5.3

It is clear that if $|I| < \infty$, then $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$.

The direct sum as defined above is often called an *external* direct sum. This relates as follows with the usual notion of *internal* direct sum:

Definition 5.4 (*Internal direct sums*)

Let M be an R-module and N_1, N_2 be two R-submodules of M. We write $M = N_1 \oplus N_2$ if every $m \in M$ can be written in a unique way as $m = n_1 + n_2$, where $n_1 \in N_1$ and $n_2 \in N_2$.

In fact $M = N_1 \oplus N_2$ (internal direct sum) if and only if $M = N_1 + N_2$ and $N_1 \cap N_2 = \{0\}$.

Proposition 5.5

If N_1, N_2 and M are as above and $M = N_1 \oplus N_2$ then the homomorphism of R-modules

$$\begin{array}{cccc} \varphi\colon & M & \longrightarrow & N_1 \times N_2 = N_1 \oplus N_2 \ \text{(external direct sum)} \\ & m = n_1 + n_2 & \mapsto & (n_1, n_2), \end{array}$$

is an isomorphism of R-modules.

The above generalises to arbitrary internal direct sums $M = \bigoplus_{i\in I} N_i$.

6 Exact Sequences

Definition 6.1 (*Exact sequence*)

A sequence $L \xrightarrow{\varphi} M \xrightarrow{\psi} N$ of R-modules and R-homomorphisms is said to be **exact** (**at** M) if $\operatorname{Im}\varphi = \ker\psi$.

Remark 6.2 (*Injectivity/surjectivity/short exact sequences*)

(a) $L \xrightarrow{\varphi} M$ is injective $\Longleftrightarrow 0 \longrightarrow L \xrightarrow{\varphi} M$ is exact at L.

(b) $M \xrightarrow{\psi} N$ is surjective $\Longleftrightarrow M \xrightarrow{\psi} N \longrightarrow 0$ is exact at N.

(c) $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ is exact (i.e. at L, M and N) if and only if φ is injective, ψ is surjective and ψ induces an isomorphism $\overline{\psi} : M/\operatorname{Im}\varphi \longrightarrow N$.
Such a sequence is called a **short exact sequence** (s.e.s. in short).

(d) If $\varphi \in \operatorname{Hom}_R(L, M)$ is an injective morphism, then there is a s.e.s.

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\pi} \operatorname{coker}(\varphi) \longrightarrow 0$$

where π is the canonical projection.

(d) If $\psi \in \operatorname{Hom}_R(M, N)$ is a surjective morphism, then there is a s.e.s.

$$0 \longrightarrow \ker(\varphi) \xrightarrow{i} M \xrightarrow{\psi} N \longrightarrow 0\,,$$

where i is the canonical inclusion.

Proposition 6.3

Let Q be an R-module. Then the following holds:

(a) $\mathrm{Hom}_R(Q,-) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a *left* exact covariant functor. In other words, if $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ is a s.e.s of R-modules, then the induced sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_R(Q,L) \arrow[r, "\varphi_*"] & \mathrm{Hom}_R(Q,M) \arrow[r, "\psi_*"] & \mathrm{Hom}_R(Q,N) \end{tikzcd}$$

is an exact sequence of abelian groups. (Here $\varphi_* := \mathrm{Hom}_R(Q,\varphi)$, that is $\varphi_*(\alpha) = \varphi \circ \alpha$ and similarly for ψ_*.)

(b) $\mathrm{Hom}_R(-,Q) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a *left* exact contravariant functor. In other words, if $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ is a s.e.s of R-modules, then the induced sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_R(N,Q) \arrow[r, "\psi^*"] & \mathrm{Hom}_R(M,Q) \arrow[r, "\varphi^*"] & \mathrm{Hom}_R(L,Q) \end{tikzcd}$$

is an exact sequence of abelian groups. (Here $\varphi^* := \mathrm{Hom}_R(\varphi,Q)$, that is $\varphi^*(\alpha) = \alpha \circ \varphi$ and similarly for ψ^*.)

Remark 6.4

Notice that $\mathrm{Hom}_R(Q,-)$ and $\mathrm{Hom}_R(-,Q)$ are not *right* exact in general. See Exercise 12.

Lemma 6.5 (*The snake lemma*)

Suppose we are given the following commutative diagram of R-modules and R-module homomorphisms with exact rows:

$$\begin{tikzcd} & L \arrow[r, "\varphi"] \arrow[d, "f"] & M \arrow[r, "\psi"] \arrow[d, "g"] & N \arrow[r] \arrow[d, "h"] & 0 \\ 0 \arrow[r] & L' \arrow[r, "\varphi'"] & M' \arrow[r, "\psi'"] & N' & \end{tikzcd}$$

Then the following hold:

(a) There exists an exact sequence

$$\begin{tikzcd} \ker f \arrow[r, "\varphi"] & \ker g \arrow[r, "\psi"] & \ker h \arrow[r, "\delta"] & \operatorname{coker} f \arrow[r, "\overline{\varphi'}"] & \operatorname{coker} g \arrow[r, "\overline{\psi'}"] & \operatorname{coker} h, \end{tikzcd}$$

where $\overline{\varphi'}, \overline{\psi'}$ are the morphisms induced by the universal property of the quotient, and $\delta(n) = \pi_L \circ \varphi'^{-1} \circ g \circ \psi^{-1}(n)$ for every $n \in \ker(h)$ (here $\pi_L : L \longrightarrow \operatorname{coker}(f)$ is the canonical homomorphism). The map δ is called the **connecting homomorphism**.

(b) If $\varphi : L \longrightarrow M$ is injective, then $\varphi|_{\ker f} : \ker f \longrightarrow \ker g$ is injective.

(c) If $\psi' : M' \longrightarrow N'$ is surjective, then $\overline{\psi'} : \operatorname{coker} g \longrightarrow \operatorname{coker} h$ is surjective.

Proof: (a) First, we check that δ is well-defined. Let $n \in \ker h$ and choose two preimages $m_1, m_2 \in M$ of n under ψ. Hence $m_1 - m_2 \in \ker \psi = \operatorname{Im} \varphi$. Thus, there exists $l \in L$ such that $m_1 = \varphi(l) + m_2$. Then, we have

$$g(m_1) = g \circ \varphi(l) + g(m_2) = \varphi' \circ f(l) + g(m_2).$$

Since $n \in \ker h$, for $i \in \{1,2\}$ we have

$$\psi' \circ g(m_i) = h \circ \psi(m_i) = h(n) = 0,$$

so that $g(m_i) \in \ker \psi' = \operatorname{Im} \varphi'$. Therefore, there exists $l'_i \in L'$ such that $\varphi'(l'_i) = g(m_i)$. It follows that

$$g(m_2) = \varphi'(l'_2) = \varphi' \circ f(l) + \varphi'(l'_1).$$

Since φ' is injective, we obtain $l'_2 = f(l) + l'_1$. Hence, l'_1 and l'_2 have the same image in $\operatorname{coker} f$. Therefore, δ is well-defined.

We now want to check the exactness at $\ker h$. Let $m \in \ker g$. Then $g(m) = 0$, so that $\delta\psi(m) = 0$ and thus $\operatorname{Im} \psi|_{\ker h} \subset \ker \delta$. Conversely, let $m \in \ker \delta$. With the previous notation, this means that $\overline{l'_1} = 0$, and thus $l'_1 = f(\tilde{l})$ for some $\tilde{l} \in L$. We have

$$g \circ \varphi(\tilde{l}) = \varphi' \circ f(\tilde{l}) = \varphi'(l'_1) = g(m_1).$$

Hence, $m_1 - \varphi(\tilde{l}) \in \ker g$. It remains to check that this element is sent to n by ψ. We get

$$\psi\big(m_1 - \varphi(\tilde{l})\big) = \psi(m_1) - \psi \circ \varphi(\tilde{l}) = \psi(m_1) = n.$$

Hence $\operatorname{Im} \psi|_{\ker h} = \ker \delta$.

The fact that δ is an R-homomorphism, and the exactness at the other points are checked in a similar fashion.

(b) Is obvious.

(c) Is a a direct consequence of the universal property of the quotient. ■

Remark 6.6

The name of the lemma comes from the following diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & \ker f \arrow[r, dotted, "\varphi"] \arrow[d] & \ker g \arrow[r, dotted, "\psi"] \arrow[d] & \ker h \arrow[d] \arrow[lldddd, dashed, rounded corners, "\delta"] & \\
 & L \arrow[r, "\varphi"] \arrow[d, "f"] & M \arrow[r, "\psi"] \arrow[d, "g"] & N \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & L' \arrow[r, "\varphi'"'] \arrow[d] & M' \arrow[r, "\psi'"'] \arrow[d] & N' \arrow[d] & \\
 & \operatorname{coker} f \arrow[r, dotted, "\overline{\varphi}'"] \arrow[d] & \operatorname{coker} g \arrow[r, dotted, "\overline{\psi}'"] \arrow[d] & \operatorname{coker} h \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

If fact the snake lemma holds in any abelian category. In particular, it holds for the categories of chain and cochain complexes, which we will study in Chapter 3.

Lemma-Definition 6.7

A s.e.s. $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ of R-modules is called **split** iff it satisfies the following equivalent conditions:

(a) There exists an R-homomorphism $\sigma : N \longrightarrow M$ such that $\psi \circ \sigma = \mathrm{id}_N$ (σ is called a **section** for ψ).

(b) There exists an R-homomorphism $\rho : M \longrightarrow L$ such that $\rho \circ \varphi = \mathrm{id}_L$ (ρ is called a **retraction** for φ).

(c) The submodule $\operatorname{Im}\varphi = \ker\psi$ is a **direct summand** of M, that is there exists a submodule M' of M such that $M = \operatorname{Im}\varphi \oplus M'$.

Example 6

The s.e.s. of $\mathbb{Z}$-modules

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\varphi"] & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \arrow[r, "\pi"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

defined by $\varphi([1]) = ([1],[0])$ and where π is the canonical projection into the cokernel of φ is split but clearly the s.e.s.

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\varphi"] & \mathbb{Z}/4\mathbb{Z} \arrow[r, "\pi"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

defined by $\varphi([1]) = ([2])$ and where π is the canonical projection onto the cokernel of φ is not split as

$$\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\,.$$

7 Free, Injective and Projective Modules

Free modules

Definition 7.1 (*Generating set / R-basis / free R-module*)

Let M be an R-module and $X \subseteq M$ be a subset.

(a) M is said to be **generated** by X if every element of M can be written as an R-linear combination $\sum_{x\in X} \lambda_x x$, that is, with $\lambda_x \in R$ almost everywhere 0.

(b) X is an R-**basis** (or a **basis**) if X generates M and if every element of M can be written *in a unique way* as an R-linear combination $\sum_{x\in X} \lambda_x X$ (i.e. with $\lambda_s \in R$ almost everywhere 0).

(c) M is called **free** if it admits an R-basis.
Notation: In this case we write $M = \bigoplus_{x\in X} Rx \cong \bigoplus_{x\in X} R =: R^{(X)}$.

Remark 7.2

(a) When we write the sum $\sum_{x\in X}\lambda_x X$, we always assume that the λ_s are 0 almost everywhere.

(b) Let X be a generating set for M. Then, X is a basis of M if and only if X is R-linearly independent.

(c) If R is a field, then every R-module is free. (R-vector spaces.)

Proposition 7.3 (*Universal property of free modules*)

Let P be a free R-module with basis X and let $i : X \hookrightarrow P$ be the canonical inclusion. For every R-module M and for every *map* (of sets) $\varphi : X \longrightarrow M$, there exists a unique morphism of R-modules $\tilde{\varphi} : P \longrightarrow M$ such that the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "\varphi"] \arrow[d, hook, "i"'] \arrow[dr, phantom, "\circlearrowleft"] & M \\
P \arrow[ur, dashed, "\exists!\,\tilde{\varphi}"'] &
\end{tikzcd}$$

The morphism $\tilde{\varphi}$ is called the **extension by R-linearity** of φ.

Proof: If $P \ni m = \sum_{x\in X}\lambda_x x$ (unique expression), then we set $\tilde{\varphi}(m) = \sum_{x\in X}\lambda_x\varphi(x)$. It is then easy to check $\tilde{\varphi}$ has the required properties. ■

Proposition 7.4 (*Properties of free modules*)

(a) Every R-module M is isomorphic to a quotient of a free R-module.

(b) If P is a free R-module, then $\operatorname{Hom}_R(P,-)$ is an exact functor.

Proof: (a) Choose a set $\{x_i\}_{i\in I}$ of generators of M (take all elements of M if necessary). Then define

$$\begin{aligned} \varphi : \bigoplus_{i\in I} R &\longrightarrow M \\ (r_i)_{i\in I} &\longmapsto \sum_{i\in I} r_i x_i . \end{aligned}$$

It follows that $M \cong \left(\bigoplus_{i\in I} R\right)\big/_{\ker\varphi}\cdot$

(b) We know that $\operatorname{Hom}(P,-)$ is left exact for any R-module P. It remains to prove that if $\psi : M \longrightarrow N$ is a surjective R-linear maps, then $\psi_* : \operatorname{Hom}_R(P,M) \longrightarrow \operatorname{Hom}_R(P,N) : \beta \longrightarrow \psi_*(\beta) = \psi\circ\beta$ is also surjective. So let $\alpha \in \operatorname{Hom}_R(P,N)$. We have the following situation:

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "\exists?"'] \arrow[d, "\alpha"] & \\
M \arrow[r, two heads, "\psi"'] & N \arrow[r, two heads] & 0
\end{tikzcd}$$

Let $\{e_i\}_{i\in I}$ be an R-basis of P. Each $\alpha(e_i) \in N$ is in the image of ψ, so that for each $i \in I$ there exists $m_i \in M$ such that $\psi(m_i) = \alpha(e_i)$. Hence, there is a map $\beta : \{e_i\}_{i\in I} \longrightarrow M, e_i \mapsto m_i$. By the universal property of free modules this induces an R-linear map $\tilde{\beta} : P \longrightarrow M$ such that $\tilde{\beta}(e_i) = m_i$ $\forall\ i \in I$. Thus

$$\psi\circ\tilde{\beta}(e_i) = \psi(m_i) = \alpha(e_i)\,,$$

so that $\psi\circ\tilde{\beta}$ and α coincide on the basis $\{e_i\}_{i\in I}$. By the uniqueness of $\tilde{\beta}$, we have $\alpha = \psi\circ\tilde{\beta} = \psi_*(\tilde{\beta})$. ■

Injective modules

Proposition-Definition 7.5 (*Injective module*)

An R-module I is called **injective** iff it satisfies the following equivalent conditions:

(a) The functor $\mathrm{Hom}_R(-, I)$ is exact.

(b) If $\varphi \in \mathrm{Hom}_R(L, M)$ is injective, then $\varphi^* : \mathrm{Hom}_R(M, I) \longrightarrow \mathrm{Hom}_R(L, I)$ is surjective (hence, any R-linear map $\alpha : L \longrightarrow I$ can be lifted to an R-linear map $\beta : M \longrightarrow I$, i.e., $\beta \circ \varphi = \alpha$).

(c) If $\eta : I \longrightarrow M$ is an injective R-homomorphism, then η splits, i.e., there exists $\rho : M \longrightarrow I$ such that $\rho \circ \eta = \mathrm{Id}_I$.

Remark 7.6

Note that Condition (b) is particularly interesting when $L \subseteq M$ is an R-submodule and φ is the canonical inclusion.

Projective modules

Proposition-Definition 7.7 (*Projective module*)

An R-module P is called **projective** iff it satisfies the following equivalent conditions:

(a) The functor $\mathrm{Hom}_R(P, -)$ is exact.

(b) If $\psi \in \mathrm{Hom}_R(M, N)$ is a surjective morphism of R-modules, then the morphism of abelian groups $\psi_* : \mathrm{Hom}_R(P, M) \longrightarrow \mathrm{Hom}_R(P, N)$ is surjective.

(c) If $\pi : M \longrightarrow P$ is a surjective R-homomorphism, then π splits, i.e., there exists $\sigma : P \longrightarrow M$ such that $\pi \circ \sigma = \mathrm{Id}_P$.

(d) P is isomorphic to a direct summand of a free R-module.

Example 7

(a) If $R = \mathbb{Z}$, then every submodule of a free $\mathbb{Z}$-module is again free (main theorem on $\mathbb{Z}$-modules).

(b) Let e be an idempotent in R, that is $e^2 = e$. Then, $R \cong Re \oplus R(1 - e)$ and Re is projective but not free if $e \neq 0, 1$.

(c) A product of modules $\{I_j\}_{j \in J}$ is injective if and only if each I_j is injective.

(d) A direct sum of modules $\{P_i\}_{i \in I}$ is projective if and only if each P_i is projective.

8 Tensor Products

Definition 8.1 (***Tensor product of R-modules***)

Let M be a right R-module and let N be a left R-module. Let F be the free abelian group (= free $\mathbb{Z}$-module) with basis $M \times N$. Let G be the subgroup of F generated by all the elements

$$\begin{aligned}&(m_1+m_2,n)-(m_1,n)-(m_2,n), \quad \forall m_1,m_2 \in M, \forall n \in N,\\ &(m,n_1+n_2)-(m,n_1)-(m,n_2), \quad \forall m \in M, \forall n_1,n_2 \in N, \text{ and}\\ &(mr,n)-(m,rn), \quad \forall m \in M, \forall n \in N, \forall r \in R.\end{aligned}$$

The **tensor product of M and N (balanced over R)**, is the abelian group $M \otimes_R N := F/G$. The class of $(m,n) \in F$ in $M \otimes_R N$ is denoted by $m \otimes n$.

Remark 8.2

(a) $M \otimes_R N = \langle m \otimes n \mid m \in M, n \in N \rangle_{\mathbb{Z}}$.

(b) In $M \otimes_R N$, we have the relations

$$\begin{aligned}&(m_1+m_2)\otimes n = m_1 \otimes n + m_2 \otimes n, \quad \forall m_1,m_2 \in M, \forall n \in N,\\ &m \otimes (n_1+n_2) = m \otimes n_1 + m \otimes n_2, \quad \forall m \in M, \forall n_1,n_2 \in N, \text{ and}\\ &mr \otimes n = m \otimes rn, \quad \forall m \in M, \forall n \in N, \forall r \in R.\end{aligned}$$

In particular, $m \otimes 0 = 0 = 0 \otimes n \ \forall\ m \in M,\ \forall\ n \in N$ and $(-m) \otimes n = -(m \otimes n) = m \otimes (-n)$ $\forall\ m \in M,\ \forall\ n \in N$.

Definition 8.3 (***R-balanced map***)

Let M and N be as above and let A be an abelian group. A map $f : M \times N \longrightarrow A$ is called **R-balanced** if

$$\begin{aligned}&f(m_1+m_2,n) = f(m_1,n)+f(m_2,n), \quad \forall m_1,m_2 \in M, \forall n \in N,\\ &f(m,n_1+n_2) = f(m,n_1)+f(m,n_2), \quad \forall m \in M, \forall n_1,n_2 \in N,\\ &f(mr,n) = f(m,rn), \quad \forall m \in M, \forall n \in N, \forall r \in R.\end{aligned}$$

Remark 8.4

The canonical map $t : M \times N \longrightarrow M \otimes_R N, (m,n) \mapsto m \otimes n$ is R-balanced.

Proposition 8.5 (***Universal property of the tensor product***)

Let M be a right R-module and let N be a left R-module. For every abelian group A and for every R-balanced map $f : M \times N \longrightarrow A$ there exists a unique homomorphism of abelian groups $\overline{f} : M \otimes_R N \longrightarrow A$ such that the following diagram commutes:

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "t"'] \arrow[dr, phantom, "\circlearrowleft"] & A \\ M \otimes_R N \arrow[ur, dashed, "\exists ! \overline{f}"'] & \end{tikzcd}$$

Proof: Let $\iota : M \times N \longrightarrow F$ denote the canonical inclusion, and let $\pi : F \longrightarrow F/G$ denote the canonical projection. By the universal property of the free $\mathbb{Z}$-module, there exists a unique $\mathbb{Z}$-linear map $\tilde{f} : F \longrightarrow A$ such that $\tilde{f} \circ \iota = f$. Since f is R-balanced, we have that $G \subseteq \ker(\tilde{f})$. Therefore, the universal property of the quotient yields the existence of a unique homomorphism of abelian groups $\overline{f} : F/G \longrightarrow A$ such that $\overline{f} \circ \pi = \tilde{f}$:

$$\begin{tikzcd}
M \times N \arrow[rr, "f"] \arrow[d, "\iota"'] \arrow[dd, bend right, "t"'] & & A \\
F \arrow[urr, dashed, "\tilde{f}"] \arrow[d, "\pi"'] & & \\
M \otimes_R N \cong F/G \arrow[uurr, dashed, "\overline{f}"'] & &
\end{tikzcd}$$

Clearly $t = \pi \circ \iota$, and hence $\overline{f} \circ t = \overline{f} \circ \pi \circ \iota = \tilde{f} \circ \iota = f$. ■

Remark 8.6

(a) Let $\{M_i\}_{i\in I}$ be a collection of right R-modules, M be a right R-module, N be a left R-module and $\{N_j\}_{i\in J}$ be a collection of left R-modules. Then, we have

$$(\bigoplus_{i\in I} M_i) \otimes_R N \cong \bigoplus_{i\in I}(M_i \otimes_R N)$$
$$M \otimes_R \bigoplus_{j\in J} N_j \cong \bigoplus_{j\in J}(M \otimes_R N_j).$$

(b) For every R-module M, we have $R \otimes_R M \cong M$ via $r \otimes m \mapsto rm$.

(c) If P is a free left R-module with basis X, then $M \otimes_R P \cong \bigoplus_{x\in X} M$.

(d) Let Q be a ring. Let M be a (Q, R)-bimodule and let N be an (R, S)-module. Then $M \otimes_R N$ can be endowed with the structure of a (Q, S)-bimodule via

$$q(m \otimes n)s = qm \otimes ns, \quad \forall q \in Q, \forall s \in S, \forall m \in M, \forall n \in N.$$

(e) If R is commutative, then any R-module can be viewed as an (R, R)-bimodule. Then, in particular, $M \otimes_R N$ becomes an R-module.

(f) **Tensor product of morphisms:** Let $f : M \longrightarrow M'$ be a morphism of right R-modules and $g : N \longrightarrow N'$ be a morphism of left R-modules. Then, by the universal property of the tensor product, there exists a unique $\mathbb{Z}$-linear map $f \otimes g : M \otimes_R N \longrightarrow M' \otimes_R N'$ such that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Proposition 8.7 (*Right exactness of the tensor product*)

(a) Let N be a left R-module. Then $- \otimes_R N : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$ is a right exact covariant functor.

(b) Let M be a right R-module. Then $M \otimes_R - : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a right exact covariant functor.

Remark 8.8

The functors $-\otimes_R N$ and $M\otimes_R -$ are not left exact in general.

Definition 8.9 (*Flat module*)

A left R-module N is called **flat** if the functor $-\otimes_R N : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$ is a left exact functor.

Proposition 8.10

Any projective R-module is flat.

Proof: To begin with, we note that a direct sum of modules is flat if and only if each module in the sum is flat. Next, consider the free R-module $P=\bigoplus_{x\in X} Rx$. If

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\varphi"] & M_2 \arrow[r, "\psi"] & M_3 \arrow[r] & 0 \end{tikzcd}$$

is a short exact sequence of right R-modules, then we obtain

$$\begin{tikzcd} 0 \arrow[r] & M_1\otimes_R\left(\bigoplus_{x\in X} R\right) \arrow[r, "\varphi\otimes\mathrm{Id}_P"] \arrow[d, "\cong"] & M_2\otimes_R\left(\bigoplus_{x\in X} R\right) \arrow[r, "\psi\otimes\mathrm{Id}_P"] \arrow[d, "\cong"] & M_3\otimes_R\left(\bigoplus_{x\in X} R\right) \arrow[r] \arrow[d, "\cong"] & 0 \\ 0 \arrow[r] & \bigoplus_{x\in X} M_1 \arrow[r, "(\varphi)_{x\in X}"] & \bigoplus_{x\in X} M_2 \arrow[r, "(\psi)_{x\in X}"] & \bigoplus_{x\in X} M_3 \arrow[r] & 0. \end{tikzcd}$$

Since the original sequence is exact, so is the bottom sequence, and therefore so is the top sequence. Hence, $-\otimes_R P$ is exact when P is free.
Now, if N is a projective R-module, then $N\oplus N'=P'$ for some free R-module P' and for some R-module N'. It follows that N is flat, by the initial remark. ■

9 Exercises for Chapter 2

Exercise 9

Let M, N be R-modules. Prove that:

(a) $\mathrm{End}_R(M)$, endowed with the pointwise addition and the usual composition of maps, is a ring.

(b) If R is commutative then the abelian group $\mathrm{Hom}_R(M, N)$ is a left R-module.

Exercise 10

Prove:

(a) the universal property of the direct product.

(b) the universal property of the direct sum.

Exercise 11

Prove that if $\varphi : M \longrightarrow N$ is an R-module homomorphism, then there is always an exact sequence

$$0 \longrightarrow \ker(\varphi) \longrightarrow M \xrightarrow{\varphi} N \longrightarrow \mathrm{coker}(\varphi) \longrightarrow 0\,.$$

Compute the sequences associated with the following $\mathbb{Z}$-homomorphisms:

(i) $\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z}$, multiplication by a prime p in $\mathbb{Z}$;

(ii) $\mathbb{Z}/15\mathbb{Z} \xrightarrow{\cdot 3} \mathbb{Z}/15\mathbb{Z}$, multiplication by 3.

Exercise 12

Let Q be an R-module and let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact sequence of R-modules.

(a) Find a counterexample in which the functor $\mathrm{Hom}_R(Q, -)$ does not preserve surjectivity, i.e find a surjective R-homomorphism $g : B \longrightarrow C$ such that the induced homomorphism $g_* : \mathrm{Hom}_R(Q, B) \longrightarrow \mathrm{Hom}_R(Q, C)$ is not surjective.

(b) Prove that the induced sequence of abelian groups

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_R(C, Q) \arrow[r, "g^*"] & \mathrm{Hom}_R(B, Q) \arrow[r, "f^*"] & \mathrm{Hom}_R(A, Q) \end{tikzcd}$$

is exact.

Find a counterexample of an injective R-homomorphism $f : A \longrightarrow B$ such that the induced homomorphism $f^* : \mathrm{Hom}_R(B, Q) \longrightarrow \mathrm{Hom}_R(A, Q)$ is not surjective.

Exercise 13

Let I and J be two-sided ideals of R and let M be a left R-module.

(a) Prove that there is an isomorphism of left R-modules $R/I \otimes_R M \cong M/IM$.

(b) Prove that there is an R-isomorphism $R/I \otimes_R R/J \cong R/(I+J)$.

(c) Let m, n be positive integers and A be a torsion abelian group. Compute

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}\,,\;\; A \otimes_{\mathbb{Z}} \mathbb{Q}\,,\;\; \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}\,,\;\; \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}\,.$$

Exercise 14 (*Extension of scalars*)

Let R and S be rings and let $f : R \longrightarrow S$ be a ring homomorphism.

(a) **Extension of scalars**: Prove that for every left R-module M, the tensor product $S \otimes_R M$ can be endowed with a left S-module structure via $x \cdot (s \otimes m) = xs \otimes m$, $\forall\, x, s \in S, m \in M$.

(b) Prove that the map $\iota : M \longrightarrow S \otimes_R M : m \mapsto \iota(m) = 1 \otimes m$ is an R-homomorphism, for every left R-module M.

(c) **Universal property of the extension of scalars**: Prove that for every left S-module N and for every R-homomorphism $g : M \longrightarrow N$ (where N is seen as an R-module via restriction of scalars), there exists a unique S-homomorphism $\tilde{g} : S \otimes_R M \longrightarrow N$ such that $\tilde{g} \circ \iota = g$, that is such that the following diagram commutes:

$$\begin{tikzcd}
M \arrow[r, "g"] \arrow[d, "\iota"'] & N \\
S \otimes_R M \arrow[ur, dashed, "\tilde{g}"', "\circlearrowleft"] &
\end{tikzcd}$$

(d) Prove that if M is a free left R-module with basis $\{e_i\}_{i \in I}$, then $S \otimes_R M$ is a free S-module with basis $\{1 \otimes e_i\}_{i \in I}$.

(e) Assume $R \subseteq S$ is an extension of commutative rings such that S is a free R-module of finite rank n. Prove that $S \otimes_R M$ is R-isomorphic to a direct sum of n copies of M.

(f) If $S \cong R/I$ is a quotient of R by a two-sided ideal I and $f : R \longrightarrow R/I$ is the quotient morphism, recall that $S \otimes_R M = R/I \otimes_R M \cong M/IM$ and deduce that the map ι is not necessarily injective.

Chapter 3. Homological Algebra

The aim of this chapter is to introduce the fundamental results of homological algebra. Homological algebra appeared in the 1800's and is nowadays a very useful tool in several branches of mathematics, such as algebraic topology, commutative algebra, algebraic geometry, and, of particular interest to us, group theory.

Throughout this chapter R denotes a ring, and unless otherwise specified, all rings are assumed to be *unital* and *associative*.

Reference:

[Rot09] J. J. Rotman, *An introduction to homological algebra. Second ed.*, Universitext, Springer, New York, 2009.

[Wei94] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

10 Chain and Cochain Complexes

Definition 10.1 (*Chain complex*)

(a) A **chain complex** (or simply a **complex)** of R-modules is a sequence

$$(C_\bullet, d_\bullet) = \left(\cdots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \right)$$

where for each $n \in \mathbb{Z}$, C_n is an R-modules and $d_n \in \operatorname{Hom}_R(C_n, C_{n-1})$ satisfies $d_n \circ d_{n+1} = 0$. We often write simply $C_\bullet$ instead of $(C_\bullet, d_\bullet)$.

(b) The integer n is called the **degree** of the R-module C_n.

(c) The R-homomorphisms d_n ($n \in \mathbb{Z}$) are called the **differential maps**.

(d) A complex $C_\bullet$ is called **non-negative** (resp. **positive**) if $C_n = 0$ for all $n \in \mathbb{Z}_{<0}$ (resp. for all $n \in \mathbb{Z}_{\leqslant 0}$).

To keep notation light we often write $C_\bullet$ instead of $(C_\bullet, d_\bullet)$ and simply d for all differential maps, so the condition $d_n \circ d_{n+1} = 0$ can be written as $d^2 = 0$. If there is an integer N such that $C_n = 0$ for all

$n \leqslant N$, then we omit to write the zero modules and zero maps on the right-hand side of the complex:

$$\cdots \longrightarrow C_{N+2} \xrightarrow{d_{N+2}} C_{N+1} \xrightarrow{d_{N+1}} C_N$$

Similarly, if there is an integer N such that $C_n = 0$ for all $n \geqslant N$, then we omit to write the zero modules and zero maps on the left-hand side of the complex:

$$C_N \xrightarrow{d_N} C_{N-1} \xrightarrow{d_{N-1}} C_{N-2} \longrightarrow \cdots$$

Definition 10.2 (*Morphism of complexes*)

A **morphism of (chain) complexes** (or a **chain map**) between two chain complexes $(C_\bullet, d_\bullet)$ and $(D_\bullet, d'_\bullet)$, written $\varphi_\bullet : (C_\bullet, d_\bullet) \longrightarrow (D_\bullet, d'_\bullet)$ or simply $\varphi_\bullet : C_\bullet \longrightarrow D_\bullet$, is a familiy of R-homomorphisms $\varphi_n : C_n \longrightarrow D_n$ ($n \in \mathbb{Z}$) such that the diagram

$$\begin{tikzcd}
\cdots \arrow[r, "d_{n+2}"] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "\varphi_{n+1}"'] & C_n \arrow[r, "d_n"] \arrow[d, "\varphi_n"'] & C_{n-1} \arrow[r, "d_{n-1}"] \arrow[d, "\varphi_{n-1}"'] & \cdots \\
\cdots \arrow[r, "d'_{n+2}"] & D_{n+1} \arrow[r, "d'_{n+1}"] & D_n \arrow[r, "d'_n"] & D_{n-1} \arrow[r, "d'_{n-1}"] & \cdots
\end{tikzcd}$$

commutes, i.e. such that $\varphi_n \circ d_{n+1} = d'_{n+1} \circ \varphi_{n+1}$ for each $n \in \mathbb{Z}$.

Notation. Chain complexes together with morphisms of chain complexes (and composition given by degreewise composition of the underlying R-morphisms) form a category, which we denote by **Ch(${}_R$Mod)**.

Definition 10.3 (*Subcomplex / quotient complex*)

(a) A **subcomplex** $C'_\bullet$ of a chain complex $(C_\bullet, d_\bullet)$ is a family of R-modules $C'_n \leqslant C_n$ ($n \in \mathbb{Z}$) such that $d_n(C'_n) \subseteq C'_{n-1}$ for every $n \in \mathbb{Z}$.
In this case, $(C'_\bullet, d_\bullet)$ becomes a chain complex and we write $C'_\bullet \hookrightarrow C_\bullet$ for the chain map given by the canonical inclusion of C'_n into C_n for each $n \in \mathbb{Z}$ is a chain map.

(b) If $C'_\bullet$ is a subcomplex of $C_\bullet$, then the **quotient complex** $C_\bullet/C'_\bullet$ is by the definition the familiy of R-modules C_n/C'_n ($n \in \mathbb{Z}$) together with the differential maps $\overline{d}_n : C_n/C'_n \longrightarrow C_{n-1}/C'_{n-1}$ ($n \in \mathbb{Z}$) induced by the maps d_n ($n \in \mathbb{Z}$) via the universal property of the quotient of R-modules.
In this case, the map $\pi_\bullet : C_\bullet \longrightarrow C_\bullet/C'_\bullet$ defined for each $n \in \mathbb{Z}$ to be the canonical projection $\pi_n : C_n \longrightarrow C_n/C'_n$ is a chain map and is called the **quotient (chain) map**.

Definition 10.4 (*Kernel / image / cokernel*)

Let $\varphi_\bullet : (C_\bullet, d_\bullet) \longrightarrow (D_\bullet, d'_\bullet)$ be a chain map. Then:

(a) the **kernel** $\ker \varphi_\bullet$ of $\varphi_\bullet$ is the subcomplex $(\{\ker \varphi_n\}_{n\in\mathbb{Z}}, d_\bullet)$ of $C_\bullet$;

(b) the **image** $\operatorname{Im} \varphi_\bullet$ of $\varphi_\bullet$ is the subcomplex $(\{\operatorname{Im} \varphi_n\}_{n\in\mathbb{Z}}, d'_\bullet)$ of $D_\bullet$;

(c) the **cokernel** of $\varphi_\bullet$ is the quotient complex $\operatorname{coker} \varphi_\bullet := D_\bullet / \operatorname{Im} \varphi_\bullet$.

With the notions of kernel and cokernel defined above, one can prove that **Ch($_R$Mod)** is in fact an abelian category.

Definition 10.5 (*Cycles, boundaries, homology*)

Let $(C_\bullet, d_\bullet)$ be a chain complex of R-modules, and let $n \in \mathbb{Z}$.

(a) An n**-cycle** is an element of $\ker d_n =: Z_n(C_\bullet) =: Z_n$.

(b) An n**-boundary** is an element of $\operatorname{Im} d_{n+1} =: B_n(C_\bullet) := B_n$.
[Clearly, since $d_n \circ d_{n+1} = 0$, we have $B_n \subseteq Z_n \subseteq C_n$.]

(c) The n**-th homology module** (or simply **group**) of $C_\bullet$ is $H_n(C_\bullet) := Z_n/B_n$.

In fact, for each $n \in \mathbb{Z}$, $H_n(-) : \mathbf{Ch}(_R\mathbf{Mod}) \longrightarrow {}_R\mathbf{Mod}$ is a covariant additive functor (Exercise Sheet 4), which we define on morphisms as follows:

Lemma 10.6

Let $\varphi_\bullet : C_\bullet \longrightarrow D_\bullet$ be a morphism of chain complexes between $(C_\bullet, d_\bullet)$ and $(D_\bullet, d'_\bullet)$. Then $\varphi_\bullet$ induces an R-homomorphism

$$\begin{array}{rccc} H_n(\varphi_\bullet): & H_n(C_\bullet) & \longrightarrow & H_n(D_\bullet) \\ & z_n + B_n(C_\bullet) & \mapsto & \varphi_n(z_n) + B_n(D_\bullet) \end{array}$$

for each $n \in \mathbb{Z}$. To simplify, this map is often denoted by φ_* instead of $H_n(\varphi_\bullet)$.

Proof: Fix $n \in \mathbb{Z}$, and let $\pi_n : Z_n(C_\bullet) \longrightarrow Z_n(C_\bullet)/B_n(C_\bullet)$, resp. $\pi'_n : Z_n(D_\bullet) \longrightarrow Z_n(D_\bullet)/B_n(D_\bullet)$, be the quotient chain maps.
First, notice that $\varphi_n(Z_n(C_\bullet)) \subseteq Z_n(D_\bullet)$ because if $z \in Z_n$, then $d'_n \circ \varphi_n(z) = \varphi_{n-1} \circ d_n(z) = 0$. Hence, we have $\varphi_n(z) \in Z_n(D_\bullet)$.
Similarly, we have $\varphi_n(B_n(C_\bullet)) \subseteq B_n(D_\bullet)$. Indeed, if $b \in B_n(C_\bullet)$, then $b = d_{n+1}(a)$ for some $a \in C_{n+1}$, and because $\varphi_\bullet$ is a chain map we have $\varphi_n(b) = \varphi_n \circ d_{n+1}(a) = d'_{n+1} \circ \varphi_{n+1}(a) \in B_n(D_\bullet)$. Thus $B_n(C_\bullet) \subseteq \ker(\pi'_n \circ \varphi_n)$ for each $n \in \mathbb{Z}$ and herefore, by the universal property of the quotient, there exists a unique R-homomorphism $\overline{\pi'_n \circ \varphi_n}$ such that the following diagram commutes:

$$\begin{tikzcd} Z_n(C_\bullet) \arrow[r, "\varphi_n"] \arrow[d, "\pi_n"'] & Z_n(D_\bullet) \arrow[r, "\pi'_n"] & Z_n(D_\bullet)/B_n(D_\bullet) \\ Z_n(C_\bullet)/B_n(C_\bullet) \arrow[rru, dashed, "\overline{\pi'_n \circ \varphi_n}"'] & & \end{tikzcd}$$

Set $H_n(\varphi_\bullet) := \overline{\pi'_n \circ \varphi_n}$. The claim follows. ■

It should be thought that the homology module $H_n(C_\bullet)$ measures the "non-exactness" of the sequence

$$C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \ .$$

Moroever, the functors $H_n(-)$ ($n \in \mathbb{Z}$) are neither left exact, nor right exact in general. As a matter of fact, using the Snake Lemma, we can use s.e.s. of complexes to produce so-called "long exact sequences" of R-modules.

Theorem 10.7 (*Long exact sequence in homology*)

Let $0_\bullet \longrightarrow C_\bullet \xrightarrow{\varphi_\bullet} D_\bullet \xrightarrow{\psi_\bullet} E_\bullet \longrightarrow 0_\bullet$ be a s.e.s. of chain complexes. Then there is a long exact sequence

$$\cdots \xrightarrow{\delta_{n+1}} H_n(C_\bullet) \xrightarrow{\varphi_*} H_n(D_\bullet) \xrightarrow{\psi_*} H_n(E_\bullet) \xrightarrow{\delta_n} H_{n-1}(C_\bullet) \xrightarrow{\varphi_*} H_{n-1}(D_\bullet) \xrightarrow{\psi_*} \cdots$$

where for each $n \in \mathbb{Z}$, $\delta_n : H_n(E_\bullet) \longrightarrow H_{n-1}(C_\bullet)$ is an R-homomorphism, called **connecting homomorphism**.

Note: Here $0_\bullet$ simply denotes the **zero complex**, that is the complex

$$\cdots \longrightarrow 0 \xrightarrow{0} 0 \xrightarrow{0} 0 \longrightarrow \cdots$$

consisting of zero modules and zero morphisms. We often write simply 0 instead of $0_\bullet$.

Proof: To simplify, we denote all differential maps of the three complexes $C_\bullet$, $D_\bullet$, $E_\bullet$ with the same letter d, and we fix $n \in \mathbb{Z}$. First, we apply the "non-snake" part of the Snake Lemma to the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & C_n \arrow[r, "\varphi_n"] \arrow[d, "d_n"] & D_n \arrow[r, "\psi_n"] \arrow[d, "d_n"] & E_n \arrow[r] \arrow[d, "d_n"] & 0 \\
0 \arrow[r] & C_{n-1} \arrow[r, "\varphi_{n-1}"] & D_{n-1} \arrow[r, "\psi_{n-1}"] & E_{n-1} \arrow[r] & 0
\end{tikzcd}$$

and we obtain two exact sequences of R-homomorphisms

$$0 \longrightarrow Z_n(C_\bullet) \xrightarrow{\varphi_n} Z_n(D_\bullet) \xrightarrow{\psi_n} Z_n(E_\bullet) \ ,$$

and

$$C_{n-1}/\operatorname{Im} d_n \xrightarrow{\overline{\varphi_{n-1}}} D_{n-1}/\operatorname{Im} d_n \xrightarrow{\overline{\psi}_{n-1}} E_{n-1}/\operatorname{Im} d_n \longrightarrow 0.$$

Shifting indices in both sequences we obtain similar sequences in degrees $n-1$, and n respectively. Therefore, we have a commutative diagram with exact rows of the form

$$\begin{tikzcd}
 & C_n/\operatorname{Im} d_{n+1} \arrow[r, "\overline{\varphi_n}"] \arrow[d, "\overline{d_n}"] & D_n/\operatorname{Im} d_{n+1} \arrow[r, "\overline{\psi_n}"] \arrow[d, "\overline{d_n}"] & E_n/\operatorname{Im} d_{n+1} \arrow[r] \arrow[d, "\overline{d_n}"] & 0 \\
0 \arrow[r] & Z_{n-1}(C_\bullet) \arrow[r, "\varphi_{n-1}"] & Z_{n-1}(D_\bullet) \arrow[r, "\psi_{n-1}"] & Z_{n-1}(E_\bullet) \, , &
\end{tikzcd}$$

where $\overline{d_n} : C_n/\operatorname{Im} d_{n+1} \longrightarrow Z_{n-1}(C_\bullet)$ is the unique R-homomorphism induced by the universal property of the quotient by $d_n : C_n \longrightarrow C_{n-1}$ (as $\operatorname{Im} d_{n+1} \subseteq \ker d_n$ by definition of a chain complex), and similarly for $D_\bullet$ and $E_\bullet$. Therefore, the Snake Lemma yields the existence of the connecting homomorphisms

$$\delta_n : \underbrace{\ker \overline{d_n}(E_\bullet)}_{=H_n(E_\bullet)} \longrightarrow \underbrace{\operatorname{coker} \overline{d_n}(C_\bullet)}_{=H_{n-1}(C_\bullet)}$$

for each $n \in \mathbb{Z}$ as well as the required long exact sequence:

$$\cdots \xrightarrow{\delta_{n+1}} \underbrace{H_n(C_\bullet)}_{=\ker \overline{d_n}} \xrightarrow{\varphi_*} \underbrace{H_n(D_\bullet)}_{=\ker \overline{d_n}} \xrightarrow{\psi_*} \underbrace{H_n(E_\bullet)}_{=\ker \overline{d_n}} \xrightarrow{\delta_n} \underbrace{H_{n-1}(C_\bullet)}_{=\operatorname{coker} \overline{d_n}} \xrightarrow{\varphi_*} \underbrace{H_{n-1}(D_\bullet)}_{=\operatorname{coker} \overline{d_n}} \xrightarrow{\psi_*} \cdots$$

■

We now describe some important properties of chain maps and how they relate with the induced morphisms in homology.

Definition 10.8 (***Quasi-isomorphism***)

A chain map $\varphi_\bullet : C_\bullet \longrightarrow D_\bullet$ is called a **quasi-isomorphism** if $H_n(\varphi_\bullet)$ is an isomorphism for all $n \in \mathbb{Z}$.

Remark 10.9

(a) Bourbaki uses the nicer *homologism* instead of the somewhat misleading *quasi-isomorphism*.

(b) **Warning:** A quasi-isomorphism $\varphi_\bullet : C_\bullet \longrightarrow D_\bullet$ does not imply that the complexes $C_\bullet$ and $D_\bullet$ are isomorphic as chain complexes. See Exercise Sheet 5 for a counter-example.

(c) In general complexes are not exact sequences, but if they are, then their homology vanishes, so that there is a quasi-isomorphism from the zero complex. In fact, if $C_\bullet$ is a chain complex of R-modules, then the following assertions are equivalent:

(1) $C_\bullet$ is **exact** (i.e. exact at C_n for each $n \in \mathbb{Z}$);

(2) $C_\bullet$ is **acyclic** , that is, $H_n(C_\bullet) = 0$ for all $n \in \mathbb{Z}$;

(3) the chain map $0_\bullet \longrightarrow C_\bullet$ is a quasi-isomorphism.

Definition 10.10 (***Homotopic chain maps / homotopy equivalence***)

Two chain maps $\varphi_\bullet, \psi_\bullet : (C_\bullet, d_\bullet) \longrightarrow (D_\bullet, d'_\bullet)$ are called **(chain) homotopic** if there exists a familiy of R-homomorphisms $\{s_n : C_n \longrightarrow D_{n+1}\}_{n\in\mathbb{Z}}$ such that

$$\varphi_n - \psi_n = d'_{n+1} \circ s_n + s_{n-1} \circ d_n$$

for each $n \in \mathbb{Z}$.

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "\varphi_{n+1}-\psi_{n+1}"'] & C_n \arrow[r, "d_n"] \arrow[d, "\varphi_n-\psi_n"] \arrow[dl, "s_n"'] & C_{n-1} \arrow[r] \arrow[d, "\varphi_{n-1}-\psi_{n-1}"] \arrow[dl, "s_{n-1}"] & \cdots \\
\cdots \arrow[r] & D_{n+1} \arrow[r, "d'_{n+1}"'] & D_n \arrow[r, "d'_n"'] & D_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

In this case, we write $\varphi_\bullet \sim \psi_\bullet$.
Moreover, a chain map $\varphi_\bullet : C_\bullet \longrightarrow D_\bullet$ is called a **homotopy equivalence** if there exists a chain map $\sigma_\bullet : D_\bullet \longrightarrow C_\bullet$ such that $\sigma_\bullet \circ \varphi_\bullet \sim \mathrm{id}_{C_\bullet}$ and $\varphi_\bullet \circ \sigma_\bullet \sim \mathrm{id}_{D_\bullet}$.

Note: One easily checks that $\sim$ is an equivalence relation on the class of chain maps.

Proposition 10.11

If $\varphi_\bullet, \psi_\bullet : C_\bullet \longrightarrow D_\bullet$ are homotopic chain maps, then they induce the same morphisms in homology, that is,

$$H_n(\varphi_\bullet) = H_n(\psi_\bullet) : H_n(C_\bullet) \longrightarrow H_n(D_\bullet) \quad \forall n \in \mathbb{Z}.$$

Proof: Fix $n \in \mathbb{Z}$ and let $z \in Z_n(C_\bullet)$. Then, with the notation of Definition 10.10, we have

$$\big(\varphi_n - \psi_n\big)(z) = \big(d'_{n+1}s_n + s_{n-1}d_n\big)(z) = \underbrace{d'_{n+1}s_n(z)}_{\in B_n(D_\bullet)} + \underbrace{s_{n-1}d_n(z)}_{=0} \in B_n(D_\bullet).$$

Hence, for every $z + B_n(C_\bullet) \in H_n(C_\bullet)$, we have

$$\left(H_n(\varphi_\bullet) - H_n(\psi_\bullet)\right)\left(z + B_n(C_\bullet)\right) = (\varphi_n - \psi_n)(z) + B_n(D_\bullet) = 0 + B_n(D_\bullet)\,.$$

In other words, $H_n(\varphi_\bullet) - H_n(\psi_\bullet) \equiv 0$ and it follows that $H_n(\varphi_\bullet) = H_n(\psi_\bullet)$. ■

Remark 10.12 (*Out of the scope of the lecture!*)

Homotopy of complexes leads to considering the so-called **homomotopy category** of R-modules, denoted $\mathbf{Ho(}_R\mathbf{Mod)}$, which is very useful in algebraic topology or representation theory of finite groups for example. It is defined as follows:

- The objects are the chain complexes, i.e. $\operatorname{Ob}\mathbf{Ho(}_R\mathbf{Mod)} = \operatorname{Ob}\mathbf{Ch(}_R\mathbf{Mod)}$.
- The morphisms are given by $\operatorname{Hom}_{\mathbf{Ho(}_R\mathbf{Mod)}}(C_\bullet, D_\bullet) := \operatorname{Hom}_{\mathbf{Ch(}_R\mathbf{Mod)}}(C_\bullet, D_\bullet)/\sim$.

It is an additive category, but it is not abelian in general though. The isomorphisms in the homotopy category are exactly the classes of the homotopy equivalences.

Dualising the concepts we have defined so far yields the so-called "cochain complexes" and the notion of "cohomology".

Definition 10.13 (*Cochain complex / cohomology*)

(a) A **cochain complex** of R-modules is a sequence

$$(C^\bullet, d^\bullet) = \left(\cdots \longrightarrow C^{n-1} \xrightarrow{d^{n-1}} C^n \xrightarrow{d^n} C^{n+1} \longrightarrow \cdots\right),$$

where for each $n \in \mathbb{Z}$, C^n is an R-module and $d^n \in \operatorname{Hom}_R(C^n, C^{n+1})$ satisfies $d^n \circ d^{n-1} = 0$. To keep notation light, we often write $C^\bullet$ instead of $(C^\bullet, d^\bullet)$ and d instead of d^n.

(b) The elements of $Z^n := Z^n(C^\bullet) := \ker d^n$ are called n**-cocycles**.

(c) The elements of $B^n := B^n(C^\bullet) := \operatorname{Im} d^{n-1}$ are called n**-coboundaries**.

(d) The n**-th cohomology module** (or simply **group**) of $C^\bullet$ is $H^n(C^\bullet) := Z_n/B_n$.

Similarly to the case of chain complexes, we can define:

- **Morphisms of cochain complexes** (or simply **cochain maps**) $\varphi^\bullet : (C^\bullet, d^\bullet) \longrightarrow (D^\bullet, \tilde{d}^\bullet)$, or simply $\varphi^\bullet : C^\bullet \longrightarrow D^\bullet$, as being a familiy of R-homomorphisms $\varphi^n : C^n \longrightarrow D^n$ ($n \in \mathbb{Z}$) such that $\varphi^n \circ d^{n-1} = \tilde{d}^{n-1} \circ \varphi^{n-1}$ for each $n \in \mathbb{Z}$, that is, such that the following diagram commutes:

$$\begin{tikzcd}
\cdots \arrow[r, "d^{n-2}"] & C^{n-1} \arrow[r, "d^{n-1}"] \arrow[d, "\varphi^{n-1}"'] & C^n \arrow[r, "d^n"] \arrow[d, "\varphi^n"'] & C^{n+1} \arrow[r, "d^{n+1}"] \arrow[d, "\varphi^{n+1}"'] & \cdots \\
\cdots \arrow[r, "\tilde{d}^{n-2}"] & D^{n-1} \arrow[r, "\tilde{d}^{n-1}"] & D^n \arrow[r, "\tilde{d}^n"] & D^{n+1} \arrow[r, "\tilde{d}^{n+1}"] & \cdots
\end{tikzcd}$$

- subcomplexes, quotient complexes;
- kernels, images, cokernels of morphisms of cochain complexes;
- for each $n \in \mathbb{Z}$, $H^n(-)$ on morphisms $\varphi^\bullet : C^\bullet \longrightarrow D^\bullet$ through

$$\varphi^* := H^n(\varphi^\bullet) : H^n(C^\bullet) \longrightarrow H^n(D^\bullet), z + B^n(D^\bullet) \mapsto \varphi^n(z) + B^n(D^\bullet)$$

  so that $H_n(-)$: $\mathbf{CoCh}({}_R\mathbf{Mod}) \longrightarrow {}_R\mathbf{Mod}$ is a covariant additive functor;
- quasi-isomorphisms, homotopic chain maps and homotopy equivalences.

Moreover,

- homotopic chain maps induce the same R-homomorphisms in cohomology; and
- cochain complexes together with morphisms of cochain complexes (and composition given by degreewise composition of R-morphisms) form an abelian category, which we will denote by **CoCh(${}_R$Mod)**.

Exercise: formulate these definitions in a formal way.

Theorem 10.14 (*Long exact sequence in cohomology*)

Let $0^\bullet \longrightarrow C^\bullet \xrightarrow{\varphi^\bullet} D^\bullet \xrightarrow{\psi^\bullet} E^\bullet \longrightarrow 0^\bullet$ be a s.e.s. of cochain complexes. Then, for each $n \in \mathbb{Z}$, there exists a connecting R-homomorphism $\delta^n : H^n(E^\bullet) \longrightarrow H^{n+1}(C^\bullet)$ such that the sequence

$$\cdots \xrightarrow{\delta^{n-1}} H^n(C^\bullet) \xrightarrow{\varphi^*} H^n(D^\bullet) \xrightarrow{\psi^*} H^n(E^\bullet) \xrightarrow{\delta^n} H^{n+1}(C^\bullet) \xrightarrow{\varphi^*} H^{n+1}(D^\bullet) \xrightarrow{\psi^*} \cdots$$

is an exact sequence of R-modules

Proof: Similar to the proof of the long exact sequence in homology (Theorem 10.7), i.e. follows from the Snake Lemma. (Cochain complexes are just chain complexes with a reversed grading!) ■

11 Projective Resolutions

Definition 11.1 (*Projective resolution*)

Let M be an R-module.

(a) A **resolution** of M is a non-negative chain complex of projective (respectively free) R-modules

$$(P_\bullet, d_\bullet) = \big(\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \big)$$

which is exact at P_n for every $n \geqslant 1$ and such that $H_0(P_\bullet) = P_0/\operatorname{Im} d_1 \cong M$.
If the R-module P_n is projective (resp. free) for each $n \geqslant 0$, then $(P_\bullet, d_\bullet)$ is called a **projective resolution** (respectively a **free resolution**) of M.

(b) Let $\varepsilon : P_0 \twoheadrightarrow M$ denote the quotient homomorphism. Then the exact complex

$$\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0 \ ,$$

is called the **augmented complex** or **augmented resolution** associated to $(P_\bullet, d_\bullet)$. For this reason, (projective/free) resolutions of M are often denoted by $P_\bullet \overset{\epsilon}{\twoheadrightarrow} M$.

Example 8

(a) The $\mathbb{Z}$-module $M = \mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{Z}_{>1})$ admits the projective resolution $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$.

(b) If M is a projective R-module, then a projective resolution $P_\bullet$ of M can be chosen such that $P_n = 0$ for all $n \geqslant 1$, $P_0 = M$ and with augmentation map is $\varepsilon = \mathrm{Id}_M$.

We now prove that projective resolutions do exist, and consider the question of how "unique" they are.

Proposition 11.2

Any R-module has a projective resolution. (It can even chosen to be free.)

Proof: Let M be an R-module. We use the fact that every R-module is a quotient of a free R-module (Proposition 7.4). Thus there exists a free module P_0 together with a surjective R-linear map $\varepsilon : P_0 \twoheadrightarrow M$ such that $M \cong P_0/\ker\varepsilon$. Next, let P_1 be a free R-module together with a surjective R-linear map $d_1 : P_1 \twoheadrightarrow \ker\varepsilon \subseteq P_0$ such that $P_1/\ker d_1 \cong \ker\varepsilon$:

$$\begin{tikzcd}
P_1 \arrow[rr, dashed, "d_1"] \arrow[dr, two heads, "d_1"'] & & P_0 \arrow[r, two heads, "\varepsilon"] & M . \\
& \ker\varepsilon \arrow[ur, hook] & &
\end{tikzcd}$$

Inductively, assuming that the R-homomorphism $d_{n-1} : P_{n-1} \longrightarrow P_{n-2}$ has already been defined, then there exists a free R-module P_n and a surjective R-linear map $d_n : P_n \twoheadrightarrow \ker d_{n-1} \subseteq P_{n-1}$ with $P_n/\ker d_n \cong \ker d_{n-1}$. The claim follows. ■

Theorem 11.3 (*Lifting Theorem*)

Let $(P_\bullet, d_\bullet)$ and $(Q_\bullet, d'_\bullet)$ be two non-negative chain complexes such that

1. P_n is a projective R-module for every $n \geqslant 0$;
2. $Q_\bullet$ is exact at Q_n for every $n \geqslant 1$ (i.e. $H_n(Q_\bullet) = 0$ for every $n \geqslant 1$).

Let $\varepsilon : P_0 \twoheadrightarrow H_0(P_\bullet)$ and $\varepsilon' : Q_0 \twoheadrightarrow H_0(Q_\bullet)$ be the quotient homomorphims.

If $f : H_0(P_\bullet) \longrightarrow H_0(Q_\bullet)$ is an R-homomorphism, then there exists a chain map $\varphi_\bullet : P_\bullet \longrightarrow Q_\bullet$ inducing the given map f in degree-zero homology, that is such that $H_0(\varphi_\bullet) = f$ and $f \circ \varepsilon = \varepsilon' \circ \varphi_0$. Moreover, such a chain map $\varphi_\bullet$ is unique up to homotopy.

In the situation of the Theorem, it is said that $\varphi_\bullet$ **lifts** f.

Proof: **Existence.** Beacuse P_0 is projective and ε' is surjective, by definition (Def. 7.7), there exists an R-linear map $\varphi_0 : P_0 \longrightarrow Q_0$ such that the following diagram commutes

$$\begin{tikzcd}
\cdots \arrow[r, "d_1"] & P_0 \arrow[r, two heads, "\varepsilon"] \arrow[d, dashed, "\exists\varphi_0"] \arrow[dr, phantom, "\circlearrowleft"] & H_0(P_\bullet) = P_0/\operatorname{Im} d_1 \arrow[d, "f"] \\
\cdots \arrow[r, "d'_1"] & Q_0 \arrow[r, two heads, "\varepsilon'"] & H_0(Q_\bullet) = Q_0/\operatorname{Im} d'_1 ,
\end{tikzcd}$$

that is $f\circ\varepsilon=\varepsilon'\circ\varphi_0$. But then, $\varepsilon'\circ\varphi_0\circ d_1=f\circ\underbrace{\varepsilon\circ d_1}_{=0}=0$, so that $\operatorname{Im}(\varphi_0\circ d_1)\subseteq\ker\varepsilon'=\operatorname{Im}d_1'$. Again by Definition 7.7, since P_1 is projective and d_1' is surjective onto its image, there exists an R-linear map $\varphi_1:P_1\longrightarrow Q_1$ such that $\varphi_0\circ d_1=d_1'\circ\varphi_1$:

$$\begin{tikzcd}
P_1 \arrow[rr, "d_1"] \arrow[d, dashed, "\exists\varphi_1"'] \arrow[dr, "\varphi_0\circ d_1"] \arrow[d, phantom, "\circlearrowleft", shift left=4ex] & & P_0 \arrow[d, "\varphi_0"] \\
Q_1 \arrow[r, two heads, "d_1'"'] & \operatorname{Im}d_1'=\ker\varepsilon' \arrow[r, hook, "\text{inc}"'] & Q_0
\end{tikzcd}$$

The morphisms $\varphi_n:P_n\longrightarrow Q_n$ are constructed similarly by induction on n. Hence the existence of a chain map $\varphi_\bullet:P_\bullet\longrightarrow Q_\bullet$ as required.

Uniqueness. For the uniqueness statement, suppose $\psi_\bullet:P_\bullet\longrightarrow Q_\bullet$ also lifts the given morphism f. We have to prove that $\varphi_\bullet\sim\psi_\bullet$ (or equivalently that $\varphi_\bullet-\psi_\bullet$ is homotopic to the zero chain map).

For each $n\geqslant 0$ set $\sigma_n:=\varphi_n-\psi_n$, so that $\sigma_\bullet:P_\bullet\longrightarrow Q_\bullet$ is becomes a chain map. In particular $\sigma_0=\varphi_0-\psi_0=H_0(\varphi_\bullet)-H_0(\psi_\bullet)=f-f=0$. Then we let $s_{-2}:0\longrightarrow H_0(Q_\bullet)$ and $s_{-1}:H_0(P_\bullet)\longrightarrow Q_0$ be the zero maps. Therefore, in degree zero, we have the following maps:

$$\begin{tikzcd}
P_0 \arrow[r, two heads, "\varepsilon"] & H_0(P_\bullet) \arrow[r, "0"] \arrow[dl, "s_{-1}"] \arrow[d, "0"] & 0 \arrow[dl, "s_{-2}"] \\
Q_0 \arrow[r, two heads, "\varepsilon'"'] & H_0(Q_\bullet) \arrow[r, "0"'] & 0\,,
\end{tikzcd}$$

where clearly $0=s_{-2}\circ 0+\varepsilon'\circ s_{-1}$. This provides us with the starting point for the construction of a homotopy $s_n:P_n\longrightarrow Q_{n+1}$ ($n\geqslant 0$) by induction on n. So let $n\geqslant 0$ and suppose $s_i:P_i\longrightarrow Q_{i+1}$ is already constructed for each $-2\leqslant i\leqslant n-1$ and satisfies $d_{i+1}'\circ s_i+s_{i-1}\circ d_i=\sigma_i$ for each $i\geqslant -1$, and where we identify

$$P_{-1}=H_0(P_\bullet),\quad Q_{-1}=H_0(Q_\bullet),\quad P_{-2}=0=Q_{-2},\quad d_0=\varepsilon,\quad d_0'=\varepsilon',\quad d_{-1}=0=d_{-1}'\,.$$

Now, we check that the image of $\sigma_n-s_{n-1}\circ d_n$ is contained in $\ker d_n'=\operatorname{Im}d_{n+1}'$:

$$\begin{aligned}
d_n'\circ\big(\sigma_n-s_{n-1}\circ d_n\big)&=d_n'\circ\sigma_n-d_n'\circ s_{n-1}\circ d_n\\
&=d_n'\circ\sigma_n-\big(\sigma_{n-1}-s_{n-2}\circ d_{n-1}\big)\circ d_n\\
&=d_n'\circ\sigma_n-\sigma_{n-1}\circ d_n\\
&=\sigma_{n-1}\circ d_n-\sigma_{n-1}\circ d_n=0\,,
\end{aligned}$$

where the last-nut-one equality holds because both $\sigma_\bullet$ is a chain map. Therefore, again by Definition 7.7, since P_n is projective and d_{n+1}' is surjective onto its image, there exists an R-linear map $s_n:P_n\longrightarrow Q_{n+1}$ such that $d_{n+1}'\circ s_n=\sigma_n-s_{n-1}\circ d_n$:

$$\begin{tikzcd}
 & P_n \arrow[r, "d_n"] \arrow[dl, dashed, "\exists s_n"'] \arrow[d, "\sigma_n-s_{n-1}\circ d_n"'] & P_{n-1} \arrow[r, "d_{n-1}"] \arrow[dl, "s_{n-1}"'] \arrow[d, "\sigma_{n-1}"'] & P_{n-2} \arrow[r] \arrow[dl, "s_{n-2}"'] \arrow[d, "\sigma_{n-2}"'] & \cdots \arrow[dl] \\
Q_{n+1} \arrow[r, "d_{n+1}'"'] & Q_n \arrow[r, "d_n'"'] & Q_{n-1} \arrow[r, "d_{n-1}'"'] & Q_{n-2} \arrow[r] & \cdots
\end{tikzcd}$$

Hence we have $\varphi_n-\psi_n=\sigma_n=d_{n+1}'\circ s_n+s_{n-1}\circ d_n$, as required. ■

As a corollary, we obtain the required statement on the uniqueness of projective resolutions:

Theorem 11.4 (*Comparison Theorem*)

Let $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$ and $Q_\bullet \overset{\varepsilon'}{\twoheadrightarrow} M$ be two projective resolutions of an R-module M. Then $P_\bullet$ and $Q_\bullet$ are homotopy equivalent. More precisely, there exist chain maps $\varphi_\bullet : P_\bullet \longrightarrow Q_\bullet$ and $\psi_\bullet : Q_\bullet \longrightarrow P_\bullet$ lifting the identity on M and such that $\psi_\bullet \circ \varphi_\bullet \sim \mathrm{Id}_{P_\bullet}$ and $\varphi_\bullet \circ \psi_\bullet \sim \mathrm{Id}_{Q_\bullet}$.

Proof: Consider the identity morphism $\mathrm{Id}_M : M \longrightarrow M$.

By the Lifting Theorem, there exists a chain map $\varphi_\bullet : P_\bullet \longrightarrow Q_\bullet$, unique up to homotopy, such that $H_0(\varphi_\bullet) = \mathrm{Id}_M$ and $\mathrm{Id}_M \circ \varepsilon = \varepsilon' \circ \varphi_0$. Likewise, there exists a chain map $\psi_\bullet : Q_\bullet \longrightarrow P_\bullet$, unique up to homotopy, such that $H_0(\varphi_\bullet) = \mathrm{Id}_M$ and $\mathrm{Id}_M \circ \varepsilon' = \varepsilon \circ \psi_0$.

$$\begin{tikzcd}
\cdots \arrow[r] & P_n \arrow[r, "d_n"] \arrow[dd, dashed, shift left, "\exists\varphi_n"] & \cdots \arrow[r] & P_1 \arrow[r, "d_1"] \arrow[dd, dashed, shift left, "\exists\varphi_1"] \arrow[ddr, phantom, "\circlearrowleft"] & P_0 \arrow[r, "\varepsilon"] \arrow[dd, dashed, shift left, "\exists\varphi_0"] \arrow[ddr, phantom, "\circlearrowleft"] & M \arrow[r] \arrow[dd, shift left, "\mathrm{Id}_M"] & 0 \\
\cdots & & \cdots & & & & \\
\cdots \arrow[r] & Q_n \arrow[r, "d'_n"'] \arrow[uu, dashed, shift left, "\exists\psi_n"] & \cdots \arrow[r] & Q_1 \arrow[r, "d'_1"'] \arrow[uu, dashed, shift left, "\exists\psi_1"] & Q_0 \arrow[r, "\varepsilon'"] \arrow[uu, dashed, shift left, "\exists\psi_0"] & M \arrow[r] \arrow[uu, shift left, "\mathrm{Id}_M"] & 0
\end{tikzcd}$$

Now, $\psi_\bullet \circ \varphi_\bullet$ and $\mathrm{Id}_{P_\bullet}$ are both chain maps that lift the identity map $\mathrm{Id} : H_0(P_\bullet) \longrightarrow H_0(P_\bullet)$. Therefore, by the uniqueness statement in the Lifting Theorem, we have $\psi_\bullet \circ \varphi_\bullet \sim \mathrm{Id}_{P_\bullet}$. Likewise, $\varphi_\bullet \circ \psi_\bullet$ and $\mathrm{Id}_{Q_\bullet}$ are both chain maps that lift the identity map $\mathrm{Id}_M : H_0(Q_\bullet) \longrightarrow H_0(Q_\bullet)$, therefore they are homotopic, that is $\varphi_\bullet \circ \psi_\bullet \sim \mathrm{Id}_{Q_\bullet}$. ■

Another way to construct projective resolutions is given by the following Lemma, often called the *Horseshoe Lemma*, because it requires to fill in a horseshoe-shaped diagram:

Lemma 11.5 (*Horseshoe Lemma*)

Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be a short exact sequence of R-modules. Let $P'_\bullet \overset{\varepsilon'}{\twoheadrightarrow} M'$ be a resolution of M' and $P''_\bullet \overset{\varepsilon''}{\twoheadrightarrow} M''$ be a **projective** resolution of M''.

$$\begin{tikzcd}
 & \vdots \arrow[d] & & \vdots \arrow[d] & \\
 & P'_1 \arrow[d] & & P''_1 \arrow[d] & \\
 & P'_0 \arrow[d, "\varepsilon'"'] & & P''_0 \arrow[d, "\varepsilon''"'] & \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

Then, there exists a resolution $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$ of M such that $P_n \cong P'_n \oplus P''_n$ for each $n \in \mathbb{Z}_{\geqslant 0}$ and the s.e.s. $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ lifts to a s.e.s. of chain complexes $0_\bullet \longrightarrow P'_\bullet \xrightarrow{i_\bullet} P_\bullet \xrightarrow{\pi_\bullet} P''_\bullet \longrightarrow 0_\bullet$ where $i_\bullet$ and $\pi_\bullet$ are the canonical injection and projection. Moreover, if $P'_\bullet \overset{\varepsilon'}{\twoheadrightarrow} M'$ is a projective resolution, then so is $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$.

Proof: Exercise.

[Hint: Proceed by induction on n, and use the Snake Lemma.]

■

Finally, we note that dual to the notion of a projective resolution is the notion of an injective resolution:

Definition 11.6 (*Injective resolution*)

Let M be an R-module. An **injective resolution** of M is a non-negative cochain complex of injective R-modules

$$(I^\bullet, d^\bullet) = \big(I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots\big)$$

which is exact at I^n for every $n \geqslant 1$ and such that $H^0(I^\bullet) = \ker d^0/0 \cong M$.

Notation: Letting $\iota : M \hookrightarrow I^0$ denote the natural injection, we have a so-called **augmented complex**

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

associated to the injective resolution $(I^\bullet, d^\bullet)$, and this augmented complex is exact. Hence we will also denote injective resolutions of M by $M \overset{\iota}{\hookrightarrow} I^\bullet$.

Remark 11.1

Similarly to projective resolutions, one can prove that an injective resolution always exists. There is also a Lifting Theorem and a Comparison Theorem for injective resolutions, so that they are unique up to homotopy (of cochain complexes).

12 Ext and Tor

We now introduce the Ext and Tor groups, which are cohomology and homology groups obtained from applying Hom and tensor product functors to projective/injective resolutions. We will see later that Ext groups can be used in group cohomology to classify abelian group extensions.

Definition 12.1 (Ext-*groups*)

Let M and N be two left R-modules and let $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$ be a projective resolution of M. For $n \in \mathbb{Z}_{\geqslant 0}$, the **n-th Ext-group** of M and N is

$$\operatorname{Ext}^n_R(M, N) := H^n\big(\operatorname{Hom}_R(P_\bullet, N)\big),$$

that is, the n-th cohomology group of the cochain complex $\operatorname{Hom}_R(P_\bullet, N)$.

Recipe:

1. Choose a projective resolution $P_\bullet$ of M.
2. Apply the left exact contravariant functor $\operatorname{Hom}_R(-, N)$ to the *projective resolution*

   $$P_\bullet = \big(\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0\big)$$

   to obtain a *cochain* complex

   $$\operatorname{Hom}_R(P_0, N) \xrightarrow{d_1^*} \operatorname{Hom}_R(P_1, N) \xrightarrow{d_2^*} \operatorname{Hom}_R(P_3, N) \xrightarrow{d_3^*} \cdots.$$

of *abelian groups* (which is not exact in general).

3. Compute the cohomology of this new complex.

First of all, we have to check that the definition of the abelian groups $\mathrm{Ext}^n_R(M, N)$ is independent from the choice of the projective resolution of M.

Proposition 12.2

If $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$ and $Q_\bullet \overset{\varepsilon'}{\twoheadrightarrow} M$ are two projective resolutions of M, then the groups $H^n\big(\mathrm{Hom}_R(P_\bullet, N)\big)$ and $H^n\big(\mathrm{Hom}_R(Q_\bullet, N)\big)$ are (canonically) isomorphic, via the homomorphisms induced by the chain maps between $P_\bullet$ and $Q_\bullet$ given by the Comparison Theorem applied to the identity morphism Id_M.

Proof: By the Comparison Theorem, there exist chain maps $\varphi_\bullet : P_\bullet \longrightarrow Q_\bullet$ and $\psi_\bullet : Q_\bullet \longrightarrow P_\bullet$ lifting the identity on M and such that $\psi_\bullet \circ \varphi_\bullet \sim \mathrm{Id}_{P_\bullet}$ and $\varphi_\bullet \circ \psi_\bullet \sim \mathrm{Id}_{Q_\bullet}$.
Now, applying the functor $\mathrm{Hom}_R(-, N)$ yields morphisms of cochain complexes

$$\varphi^* : \mathrm{Hom}_R(Q_\bullet, N) \longrightarrow \mathrm{Hom}_R(P_\bullet, N) \quad \text{and} \quad \psi^* : \mathrm{Hom}_R(P_\bullet, N) \longrightarrow \mathrm{Hom}_R(Q_\bullet, N)\,.$$

Since $\varphi_\bullet \circ \psi_\bullet \sim \mathrm{Id}_{Q_\bullet}$ and $\psi_\bullet \circ \varphi_\bullet \sim \mathrm{Id}_{P_\bullet}$, it follows that $\varphi^* \circ \psi^* \sim \mathrm{Id}_{\mathrm{Hom}_R(P_\bullet, N)}$ and $\psi^* \circ \varphi^* \sim \mathrm{Id}_{\mathrm{Hom}_R(Q_\bullet, N)}$. But then, passing to cohomology, φ^* induces a group homomorphism

$$\overline{\varphi^*} : H^n\big(\mathrm{Hom}_R(Q_\bullet, N)\big) \longrightarrow H^n\big(\mathrm{Hom}_R(P_\bullet, N)\big)$$

(see Exercise 1, Exercise Sheet 5). Since $\varphi_\bullet$ is unique up to homotopy, so is φ^*, and hence $\overline{\varphi^*}$ is unique because homotopic chain maps induce the same morphisms in cohomology. Likewise, there is a unique homomorphism $\overline{\psi^*} : H^n\big(\mathrm{Hom}_R(P_\bullet, N)\big) \longrightarrow H^n\big(\mathrm{Hom}_R(Q_\bullet, N)\big)$ of abelian groups induced by $\psi_\bullet$. Finally, $\varphi^* \circ \psi^* \sim \mathrm{Id}$ and $\psi^* \circ \varphi^* \sim \mathrm{Id}$ imply that $\overline{\varphi^*} \circ \overline{\psi^*} = \mathrm{Id}$ and $\overline{\psi^*} \circ \overline{\varphi^*} = \mathrm{Id}$. Therefore, $\overline{\varphi^*}$ and $\overline{\psi^*}$ are canonically defined isomorphisms. ■

Proposition 12.3 (*Properties of* $\mathrm{Ext}^n_R(-,-)$)

Let M, M_1, M_2 and N, N_1, N_2 be R-modules and let $n \in \mathbb{Z}_{>0}$ be an integer. The following holds:

(a) $\mathrm{Ext}^0_R(M, N) \cong \mathrm{Hom}_R(M, N)$.

(b) Any morphism of R-modules $\alpha : M_1 \longrightarrow M_2$ induces a group homomorphism

$$\alpha^* : \mathrm{Ext}^n_R(M_2, N) \longrightarrow \mathrm{Ext}^n_R(M_1, N)\,.$$

(c) Any morphism of R-modules $\beta : N_1 \longrightarrow N_2$ induces a group homomorphism

$$\beta_* : \mathrm{Ext}^n_R(M, N_1) \longrightarrow \mathrm{Ext}^n_R(M, N_2)\,.$$

(d) If P is a projective R-module, then $\mathrm{Ext}^n_R(P, N) = 0$ for all $n \geqslant 1$.

(e) If I is an injective R-module, then $\mathrm{Ext}^n_R(M, I) = 0$ for all $n \geqslant 1$.

Proof: (a) Let $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$ be a projective resolution of M. Applying the left exact functor $\mathrm{Hom}_R(-, N)$ to the resolution $P_\bullet$ yields the cochain complex

$$\mathrm{Hom}_R(P_0, N) \xrightarrow{d_1^*} \mathrm{Hom}_R(P_1, N) \xrightarrow{d_2^*} \mathrm{Hom}_R(P_2, N) \xrightarrow{d_3^*} \cdots\,.$$

Therefore,

$$\mathrm{Ext}^0_R(M,N) = H^0\big(\mathrm{Hom}_R(P_\bullet,N)\big) = \ker d_1^*/0 \cong \ker d_1^*\,.$$

Now, the tail $\cdots \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0$ of the augmented complex $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$ is an exact sequence of R-modules, so that the induced sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_R(M,N) \arrow[r, "\varepsilon^*"] & \mathrm{Hom}_R(P_0,N) \arrow[r, "d_1^*"] & \cdots \end{tikzcd}$$

is exact at $\mathrm{Hom}_R(M,N)$ and at $\mathrm{Hom}_R(P_0,N)$ and it follows that

$$\mathrm{Ext}^0_R(M,N) \cong \ker d_1^* = \mathrm{Im}\,\varepsilon^* \cong \mathrm{Hom}_R(M,N)$$

because ε^* is injective.

(b) Let $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M_1$ be a projective resolution of M_1 and $P'_\bullet \overset{\varepsilon'}{\twoheadrightarrow} M_2$ be a projective resolution of M_2. The Lifting Theorem implies that α lifts to a chain map $\varphi_\bullet : P_\bullet \longrightarrow P'_\bullet$. Then, $\varphi_\bullet$ induces a morphism of cochain complexes $\varphi^* : \mathrm{Hom}_R(P'_\bullet,N) \longrightarrow \mathrm{Hom}_R(P_\bullet,N)$ and then φ^* induces a morphism in cohomology

$$\overline{\varphi^*} : \mathrm{Ext}^n_R(M_2,N) \longrightarrow \mathrm{Ext}^n_R(M_1,N)\,.$$

Thus, we set $\alpha^* := \overline{\varphi^*}$.

(c) Let $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$ be a projective resolution of M. Then, there is a morphism of cochain complexes $\beta^\bullet : \mathrm{Hom}_R(P_\bullet,N_1) \longrightarrow \mathrm{Hom}_R(P_\bullet,N_2)$ induced by β, which, in turn, induces a homomorphism of abelian groups β_* in cohomology.

(d) Since P is projective, we may choose $\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow P$ as a projective resolution of P (i.e. $P_0 := P$, $P_n = 0$ for any $n \geqslant 1$), augmented by the identity morphism $\mathrm{Id}_P : P \longrightarrow P$. Then the induced cochain complex is

$$\begin{tikzcd} \mathrm{Hom}_R(P,N) \arrow[r, "0"] & 0 \arrow[r, "0"] & 0 \arrow[r, "0"] & \cdots, \end{tikzcd}$$

so that clearly $\mathrm{Ext}^n_R(P,N) = 0$ if $n \geqslant 1$.

(e) Let $P_\bullet \overset{\varepsilon}{\twoheadrightarrow} M$ be a projective resolution of M. Since I is injective, the functor $\mathrm{Hom}_R(-,I)$ is exact. Therefore the induced cochain complex

$$\begin{tikzcd} \mathrm{Hom}_R(P_0,I) \arrow[r, "d_1^*"] & \mathrm{Hom}_R(P_1,I) \arrow[r, "d_2^*"] & \mathrm{Hom}_R(P_2,I) \arrow[r, "d_3^*"] & \cdots \end{tikzcd}$$

is exact in degree $n \geqslant 1$ and its cohomology is zero. The claim follows. ■

Remark 12.4

Using the proposition one can prove that for every $n \in \mathbb{Z}_{\geqslant 0}$, $\mathrm{Ext}^n_R(-,N) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a contravariant additive functor, and $\mathrm{Ext}^n_R(M,-) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a covariant additive functor.

Theorem 12.5 (*Long exact sequences of* Ext*-groups*)

Let M, N be R-modules.

(a) Any s.e.s. $0 \longrightarrow N_1 \xrightarrow{\varphi} N_2 \xrightarrow{\psi} N_3 \longrightarrow 0$ of R-modules induces a long exact sequence of abelian groups

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ext}^0_R(M,N_1) \arrow[r, "\varphi_*"] & \mathrm{Ext}^0_R(M,N_2) \arrow[r, "\psi_*"] & \mathrm{Ext}^0_R(M,N_3) \arrow[r, "\delta^0"] & \mathrm{Ext}^1_R(M,N_1) \arrow[r] & \ldots \\ \ldots \arrow[r] & \mathrm{Ext}^n_R(M,N_1) \arrow[r, "\varphi_*"] & \mathrm{Ext}^n_R(M,N_2) \arrow[r, "\psi_*"] & \mathrm{Ext}^n_R(M,N_3) \arrow[r, "\delta^n"] & \mathrm{Ext}^{n+1}_R(M,N_1) \arrow[r] & \ldots\,. \end{tikzcd}$$

(b) Any s.e.s. $0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$ of R-modules induces a long exact sequence of abelian groups

$$0 \longrightarrow \mathrm{Ext}^0_R(M_3, N) \xrightarrow{\beta^*} \mathrm{Ext}^0_R(M_2, N) \xrightarrow{\alpha^*} \mathrm{Ext}^0_R(M_1, N) \xrightarrow{\delta^0} \mathrm{Ext}^1_R(M_3, N) \longrightarrow \dots$$
$$\dots \longrightarrow \mathrm{Ext}^n_R(M_3, N) \xrightarrow{\beta^*} \mathrm{Ext}^n_R(M_2, N) \xrightarrow{\alpha^*} \mathrm{Ext}^n_R(M_1, N) \xrightarrow{\delta^n} \mathrm{Ext}^{n+1}_R(M_3, N) \longrightarrow \dots .$$

Proof: (a) Let $P_\bullet$ be a projective resolution of M. Then there is an induced short exact sequence of cochain complexes

$$0 \longrightarrow \mathrm{Hom}_R(P_\bullet, N_1) \xrightarrow{\varphi^\bullet} \mathrm{Hom}_R(P_\bullet, N_2) \xrightarrow{\psi^\bullet} \mathrm{Hom}_R(P_\bullet, N_3) \longrightarrow 0$$

because each module P_n is projective. Indeed, at each degree $n \in \mathbb{Z}_{\geqslant 0}$ this sequence is

$$0 \longrightarrow \mathrm{Hom}_R(P_n, N_1) \xrightarrow{\varphi_*} \mathrm{Hom}_R(P_n, N_2) \xrightarrow{\psi_*} \mathrm{Hom}_R(P_n, N_3) \longrightarrow 0$$

obtained by applying the functor $\mathrm{Hom}_R(P_n, -)$, which is exact as P_n is projective. It is then easily checked that this gives a s.e.s. of cochain complexes, that is that the induced differential maps commute with the induced homomorphisms φ_*. Thus, applying Theorem 10.14 yields the required long exact sequence in cohomology.

(b) Let $P_\bullet$ be a projective resolution of M_1 and let $Q_\bullet$ be a projective resolution of M_3. By the Horseshoe Lemma (Lemma 11.5), there exists a projective resolution $R_\bullet$ of M_2 and a short exact sequence of chain complexes

$$0 \longrightarrow P_\bullet \longrightarrow R_\bullet \longrightarrow Q_\bullet \longrightarrow 0\,,$$

lifting the initial s.e.s. of R-modules. Since Q_n is projective for each $n \geqslant 0$, the sequences

$$0 \longrightarrow P_n \longrightarrow R_n \longrightarrow Q_n \longrightarrow 0$$

are split exact for each $n \geqslant 0$. Therefore applying $\mathrm{Hom}_R(-, N)$ yields a split exact s.e.s.

$$0 \longrightarrow \mathrm{Hom}_R(Q_n, N) \longrightarrow \mathrm{Hom}_R(R_n, N) \longrightarrow \mathrm{Hom}_R(P_n, N) \longrightarrow 0$$

for each for each $n \geqslant 0$. It follows that there is a s.e.s. of cochain complexes

$$0 \longrightarrow \mathrm{Hom}_R(Q_\bullet, N) \longrightarrow \mathrm{Hom}_R(R_\bullet, N) \longrightarrow \mathrm{Hom}_R(P_\bullet, N) \longrightarrow 0.$$

The associated long exact sequence in cohomology (Theorem 10.14) is the required long exact sequence. ■

The above results show that the Ext groups “measure” and "repair" the non-exactness of the functors $\mathrm{Hom}_R(M, -)$ and $\mathrm{Hom}_R(-, N)$.

The next result is called “dimension-shifting” in the literature (however, it would be more appropriate to call it “degree-shifting”); it provides us with a method to compute Ext-groups by induction.

Remark 12.6 (*Dimension shifting*)

Let N be an R-module and consider a s.e.s.

$$0 \longrightarrow L \xrightarrow{\alpha} P \xrightarrow{\beta} M \longrightarrow 0$$

of R-modules, where is P projective (if M is given, take e.g. P free mapping onto M, with kernel L). Then $\operatorname{Ext}^n_R(P, N) = 0$ for all $n \geqslant 1$ and applying the long exact sequence of Ext-groups yields at each degree $n \geqslant 1$ an exact sequence of the form

$$0 \xrightarrow{\alpha^*} \operatorname{Ext}^n_R(L, N) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R(M, N) \xrightarrow{\beta^*} 0,$$

where the connecting homomorphism δ^n is therefore forced to be an isomorphism:

$$\operatorname{Ext}^{n+1}_R(M, N) \cong \operatorname{Ext}^n_R(L, N)\,.$$

Note that the same method applies to the second variable with a short exact sequence whose middle term is injective.

A consequence of the dimension shifting argument is that it allows us to deal with direct sums and products of modules in each variable of the Ext-groups. For this we need the following lemma:

Lemma 12.7

Consider the following commutative diagram of R-modules with exact rows:

$$\begin{tikzcd}
A' \arrow[r, "\alpha"] \arrow[d, "f"'] & A \arrow[r, "\beta"] \arrow[d, "g"'] & A'' \arrow[r] & 0 \\
B' \arrow[r, "\varphi"'] & B \arrow[r, "\psi"'] & B'' \arrow[r] & 0
\end{tikzcd}$$

Then there exists a morphism $h \in \operatorname{Hom}_R(A'', B'')$ such that $h \circ \beta = \psi \circ g$. Moreover, if f and g are isomorphisms, then so is h.

Proof: See Exercise 28. ■

Proposition 12.8 (Ext *and direct sums*)

(a) Let $\{M_i\}_{i\in I}$ be a family of R-modules and let N be an R-module. Then

$$\operatorname{Ext}^n_R\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \operatorname{Ext}^n_R(M_i, N) \quad \forall\, n \geqslant 0\,.$$

(b) Let M be an R-module and let $\{N_i\}_{i\in I}$ be a family of R-modules. Then

$$\operatorname{Ext}^n_R\left(M, \prod_{i\in I} N_i\right) \cong \prod_{i\in I} \operatorname{Ext}^n_R(M, N_i) \quad \forall\, n \geqslant 0.$$

Proof: (a) **Case** $n = 0$. By Proposition 12.3(a) and the universal property of the direct sum (Proposition 5.2), we have

$$\mathrm{Ext}^0_R\left(\bigoplus_{i\in I} M_i, N\right) \cong \mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N) \cong \prod_{i\in I} \mathrm{Ext}^0_R(M_i, N)\,.$$

Now, suppose that $n \geqslant 1$ and choose for each $i \in I$ a s.e.s. of R-modules

$$0 \longrightarrow L_i \longrightarrow P_i \longrightarrow M_i \longrightarrow 0,$$

where P_i is projective (e.g. choose P_i free with quotient isomorphic to M_i and kernel L_i). These sequences induce a s.e.s.

$$0 \longrightarrow \bigoplus_{i\in I} L_i \longrightarrow \bigoplus_{i\in I} P_i \longrightarrow \bigoplus_{i\in I} M_i \longrightarrow 0\,.$$

Case $n \geqslant 1$**:** We proceed by induction on n.
First, for n=1, using a long exact sequence of Ext-groups, we obtain a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_R(\bigoplus_{i\in I} P_i, N) \arrow[r] \arrow[d, "\cong"] \arrow[rd, phantom, "\circlearrowleft"] & \mathrm{Hom}_R(\bigoplus_{i\in I} L_i, N) \arrow[r, "\delta^0"] \arrow[d, "\cong"] & \mathrm{Ext}^1_R(\bigoplus_{i\in I} M_i, N) \arrow[r] & \mathrm{Ext}^1_R(\bigoplus_{i\in I} P_i, N) \\
\prod_{i\in I} \mathrm{Hom}_R(P_i, N) \arrow[r] & \prod_{i\in I} \mathrm{Hom}_R(L_i, N) \arrow[r] & \prod_{i\in I} \mathrm{Ext}^1_R(M_i, N) \arrow[r] & \prod_{i\in I} \mathrm{Ext}^1_R(P_i, N)
\end{tikzcd}$$

with the following properties:

- the morphisms of the bottom row are induced componentwise;
- both rows are exact; and
- the two vertical isomorphisms are given by the case $n = 0$.

Since P_i is projective for every $i \in I$, so is $\bigoplus_{i\in I} P_i$, thus Proposition 12.3 yields

$$\mathrm{Ext}^1_R\left(\bigoplus_{i\in I} P_i, N\right) \cong 0 \cong \prod_{i\in I} \mathrm{Ext}^1_R(P_i, N)\,.$$

Therefore Lemma 28 yields

$$\mathrm{Ext}^1_R\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \mathrm{Ext}^1_R(M_i, N)\,.$$

Now assume that $n \geqslant 2$ and assume that the claim holds for the $(n-1)$-st Ext-groups, that is

$$\mathrm{Ext}^{n-1}_R\left(\bigoplus_{i\in I} L_i, N\right) \cong \prod_{i\in I} \mathrm{Ext}^{n-1}_R(L_i, N)\,.$$

Then, applying the Dimension Shifting argument yields

$$\mathrm{Ext}^{n-1}_R\left(\bigoplus_{i\in I} L_i, N\right) \cong \mathrm{Ext}^{n}_R\left(\bigoplus_{i\in I} M_i, N\right)\,.$$

and

$$\mathrm{Ext}^{n-1}_R(L_i, N) \cong \mathrm{Ext}^n_R(M_i, N) \quad \forall i \in I\,,$$

so that

$$\prod_{i\in I} \mathrm{Ext}^{n-1}_R(L_i, N) \cong \prod_{i\in I} \mathrm{Ext}^n_R(M_i, N)\,.$$

Hence the required isomorphism

$$\mathrm{Ext}^{n}_R\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \mathrm{Ext}^n_R(M_i, N)\,.$$

(b) Similar to (a): proceed by induction and apply a dimension shift. (In this case, we use s.e.s.'s with injective middle terms.) ■

To end this chapter, we introduce the Tor-groups, which "measure" the non-exactness of the functors $M \otimes_R -$ and $- \otimes_R N$.

Definition 12.9 (Tor-*groups*)

Let M be a right R-module and N be a left R-module. Let $P_\bullet$ be a projective resolution of N. For $n \in \mathbb{Z}_{\geqslant 0}$, the **n-th Tor-group** of M and N is

$$\operatorname{Tor}_n^R(M, N) := H_n(M \otimes_R P_\bullet),$$

that is, the n-th homology group of the chain complex $M \otimes_R P_\bullet$.

Proposition 12.10

Let M, M_1, M_2, M_3 be right R-modules and let N, N_1, N_2, N_3 be left R-modules and let $n \in \mathbb{Z}_{>0}$.

(a) The group $\operatorname{Tor}_n^R(M, N)$ is independant of the choice of the projective resolution of N.

(b) $\operatorname{Tor}_0^R(M, N) \cong M \otimes_R N$.

(c) $\operatorname{Tor}_n^R(-, N) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is an additive covariant functor.

(d) $\operatorname{Tor}_n^R(M, -) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is an additive covariant functor.

(e) $\operatorname{Tor}_n^R(M_1 \oplus M_2, N) \cong \operatorname{Tor}_n^R(M_1, N) \oplus \operatorname{Tor}_n^R(M_2, N)$.

(f) $\operatorname{Tor}_n^R(M, N_1 \oplus N_2) \cong \operatorname{Tor}_n^R(M, N_1) \oplus \operatorname{Tor}_n^R(M, N_2)$.

(g) If either M or N is flat (so in particular if either M or N is projective), then $\operatorname{Tor}_n^R(M, N) = 0$ for all $n \geqslant 1$.

(h) Any s.e.s. $0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$ of right R-modules induces a long exact sequence

$$\begin{tikzcd} \cdots \arrow[r] & \operatorname{Tor}_{n+1}^R(M_3, N) \arrow[r, "\delta_{n+1}"] & \operatorname{Tor}_n^R(M_1, N) \arrow[r, "\alpha_*"] & \operatorname{Tor}_n^R(M_2, N) \arrow[r, "\beta_*"] & \operatorname{Tor}_n^R(M_3, N) \arrow[r, "\delta_n"] & \cdots \\ \cdots \arrow[r] & \operatorname{Tor}_1^R(M_3, N) \arrow[r, "\delta_1"] & M_1 \otimes_R N \arrow[r, "\alpha \otimes \mathrm{Id}_N"] & M_2 \otimes_R N \arrow[r, "\beta \otimes \mathrm{Id}_N"] & M_3 \otimes_R N \arrow[r] & 0 \end{tikzcd}$$

of abelian groups.

(i) Any s.e.s. $0 \longrightarrow N_1 \xrightarrow{\alpha} N_2 \xrightarrow{\beta} N_3 \longrightarrow 0$ of left R-modules induces a long exact sequence

$$\begin{tikzcd} \cdots \arrow[r] & \operatorname{Tor}_{n+1}^R(M, N_3) \arrow[r, "\delta_{n+1}"] & \operatorname{Tor}_n^R(M, N_1) \arrow[r, "\alpha_*"] & \operatorname{Tor}_n^R(M, N_2) \arrow[r, "\beta_*"] & \operatorname{Tor}_n^R(M, N_3) \arrow[r, "\delta_n"] & \cdots \\ \cdots \arrow[r] & \operatorname{Tor}_1^R(M, N_3) \arrow[r, "\delta_1"] & M \otimes_R N_1 \arrow[r, "\mathrm{Id}_M \otimes \alpha"] & M \otimes_R N_2 \arrow[r, "\mathrm{Id}_M \otimes \beta"] & M \otimes_R N_3 \arrow[r] & 0 \end{tikzcd}$$

of abelian groups.

The proof of the above results are in essence similar to the proofs given for the Ext-groups.

13 Exercises for Chapter 3

Exercise 15

Verify that for each $n \in \mathbb{Z}$,

$$H_n(-) : \mathbf{Ch}(_R\mathbf{Mod}) \longrightarrow {_R\mathbf{Mod}} \text{ and } H^n(-) : \mathbf{CoCh}(_R\mathbf{Mod}) \longrightarrow {_R\mathbf{Mod}}$$

are covariant functors.

Exercise 16

(a) Let p be a prime number and consider the following chain complexes of $\mathbb{Z}$-modules:

$$\cdots \to 0 \to \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \to 0 \to \cdots$$

$$\cdots \to 0 \to \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0 \to \cdots$$

$$\cdots \to 0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \to 0 \to \cdots$$

$$\cdots \to 0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/6\mathbb{Z} \to 0 \to \cdots$$

Compute the homology modules of each complex.

(b) Consider the following morphism of chain complexes of abelian groups:

$$\begin{tikzcd}
\cdots \arrow[r, "0"] & \mathbb{Z} \arrow[r, "="] \arrow[d] & \mathbb{Z} \arrow[r, "0"] \arrow[d] & \mathbb{Z} \arrow[r, "="] \arrow[d] & \mathbb{Z} \arrow[r, "0"] \arrow[d] & \mathbb{Z} \arrow[r, "\cdot p"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, "\pi"] & 0 \\
\cdots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Compute the homology of both the horizontal chain complexes and prove that each map induced in homology by the vertical maps is an isomorphism.

Exercise 17

Let $C_\bullet$ be a chain complex of R-modules. Prove that TFAE:

(a) $C_\bullet$ is **exact**, i.e. exact at C_n for each $n \in \mathbb{Z}$;

(b) $C_\bullet$ is **acyclic**, i.e. $H_n(C_\bullet) = 0$ for all $n \in \mathbb{Z}$;

(c) the chain map $0_\bullet \longrightarrow C_\bullet$ is a quasi-isomorphism.

Exercise 18

(a) Let $\mathbf{0}_\bullet \longrightarrow \mathbf{A}_\bullet \longrightarrow \mathbf{B}_\bullet \longrightarrow \mathbf{C}_\bullet \longrightarrow \mathbf{0}_\bullet$ be a s.e.s. of chain complexes. Prove that if two of the three complexes $\mathbf{A}_\bullet, \mathbf{B}_\bullet, \mathbf{C}_\bullet$ are exact, then so is the third.

(b) Let $\varphi_\bullet$ be a morphism of chain complexes. Prove that if $\ker(\varphi_\bullet)$ and $\operatorname{coker}(\varphi_\bullet)$ are acyclic, then $\varphi_\bullet$ is a quasi-isomorphism.

Exercise 19

Let K be a field and let $\mathbf{C}_\bullet$ be a complex of K-vector spaces which is bounded below and above, i.e. assume $C_m = 0$ for every index m greater than $N \in \mathbb{Z}_{>0}$ or less than 0. Prove that

$$\sum_{n=0}^{N}(-1)^n \dim_k C_n = \sum_{n=0}^{N}(-1)^n \dim_k H_n(\mathbf{C}_\bullet)\,.$$

This number is called the *Euler-Poincaré characteristic* of the complex $\mathbf{C}_\bullet$.

Definition. A chain complex $\mathbf{C}_\bullet$ of R-modules is called **split exact** if it is exact and if moreover for each $n \in \mathbb{Z}$, $Z_n := Z_n(\mathbf{C}_\bullet)$ is a direct summand of C_n, i.e. $C_n = Z_n \oplus U_n$ for some R-module U_n.

Example 9

Let $(\mathbf{C}_\bullet, \mathbf{d}_\bullet)$ be a chain complex of R-modules.

(a) With the notation of the definition, prove that:

(i) If $\mathbf{C}_\bullet$ is split exact, d_n induces an isomorphism $U_n \xrightarrow{\cong} Z_{n-1}$ for all $n \in \mathbb{Z}$.

(ii) The inverse of the isomorphism of (a) induces an R-homomorphism $s_n : C_{n-1} \longrightarrow C_n$ such that $\ker(s_n) = U_{n-1}$ and $\operatorname{Im}(s_n) = U_n$.

(iii) $\mathbf{C}_\bullet$ is split exact if and only if $\operatorname{Id}_{\mathbf{C}_\bullet}$ is homotopic to the zero chain map.

(b) Prove that $(\mathbf{C}_\bullet, \mathbf{d}_\bullet)$ is split exact if and only if $\mathbf{C}_\bullet$ is exact and there are R-homomorphisms $s_n : C_n \longrightarrow C_{n+1}$ such that $d_{n+1}s_nd_{n+1} = d_{n+1}$.

(Hint: For the sufficient condition, prove $\ker(sd) \subseteq \operatorname{Im}(ds)$ (where we omit the indices for clarity).)

(c) For $R \in \{\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\}$ prove that the following complex of R-modules is acyclic but not split exact:

$$\cdots \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cdot 2} \cdots$$

Exercise 20

Formulate the following definitions formally:

- of a subcomplex and of a quotient complex of cochain complexes;
- of kernels, images, and cokernels of morphisms of cochain complexes;
- of a quasi-isomorphisms, homotopic chain maps and homotopy equivalences.

Exercise 21

Consider the two non-negative chain complexes of $\mathbb{Z}$-modules

$$P_\bullet := (0 \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 4} \mathbb{Z}) \quad \text{and} \quad Q_\bullet := (0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\mathrm{Id}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z})$$

where the rightmost module is assumed to be in degree zero. Let

$$f : H_0(P_\bullet) = \mathbb{Z}/4\mathbb{Z} \longrightarrow H_0(Q_\bullet) = \mathbb{Z}/2\mathbb{Z}$$

be the unique non-zero $\mathbb{Z}$-linear map.

(a) Find all possible chain maps $\varphi_\bullet : P_\bullet \longrightarrow Q_\bullet$ lifting f.

(b) Construct homotopies between the different liftings of part (a).

Exercise 22

Prove the Horseshoe Lemma.

Exercise 23

(a) State a Lifting Theorem for injective modules, and give a sketch of proof.

(b) State a Comparison Theorem for injective resolutions, and give a sketch of proof.

Exercise 24

Let M, M', M'' and N be R-modules, let $\alpha : M \longrightarrow M'$ and $\beta : M' \longrightarrow M''$ be R-linear maps, and let $\alpha^* : \operatorname{Ext}^n_R(M', N) \longrightarrow \operatorname{Ext}^n_R(M, N)$ and $\beta^* : \operatorname{Ext}^n_R(M'', N) \longrightarrow \operatorname{Ext}^n_R(M', N)$ be the induced $\mathbb{Z}$-linear maps. Prove that $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$.

Exercise 25

(a) Prove that if $\operatorname{Ext}^1_R(M, N) = 0$, then any s.e.s. $0 \longrightarrow N \longrightarrow X \longrightarrow M \longrightarrow 0$ of R-modules splits.

(b) Let P be an R-module. Prove that the following assertions are equivalent:

(i) P is projective;

(ii) $\operatorname{Ext}^n_R(P, N) = 0$ for every $n \geqslant 1$ and each R-module N; and

(iii) $\operatorname{Ext}^1_R(P, N) = 0$ for each R-module N.

Exercise 26

Let A be a $\mathbb{Z}$-module and let p be a positive prime number. Prove that:

(a) $\operatorname{Tor}^{\mathbb{Z}}_\bullet(A, \mathbb{Z}/p\mathbb{Z})$ is the homology of the complex $0 \longrightarrow A \xrightarrow{\cdot p} A \longrightarrow 0$;

(b) $\operatorname{Tor}^{\mathbb{Z}}_0(A, \mathbb{Z}/p\mathbb{Z}) \cong A/pA$,

$\operatorname{Tor}^{\mathbb{Z}}_1(A, \mathbb{Z}/p\mathbb{Z}) \cong A_p := \{a \in A \mid p \cdot a = 0\}$,

$\operatorname{Tor}^{\mathbb{Z}}_n(A, \mathbb{Z}/p\mathbb{Z}) = 0$ if $n \geqslant 2$;

(c) $\operatorname{Ext}^\bullet_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A)$ is the cohomology of the complex $0 \longrightarrow A \xrightarrow{\cdot p} A \longrightarrow 0$;

(d) $\operatorname{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A) \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A) \cong A_p$,

$\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A) \cong A/pA$,

$\operatorname{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A) = 0$ if $n \geqslant 2$.

Exercise 27

Let K be a field and let $A := K[t]/(t^2)$. Write K for the trivial A-module.

(a) Find a projective resolution of K. (Hint: use multiplication by $\bar{t} := t + (t^2)$, the class of t in the quotient.)

(b) Prove that

$$\operatorname{Ext}_A^n(K, M) \cong \begin{cases} M_{\bar{t}} & \text{if } n = 0, \\ M_{\bar{t}}/\bar{t}M & \text{if } n \geqslant 1\,, \end{cases}$$

where $M_{\bar{t}} = \{m \in M \,|\, \bar{t} \cdot m = 0\}$.

Exercise 28

Consider the following commutative diagram of R-modules with exact rows:

$$\begin{tikzcd} A' \arrow[r, "\alpha"] \arrow[d, "f"'] & A \arrow[r, "\beta"] \arrow[d, "g"'] & A'' \arrow[r] & 0 \\ B' \arrow[r, "\varphi"'] & B \arrow[r, "\psi"'] & B'' \arrow[r] & 0 \end{tikzcd}$$

Prove that there exists a morphism $h \in \operatorname{Hom}_R(A'', B'')$ such that $h \circ \beta = \psi \circ g$. Moreover, if f and g are isomorphisms, then so is h.

Exercise 29 (*Generalised Dimension Shifting*)

(a) Let M and N be R-modules. Let $(P_\bullet, d_\bullet)$ be a projective resolution of M and set $K_i := \ker d_i$ for each $i \in \mathbb{Z}_{\geqslant 0}$. Then for every $n \in \mathbb{Z}_{\geqslant 2}$, we have

$$\operatorname{Ext}_R^n(M, N) \cong \operatorname{Ext}_R^{n-1}(K_0, N) \cong \ldots \cong \operatorname{Ext}_R^2(K_{n-3}, N) \cong \operatorname{Ext}_R^1(K_{n-2}, N)\,.$$

(b) State and prove a similar result for the Tor-groups.

Exercise 30

Let M be a right R-module and let N be a left R-module.

(a) Define $\operatorname{tor}_n^R(M, N)$ using a projective resolution of M and applying $- \otimes_R N$.

(b) Prove that $\operatorname{tor}_n^R(M, N) \cong \operatorname{Tor}_n^R(M, N)$ using dimension shifting.

Exercise 31

Let M, N be R-modules.

(a) Define $\operatorname{ext}_R^n(M, N)$ using an injective resolution of N and applying $\operatorname{Hom}_R(M, -)$.

(b) Prove that $\operatorname{ext}_R^n(M, I) = 0$, $\forall\, n \geqslant 1$, if I is an injective R-module.

(c) Prove that $\operatorname{ext}_R^n(M, N) \cong \operatorname{Ext}_R^n(M, N)$ using dimension shifting.

Chapter 4. Cohomology of Groups

Throughout this chapter we assume that we are given a group G and consider modules over the group algebra KG of G over a commutative ring K. The main aim of this chapter is to introduce the *cohomology groups* of G and describe concrete projective resolutions which shall allow use to compute them in some cases.

Notation for the chapter. Throughout this chapter we let $(G, \cdot)$ (in multiplicative notation) denote a group and $(K, +, \cdot)$ denote an (associative and unital). commutative ring.

References:

[Bro94] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994.

[Eve91] L. Evens, *The cohomology of groups*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1991.

[Rot09] J. J. Rotman, *An introduction to the theory of groups. Fourth ed.*, Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[Wei94] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

14 Modules over the Group Algebra

Lemma-Definition 14.1 (*Group algebra*)

If G is a group and K is a commutative ring, we may form the **group ring** KG whose elements are the formal linear combinations $\sum_{g\in G} \lambda_g g$ ($\lambda_g \in K$), and addition and multiplication are given by

$$\sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_{g\in G} (\lambda_g + \mu_g) g \quad \text{and} \quad \big(\sum_{g\in G} \lambda_g g\big) \cdot \big(\sum_{h\in G} \mu_h h\big) = \sum_{g,h\in G} (\lambda_g \mu_h) gh\,.$$

Thus KG is a K-algebra, which as a K-module is free with basis G. Hence we usually call KG the **group algebra of G over K** rather than simply *group ring*.

Proof: By definition KG is a free K-module with basis G, and the multiplication in G is extended by K-bilinearity to the multiplication $KG \times KG \longrightarrow KG$. It is then straightforward to check that this makes KG into a K-algebra. ■

Remark 14.2

Clearly:

- $1_{KG} = 1_K \cdot 1_G = 1_G$;
- the K-rank of KG is $|G|$;
- KG is commutative if and only if G is an abelian group.

In this lecture, we will mainly work with the following commutative rings: $K = \mathbb{Z}$ the ring of integers, and fields.

Remark 14.3

(a) **KG-modules and K-representations**:
If K is a field, then specifying a KG-module V is the same thing as specifying a K-vector space V together with a K-linear action of G on V, i.e. a group homomorphism

$$G \longrightarrow \mathrm{Aut}_K(V) =: \mathrm{GL}(V)\,,$$

or in other words a *linear representation of G over K*.

Similarly, if $K = \mathbb{Z}$, then specifying a $\mathbb{Z}G$-module M is the same thing as specifying a $\mathbb{Z}$-module M together with a $\mathbb{Z}$-linear action of G on M, i.e. a group homomorphism

$$G \longrightarrow \mathrm{Aut}_{\mathbb{Z}}(M)$$

also called an *integral representation of G*.

(b) **Left and right KG-modules**:
Since G is a group, the map $KG \longrightarrow KG$ such that $g \mapsto g^{-1}$ for each $g \in G$ is an anti-automorphism. It follows that any *left* KG-module M may be regarded as a *right* KG-module via the right G-action $m \cdot g := g^{-1}m$. Thus the sidedness of KG-modules is not usually an issue.

(c) **The trivial KG-module**:
The commutative ring K itself can be seen as a KG-module via the G-action

$$\begin{aligned} \cdot\, : G \times K &\longrightarrow K \\ (g, \lambda) &\longmapsto g \cdot \lambda := \lambda \end{aligned}$$

extended by K-linearity to the whole of KG. This module is called **the trivial** KG-module. An arbitrary KG-module A on which G acts trivially is also called **a trivial KG-module**.

(d) **Tensor products of KG-modules balanced over K**:
If M and N are two **left** KG-modules, then the tensor product $M \otimes_K N$ of M and N balanced over K can be made into a KG-module via the *diagonal action* of G, i.e.

$$g \cdot (m \otimes n) := gm \otimes gn \qquad \forall\, g \in G, \forall m \in M, \forall\, n \in N\,.$$

(e) **Morphisms of KG-modules**:
If M and N are two KG-modules, then the abelian group $\mathrm{Hom}_K(M, N)$ can be made into a KG-module via the *conjugation action* of G, i.e.

$$(g \cdot f)(m) := g \cdot f(g^{-1} \cdot m) \qquad \forall\, g \in G, \forall m \in M\,.$$

(f) **The augmentation map and the augmentation ideal**:
The map

$$\varepsilon : KG \longrightarrow K, \sum_{g \in G} \lambda_g g \mapsto \sum_{g \in G} \lambda_g$$

is a surjective K-algebra homomorphism, called **augmentation homomorphism (or map)**. Its kernel $\ker(\varepsilon) =: IG$ is an ideal and it is called the **augmentation ideal** of KG. Clearly,

$$KG/IG \cong K$$

as K-algebras.
Notice that ε is hence also a homomorphism of KG-modules, so that we can also see IG as a KG-submodule of KG.

Lemma 14.4

The following assertions hold.

(a) The augmentation ideal IG is a free K-module with K-basis $\{g - 1 \mid g \in G\backslash\{1\}\}$.

(b) If X is a set of generators for the group G, then IG is generated as a KG-module by the set $\{x - 1 \mid x \in X\}$.

(c) If M is a KG-module, then $IG \cdot M = \langle g \cdot m - m \mid g \in G, m \in M\rangle_K$.

(d) There is an isomorphism of abelian groups $(IG/(IG)^2, +) \cong (G_{ab}, \cdot)$, where $G_{ab} := G/[G, G]$ denotes the abelianisation of G.

Proof: (a) First of all, the set $S := \{g - 1 \mid g \in G\backslash\{1\}\}$ is clearly contained in $\ker\varepsilon$ by definition of ε. The set S is K-linearly independent since

$$\begin{aligned} 0 &= \sum_{g \in G\backslash\{1\}} \lambda_g(g-1) \qquad (\lambda_g \in K) \\ &= \sum_{g \in G\backslash\{1\}} \lambda_g g - \sum_{g \in G\backslash\{1_G\}} \lambda_g \end{aligned}$$

implies that $\lambda_g = 0$ for every $g \in G\backslash\{1\}$, because G is K-linearly independent in KG.
To prove that S spans IG as a K-module, let $\sum_{g \in G} \lambda_g g$ ($\lambda_g \in K$) be an element of $IG = \ker\varepsilon$. Hence

$$0 = \varepsilon(\sum_{g \in G} \lambda_g g) = \sum_{g \in G} \lambda_g$$

and it follows that

$$\sum_{g \in G} \lambda_g g = \sum_{g \in G} \lambda_g g - 0 = \sum_{g \in G} \lambda_g g - \sum_{g \in G} \lambda_g = \sum_{g \in G} \lambda_g(g-1) = \sum_{g \in G\backslash\{1\}} \lambda_g(g-1)\,.$$

(b) Clearly, for every elements $g_1, g_2 \in G$ we have:

$$g_1g_2 - 1 = g_1(g_2 - 1) + (g_1 - 1) \quad \text{and} \quad g_1^{-1} - 1 = -g_1^{-1}(g_1 - 1)$$

Therefore $\{g - 1 \mid g \in G\backslash\{1\}\} \subseteq \langle\{x - 1 \mid x \in X\}\rangle_{KG}$, which implies that

$$IG = \langle\{g - 1 \mid g \in G\backslash\{1\}\rangle_K \subseteq \langle\{x - 1 \mid x \in X\}\rangle_{KG} \subseteq IG$$

and hence equality holds.

(c) Follows from (a).

(d) Exercise 33. ■

Definition 14.5 (*G-fixed points and G-cofixed points*)

Let M be a KG-module.

(a) The G-**fixed points** of M are by definition $M^G := \{m \in M \mid g \cdot m = m \; \forall \, g \in G\}$.

(b) The G-**cofixed points** of M are by definition $M_G := M/(IG \cdot M)$.

Remark 14.6

If M and N are KG-modules, then the following assertions holds:

(a) M^G is the largest KG-submodule of M on which G acts trivially;

(b) M_G is the largest quotient of M on which G acts trivially;

(c) $\mathrm{Hom}_K(M, N)^G = \mathrm{Hom}_{KG}(M, N)$;

(d) $(M \otimes_K N)_G \cong M \otimes_{KG} N$.

See Exercise 32.

15 (Co)homology of Groups

We can eventually define the homology and cohomology groups of a given group G.

Definition 15.1 (*Homology and cohomology of a group*)

Let A be a KG-module and let $n \in \mathbb{Z}_{\geqslant 0}$. Define:

(a) $H_n(G, A) := \mathrm{Tor}_n^{KG}(K, A)$, the n**-th homology group of** G **with coefficients in** A;

(b) $H^n(G, A) := \mathrm{Ext}^n_{KG}(K, A)$, the n**-th cohomology group of** G **with coefficients in** A.

Remark 15.2

A priori the definition of the homology and cohomology groups $H_n(G, A)$ and $H^n(G, A)$ seem to depend on the base ring K, but in fact it is not the case. Indeed, it can be proven that there are group isomorphisms

$$\operatorname{Tor}_n^{KG}(K,A) \cong \operatorname{Tor}_n^{\mathbb{Z}G}(\mathbb{Z},A) \qquad \text{and} \qquad \operatorname{Ext}^n_{KG}(K,A) \cong \operatorname{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},A)$$

for each $n \in \mathbb{Z}_{\geqslant 0}$ and every KG-module A, which can also be seen as a $\mathbb{Z}G$-module via the unique ring homomorphism $\mathbb{Z} \longrightarrow K$ (mapping $1_{\mathbb{Z}}$ to 1_K). See Exercise 34.

In view of the above remark, from now on, unless otherwise stated, we specify the ring K to $\mathbb{Z}$.

Proposition 15.3 (*Long exact sequences*)

Let $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ be a short exact sequence of $\mathbb{Z}G$-modules. Then there are long exact sequences of abelian groups in homology and cohomology:

(a)

$$\begin{tikzcd}
\cdots \arrow[r] & H_{n+1}(G,C) \arrow[r, "\delta_{n+1}"] & H_n(G,A) \arrow[r, "\varphi_*"] & H_n(G,B) \arrow[r, "\psi_*"] & H_n(G,C) \arrow[r] & \cdots \\
\cdots \arrow[r] & H_1(G,C) \arrow[r, "\delta_1"] & H_0(G,A) \arrow[r, "\varphi_*"] & H_0(G,B) \arrow[r, "\psi_*"] & H_0(G,C) \arrow[r] & 0
\end{tikzcd}$$

(b)

$$\begin{tikzcd}
0 \arrow[r] & H^0(G,A) \arrow[r, "\varphi_*"] & H^0(G,B) \arrow[r, "\psi_*"] & H^0(G,C) \arrow[r, "\delta^0"] & H^1(G,A) \arrow[r] & \cdots \\
\cdots \arrow[r] & H^n(G,A) \arrow[r, "\varphi_*"] & H^n(G,B) \arrow[r, "\psi_*"] & H^n(G,C) \arrow[r, "\delta^n"] & H^{n+1}(G,A) \arrow[r] & \cdots
\end{tikzcd}$$

Proof: By definition of the homology and cohomology groups of G, (b) is a special case of Proposition 12.5(a) and (a) is a special case of Theorem 12.10(i). ■

To start our investigation we characterise the (co)homology of groups in degree zero:

Proposition 15.4

Let A be a $\mathbb{Z}G$-module. Then

(a) $H_0(G,A) \cong \mathbb{Z} \otimes_{\mathbb{Z}G} A \cong A_G$, and

(b) $H^0(G,A) \cong \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},A) \cong A^G$

as abelian groups.

Proof: (a) By Definition and Proposition 12.10(b) we have

$$H_0(G,A) = \operatorname{Tor}_0^{\mathbb{Z}G}(\mathbb{Z},A) \cong \mathbb{Z} \otimes_{\mathbb{Z}G} A\,.$$

Moreover, Remark 14.6(d) yields $\mathbb{Z} \otimes_{\mathbb{Z}G} A \cong (\mathbb{Z} \otimes_{\mathbb{Z}} A)_G \cong A_G$.

(b) By Definition and Proposition 12.3(a) we have

$$H^0(G,A) = \operatorname{Ext}^0_{\mathbb{Z}G}(\mathbb{Z},A) \cong \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},A)\,.$$

Moreover, Remark 14.6(c) yields $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},A) = \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z},A)^G \cong A^G$. ■

Next, the degree-one (co)homology groups with coefficients in a trivial $\mathbb{Z}G$-module can also be characterised using the augmentation ideal.

Remark 15.5

If A is a trivial $\mathbb{Z}G$-module, then there are several interpretations of the 1st homology and cohomology groups of G which easily follow from the results we have seen so far:

(a) $H_1(G,A) \cong IG \otimes_{\mathbb{Z}G} A \cong IG/(IG)^2 \otimes_{\mathbb{Z}G} A \cong IG/(IG)^2 \otimes_{\mathbb{Z}} A \cong G_{ab} \otimes_{\mathbb{Z}} A$;

(b)
$$\begin{aligned} H^1(G,A) &\cong \mathrm{Hom}_{\mathbb{Z}G}(IG,A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG/(IG)^2,A) \\ &\cong \mathrm{Hom}_{\mathbb{Z}}(IG/(IG)^2,A) \cong \mathrm{Hom}_{\mathbb{Z}}(G_{ab},A) \cong \mathrm{Hom}_{\mathbf{Grp}}(G,A). \end{aligned}$$

See Exercise 33.

Corollary 15.6

If $\mathbb{Z}$ denotes the trivial $\mathbb{Z}G$-module, then $H_1(G,\mathbb{Z}) \cong IG/(IG)^2 \cong G_{ab}$.

Proof: This is straightforward from Remark 15.5. ■

16 The Bar Resolution

In order to compute the (co)homology of groups, we need *concrete* projective resolutions of $\mathbb{Z}$ as a $\mathbb{Z}G$-module.

Notation 16.1

Let $n \in \mathbb{Z}_{\geqslant 0}$ be a non-negative integer. Let F_n be the free $\mathbb{Z}$-module with $\mathbb{Z}$-basis consisting of all $(n+1)$-tuples $(g_0, g_1, \dots, g_n)$ of elements of G. Then the group G acts on F_n via

$$g \cdot (g_0, g_1, \dots, g_n) = (gg_0, gg_1, \dots, gg_n),$$

and it follows that F_n is a free $\mathbb{Z}G$-module with $\mathbb{Z}G$-basis $\mathcal{B}_n := \{(1, g_1, \dots, g_n) \mid g_i \in G\}$. First, for each $0 \leqslant i \leqslant n$, define maps

$$\begin{array}{cccc} \partial_i : & G^{n+1} & \longrightarrow & G^n \\ & (g_0, \dots, g_n) & \mapsto & (g_0, \dots, \check{g}_i, \dots, g_n), \end{array}$$

where the check notation means that g_i is deleted from the initial $(n+1)$-tuple in order to produce an n-tuple, and extend them by $\mathbb{Z}$-linearity to the whole of F_n. If $n \geqslant 1$, define

$$\begin{aligned} d_n : F_n &\longrightarrow F_{n-1} \\ x &\longmapsto \sum_{i=0}^{n} (-1)^i \partial_i(x). \end{aligned}$$

Since the maps ∂_i are $\mathbb{Z}G$-linear by definition, so is d_n. Finally consider the augmentation map

$$\begin{aligned} \varepsilon : F_0 = \mathbb{Z}G &\longrightarrow \mathbb{Z} \\ g &\longmapsto 1 \quad \forall g \in G. \end{aligned}$$

Proposition 16.2

The sequence $\cdots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} F_{n-1} \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} F_0$ is a free $\mathbb{Z}G$-resolution of the trivial $\mathbb{Z}G$-module.

Proof: Set $F_{-1} := \mathbb{Z}$ and $d_0 := \varepsilon$ (note that $\varepsilon = d_0$ is consistent with the definition of d_n). We have to prove that the resulting sequence

$$(F_\bullet, d_\bullet) \overset{\varepsilon}{\twoheadrightarrow} \mathbb{Z} := \left(\cdots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} F_{n-1} \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} F_0 \xrightarrow{d_0} F_{-1} \right)$$

is an exact complex.

- **Claim 1**: $d_{n-1} \circ d_n = 0$ for every $n \geqslant 1$.
  Indeed: Let $(g_0, \ldots, g_n) \in G^{n+1}$ be a basis element. Then

$$(d_{n-1} \circ d_n)(g_0, \ldots, g_n) = \sum_{i=0}^{n-1} \sum_{j=0}^{n} (-1)^i (-1)^j (\partial_i \circ \partial_j)(g_0, \ldots, g_n)\,.$$

  Now let $0 \leqslant i_0 < j_0 \leqslant n$. If we remove g_{j_0} first and then g_{i_0}, we get

$$(\partial_{i_0} \circ \partial_{j_0})(g_0, \ldots, g_n) = (-1)^{i_0+j_0} \big(g_0, \ldots, \breve{g}_{i_0}, \ldots, \breve{g}_{j_0}, \ldots, g_n\big)\,.$$

  On the other hand, if we remove g_{i_0} first, then g_{j_0} is shifted to position $j_0 - 1$ and must be removed with sign $(-1)^{j_0-1}$. So both terms cancel and it follows that $d_{n-1} \circ d_n$ is the zero map.

- **Claim 2**: $F_\bullet \overset{\varepsilon}{\twoheadrightarrow} \mathbb{Z}$ is an exact complex.
  Indeed: by definition of the modules F_n ($n \geqslant 0$), we may view $(F_\bullet, d_\bullet)$ as a complex of $\mathbb{Z}$-modules. In fact it suffices to prove that there exists a homotopy between $\mathrm{Id}_{F_\bullet}$ and the zero chain map. For $n \geqslant 0$, define

$$\begin{array}{rccc} s_n : & F_n & \longrightarrow & F_{n+1} \\ & (g_0, \ldots, g_n) & \mapsto & (1, g_0, \ldots, g_n)\,, \end{array}$$

  let $s_{-1} : \mathbb{Z} = F_{-1} \longrightarrow F_0 \cong \mathbb{Z}G$ be the $\mathbb{Z}$-homomorphism sending 1 to (1), and let $s_i := 0$ for all $i \leqslant -2$. For $n \geqslant 0$ and $(g_0, \ldots, g_n) \in G^{n+1}$ compute

$$\begin{aligned}\big(d_{n+1} \circ s_n + s_{n-1} \circ d_n\big)(g_0, \ldots, g_n) &= (g_0, \ldots, g_n) + \sum_{j=1}^{n+1} (-1)^j \big(1, g_0, \ldots, \breve{g}_{j-1}, \ldots, g_n\big) \\ &\quad + \sum_{i=0}^{n} (-1)^i \big(1, g_0, \ldots, \breve{g}_i, \ldots, g_n\big) \\ &= (g_0, \ldots, g_n),\end{aligned}$$

  and it is clear that $d_{n+1} \circ s_n + s_{n-1} \circ d_n = \mathrm{Id}_{F_n}$ for every $n \leqslant -1$, as required. ■

Notation 16.3 (*Bar notation*)

Given $n \in \mathbb{Z}_{\geqslant 0}$, set

$$[g_1|g_2|\ldots|g_n] := \big(1, g_1, g_1g_2, g_1g_2g_3, \ldots, g_1 \cdot \ldots \cdot g_n\big) \in G^{n+1}\,.$$

With this notation, we have

$$(1, h_1, \ldots, h_n) = \big[h_1|h_1^{-1}h_2|h_2^{-1}h_3|\ldots|h_{n-1}^{-1}h_n\big].$$

Hence F_n becomes a free $\mathbb{Z}G$-module with basis $\{[g_1|\dots|g_n] \mid g_i \in G\} =: \underline{G}^n$, which as a set is in bijection with G^n. In particular F_0 is the free $\mathbb{Z}G$-module with basis $\{[\,]\}$ (empty symbol). With this notation, for every $n \geqslant 1$ and every $0 \leqslant i \leqslant n$, we have

$$\partial_i[g_1|\dots|g_n] = \begin{cases} g_1 \cdot [g_2|\dots|g_n] & i = 0, \\ [g_1|\dots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\dots|g_n] & 1 \leqslant i \leqslant n-1, \\ [g_1|\dots|g_{n-1}] & i = n. \end{cases}$$

Because of this notation the resolution of Proposition 16.2 is known as the **bar resolution**.

In fact, it is possible to render computations easier, by considering a slight alteration of the bar resolution called the **normalised bar resolution**.

Notation 16.4 (*The normalised bar notation*)

Let $n \in \mathbb{Z}_{\geqslant 0}$, and let F_n be as above and let D_n be the $\mathbb{Z}G$-submodule of F_n generated by all elements $[g_1|\dots|g_n]$ of F_n such that at least one of the coefficients g_i is equal to 1. In other words, if $(1, h_1, \dots, h_n) \in F_n$, then:

$$(1, h_1, \dots, h_n) \in D_n \quad \Longleftrightarrow \quad \exists\, 1 \leqslant i \leqslant n-1 \quad \text{such that} \quad h_i = h_{i+1}\,.$$

Lemma 16.5

The following assertions hold:

(a) $(D_\bullet, d_\bullet)$ is a subcomplex of $(F_\bullet, d_\bullet)$;

(b) $s_n(D_n) \subset D_{n+1}$ for all $n \geqslant 0$.

Proof: (a) Let $n \geqslant 1$. We have to prove that $d_n(D_n) \subseteq D_{n-1}$. So let $(1, h_1, \dots, h_n) \in D_n$, so that there is an index $1 \leqslant i \leqslant n-1$ such that $h_i = h_{i+1}$. Then, clearly

$$\partial_j(1, h_1, \dots, h_n) \in D_{n-1} \quad \text{for each } 0 \leqslant j \leqslant n \text{ such that } j \neq i, i+1\,.$$

On the other hand, we have the equality $\partial_i(1, h_1, \dots, h_n) = \partial_{i+1}(1, h_1, \dots, h_n)$ and in the alternating sum $d_n(1, h_1, \dots, h_n) = \sum_{i=0}^{n}(-1)^i\partial_i(1, h_1, \dots, h_n)$, the signs of ∂_i and ∂_{i+1} are opposite to each other. Therefore, we are left with a sum over $j \neq i, i+1$.

(b) Obvious by definition of s_n. ■

Corollary 16.6

Set $\overline{F}_n := F_n/_{D_n}$ for every $n \geqslant 0$. Then $(\overline{F}_\bullet, \overline{d}_\bullet)$ is a free $\mathbb{Z}G$-resolution of the trivial module.

Proof: Since $D_\bullet$ is a subcomplex of $F_\bullet$, we can form the quotient complex $(\overline{F}_\bullet, \overline{d}_\bullet)$, which consists of free $\mathbb{Z}G$-modules. Now by the Lemma, $s_n(D_n) \subset D_{n+1}$ for each $n \geqslant 0$, therefore D_n is in the kernel of s_n post-composed with the quotient map $F_{n+1} \longrightarrow F_{n+1}/D_{n+1}$ and each $\mathbb{Z}$-linear map $s_n : F_n \longrightarrow F_{n+1}$ induces a $\mathbb{Z}$-linear maps $\overline{s}_n : \overline{F}_n \longrightarrow \overline{F}_{n+1}$ via the Universal Property of the quotient. Hence, similarly to the proof of Proposition 16.2, we get a homotopy $\{\overline{s}_n \mid n \in \mathbb{Z}\}$ and we conclude that the sequence

$$\begin{tikzcd} \cdots \arrow[r] & \overline{F}_n \arrow[r, "\overline{d}_n"] & \overline{F}_{n-1} \arrow[r] & \cdots \arrow[r, "\overline{d}_1"] & \overline{F}_0 \arrow[r, "\overline{\varepsilon}=\overline{d}_0"] & \mathbb{Z} \arrow[r] & 0. \end{tikzcd}$$

is exact, as required. ■

Definition 16.7 (*Normalised bar resolution*)

The chain complex $(\overline{F}_\bullet, \overline{d}_\bullet)$ is called the **normalised bar resolution** of $\mathbb{Z}$ as a $\mathbb{Z}G$-module.

Example 10 (*Bar resolution in low degrees*)

In low degrees the bar resolution has the form

$$\begin{tikzcd}
\cdots \arrow[r] & F_2 \arrow[r, "d_2"] & F_1 \arrow[r, "d_1"] & F_0 \arrow[r, "\varepsilon"] & \mathbb{Z} \arrow[r] & 0 \\
\text{bases elts:} & {[g_1|g_2]} & {[g]} & {[\,]} & &
\end{tikzcd}$$

with

- $\varepsilon([\,]) = 1$;
- $d_1([g]) = \partial_0([g]) - \partial_1([g]) = g[\,] - [\,]$;
- $d_2[g_1|g_2] = \partial_0([g_1|g_2]) - \partial_1([g_1|g_2]) + \partial_2([g_1|g_2]) = g_1[g_2] - [g_1g_2] + [g_1]$.

Similar formulae hold for $\overline{F}_\bullet$. (Exercise!)

17 Cocycles and Coboundaries

We now use the (normalised) bar resolution in order to compute the cohomology groups $H^n(G, A)$ ($n \geqslant 0$), where A is an arbitrary $\mathbb{Z}G$-module. To this end, we need to consider the cochain complex $\mathrm{Hom}_{\mathbb{Z}G}(F_\bullet, A)$. Define

$$C^n(G, A) := \mathrm{Hom}_{\mathbf{Set}}(\underline{G}^n, A)$$

to be the set of all maps from $\underline{G}^n$ to A, so that clearly there is an isomorphism of $\mathbb{Z}$-modules

$$\mathrm{Hom}_{\mathbb{Z}G}(F_n, A) \xrightarrow{\cong} C^n(G, A)$$

mapping $f \mapsto f|_{\underline{G}_n}$. Using this isomorphism, we see that the corresponding differential maps are:

$$\begin{aligned} d_n^* : C^{n-1}(G, A) &\longrightarrow C^n(G, A) \\ f &\longmapsto d_n^*(f) \end{aligned}$$

where

$$\begin{aligned} d_n^*(f)\big([g_1|\dots|g_n]\big) = f\big(g_1[g_2|\dots|g_n]\big) &+ \sum_{i=1}^{n-1} (-1)^i f\big([g_1|\dots|g_ig_{i+1}|\dots|g_n]\big) \\ &+ (-1)^n f\big([g_1|\dots|g_{n-1}]\big)\,. \end{aligned}$$

Definition 17.1 (*n-cochains, n-cocycles, n-coboundaries*)

With the above notation:

(a) The elements of $C^n(G, A)$ are called the n**-cochains** of G.

(b) If $f \in C^n(G, A)$ is such that $d_{n+1}^* f = 0$, then f is called an n**-cocycle** of G, and the the set of all n-cocycles is denoted $Z^n(G,A)$.

(c) If $f \in C^n(G,A)$ is in the image of $d_n^* : C^{n-1}(G,A) \longrightarrow C^n(G,A)$, then f is called an n-**coboundary** of G. We denote by $B^n(G,A)$ the set of all n-coboundaries.

Proposition 17.2

Let A be a $\mathbb{Z}G$-module and $n \geqslant 0$. Then $H^n(G,A) \cong Z^n(G,A)/B^n(G,A)$.

Proof: Compute cohomology via the bar resolution and replace the $\mathbb{Z}$-module $\mathrm{Hom}_{\mathbb{Z}G}(F_n, A)$ by its isomorphic $\mathbb{Z}$-module $C^n(G,A)$. The claim follows. ■

Remark 17.3

If we used the normalised bar resolution instead, the n-cochains are replaced by the n-cochains vanishing on n-tuples $[g_1|\ldots|g_n]$ having (at least) one of coefficient g_i equal to 1. (This is because $\mathrm{Hom}_{\mathbb{Z}G}(\overline{F}_n, A) \subset \mathrm{Hom}_{\mathbb{Z}G}(F_n, A)$). We denote these by $\overline{C}^n(G,A)$, and thus $\overline{C}^n(G,A) \subseteq C^n(G,A)$. The set of resulting normalised n-cocycles is denoted by $\overline{Z}^n(G,A)$, and the set of resulting normalised n-coboundaries by $\overline{B}^n(G,A)$. It follows that

$$H^n(G,A) \cong Z^n(G,A)/B^n(G,A) \cong \overline{Z}^n(G,A)/\overline{B}^n(G,A)\,.$$

18 Exercises for Chapter 4

Exercise 32

(a) Let M and N be KG-modules. Prove that:

(i) M^G is the largest submodule of M on which G acts trivially;

(ii) M_G is the largest quotient of M on which G acts trivially;

(iii) $\mathrm{Hom}_K(M,N)^G = \mathrm{Hom}_{KG}(M,N)$;

(iv) $(M \otimes_K N)_G \cong M \otimes_{KG} N$.

(b) Prove that if G is finite, then $(KG)^G = \langle \sum_{g \in G} g \rangle_K$ and if G is infinite, then $(KG)^G = 0$.

Exercise 33

(a) Prove that there is an isomorphism of abelian groups $(IG/(IG)^2, +) \cong (G_{ab}, \cdot)$, where G_{ab} denotes the abelianisation of G;

(b) Assume A is a trivial $\mathbb{Z}G$-module. Prove that there are group isomorphisms

(i) $H_1(G,A) \cong IG \otimes_{\mathbb{Z}G} A \cong IG/(IG)^2 \otimes_{\mathbb{Z}G} A \cong IG/(IG)^2 \otimes_{\mathbb{Z}} A \cong G_{ab} \otimes_{\mathbb{Z}} A$;

(ii) $H^1(G,A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG,A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG/(IG)^2,A)$
$\cong \mathrm{Hom}_{\mathbb{Z}}(IG/(IG)^2,A) \cong \mathrm{Hom}_{\mathbb{Z}}(G_{ab},A) \cong \mathrm{Hom}_{\mathbf{Grp}}(G,A)$.

Exercise 34

Let A be a KG-module.

(a) Prove that if F is a free $\mathbb{Z}G$-module, then

$$\mathrm{Hom}_{KG}(K \otimes_{\mathbb{Z}} F, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(F, A)\,.$$

[Hint: Given a $\mathbb{Z}$-basis X of F, prove that $K \otimes_{\mathbb{Z}} F$ is also free and describe a K-basis.]

(b) Prove that $\mathrm{Ext}^n_{KG}(K, A) \cong \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$ for every $n \geqslant 0$.
[Hint: Given a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module, construct a free resolution of K as a KG-module, using the "same" bases.]

(c) Sketch similar arguments to prove that $\mathrm{Tor}^{KG}_n(K, A) \cong \mathrm{Tor}^{\mathbb{Z}G}_n(\mathbb{Z}, A)$ for every $n \geqslant 0$.

Chapter 5. Easy Cohomology

In this short chapter we consider some cases in which the cohomology groups of a group G have an easy interpretation. This is for example the case in low degrees (zero, one, two). Next we consider families of groups whose cohomology groups are easy to compute with the methods we have so far at our disposal.

References:

[Bro94] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994.

[Eve91] L. Evens, *The cohomology of groups*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1991.

[Rot09] J. J. Rotman, *An introduction to the theory of groups. Fourth ed.*, Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[Wei94] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

Notation for the chapter. Throughout this chapter we let $(G, \cdot)$ (in multiplicative notation) denote a group and A denote a $\mathbb{Z}G$-module.

19 Low-degree Cohomology

A. Degree-zero cohomology.

We have already proved in Proposition 15.4 that $H^0(G, A) \cong A^G$, the G-fixed points of A.
In particular, if A is a trivial $\mathbb{Z}G$-module, then $H^0(G, A) = A$.

B. Degree-one cohomology.

Using the bar resolution to compute $H^1(G, A)$ yields $H^1(G, A) = Z^1(G, A)/B^1(G, A)$.

<u>**1-cocycles**</u>: By definition, and the description of the differential maps of the bar resolution, we have

$$\begin{aligned} Z^1(G, A) &= \{f \in \mathrm{Hom}_{\mathbf{Set}}(\underline{G}^1, A) \mid d_2^*(f) = 0\} \\ &= \{f \in \mathrm{Hom}_{\mathbf{Set}}(\underline{G}^1, A) \mid 0 = f(g_1[g_2]) - f([g_1 g_2]) + f([g_1]) \ \forall\, [g_1|g_2] \in \underline{G}^2\} \end{aligned}$$

In other words, a map $f : G \longrightarrow A$ is a 1-cocycle if and only if it satisfies the

$$\boxed{\textbf{1-cocycle identity:} \qquad f(g_1 \cdot g_2) = g_1 \cdot f(g_2) + f(g_1) \qquad \forall\, g_1, g_2 \in G}\,.$$

<u>**1-coboundaries**</u>: $C^0(G,A) = \mathrm{Hom}_{\mathbf{Set}}(\{[\ ]\}, A) = \{f_a : \{[\ ]\} \longrightarrow A, [\ ] \mapsto a \mid a \in A\} \xleftrightarrow{\text{bij.}} A$. It follows that the differential map

$$d_1^* : C^0(G,A) \longrightarrow C^1(G,A)$$

is such that $d_1^*(f_a)(g) = f_a(g[\ ]) - f_a([\ ]) = ga - a$ for every $g \in G$ and every $a \in A$. Therefore, $f : G \longrightarrow A$ is a 1-coboundary if and only if there exists $a \in A$ such that $f(g) = ga - a$ for every $g \in G$.

Definition 19.1 (*Derivation, principal derivation*)

Let A be a $\mathbb{Z}G$-module and let $f : G \longrightarrow A$ be a map.

(a) If f satisfies the 1-cocycle identity, then it is called a **derivation** of G. We denote by $\mathrm{Der}(G,A)$ the set of all derivations of G to A.

(b) If, moreover, there exists $a \in A$ such that $f(g) = ga - a$ for every $g \in G$, then f is called a **principal derivation** (or an **inner derivation**) of G. We denote by $\mathrm{Inn}(G,A)$ the set of all inner derivations of G to A.

Remark 19.2

It follows from the above that $H^1(G,A) \cong Z^1(G,A)/B^1(G,A) = \mathrm{Der}(G,A)/\mathrm{Inn}(G,A)$.

Example 11

Let A be a trivial $\mathbb{Z}G$-module. In this case, the 1-cocycle identity becomes

$$f(g \cdot h) = f(g) + f(h)\,,$$

so that $Z^1(G,A) = \mathrm{Hom}_{\mathbf{Grp}}\big((G,\cdot),(A,+)\big)$. Furthermore $B^1(G,A) = 0$. Therefore

$$H^1(G,A) = \mathrm{Hom}_{\mathbf{Grp}}\big((G,\cdot),(A,+)\big)\,.$$

Compare with Remark 15.5(b).

C. Degree-two cohomology.

Again using the bar resolution to compute $H^2(G,A)$ yields $H^2(G,A) = Z^2(G,A)/B^2(G,A)$.

<u>**2-cocycles**</u>: By definition, and the description of the differential maps of the bar resolution, we have

$$\begin{aligned} Z^2(G,A) &= \{f \in \mathrm{Hom}_{\mathbf{Set}}(\underline{G}^2, A) \mid d_3^*(f) = 0\} \\ &= \{f \in \mathrm{Hom}_{\mathbf{Set}}(\underline{G}^2, A) \mid 0 = f(g_1[g_2|g_3]) - f([g_1g_2|g_3]) \\ &\qquad\qquad + f([g_1|g_2g_3]) - f([g_1|g_2])\ \forall\,[g_1|g_2|g_3] \in \underline{G}^3\} \end{aligned}$$

In other words, a map $f : G \times G \longrightarrow A$ is a 2-cocycle if and only if it satisfies the

$$\boxed{\textbf{2-cocycle identity:} \qquad g_1 f(g_2,g_3) + f(g_1, g_2g_3) = f(g_1g_2, g_3) + f(g_1,g_2) \qquad \forall\, g_1,g_2,g_3 \in G}\,.$$

2-coboundaries: If $\phi \in C^1(G, A)$, then

$$d_2^*(\phi)([g_1|g_2]) = \phi(g_1[g_2]) - \phi([g_1g_2]) + \phi([g_1]) \qquad \forall\, [g_1|g_2] \in \underline{G}^2\,.$$

Therefore a map $f : G \times G \longrightarrow A$ is a 2-coboundary if and only if there exists a map $c : G \longrightarrow A$ such that

$$f(g_1, g_2) = g_1\, c(g_2) - c(g_1g_2) + c(g_1) \qquad \forall\, g_1, g_2 \in G\,.$$

20 Cohomology of Cyclic Groups

Cyclic groups, finite and infinite, are a family of groups, for which cohomology is easy to compute. Of course, we could use the bar resolution, but it turns out that in this case, there is a more efficient resolution to be used, made up of free modules of rank 1.

Notation 20.1

If A is a $\mathbb{Z}G$-module and $x \in \mathbb{Z}G$, then we let $m_x : A \longrightarrow A, x \mapsto x \cdot a$ denote the left action of x on A (or left external multiplication by x in A).

Proposition 20.2 (***Free resolution of finite cyclic groups***)

Let C_n be a finite cyclic group of order $n \in \mathbb{Z}_{>0}$ generated by g, and let $t := \sum_{i=0}^{n-1} g^i \in \mathbb{Z}C_n$. Then

$$\cdots \xrightarrow{m_t} \mathbb{Z}C_n \xrightarrow{m_{g-1}} \mathbb{Z}C_n \xrightarrow{m_t} \mathbb{Z}C_n \xrightarrow{m_{g-1}} \mathbb{Z}C_n\,,$$

is a free $\mathbb{Z}C_n$-resolution of the trivial $\mathbb{Z}C_n$-module.

Proof: Set $G := C_n$. By Lemma 14.4,

$$IG = \langle \{g^i - 1 \mid 1 \leqslant i \leqslant n-1\} \rangle_{\mathbb{Z}} = \langle g - 1 \rangle_{\mathbb{Z}G}\,.$$

Therefore, the image of m_{g-1} is equal to IG, which is the kernel of the augmentation map $\varepsilon : \mathbb{Z}G \longrightarrow \mathbb{Z}$. Now, let $x = \sum_{i=0}^{n-1} \lambda_i\, g^i \in \mathbb{Z}G$. Then, $tx = \sum_{i=0}^{n-1} \lambda_i\, t$. Hence

$$\ker(m_t) = \{ \sum_{i=0}^{n-1} \lambda_i g^i \mid \sum_{i=0}^{n-1} \lambda_i = 0 \}$$

and we claim that this is equal to the image of m_{g-1}. Indeed, the inclusion $\operatorname{Im}(m_{g-1}) \subseteq \ker(m_t)$ is clear, and conversely, if $h = \sum_{i=0}^{n-1} \lambda_i g^i \in \ker(m_t)$, then $\sum_{i=0}^{n-1} \lambda_i = 0$, so that $h \in \ker(\varepsilon) = IG = \operatorname{Im}(m_{g-1})$, whence $\ker(m_t) \subseteq \operatorname{Im}(m_{g-1})$. Finally, we claim that $\ker(m_{g-1}) = \operatorname{Im}(m_t)$. We have

$$
\begin{aligned}
\sum_{i=0}^{n-1} \lambda_i g^i \in \ker(m_{g-1}) \iff (g-1)\left(\sum_{i=0}^{n-1} \lambda_i g^i\right) = 0 &\iff \sum_{i=0}^{n-1} \lambda_i g^{i+1} - \sum_{i=0}^{n-1} \lambda_i g^i = 0 \\
&\iff \sum_{j=0}^{n-1} \lambda_{j-1} g^j - \sum_{i=0}^{n-1} \lambda_i g^i = 0, \ (\lambda_{-1} := \lambda_{n-1}) \\
&\iff \sum_{i=0}^{n-1} (\lambda_{i-1} - \lambda_i) g^i = 0 \\
&\iff \forall\, 0 \leqslant i \leqslant n-1,\ \lambda_{i-1} = \lambda_i =: \lambda \\
&\iff \sum_{i=0}^{n-1} \lambda_i g^i = \lambda t \iff \sum_{i=0}^{n-1} \lambda_i g^i \in \operatorname{Im}(m_t).
\end{aligned}
$$

■

Theorem 20.3 (*Cohomology of finite cyclic groups*)

Let $C_n = \langle g \mid g^n = 1 \rangle$ be a finite cyclic group of order $n \in \mathbb{Z}_{>0}$ and let A be a $\mathbb{Z}C_n$-module. Then

$$
H^m(C_n, A) \cong \begin{cases} A^{C_n} & \text{if } m = 0, \\ A^{C_n}/\operatorname{Im}(m_t) & \text{if } m \geqslant 2, m \text{ even}, \\ \ker(m_t)/\operatorname{Im}(m_{g-1}) & \text{if } m \geqslant 1, m \text{ odd}, \end{cases}
$$

where $t = \sum_{i=0}^{n-1} g^i \in \mathbb{Z}C_n$ and for $x \in \{t, g-1\}$, m_x denotes left external multiplication by x in A.

Proof: By Proposition 20.2 the trivial $\mathbb{Z}G$-module $\mathbb{Z}$ admits the projective resolution

$$
\ldots \xrightarrow{m_t} \mathbb{Z}C_n \xrightarrow{m_{g-1}} \mathbb{Z}C_n \xrightarrow{m_t} \mathbb{Z}C_n \xrightarrow{m_{g-1}} \mathbb{Z}C_n \,.
$$

For $m = 0$, we already know that $H^0(C_n, A) = A^{C_n}$. For $m > 0$, applying the functor $\operatorname{Hom}_{\mathbb{Z}C_n}(-, A)$ yields the cochain complex

$$
\operatorname{Hom}_{\mathbb{Z}C_n}(\mathbb{Z}C_n, A) \xrightarrow{m_{g-1}^*} \operatorname{Hom}_{\mathbb{Z}C_n}(\mathbb{Z}C_n, A) \xrightarrow{m_t^*} \operatorname{Hom}_{\mathbb{Z}C_n}(\mathbb{Z}C_n, A) \xrightarrow{m_{g-1}^*} \cdots ,
$$

where in each degree there is an isomorphism $\operatorname{Hom}_{\mathbb{Z}C_n}(\mathbb{Z}C_n, A) \xrightarrow{\cong} A$, $f \mapsto f(1)$. Hence for $x \in \{g-1, t\}$, there are commutative diagrams of the form

$$
\begin{tikzcd}
\operatorname{Hom}_{\mathbb{Z}C_n}(\mathbb{Z}C_n, A) \arrow[r, "m_x^*"] \arrow[d, "\cong"] \arrow[dr, phantom, "\circlearrowleft"] & \operatorname{Hom}_{\mathbb{Z}C_n}(\mathbb{Z}C_n, A) \arrow[d, "\cong"] \\
A \arrow[r, "m_x"] & A\,.
\end{tikzcd}
$$

Hence, the initial cochain complex is isomorphic to the cochain complex

$$
\begin{tikzcd}
 & A \arrow[r, "m_{g-1}"] & A \arrow[r, "m_t"] & A \arrow[r, "m_{g-1}"] & A \arrow[r, "m_t"] & \cdots \\
\text{(degree)} & 0 & 1 & 2 & 3 &
\end{tikzcd}
$$

and the claim follows. ■

For infinite cyclic groups the situation is even simpler:

Theorem 20.4 (*Cohomology of infinite cyclic groups*)

If $G = \langle g \rangle$ is an infinite cyclic group, then $0 \longrightarrow \mathbb{Z}G \xrightarrow{m_{g-1}} \mathbb{Z}G$ is a free resolution of the trivial $\mathbb{Z}G$-module, and

$$H^n(G,A) = \begin{cases} A^G & \text{if } n = 0, \\ A/\operatorname{Im}(m_{g-1}) & \text{if } n = 1, \\ 0 & \text{if } n \geqslant 2. \end{cases}$$

where the second m_{g-1} denotes the left external multiplication by $g - 1$ in A.

Proof: Exercise 37. ■

21 Exercises for Chapter 5

Exercise 35

Let A be a $\mathbb{Z}G$-module. Prove that $\operatorname{Der}(G,A) \cong \operatorname{Hom}_{\mathbb{Z}G}(IG,A)$ via the map sending a derivation d to the homomorphism $\tilde{d}$ such that $\tilde{d}(g-1) = d(g)$, $\forall g \in G\backslash\{1\}$.

Exercise 36

Let A be a left $\mathbb{Z}G$-module, and let $A \rtimes G$ be the semi-direct product of $(A,+)$ by $(G,\cdot)$, that is, the group of all pairs $(a,g) \in A \times G$, with group law

$$(a,g)\cdot(b,h) := (a + g\cdot b, gh).$$

Let $\pi : A \rtimes G \longrightarrow G : (a,g) \mapsto g$ and let $\operatorname{Hom}'(G, A \rtimes G)$ be the set of all group homomorphisms $f : G \longrightarrow A \rtimes G$ such that $\pi \circ f = \operatorname{Id}_G$. Prove that $\operatorname{Der}(G,A)$ is in bijection with $\operatorname{Hom}'(G, A \rtimes G)$.

Exercise 37

Assume $G = \langle g \rangle$ is an infinite cyclic group. Prove that $0 \longrightarrow \mathbb{Z}G \xrightarrow{m_{g-1}} \mathbb{Z}G$ is a free resolution of the trivial $\mathbb{Z}G$-module, and

$$H^n(G,A) = \begin{cases} A^G & \text{if } n = 0, \\ A/\operatorname{Im}(m_{g-1}) & \text{if } n = 1, \\ 0 & \text{if } n \geqslant 2. \end{cases}$$

Exercise 38

Let F be a free group on a set X.

(a) Prove that $0 \longrightarrow IF \longrightarrow \mathbb{Z}F$ is a free resolution of $\mathbb{Z}$ considered as a $\mathbb{Z}F$-module.

(b) Prove that $H^n(F,A) = 0$ for all $n \geqslant 2$.

(c) Prove that, if A is a trivial $\mathbb{Z}F$-module, then $H^1(F,A) \cong \prod_{x\in X} A$.

(d) Solve Exercise 37 again.

Exercise 39

Let G be a finite cyclic group of order divisible by a prime p and let A be a trivial $\mathbb{F}_pG$-module. Prove that $H^n(G, A) \cong A$ for all $n \geqslant 0$.

Chapter 6. Cohomology and Group Extensions

In this chapter we consider connections between the short exact sequences of groups of the form $1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$ with abelian kernel and the cohomology of the group G with coefficients in A. If the sequence splits, then we shall prove that the 1st cohomology group $H^1(G, A)$ parametrises the splittings. Moreover, we shall also prove that the 2nd cohomology group $H^2(G, A)$ is in bijection with the isomorphism classes of extensions $1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$ inducing the given $\mathbb{Z}G$-module structure on A, and the neutral element of $H^2(G, A)$ corresponds, under this bijection, to a s.e.s. where E is a semi-direct product of A by G.

References:

[Bro94] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994.

[Eve91] L. Evens, *The cohomology of groups*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1991.

[Rot09] J. J. Rotman, *An introduction to the theory of groups. Fourth ed.*, Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[Wei94] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

22 Group Extensions

In Chapter 1, we have seen that if a group G is a semi-direct product of a subgroup N by a subgroup H, then this gives rise to a s.e.s. of the form

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1\,.$$

This is a special case of a so-called *group extension of N by H*.

Definition 22.1 (*Group extension*)

A **group extension** is a short exact sequence of groups (written multiplicatively) of the form

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1\,,$$

and, in this situation, we also say that the group E is an **extension of A by G**.

Convention: We shall always identify A with a normal subgroup of E and assume that i is simply the canonical inclusion of A in E. Moreover, we shall say that A is the **kernel** of the extension.

Lemma 22.2

Let $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ be a group extension, where A is an abelian group. Then A is naturally endowed with the structure of a $\mathbb{Z}G$-module.

Proof: First note that with the above notation $(A, \cdot)$ is a group written multiplicatively. Next, for each $g \in G$, choose a preimage $\widetilde{g} \in E$ of g under p, that is $p(\widetilde{g}) = g$, and define a left G-action on A via:

$$\begin{array}{rccl} *: & G \times A & \longrightarrow & A \\ & (g,a) & \mapsto & g * a := {}^{g}a := \widetilde{g} \cdot a \cdot \widetilde{g}^{-1}, \end{array}$$

First, we check that $*$ is well-defined, i.e. that this definition is independent of the choice of the preimages: indeed, if $\widehat{g} \in E$ is such that $p(\widehat{g}) = g$, then, we have

$$p(\widetilde{g} \cdot \widehat{g}^{-1}) = g \cdot g^{-1} = 1_G$$

hence $\widetilde{g} \cdot \widehat{g}^{-1} \in \ker(p) = A$, and thus, there exists $a \in A$ such that $\widetilde{g} = a\widehat{g}$. Therefore, for every $x \in A$,

$$\widetilde{g} \cdot x \cdot \widetilde{g}^{-1} = a \underbrace{\widehat{g}x\widehat{g}^{-1}}_{\in A \trianglelefteq E} a^{-1} = aa^{-1}\widehat{g}x\widehat{g}^{-1} = \widehat{g}x\widehat{g}^{-1},$$

where the last-but-one equality holds because A is abelian.
We extend $*$ by $\mathbb{Z}$-linearity to the whole of $\mathbb{Z}G$, and finally one easily checks that $(A, \cdot, *)$ is a $\mathbb{Z}G$-module. See Exercise 2, Exercise Sheet 10. ■

Convention: From now on, given a group extension $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ with A abelian, we always see A as a $\mathbb{Z}G$-module via the G-action of the proof of Lemma 22.2. We write $A_* := (A, \cdot, *)$ to indicate that we see A as a $\mathbb{Z}G$-module in this way.

Lemma 22.3

Let $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ be a group extension with A abelian. Then, A is central in E if and only if A_* is trivial as a $\mathbb{Z}G$-module.

Proof: A_* is a trivial $\mathbb{Z}G$-module $\iff {}^{g}a = a \quad \forall\, a \in A, \forall\, g \in G \iff \widetilde{g} \cdot a \cdot \widetilde{g}^{-1} = a \quad \forall\, a \in A, \forall\, \widetilde{g} \in E$

$$\iff \widetilde{g}a = a\widetilde{g} \quad \forall\, a \in A, \forall\, \widetilde{g} \in E$$

$$\iff A \subseteq Z(E).$$

■

Definition 22.4 (*Central extension*)

A group extension $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ be a group extension with A abelian satisfying the equivalent conditions of Lemma 22.3 is called a **central extension** of A by G.

Definition 22.5 (*Split extension*)

A group extension $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ **splits** iff there exists a group homomorphism $s : G \longrightarrow E$ such that $p \circ s = \mathrm{Id}_G$. In this case s is called a **(group-theoretic) section** of p, or a **splitting** of the extension.

Remark 22.6

Unlike short exact sequences of modules, it is not true that p admits a group-theoretic section if and only if i admits a group-theoretic retraction. In fact, if i admits a group-theoretic retraction, then $E \cong A \times G$. (See Exercise 40.)

Proposition 22.7

Let $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ be a group extension. Then the following assertions are equivalent.

(a) The extension splits.

(b) There exists a subgroup H of E such that $p|_H : H \longrightarrow G$ is an isomorphism.

(c) There exists a subgroup H of E such that E is the internal semi-direct product of A by H.

(d) There exists a subgroup H of E such that every element $e \in E$ can be written uniquely $e = ah$ with $a \in A$ and $h \in H$.

Proof:

(a) ⇒ (b): By (a) there exists a section $s : G \longrightarrow E$ for p. Define $H := \operatorname{Im} s$. Then $p|_H$ is an isomorphism since, on the one hand $p|_H \circ s = \mathrm{Id}_G$ by definition of s, and on the other hand for every $h \in H$, there exists $g \in G$ such that $h = s(g)$, so that

$$(s \circ p|_H)(h) = (s \circ p)(s(g)) = s(g) = h$$

and $s \circ p|_H = \mathrm{Id}_H$.

(b) ⇒ (c): By (b) there is $H \leqslant E$ such that $p|_H : H \longrightarrow G$ is an isomorphism. Hence

$$\{1\} = \ker\left(p|_H\right) = \ker(p) \cap H = A \cap H\,.$$

Now, let $e \in E$. Then $p(e) \in G \Rightarrow \left(p|_H\right)^{-1} \circ p(e) \in H$ and $p(e) = p\big(p|_H^{-1} \circ p(e)\big)$, so that

$$e \cdot \Big(\left(p|_H\right)^{-1} \circ p(e)\Big)^{-1} \in \ker p = A\,.$$

Therefore, there exists $a \in A$ such that

$$e = a \cdot \underbrace{\Big(\left(p|_H\right)^{-1} \circ p(e)\Big)}_{\in H} \in AH$$

as required.

(c) ⇒ (d): Was proven in Step 1 of the proof of Proposition 1.3.

(d) ⇒ (b): We have to prove that $p|_H : H \longrightarrow G$ is an isomorphism.

Surjectivity: Let $g \in G$. Then by surjectivity of p there exists $e \in E$ such that $g = p(e)$, and by (d), e can be written in a unique way as $e = ah$ with $a \in A$ and $h \in H$. Hence $p|_H$ is surjective since

$$g = p(e) = p(ah) = p(a)p(h) = 1 \cdot p(h) = p(h)\,.$$

Injectivity: If $h \in H$ is such that $p|_H(h) = 1$, then $h \in \ker(p) = A$, therefore

$$h = 1 \cdot h = h \cdot 1 \in AH$$

so that by uniqueness, we must have $h = 1$ and $\ker(p|_H) = \{1\}$.

(b) ⇒ (a): If $p|_H : H \longrightarrow G$ is an isomorphism, then we may define $s := \big(p|_H\big)^{-1} : G \longrightarrow E$. This is obviously a group homomorphism and hence a splitting of the extension. ■

If the equivalent conditions of the Proposition are satisfied, then there is a name for the subgroup H, it is called a complement:

Definition 22.8 (*Complement of a subgroup*)

Let E be a group and A be a normal subgroup of E. A subgroup H of E is called a **complement** of A in E if $E = AH$ and $A \cap H = 1$, i.e. if E is the internal semi-direct product of A by H.

23 H^1 and Group Extensions

In order to understand the connexion between the group extensions of the form

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

with abelian kernel and $H^1(G, A_*)$, first we need to investigate the automorphisms of E.

Definition 23.1 (*Inner automorphisms, automorphisms inducing the identity*)

Let E be a group.

(a) Given $x \in E$, write $c_x : E \longrightarrow E, e \mapsto xex^{-1}$ for the automorphism of E of conjugation by x.

(b) Set $\mathrm{Inn}(E) := \{\varphi \in \mathrm{Aut}(E) \mid \exists x \in E \text{ with } \varphi = c_x\}$.

(c) If $A \leqslant G$, then set $\mathrm{Inn}_A(E) := \{\varphi \in \mathrm{Aut}(E) \mid \exists x \in A \text{ with } \varphi = c_x\}$.

(d) If $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ is a group extension with abelian kernel, then set

$$\mathrm{Aut}_{A,G}(E) := \{\varphi \in \mathrm{Aut}(E) \mid \varphi|_A = \mathrm{Id}_A \text{ and } p \circ \varphi(e) = p(e)\ \forall\, e \in E\}.$$

We say that the elements φ of $\mathrm{Aut}_{A,G}(E)$ *induce the identity on both A and G*.

Recall (e.g. from the *Einführung in die Algebra*-lecture) that: $\mathrm{Inn}(E) \trianglelefteq \mathrm{Aut}(E)$, as $\varphi \circ c_x \circ \varphi^{-1} = c_{\varphi(x)}$ for every $x \in E$ and every $\varphi \in \mathrm{Aut}(E)$, and the quotient $\mathrm{Aut}(E)/\mathrm{Inn}(E)$ is called the **outer automorphism group** of E. Moreover, $\mathrm{Inn}(E) \cong E/Z(E)$. It is also obvious that $\mathrm{Aut}_{A,G}(E) \leqslant \mathrm{Aut}(E)$.

Theorem 23.2 (H^1 *and automorphisms*)

Let $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ be a group extension with abelian kernel. Then:

(a) $H^1(G, A_*) \cong \mathrm{Aut}_{A,G}(E)/\mathrm{Inn}_A(E)$; and

(b) if, moreover, the extension is a central extension then

$$H^1(G, A_*) \cong \mathrm{Aut}_{A,G}(E).$$

Proof:

(a) **Claim 1:** $\mathrm{Inn}_A(E) \trianglelefteq \mathrm{Aut}_{A,G}(E)$.

Indeed, clearly for each $a \in A$, $c_a|_A = \mathrm{Id}_A$ because A is abelian and, moreover,

$$p \circ c_a(e) = p\big(aea^{-1}\big) = p(a)p\big(ea^{-1}e^{-1}\big)p(e) = p(e)$$

for every $e \in E$, so that $p \circ c_a = p$. Therefore $\mathrm{Inn}_A E \leqslant \mathrm{Aut}_{A,G}(E)$, and it is a normal subgroup, because

$$\varphi \circ c_a \circ \varphi^{-1} = c_{\varphi(a)} = c_a$$

for every $a \in A$, every $\varphi \in \mathrm{Aut}_{A,G}(E)$ as $\varphi|_a = \mathrm{Id}_A$.

Claim 2: $\mathrm{Aut}_{A,G}(E) \cong Z^1(G, A_*)$.

We aim at defining a group isomorphism

$$\alpha : \quad \mathrm{Aut}_{A,G}(E) \quad \longrightarrow \quad Z^1(G, A_*) \ .$$

- To begin with, we observe that given $\varphi \in \mathrm{Aut}_{A,G}(E)$ and $x \in E$, we can write $\varphi(x) = f(x)x$ for some element $f(x) \in E$. This defines a map (of sets)

$$\begin{array}{rccc} f: & E & \longrightarrow & E \\ & x & \mapsto & \varphi(x)x^{-1} \,, \end{array}$$

such that $\mathrm{Im}(f) \subseteq A = \ker(p)$ because for every $x \in E$,

$$p(f(x)) = p(\varphi(x)x^{-1}) = \underbrace{p(\varphi(x))}_{=p(x)} p(x^{-1}) = 1_G$$

since φ induces the identity on G. Moreover, f is constant on the cosets of E modulo A because for every $a \in A$ and every $x \in E$,

$$f(xa) = \varphi(xa)\cdot(xa)^{-1} = \varphi(x)\cdot \underbrace{\varphi(a)}_{=a} \cdot a^{-1}\cdot x^{-1} = \varphi(x)x^{-1} = f(x)\,.$$

Therefore f induces a map $\overline{f} : G \longrightarrow A, g \mapsto \overline{f}(g) := f(\widetilde{g})$ where we may choose $\widetilde{g}$ arbitrarily in $p^{-1}(g)$. This is a 1-cocycle since for all $g, h \in G$, we may choose $\widetilde{gh} \in p^{-1}(gh)$, $\widetilde{g} \in p^{-1}(g)$, and $\widetilde{h} \in p^{-1}(h)$ such that $\widetilde{gh} = \widetilde{g}\widetilde{h}$, and hence

$$\begin{aligned} \overline{f}(gh) = f\big(\widetilde{gh}\big) = f(\widetilde{g}\widetilde{h}) &= \varphi(\widetilde{g})\cdot\varphi(\widetilde{h})\cdot\widetilde{h}^{-1}\cdot\widetilde{g}^{-1} \\ &= \varphi(\widetilde{g})\cdot\widetilde{g}^{-1}\cdot\widetilde{g}\cdot\overline{f}(h)\cdot\widetilde{g}^{-1} = \overline{f}(g)^g\overline{f}(h)\,, \end{aligned}$$

which is the 1-cocycle identity in multiplicative notation.

- As a consequence, we set

$$\alpha(\varphi) := \big(\overline{f} : G \longrightarrow A\big)\,.$$

To prove that this defines a group homomorphism, let $\varphi_1, \varphi_2 \in \mathrm{Aut}_{A,G}(E)$ and respectively let $\overline{f}_1, \overline{f}_2 : G \longrightarrow A$ be the associated 1-cocycles, i.e. $\alpha(\varphi_1) = \overline{f}_1$ and $\alpha(\varphi_2) = \overline{f}_2$. Then

$$\varphi_1(\widetilde{g}) = \overline{f}_1(g)\widetilde{g}, \quad \varphi_2(\widetilde{g}) = \overline{f}_2(g)\widetilde{g} \qquad \forall\, g \in G \text{ with } \widetilde{g} \in p^{-1}(g)\,,$$

and hence using the fact that A is abelian yields

$$\begin{aligned} \alpha(\varphi_1\circ\varphi_2)(g) = (\varphi_1\circ\varphi_2)(\widetilde{g})\widetilde{g}^{-1} &= \varphi_1\big(\overline{f}_2(g)\widetilde{g}\big)\widetilde{g}^{-1} \\ &= \overline{f}_2(g)\varphi_1(\widetilde{g})\widetilde{g}^{-1} \\ &= \overline{f}_2(g)\overline{f}_1(g)\widetilde{g}\widetilde{g}^{-1} \\ &= \overline{f}_2(g)\overline{f}_1(g) \\ &= \alpha(\varphi_1)(g)\cdot\alpha(\varphi_2)(g) = \big(\alpha(\varphi_1)\cdot\alpha(\varphi_2)\big)(g)\,, \end{aligned}$$

as required.

- In order to prove that α is an isomorphism, we define

$$\begin{array}{rccl} \beta: & Z^1(G,A_*) & \longrightarrow & \mathrm{Aut}_{A,G}(E) \\ & c & \mapsto & \beta(c): E \longrightarrow E, \widetilde{g} \mapsto c(g)\,\widetilde{g}\,, \end{array}$$

where $g = p(\widetilde{g})$.

First, we check that $\beta(c)$ is indeed a group homomorphism: for $\widetilde{g}, \widetilde{h} \in E$ with the above notation, we have

$$\begin{aligned} \beta(c)\big(\widetilde{g}\cdot\widetilde{h}\big) = c(gh)\widetilde{g}\widetilde{h} & \overset{\text{1-cocycle id.}}{=} c(g)\cdot {}^{g}c(h)\cdot\widetilde{g}\widetilde{h} \\ &= c(g)\widetilde{g}c(h)\widetilde{g}^{-1}\widetilde{g}\widetilde{h} \\ &= c(g)\widetilde{g}c(h)\widetilde{h} \\ &= \beta(c)(\widetilde{g})\cdot\beta(c)(\widetilde{h})\,. \end{aligned}$$

Next, if $\widetilde{g} \in A = \ker(p)$, then $g = 1_G$ and therefore

$$\beta(c)(\widetilde{g}) = c(1)\cdot\widetilde{g} = 1\cdot\widetilde{g} = \widetilde{g}\,,$$

where we use the fact that a 1-cocycle is always normalised (indeed $c(1_G) = 1_A$, since for $h \in G$, $c(1_G\cdot h) = c(1_G)\cdot {}^{(1_G)}c(h) = c(1_G)c(h)$ by the 1-cocycle identity). Thus we have proved that $\beta(c)|_A = \mathrm{Id}_A$.

Furthermore, since $c(g) \in A = \ker(p)$, $p(c(g)) = 1_G$ and we get

$$\big(p\circ\beta(c)\big)(\widetilde{g}) = p\big(c(g)\cdot\widetilde{g}\big) = \underbrace{p\big(c(g)\big)}_{=1_G}\cdot p(\widetilde{g}) = p(\widetilde{g})$$

and so $p\circ\beta(c) = p$, or in other words $\beta(c)$ induces the identity on G.

Finally, using Exercise 41 we obtain that any group homomorphism $E \longrightarrow E$ inducing the identity on A and on G must be an isomorphism. Therefore, we have proved that $\beta(c) \in \mathrm{Aut}_{A,G}(E)$ for every $c \in Z^1(G,A_*)$.

- It remains to prove that α and β are inverse to each other. Firstly,

$$\big((\alpha\circ\beta)(c)\big)(g) = \beta(c)(\widetilde{g})\cdot\widetilde{g}^{-1} = c(g)\widetilde{g}\widetilde{g}^{-1} = c(g) \quad \forall\, g\in G, \forall\, c \in Z^1(G,A_*)\,,$$

so that $\alpha\circ\beta$ is the identity on $Z^1(G,A_*)$. Secondly,

$$\big((\beta\circ\alpha)(\varphi)\big)(\widetilde{g}) = (\alpha(\varphi))(g)\cdot\widetilde{g}^{-1} = \varphi(g)\widetilde{g}\widetilde{g}^{-1} = \varphi(g) \quad \forall \widetilde{g}\in E, \forall\, \varphi \in \mathrm{Aut}_{A,G}(E)\,,$$

so that $\beta\circ\alpha$ is the identity on $\mathrm{Aut}_{A,G}(E)$.

Claim 3: $\mathrm{Inn}_A(E) \cong B^1(G,A_*)$.

- Let $a \in A$ and $c_a \in \mathrm{Inn}_A(E)$. Then for every $g \in G$,

$$\alpha(c_a)(g) = c_a(\widetilde{g})\cdot\widetilde{g}^{-1} = a\cdot\underbrace{\widetilde{g}\cdot a^{-1}\cdot\widetilde{g}^{-1}}_{\in A \trianglelefteq E} = \widetilde{g}a^{-1}\widetilde{g}^{-1}\cdot a = {}^{g}(a^{-1})a = d_1^*(a^{-1})(g)$$

and therefore $\alpha(c_a) \in B^1(G,A_*)$, i.e. $\alpha\big(\mathrm{Inn}_A E\big) \subseteq B^1(G,A_*)$.

Conversely, if $a \in A$ and $d_1^*(a) \in B^1(G,A_*)$, then $d_1^*(a)(g) = {}^{g}a\cdot a^{-1}$ and

$$\beta\big(d_1^*(a)\big)(\widetilde{g}) = d_1^*(a)(g)\cdot\widetilde{g} = {}^{g}a\cdot a^{-1}\cdot\widetilde{g} = \widetilde{g}\cdot a\cdot\underbrace{\widetilde{g}^{-1}\cdot a^{-1}\cdot\widetilde{g}}_{\in A\trianglelefteq E} = \underbrace{\widetilde{g}\cdot\widetilde{g}^{-1}}_{=1}a^{-1}\widetilde{g}\cdot a = c_{a^{-1}}(\widetilde{g}).$$

Hence $\beta\big(d_1^*(a)\big) = c_{a^{-1}} \in \mathrm{Inn}_A(E)$, and $\beta\big(B^1(G,A_*)\big) \subseteq \mathrm{Inn}_A(E)$. It follows that $\mathrm{Inn}_A(E)$ corresponds to $B^1(G,A_*)$ under the bijection given by α and β, and we obtain

$$H^1(G,A_*) = Z^1(G,A_*)/B^1(G,A_*) \cong \mathrm{Aut}_{A,G}(E)/\,\mathrm{Inn}_A(E)\,.$$

(b) If A is a central subgroup of E, then for every $a \in A$ the conjugation automorphism by a is given by $c_a : E \longrightarrow E, e \mapsto aea^{-1} = aa^{-1}e = e$, i.e. the identity on E. Thus

$$\mathrm{Inn}_A(E) = \{c_a : E \longrightarrow E \mid a \in A\} = \{\mathrm{Id}_E\}$$

and it follows from (a) that

$$H^1(G, A_*) \cong \mathrm{Aut}_{A,G}(E)/\,\mathrm{Inn}_A(E) = \mathrm{Aut}_{A,G}(E)\,. \qquad \blacksquare$$

We are now ready to parametrise the slpittings of split group extensions with abelian kernel:

Theorem 23.3 (H^1 *and splittings*)

Let $\mathcal{E}_\bullet := (\, 1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1 \,)$ be a split group extension with abelian kernel. Then the following holds:

(a) There is a bijection between $H^1(G, A_*)$ and the set $\mathcal{S}$ of A-conjugacy classes of splittings of $\mathcal{E}_\bullet$.

(b) There is a bijection between $H^1(G, A_*)$ and the set of E-conjugacy classes of complements of A in E.

Proof:

(a) Choose a splitting $s_0 : G \longrightarrow E$ and define a map

$$\begin{array}{rccc} \alpha : & \mathrm{Aut}_{A,G}(E) & \longrightarrow & \{\text{splittings of } \mathcal{E}_\bullet\} \\ & \varphi & \mapsto & \varphi \circ s_0\,. \end{array}$$

It is obvious that α is well-defined, i.e. that $\varphi \circ s_0$ is a splitting of the extension as $p\varphi s_0 = ps_0 = \mathrm{Id}_G$. Define a second map

$$\begin{array}{rccc} \beta : & \{\text{splittings of } \mathcal{E}_\bullet\} & \longrightarrow & \mathrm{Aut}_{A,G}(E) \\ & s & \mapsto & \big(\psi_s : E \longrightarrow E, as_0(g) \mapsto as(g)\big)\,, \end{array}$$

where by Proposition 22.7 an arbitrary element $x \in E$ can be written in a unique way as $x = as_0(g)$ with $a \in A$ and $g \in G$. We check that β is well-defined. Firstly, ψ_s is a group homomorphism: for every $x_1 = a_1 s_0(g_1), x_2 = a_2 s_0(g_2) \in E$, we have

$$\begin{aligned} \psi_s(x_1 \cdot x_2) = \psi_s\big(a_1 s_0(g_1) \cdot a_2 s_0(g_2)\big) &= \psi_s\big(a_1 \cdot {}^{g_1}a_2 \cdot s_0(g_1 g_2)\big) \\ &= a_1 \cdot {}^{g_1}a_2 \cdot s\big(g_1 g_2\big) \\ &= a_1 s(g_1) \cdot a_2 s(g_2) \\ &= \psi_s\big(a_1 s_0(g_1)\big) \cdot \psi_s\big(a_2 s_0(g_2)\big) = \psi_s(x_1) \cdot \psi_s(x_2)\,. \end{aligned}$$

Secondly, $\psi_s|_A = \mathrm{Id}_A$ by definition. Thirdly, $p\psi_s = p$ since for $x = as_0(g) \in E$, we have

$$(p \circ \psi_s)(x) = (p \circ \psi_s)(as_0(g)) = p(as(g)) = \underbrace{p(a)}_{=1} \cdot \underbrace{p(s(g))}_{=\mathrm{Id}_G(g)} = g = p(as_0(g))\,.$$

Finally, the fact that ψ_s is an isomorphism follows again from Exercise 41, because ψ_s induces the identity on both A and G. Whence β is well-defined.
Next, we check that α and β are inverse to each other. On the one hand,

$$(\alpha \circ \beta)(s) = \alpha(\psi_s) = \psi_s \circ s_0 \qquad \forall\, s \in \{\text{splittings of } \mathcal{E}_\bullet\}$$

but for every $g \in G$, $(\psi_s \circ s_0)(g) = \psi_s(1_A \cdot s_0(g)) = 1_G s(g) = s(g)$, hence $\alpha \circ \beta$ is the identity on the set of splittings of $\mathcal{E}_\bullet$. On the other hand, for every $\varphi \in \mathrm{Aut}_{A,G}(E)$, we have

$$(\beta \circ \alpha)(\varphi) = \beta(\varphi \circ s_0) = \psi_{\varphi \circ s_0}$$

and for each $x = as_0(g) \in E$ (with $a \in A$ and $g \in G$), we have

$$\psi_{\varphi \circ s_0}\big(as_0(g)\big) = a \cdot (\varphi \circ s_0)(g) \overset{\varphi|_A = \mathrm{Id}_A}{=} \varphi(a) \cdot (\varphi \circ s_0)(g) = \varphi\big(a \cdot s_0(g)\big)\,,$$

hence $\beta \circ \alpha$ is the identity on $\mathrm{Aut}_{A,G}(E)$.
Therefore,

$$\begin{tikzcd} \mathrm{Aut}_{A,G}(E) \arrow[r, shift left, "\alpha"] & \{\text{splittings of } \mathcal{E}_\bullet\} \arrow[l, shift left, "\beta"] \end{tikzcd}$$

are bijections (of sets). Finally, we determine the behaviour of $\mathrm{Inn}_A(E)$ under these bijections. Let $\varphi \in \mathrm{Aut}_{A,G}(E)$ and $c_b \in \mathrm{Inn}_A(E)$ with $b \in A$. Let $\varphi' = c_b \circ \varphi$. Then

$$\alpha(\varphi) = \varphi \circ s_0 \quad \text{and} \quad \alpha(c_b \circ \varphi) = c_b \circ \varphi \circ s_0\,.$$

Hence a coset modulo $\mathrm{Inn}_A(E)$ is mapped via α to an equivalence class for the action by conjugation of A on splittings

$$\begin{array}{ccc} A \times \{\text{splittings of } \mathcal{E}_\bullet\} & \longrightarrow & \{\text{splittings of } \mathcal{E}_\bullet\} \\ (b, s) & \mapsto & c_b \circ s\,. \end{array}$$

Thus passing to the quotient (group quotient on the left hand side $\mathrm{Aut}_{A,G}(E)$, and orbits of $\mathrm{Inn}_A(E)$ on the right hand side) yields a bijection

$$\begin{tikzcd} \mathrm{Aut}_{A,G}(E)/\mathrm{Inn}_A(E) \arrow[r, "\sim"] \arrow[d, leftrightarrow, "\cong", "(\text{Thm. } 23.2)"'] & \{A\text{-conjugacy classes of splittings of } \mathcal{E}_\bullet\} \\ H^1(G, A_*) & \end{tikzcd}$$

as required.

(b) By Proposition 22.7, a splitting s of $\mathcal{E}_\bullet$ corresponds to a complement $s(G)$ of A in E, and conversely, a complement H of A in E corresponds to a splitting $\big(p|_H\big)^{-1} : G \longrightarrow H$. Moreover, the A-conjugacy class of H is the same as the E-conjugacy class of H, because every $e \in E$ may be written in a unique way as $e = ah$ with $a \in A$ and $h \in H$ and so $eHe^{-1} = aHa^{-1}$. The claim follows. ■

24 H^2 and Group Extensions

Convention: In this section all group extensions are assumed to have abelian kernel.

Definition 24.1 (***Equivalent group extensions***)

Two group extensions $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ and $1 \longrightarrow A \xrightarrow{i'} E' \xrightarrow{p'} G \longrightarrow 1$ with abelian kernels are called **equivalent** if there exists a group homomorphism $\varphi : E \longrightarrow E'$ such that the following diagram commutes

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "i"] \arrow[d, "\mathrm{Id}_A"'] \arrow[dr, phantom, "\circlearrowleft"] & E \arrow[r, "p"] \arrow[d, "\varphi"] \arrow[dr, phantom, "\circlearrowleft"] & G \arrow[r] \arrow[d, "\mathrm{Id}_G"] & 1 \\ 1 \arrow[r] & A \arrow[r, "i'"] & E' \arrow[r, "p'"] & G \arrow[r] & 1. \end{tikzcd}$$

Remark 24.2

(a) In the context of Definition 24.1, the homomorphism φ is necessarily bijective. However an isomorphism of groups does not induce an equivalence of extensions in general. In other words, the same middle group E can occur in non-equivalent group extensions with the same kernel A, the same quotient G and the same induced $\mathbb{Z}G$-module structure on A. (See Example 12 at the end of the section.)

(b) Equivalence of group extensions is an equivalence relation.

Notation: If G is a group and $A_* := (A, \cdot, *)$ is a $\mathbb{Z}G$-module (which may see simply as an abelian group), then we let $\mathcal{E}(G, A_*)$ denote the set of equivalence classes of group extensions

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "i"] & E \arrow[r, "p"] & G \arrow[r] & 1 \end{tikzcd}$$

inducing the given $\mathbb{Z}G$-module structure on A.

Theorem 24.3

Let G be a group and let $A_* := (A, \cdot, *)$ be a fixed $\mathbb{Z}G$-module (written multiplicatively). Then, there is a bijection

$$H^2(G, A_*) \overset{\sim}{\longleftrightarrow} \mathcal{E}(G, A_*) \ .$$

Moreover, the neutral element of $H^2(G, A_*)$ corresponds to the class of the split extension.

Proof: We want to define a bijection $\mathcal{E}(G, A_*) \longrightarrow H^2(G, A_*)$.

- To begin with, fix an extension

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "i"] & E \arrow[r, "p"] & G \arrow[r] & 1 \end{tikzcd}$$

inducing the given action $*$ on A, and we choose a set-theoretic section $s : G \longrightarrow E$ for p, i.e. such that $p \circ s = \mathrm{Id}_G$. Possibly s is not be a group homomorphism, but for ecery $g, h \in G$ we may write

$$s(g) \cdot s(h) = f(g, h) \cdot s(gh)$$

for some element $f(g, h) \in E$. This defines a map

$$\begin{array}{rccl} f: & G \times G & \longrightarrow & E \\ & (g, h) & \mapsto & f(g, h) := s(g) \cdot s(h) \cdot s(gh)^{-1}. \end{array}$$

Furthermore, notice that $f(g, h) \in A = \ker(p)$ because

$$p\big(f(g, h)\big) = p\big(s(g)s(h)s(gh)^{-1}\big) = p\big(s(g)\big) \cdot p\big(s(h)\big) \cdot p\big(s(gh)\big)^{-1} = ghh^{-1}g^{-1} = 1_G$$

for every $g, h \in G$. Hence $f \in \mathrm{Hom}_{\mathsf{Set}}(G \times G, A)$, and as a matter of fact, f is a 2-cocycle because:

$$\big(s(g) \cdot s(h)\big) \cdot s(k) = f(g, h) \cdot s(gh) \cdot s(k) = f(g, h) \cdot f(gh, k) \cdot s(ghk)$$

and

$$\begin{aligned} s(g) \cdot \big(s(h) \cdot s(k)\big) = s(g) \cdot f(h, k) \cdot s(hk) &= s(g) \cdot f(h, k) \cdot s(g)^{-1} \cdot s(g) \cdot s(hk) \\ &= {}^{g}f(h, k) \cdot f(g, hk) \cdot s(ghk) \end{aligned}$$

for every $g, h, k \in G$. Therefore, by associativity in E, we obtain

$$f(g,h) \cdot f(gh,k) = {}^{g}f(h,k) \cdot f(g,hk),$$

which is precisely the 2-cocycle identity in multiplicative notation.
Now, we note that if we modify s by a 1-cochain $c : G \longrightarrow A$ and define

$$\begin{array}{rccl} s' : & G & \longrightarrow & E \\ & g & \longmapsto & s'(g) := c(g) \cdot s(g)\,, \end{array}$$

then the corresponding 2-cocycle is given by

$$\begin{aligned} f'(g,h) &= s'(g) \cdot s'(h) \cdot s'(gh)^{-1} \\ &= c(g) \cdot s(g) \cdot c(h) \cdot s(h) \cdot s(gh)^{-1} \cdot c(gh)^{-1} \\ &= c(g) \cdot s(g) \cdot c(h) \cdot s(g)^{-1} s(g) \cdot s(h) \cdot s(gh)^{-1} \cdot c(gh)^{-1} \\ &= c(g) \cdot s(g) \cdot c(h) \cdot s(g^{-1}) \cdot f(g,h) \cdot c(gh)^{-1} \\ &= c(g) \cdot {}^{g}c(h) \cdot c(gh)^{-1} \cdot f(g,h) && \text{(as } A \text{ is abelian)} \\ &= {}^{g}c(h) \cdot c(gh)^{-1} \cdot c(g) \cdot f(g,h) && \text{(as } A \text{ is abelian)} \\ &= (d_2^*(c))(g,h) \cdot f(g,h) \qquad \forall\, g,h \in G. \end{aligned}$$

To sum up, we have modified the 2-cocycle f by the 2-coboundary $d_2^*(c)$. Therefore, the cohomology class $[f] := fB^2(G, A_*)$ of f in $H^2(G, A_*)$ is well-defined, depending on the given extension, but does not depend on the choice of the set-theoretic section s. Hence, we may define a map

$$\begin{array}{rccl} \xi : & \mathcal{E}(G, A_*) & \longrightarrow & H^2(G, A_*) \\ & [\,1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1\,] & \longmapsto & [f]\,. \end{array}$$

· We check that ξ is well-defined. Suppose that we have two equivalent extensions

$$[\,1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1\,] = [\,1 \to A \xrightarrow{i'} E' \xrightarrow{p'} G \to 1\,] \in \mathcal{E}(G, A_*)\,,$$

that is a commutative diagram of the form

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "i"] \arrow[d, "\mathrm{Id}_A"'] \arrow[dr, phantom, "\circlearrowleft"] & E \arrow[r, "p"] \arrow[d, "\varphi"] \arrow[dr, phantom, "\circlearrowleft"] & G \arrow[r] \arrow[d, "\mathrm{Id}_G"] & 1 \\
1 \arrow[r] & A \arrow[r, "i'"] & E' \arrow[r, "p'"] & G \arrow[r] & 1
\end{tikzcd}$$

where φ is an isomorphism of $E \longrightarrow E'$. As above, we choose a set-theoretic section $s : G \longrightarrow E$ of p, and it follows that $\varphi \circ s$ is a set-theoretic section for p', since $p' \circ \varphi \circ s = p \circ s = \mathrm{Id}_G$. The corresponding 2-cocycle is given by

$$\begin{aligned} f'(g,h) = (\varphi \circ s)(g) \cdot (\varphi \circ s)(h) \cdot (\varphi \circ s)(gh)^{-1} &= \varphi\big(s(g) \cdot s(h) \cdot s(gh)^{-1}\big) \\ &= \varphi\big(f(g,h)\big) = f(g,h) \qquad \forall\, g,h \in G \end{aligned}$$

as $\varphi|_A = \mathrm{Id}_A$. Hence ξ is well-defined.

· Remark: We may choose $s : G \longrightarrow E$ is such that $s(1) = 1$, and the associated 2-cocycle is normalised. Now if we modify s by a normalised 1-cochain $c : G \longrightarrow A$ (i.e. such that $c(1) = 1$), then $d_2^*(c)$ is a normaised 2-coboundary. Therefore, we may as well use normalised cocycles/cochains/coboundaries.

- Surjectivity of ξ:
  Let $\alpha \in H^2(G, A_*)$ and choose a normalised 2-cocycle $f : G \times G \longrightarrow A$ such that $\alpha = [f]$. Construct $E_f := A \times G$ (as a set), which we endow with the product

  $$(a, g) \cdot (b, h) = \big(a \cdot {}^g b \cdot f(g, h), g \cdot h\big) \qquad \forall\, a, b \in A, \forall\, g, h \in G\,.$$

  Then $(E_f, \cdot)$ is a group whose neutral element is $(1, 1)$. (Exercise 44.) Clearly there are group homomorphisms:

  $$\begin{aligned} i : A \longrightarrow E_f, &\quad a \longmapsto (a, 1)\,, \\ p : E_f \longrightarrow G, &\quad (a, g) \longmapsto g \end{aligned}$$

  such that $\ker(p) = \operatorname{Im}(i)$, thus we get a group extension

  $$1 \longrightarrow A \xrightarrow{i} E_f \xrightarrow{p} G \longrightarrow 1.$$

  We need to prove that the cohomology class of the 2-cocycle induced by this extension via the above construction is precisely $[f]$. So consider the set-theoretic section $s : G \longrightarrow E_f, g \longmapsto (1, g)$ of p and compute that for all $g, h \in G$, we have

  $$\begin{aligned} s(g) \cdot s(h) \cdot s(gh)^{-1} &= (1, g) \cdot (1, h) \cdot (1, gh)^{-1} \\ &= \big(1 \cdot {}^g 1 \cdot f(g, h), gh\big) \cdot \big({}^{(gh)^{-1}} f(gh, (gh)^{-1})^{-1}, (gh)^{-1}\big) \\ &= (f(g, h)^{(gh)(gh)^{-1}} f(gh, (gh)^{-1}), (gh)(gh)^{-1}) \\ &= \big(f(g, h), 1\big) \end{aligned}$$

  as required.

- Injectivity of ξ:
  Let

  $$\begin{aligned} &[1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1]\,, \\ &[1 \longrightarrow A \xrightarrow{\tilde{i}} \widetilde{E} \xrightarrow{\tilde{p}} G \longrightarrow 1] \end{aligned}$$

  be two classes of group extensions in $\mathcal{E}(G, A_*)$. Choose, respectively, $s : G \longrightarrow E$ and $\tilde{s} : G \longrightarrow \widetilde{E}$ two set-theoretic section with corresponding 2-cocycles f and $\tilde{f}$ respectively. Now, assume that

  $$[f] = \big[\tilde{f}\,\big] \in H^2(G, A_*)\,.$$

  Then $\tilde{f} = d_2^*(c) \circ f$ for some 1-cochain $c : G \longrightarrow A$. Changing the choice of $\tilde{s}$ by defining $\tilde{\tilde{s}} : G \longrightarrow \widetilde{E}, g \mapsto c(g)^{-1} \cdot \tilde{s}(g)$ modifies $\tilde{f}$ into $d_2^*(c)^{-1} \circ \tilde{f}$ by the first part of the proof. But $d_2^*(c)^{-1} \circ \tilde{f} = f$, therfore, we may assume without loss of generality that the two 2-cocycles are the same. Compute the group law in E: each element of E can be written as $a \cdot s(g)$ for $a \in A$ and $g \in G$ because $s : G \longrightarrow E$ is a section for $p : E \longrightarrow G$. Hence the product is

  $$\begin{aligned} as(g) \cdot bs(h) &= as(g)bs(g)^{-1}s(g)s(h) \\ &= a{}^g bs(g)s(h) \\ &= \underbrace{a{}^g bf(g, h)}_{\in A}\, s(gh) \end{aligned}$$

  which is exactely the group law in E_f. Hence $E_f \cong E$ (via $(a, g) \mapsto a \cdot s(g)$) as groups, but also as extensions, because the latter isomorphism induces the identity on both A and G. Similarly, we get that $\widetilde{E} \cong E_f$, as group extensions. The injectivity of ξ follows.

- Finally notice that the image under ξ of the split extension

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] & A \rtimes G \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

where the action of G on A is given by $*$, and where the first map is the canonical inclusion and the second map the projection onto G, is trivial. This is because we can choose a section $s : G \longrightarrow A \rtimes G, g \mapsto (1, g)$, which is a group homomorphism. Therefore the corresponding 2-cocycle is $f : G \times G \longrightarrow A, (g, h) \mapsto 1$. This proves the 2nd claim. ■

Remark 24.4

(a) In the above proof, if we choose $s : G \longrightarrow E$ such that $s(1) = 1$, then we obtain a normalised 2-cocycle. If we modify $s : G \longrightarrow A$ by a 1-cocycle $c : G \longrightarrow A$ such that $c(1) = 1$ (a normalised 1-cochain), then dc is a normalised 2-coboundary. So we see that we can use normalised cochains, cocycles and coboundaries throughout.

(b) If the group A is not abelian, then $H^3\big(G, Z(A)\big)$ comes into play for the classification of the extensions. This is more involved.

Example 12

For example, if we want to find all 2-groups of order 2^n ($n \geqslant 3$) with a central subgroup of order 2 and a corresponding dihedral quotient, then we have to classify the *central extensions* of $G := D_{2^{n-1}}$ by $A := C_2$. By Theorem 24.3 the isomorphism classes of central extensions of the form

$$1 \longrightarrow C_2 \longrightarrow E \longrightarrow D_{2^{n-1}} \longrightarrow 1 .$$

are in bijection with $H^2(G, A_*)$, where A_* is the trivial $\mathbb{Z}G$-module. Computations$^{(*)}$ yield

$$H^2(G, A_*) \cong (\mathbb{Z}/2)^3$$

hence there are 8 isomorphism classes of such extensions. Since a presentation of $D_{2^{n-1}}$ is

$$\langle \rho, \sigma \mid \rho^2 = 1 = \sigma^2, (\rho\sigma)^{2^{n-2}} = 1 \rangle,$$

obviously E admits a presentation of the form

$$\langle r, s, t \mid rt = tr, st = ts, t^2 = 1, r^2 = t^a, s^2 = t^b, (rs)^{2^{n-2}} = t^c \ (a, b, c \in \{0, 1\}) \rangle .$$

Letting a, b, c vary, we obtain the following groups E:

(i) The case $a = b = c = 0$ gives the direct product $C_2 \times D_{2^{n-1}}$.

(ii) The case $a = b = 0$, $c = 1$ gives the dihedral group D_{2^n}.

(iii) The cases $a = c = 0$, $b = 1$ and $b = c = 0$, $a = 1$ give the group $(C_{2^{n-2}} \times C_2) \rtimes C_2$.

(iv) The cases $a = 0$, $b = c = 1$ and $b = 0$, $a = c = 1$ both give the semi-dihedral group SD_{2^n} of order 2^n.

(v) The case $c = 0$, $a = b = 1$ gives the group $C_{2^{n-2}} \rtimes C_4$.

(vi) The case $a = b = c = 1$ gives the generalised quaternion group Q_{2^n}.

If $n \geqslant 4$, the groups in cases (i)-(vi) are pairwise non-isomorphic. If $n = 3$ the above holds as well, but the groups in (ii) and (iii) are all isomorphic to D_8, and the groups in (iv) and (v) are all isomorphic to $C_2 \times C_4$.

($*$) A direct computation of 2-cocycles and 2-coboundary is possible. Alternatively, the cohomological Künneth formula yields the result easily. We will come back to this formula later in the lecture if time permits.

25 Exercises for Chapter 6

Exercise 40

Let $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ be a group extension. Prove that TFAE:

(a) i has a group-theoretic retraction;

(b) A has a normal complement in E;

(c) there is a subgroup H of E such that $E \cong A \times H$.

Exhibit examples of split extensions of groups which do not admit a group-theoretic retraction.

Exercise 41

Let $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ be a group extension.

(a) Prove that if G is a free group, then the extension splits.

(b) Prove that any group homomorphism $E \longrightarrow E$ inducing the identity on A and on G is an isomorphism.

Exercise 42

(a) Consider the dihedral 2-group $E = D_{2^n}$ $(n \geqslant 3)$ and A its cyclic subgroup of index 2. How many E-conjugacy classes of complements of A in E are there? Describe them all.

(b) Same question for $E = (\underbrace{A \times \cdots \times A}_{m \text{ factors}}) \rtimes C_m$, where A is an abelian group and C_m acts by cyclic permutations.

Exercise 43

Let G be a finite group, let A be a finite trivial $\mathbb{Z}G$-module, and assume that $\gcd(|A|, |G|) = 1$.

(a) Prove that $H^1(G, A) = 0$.

(b) Find all complements of A in $A \times G$.

Exercise 44

Let A be a $\mathbb{Z}G$-module, written multiplicatively and let $f : G \times G \longrightarrow A$ be a normalised 2-cocycle.

Let $E_f = A \times G$ with product

$$(a, g)(b, h) = (a\,{}^{g}b f(g, h), gh) \qquad \forall\,(a, g), (b, h) \in E_f.$$

Using the 2-cocycle identity, prove that E_f is a group and that the left and right inverses coincide, that is:

$$({}^{g^{-1}}a^{-1} f(g^{-1}, g)^{-1}, g^{-1}) = ({}^{g^{-1}}a^{-1}\,{}^{g^{-1}}f(g, g^{-1})^{-1}, g^{-1}) \quad \forall\,(a, g) \in E_f.$$

Moreover, verify that there is an extension $1 \longrightarrow A \longrightarrow E_f \longrightarrow G \longrightarrow 1$ associated with the 2-cocycle f which induces the given G-action on A.

Exercise 45

(a) Let $A := C_4$ and $G := C_2$.

- Find all actions by group automorphisms of G on A.
- For each such action, compute $H^2(G, A)$.
- In each case, describe all extensions of A by G inducing the given action, up to equivalence.

(b) Let $G := C_2 \times C_2$ and $A := C_2$ regarded as a trivial $\mathbb{Z}G$-module. Assume known that $H^2(G, A) \cong (\mathbb{Z}/2)^3$.

- Given $1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$ an arbitrary central extension of A by G, determine a presentation of the group E using a presentation of A and a presentation of G.
- Find all central extensions of A by G, up to equivalence, using the previous point.

(c) Classify groups of order 8 up to isomorphism.

Chapter 7. Subgroups and Cohomology

Throughout this chapter, unless otherwise stated, G denotes a group in multiplicative notation and $H \leqslant G$ a subgroup of G. The aim of the chapter is to investigate relations between the cohomology of G and the cohomology of H. This can be done using four operations called *restriction, transfer (or corestriction), induction*, and *coinduction*. As our next aim in the lecture is to prove theorems about finite groups using cohomology, we will most of the time work under the mild assumption that H has finite index in G.

References:

[Bro94] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994.

[Eve91] L. Evens, *The cohomology of groups*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1991.

26 Restriction in Cohomology

Notation 26.1 (***Restriction of*** $\mathbb{Z}G$***-modules***)

Let M be a $\mathbb{Z}G$-module. Because $\mathbb{Z}H \subseteq \mathbb{Z}G$ is a subring, we may perform a change of the base ring (see Example 4(e)) and restrict the action of $\mathbb{Z}G$ on M to an action of $\mathbb{Z}H$ on M. In this way, we regard M as a $\mathbb{Z}H$-module, which we denote by $\mathrm{Res}_H^G(M)$ or $M{\downarrow}_H^G$ (or sometimes simply by M itself again) and call the **restriction of** M **from** G **to** H.

In other words $\mathrm{Res}_H^G : {}_{\mathbb{Z}G}\mathbf{Mod} \longrightarrow {}_{\mathbb{Z}H}\mathbf{Mod}$ is a forgetful functor, which is obviously covariant. Moreover, $\mathrm{Res}_H^G(M) \cong \mathbb{Z}G \otimes_{\mathbb{Z}G} M$ as left $\mathbb{Z}H$-modules where $\mathbb{Z}G$ is seen as a $(\mathbb{Z}H, \mathbb{Z}G)$-bimodule.

Definition 26.2 (***Left transversal, right transversal***)

A **left transversal** of H in G is a set $\{g_i\}_{i\in I}$ of representatives of the left cosets of H in G. Thus $G = \coprod_{i\in I} g_iH$. Similarly, a **right transversal** of H in G is a set of representatives of the right cosets of H in G.

We want to investigate how restriction of modules interacts with the cohomology the groups G and H. To this end, first we need to understand restriction of projective resolutions.

Lemma 26.3

Let P be a free (resp. projective) right $\mathbb{Z}G$-module. Then $P\downarrow_H^G$ is a free (resp. projective) right $\mathbb{Z}H$-module. (Similarly for left modules.)

Proof: It suffices to prove that $P\downarrow_H^G$ is a free $\mathbb{Z}H$-module for $P = \mathbb{Z}G$, because an arbitrary free $\mathbb{Z}G$-module is isomorphic to a direct sum $\bigoplus \mathbb{Z}G$. So, choose a left transversal $\{g_i\}_{i\in I}$ of H in G. Then

$$\mathbb{Z}G = \bigoplus_{i\in I} g_i\mathbb{Z}H$$

and it follows that $\mathbb{Z}G$ is a free right $\mathbb{Z}H$-module. Now, if P is a projective right $\mathbb{Z}G$-module, then P is a direct summand of a free $\mathbb{Z}G$-module by Proposition-Definition 7.7, therefore by the above $P\downarrow_H^G$ is a direct summand of a free $\mathbb{Z}H$-module, hence is a projective $\mathbb{Z}H$-module. ■

Remark 26.4 (*Restriction in Cohomology*)

Let $P_\bullet = \big(\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0\big)$ be a projective resolution of the trivial $\mathbb{Z}G$-module $\mathbb{Z}$ and let M be an arbitrary $\mathbb{Z}G$-module. Then $H^n(G,M)$ is the cohomology of the cochain complex $\mathrm{Hom}_{\mathbb{Z}G}(P_\bullet, M)$. By Lemma 26.3, restricting to H yields a projective resolution

$$\mathrm{Res}_H^G(P_\bullet) = \big(\cdots \xrightarrow{d_3} P_2\downarrow_H^G \xrightarrow{d_2} P_1\downarrow_H^G \xrightarrow{d_1} P_0\downarrow_H^G\big)$$

of $\mathbb{Z} = \mathbb{Z}\downarrow_H^G$ seen as a $\mathbb{Z}H$-module. Now, there is an inclusion map of cochain complexes:

$$i_\bullet : \mathrm{Hom}_{\mathbb{Z}G}(P_\bullet, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}H}(\mathrm{Res}_H^G(P_\bullet), M\downarrow_H^G)$$

which, by functoriality, induces a homomorphism in cohomology

$$\mathrm{res}_H^G : H^n(G,M) \longrightarrow H^n(H, M\downarrow_H^G).$$

called **restriction** from G to H.

Remark 26.5

(a) The map res_H^G need not be injective in general.

(b) If the bar resolution is used to compute cohomology, then on $Z^n(G,M)$, the map res_H^G is given by ordinary restriction of cocycles from G^n to H^n.

27 Transfer in Cohomology

Assume that H has finite index in G, say $r := |G : H|$. Let $\{g_i\}_{1\leqslant i\leqslant r}$ be a left transversal for H in G. If L and M are $\mathbb{Z}G$-modules, then there is a $\mathbb{Z}$-linear map

$$\begin{aligned}\mathrm{tr}_H^G : \mathrm{Hom}_{\mathbb{Z}H}(L,M) &\longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(L,M)\\ \varphi &\longmapsto \sum_{i=1}^{r} g_i\varphi g_i^{-1}\end{aligned}$$

where g_i^{-1} denotes the action of $g_i^{-1} \in G$ on L and g_i denotes the action of $g_i \in G$ on M.

Lemma 27.1

The map tr_H^G is well-defined.

Proof:

(1) The definition of tr_H^G does not depend on the choice of the transversal:
Assume $\{g_i'\}_{1\leqslant i\leqslant r}$ is another left transversal for H in G and write $g_i' = g_ih_i$ ($1 \leqslant i \leqslant r$) for some $h_i \in H$. If $\varphi \in \mathrm{Hom}_{\mathbb{Z}H}(L, M)$ then making use of the $\mathbb{Z}H$-linearity of φ, we get

$$\sum_{i=1}^{r} g_i'\varphi(g_i')^{-1} = \sum_{i=1}^{r} g_ih_i\varphi h_i^{-1}g_i^{-1} \overset{\mathbb{Z}H\text{-lin.}}{=} \sum_{i=1}^{r} g_i\varphi h_ih_i^{-1}g_i^{-1} = \sum_{i=1}^{r} g_i\varphi g_i^{-1},$$

as required.

(2) $\mathbb{Z}G$-linearity of $\mathrm{tr}_H^G(\varphi)$:
Let $s \in G$. Then for each $1 \leqslant i \leqslant r$, we may write $sg_i = g_{\sigma(i)}h_i$, where $\sigma \in S_r$ is a permutation and $h_i \in H$ (if i and j are such that $\sigma(i) = \sigma(j)$, then we find $g_i = g_j \cdot h_j^{-1} \cdot h_i$ and thus $i = j$, since $\{g_i\}_{1\leqslant i\leqslant r}$ is a transversal). Now, let $x \in L$ and compute

$$\begin{aligned} s \cdot \big(\mathrm{tr}_H^G(\varphi)\big)(x) = \sum_{i=1}^{r} sg_i\varphi\big(g_i^{-1}x\big) = \sum_{i=1}^{r} g_{\sigma(i)}h_i\varphi\big(g_i^{-1}x\big) &= \sum_{i=1}^{r} g_{\sigma(i)}\varphi\big(h_ig_i^{-1}x\big) \\ &= \sum_{i=1}^{r} g_{\sigma(i)}\varphi\big(g_{\sigma(i)}^{-1}sx\big) \\ &= \sum_{i=1}^{r} g_{\sigma(i)}\varphi g_{\sigma(i)}^{-1}(sx) \\ &= \big(\mathrm{tr}_H^G(\varphi)\big)(sx), \end{aligned}$$

as required. ■

Assuming $(P_\bullet, d_\bullet)$ is a projective resolution of the trivial $\mathbb{Z}G$-module $\mathbb{Z}$, then for each $n \geqslant 1$, we may consider the diagram

$$\begin{tikzcd} \mathrm{Hom}_{\mathbb{Z}H}(P_{n-1}, M) \arrow[r, "\mathrm{tr}_H^G"] \arrow[d, "d_n^*"'] & \mathrm{Hom}_{\mathbb{Z}G}(P_{n-1}, M) \arrow[d, "d_n^*"] \\ \mathrm{Hom}_{\mathbb{Z}H}(P_n, M) \arrow[r, "\mathrm{tr}_H^G"'] & \mathrm{Hom}_{\mathbb{Z}G}(P_n, M), \end{tikzcd}$$

where for $\varphi \in \mathrm{Hom}_{\mathbb{Z}H}(P_{n-1}, M)$ we compute

$$(d_n^* \circ \mathrm{tr}_H^G)(\varphi) = \sum_{i=1}^{r} d_n^*\big(g_i\varphi g_i^{-1}\big) = \sum_{i=1}^{r} \big(g_i\varphi g_i^{-1}\big) \circ d_n \overset{\mathbb{Z}G\text{-lin}}{=} \sum_{i=1}^{r} g_i(\varphi \circ d_n)g_i^{-1} = \mathrm{tr}_H^G\left(d_n^*(\varphi)\right)$$

since d_n is $\mathbb{Z}G$-linear. Hence, the diagram commutes and it follows that

$$\mathrm{tr}_H^G := (\mathrm{tr}_H^G)_\bullet : \mathrm{Hom}_{\mathbb{Z}H}(P_\bullet, M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(P_\bullet, M)$$

is a cochain map, and therefore by functoriallity, for each $n \geqslant 0$, it induces a homomorphism in cohomology

$$\mathrm{tr}_H^G : H^n(H, M) \longrightarrow H^n(G, M).$$

Definition 27.2 (*Transfer*)

Let $n \in \mathbb{Z}_{\geqslant 0}$. The map $\mathrm{tr}_H^G : H^n(H, M) \longrightarrow H^n(G, M)$ is called **transfer** from H to G (or **relative trace map**, or **corestriction**).

Proposition 27.3

Suppose H has finite index in G. Then, for every $n \geqslant 0$ the composition

$$\mathrm{tr}_H^G \circ \mathrm{res}_H^G : H^n(G, M) \longrightarrow H^n(G, M)$$

is multiplication by $|G : H|$.

Proof: Set say $r := |G : H| < \infty$ and let $\{g_i\}_{1 \leqslant i \leqslant r}$ be a left transversal for H in G. Let $P_\bullet$ be a projective $\mathbb{Z}G$-resolution of $\mathbb{Z}$. For $m \in \mathbb{Z}_{\geqslant 0}$, the composition

$$\mathrm{Hom}_{\mathbb{Z}G}(P_m, M) \xrightarrow{\mathrm{inc}} \mathrm{Hom}_{\mathbb{Z}H}(P_m, M) \xrightarrow{\mathrm{tr}_H^G} \mathrm{Hom}_{\mathbb{Z}G}(P_m, M)$$

maps $\varphi \in \mathrm{Hom}_{\mathbb{Z}G}(P_m, M)$ to

$$\mathrm{tr}_H^G(\varphi) = \sum_{i=1}^{r} g_i \varphi g_i^{-1} \overset{\mathbb{Z}G\text{-lin.}}{=} \sum_{i=1}^{r} g_i g_i^{-1} \varphi = \sum_{i=1}^{r} \varphi = |G : H| \varphi .$$

These are maps of cochain complexes and induce res_H^G and tr_H^G, functorially, in cohomology, Thus, the claim follows from the fact that left multiplication by r induces left multiplication by r in cohomology. ■

28 Induction and Coinduction in Cohomology

Definition 28.1 (*Induction*)

If M is a $\mathbb{Z}H$-module, then we define $\mathrm{Ind}_H^G(M) := \mathbb{Z}G \otimes_{\mathbb{Z}H} M$, the **induction** of M from H to G.

Remark 28.2

The induced module $\mathrm{Ind}_H^G(M)$ is endowed with the structure of a left $\mathbb{Z}G$-module via the left $\mathbb{Z}G$-module structure on $\mathbb{Z}G$. This is an *extension of scalars*, as studied in Exercise 14. Hence we have a universal property for the induction of modules from G to H as given by Exercise 14(c).

Proposition 28.3 (*Universal property of the induction*)

Let M be a $\mathbb{Z}H$-module and let $\iota : M \longrightarrow \mathrm{Ind}_H^G(M), m \mapsto 1 \otimes m$ be the canonical morphism. Then for every $\mathbb{Z}G$-module N and for every $\mathbb{Z}H$-linear map $\varphi : M \longrightarrow \mathrm{Res}_H^G(N)$, there exists a unique $\mathbb{Z}G$-linear map $\tilde{\varphi} : \mathrm{Ind}_H^G(M) \longrightarrow N$ such that the following diagram commutes:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\iota"'] & N \\ \mathrm{Ind}_H^G(M) \arrow[ur, dashed, "\circlearrowleft", "\exists!\,\tilde{\varphi}"'] & \end{tikzcd}$$

In other words, there is an isomorphism of abelian groups

$$\mathrm{Hom}_{\mathbb{Z}H}\left(M, \mathrm{Res}_H^G(N)\right) \cong \mathrm{Hom}_{\mathbb{Z}G}\left(\mathrm{Ind}_H^G(M), N\right).$$

Remark 28.4

In fact, one can prove that the functor Ind_H^G is left adjoint to the functor Res_H^G. (Out of the scope of the lecture.)

Definition 28.5 (*Coinduction*)

If M is a $\mathbb{Z}H$-module, then we define $\mathrm{Coind}_H^G(M) := \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M)$, the **coinduction** of M from H to G.

Remark 28.6

The module $\mathrm{Coind}_H^G(M)$ is endowed with the structure of a left $\mathbb{Z}G$-module, using the right $\mathbb{Z}G$-module structure on $\mathbb{Z}G$. Explicitly, for $g \in G$, $\varphi \in \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M)$ and $x \in \mathbb{Z}G$, we have

$$(g \cdot \varphi)(x) = \varphi(xg)\,.$$

Proposition 28.7 (*Universal property of the coinduction*)

Let M be a $\mathbb{Z}H$-module. Let $p : \mathrm{Coind}_H^G(M) \longrightarrow M, \varphi \mapsto \varphi(1)$ be the canonical evaluation map. Then for every $\mathbb{Z}G$-module N and every $\mathbb{Z}H$-linear map $\psi : N \longrightarrow M$, there exists a unique $\mathbb{Z}G$-linear map $\tilde{\psi} : N \longrightarrow \mathrm{Coind}_H^G(M)$ such that the following diagram commutes:

$$\begin{tikzcd}
& \mathrm{Coind}_H^G(M) \arrow[d, "p"] \\
N \arrow[ur, dashed, "\exists!\,\tilde{\psi}", "\circlearrowleft"'] \arrow[r, "\psi"'] & M
\end{tikzcd}$$

Proof: Exercise. ■

Theorem 28.8 (*The Eckmann-Shapiro Lemma*)

Let M be a $\mathbb{Z}H$-module. Then for each $n \in \mathbb{Z}_{\geqslant 0}$ there are group isomorphisms

$$H_n(G, \mathrm{Ind}_H^G(M)) \cong H_n(H, M) \qquad \text{and} \qquad H^n(G, \mathrm{Coind}_H^G(M)) \cong H^n(H, M)\,.$$

Proof: Fix $n \in \mathbb{Z}_{\geqslant 0}$ and let $P_\bullet$ be a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module (hence also as a $\mathbb{Z}H$-module). Then

$$P_n \otimes_{\mathbb{Z}H} M \cong P_n \otimes_{\mathbb{Z}G} \mathbb{Z}G \otimes_{\mathbb{Z}H} M \cong P_n \otimes_{\mathbb{Z}G} \mathrm{Ind}_H^G(M)\,.$$

Now, the left-hand side gives the homology group $H_n(H, M)$, while the right-hand side gives the homology group $H_n(G, \mathrm{Ind}_H^G(M))$, hence $H_n(G, \mathrm{Ind}_H^G(M)) \cong H_n(H, M)$.
Similarly

$$\mathrm{Hom}_{\mathbb{Z}H}(P_n, M) \cong \mathrm{Hom}_{\mathbb{Z}G}(P_n, \mathrm{Coind}_H^G(M))\,,$$

where the left-hand side gives the cohomology group $H^n(H, M)$ while the right-hand side gives the cohomology group $H^n(G, \mathrm{Coind}_H^G(M))$. ■

Lemma 28.9

If M is a $\mathbb{Z}H$-module and H has finite index in G, then $\mathrm{Coind}_H^G(M) \cong \mathrm{Ind}_H^G(M)$ as $\mathbb{Z}G$-modules.

Proof: Define

$$\begin{aligned}\alpha : \mathbb{Z}G \otimes_{\mathbb{Z}H} M &\longrightarrow \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M)\\ g \otimes m &\longmapsto \varphi_{g,m} : \mathbb{Z}G \longrightarrow M\end{aligned}$$

where $g \in G$, m$\in M$ and for $s \in G$,

$$\varphi_{g,m}(s) = \begin{cases} sgm & \text{if } sg \in H \\ 0 & \text{if } sg \notin H. \end{cases}$$

It is easily check that α is $\mathbb{Z}G$-linear. Then, defining

$$\begin{aligned}\beta : \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M) &\longrightarrow \mathbb{Z}G \otimes_{\mathbb{Z}H} M\\ \psi &\longmapsto \sum_{i=1}^{r} g_i \otimes \psi(g_i^{-1}),\end{aligned}$$

where $\{g_1, \ldots, g_r\}$ is a left transversal of H in G, one easily checks that β is $\mathbb{Z}G$-linear, $\alpha \circ \beta = \mathrm{Id}$ and $\beta \circ \alpha = \mathrm{Id}$. The claim follows. ■

Corollary 28.10

If M is a $\mathbb{Z}H$-module and H has finite index in G, then $H^n(G, \mathrm{Ind}_H^G(M)) \cong H^n(H, M)$ for each $n \in \mathbb{Z}_{\geqslant 0}$.

Proof: By the previous lemma $\mathrm{Coind}_H^G(M) \cong \mathrm{Ind}_H^G(M)$. Hence the claim follows from the Eckmann-Shapiro Lemma. ■

29 Exercises for Chapter 7

Exercise 46

Let $H \leqslant G$ a subgroup and let M be a $\mathbb{Z}G$-module.

(a) Prove that there is a surjective $\mathbb{Z}G$-linear map

$$\begin{array}{rccl} \pi : & \mathrm{Ind}_H^G \mathrm{Res}_H^G(M) & \longrightarrow & M \\ & g \otimes m & \longmapsto & gm \quad \forall\, g \in G \end{array}$$

and an injective $\mathbb{Z}G$-linear map

$$\begin{array}{rccl} \varepsilon : & M & \longrightarrow & \mathrm{Coind}_H^G \mathrm{Res}_H^G(M) \\ & m & \longmapsto & \varepsilon(m) \end{array}$$

where $\varepsilon(m)(g) := gm$ for every $g \in G$.

(b) Prove that the composite map

$$H^n(G, M) \xrightarrow{\varepsilon_*} H^n(G, \mathrm{Coind}_H^G \mathrm{Res}_H^G(M)) \cong H^n(H, \mathrm{Res}_H^G(M))$$

is equal to res_H^G.

(d) Suppose that H has finite index in G. Prove that the composite map

$$H^n(H, \operatorname{Res}_H^G(M)) \cong H^n(G, \operatorname{Coind}_H^G \operatorname{Res}_H^G(M)) \cong H^n(G, \operatorname{Ind}_H^G \operatorname{Res}_H^G(M)) \xrightarrow{\pi_*} H^n(G, M)$$

is equal to tr_H^G.

(c) Prove that $\pi \circ \varepsilon$ is multiplication by $|G : H|$ in M. Deduce that $\operatorname{tr}_H^G \circ \operatorname{res}_H^G$ is multiplication by $|G : H|$ in $H^n(G, M)$.

Chapter 8. Finite Groups

The aim of this chapter is to prove several central results of the theory of finite groups: Theorems of Schur and Zassenhaus and Burnside's transfer theorem (aslo known as Burnside's normal p-complement theorem). We will see that these theorems can be stated in terms of elementary group theory, but their proofs rely on cohomological arguments.

Notation: Throughout this chapter, unless otherwise stated, G denotes a **finite** group in multiplicative notation and A be a $\mathbb{Z}G$-module.

References:

[Bro94] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994.

[Rot09] J. J. Rotman, *An introduction to the theory of groups. Fourth ed.*, Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

30 Cohomology of Finite Groups

To begin with, we collect in this section a few general results about the cohomology of finite groups.

Lemma 30.1

If G is a finite group, then $|G| \cdot H^n(G, A) = 0$ for every $n \geqslant 1$.

Proof: Let $n \in \mathbb{Z}_{\geqslant 1}$ and let $\mathbb{1}$ denote the trivial group. Because $\mathbb{1}$ is a cyclic group of order one Theorem 20.3 yields $H^n(\mathbb{1}, A) \cong 0$. Now, by Proposition 27.3, the composition of the restriction with the transfer

$$H^n(G, A) \xrightarrow{\mathrm{res}^G_{\mathbb{1}}} \underbrace{H^n(\mathbb{1}, A)}_{\cong 0} \xrightarrow{\mathrm{tr}^G_{\mathbb{1}}} H^n(G, A)$$

is multiplication by $|G : \mathbb{1}| = |G|$ and factors through 0 if $n \geqslant 1$ by the above. Therefore, multiplication by $|G|$ is zero in $H^n(G, A)$. ■

Proposition 30.2

If G is a finite group and A is a finitely generated $\mathbb{Z}G$-module then $H^0(G, A)$ is a finitely generated abelian group and $H^n(G, A)$ is a finite abelian group of exponent dividing $|G|$ for every $n \geqslant 1$.

Recall that the structure theorem for finitely generated modules over a PID states that a finitely generated abelian group B decomposes as $B = B^{tors} \oplus B^{free}$ where B^{tors} – the torsion part of B – is a finite direct sum of finite cyclic groups and B^{free} – the free part of B – is isomorphic to $\mathbb{Z}^m$ for some positive integer m.

Proof: Fix $n \in \mathbb{Z}_{\geqslant 0}$.

Claim 1: $H^n(G, A)$ is a finitely generated abelian group.

Indeed: Using the fact that $\mathbb{Z}G$ is a noetherian ring as G is finite, we may construct a projective $\mathbb{Z}G$-resolution $P_\bullet$ of $\mathbb{Z}$ in which all the modules are finitely generated abelian groups. Now, applying the functor $\mathrm{Hom}_{\mathbb{Z}G}(-, A)$ to $P_\bullet$ we obtain a cochain complex of finitely generated abelian groups since for each $m \geqslant 0$, $\mathrm{Hom}_{\mathbb{Z}G}(P_m, A) = \mathrm{Hom}_{\mathbb{Z}}(P_m, A)^G \subseteq \mathrm{Hom}_{\mathbb{Z}}(P_m, A)$, which is a finitely generated abelian group if both P_m and A are. The cohomology groups of this cochain complex are again finitely generated.

Thus the claim about $H^0(G, A)$ is proved and so is the abelianity of $H^n(G, A)$ for $n \geqslant 1$.

Claim 2: The free part $H^n(G, A)$ is a trivial if $n \geqslant 1$.

Indeed: Since $H^n(G, A)$ is a finitely generated abelian group by Claim 1 and $|G| \cdot H^n(G, A) = 0$ by Lemma 30.1, its free part must be trivial.

It follows that for $n \geqslant 1$, $H^n(G, A)$ is a torsion group, so it is finite and the claim about the exponent is straightforward from the fact that $H^n(G, A)$ is annihilated by $|G|$. ■

31 The Theorems of Schur and Zassenhaus

In this section we prove two main results of the theory of finite groups, which are often considered as one Theorem and called the *Schur-Zassenhaus Theorem.* Beacause of the methods we have developed, we differentiate between the abelian and the non-abelian case.

Theorem 31.1 (*Schur, 1904*)

Let G be a finite group and let $A_* := (A, \cdot, *)$ be a $\mathbb{Z}G$-module such that there exists $m \in \mathbb{Z}_{\geqslant 1}$ with $a^m = 1$ for all $a \in A$. If $\big(|G|, m\big) = 1$, then the following assertions hold.

(a) Every group extension $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ inducing the given G-action $*$ on A splits.

(b) Any two complements of A in E are E-conjugate.

Proof: First, we prove that the $H^n(G, A_*)$ is trivial for all $n \geqslant 1$. For convenience, write A additively in this proof. (I.e. $(A, +)$ instead $(A, \cdot)$, so that we can differentiate between the group law in A and the action of $\mathbb{Z}$ on all abelian groups involved.) Thus by assumption we have $m \cdot A = 0$. This implies that $m \cdot C^n(G, A_*) = 0$, and thus $m \cdot H^n(G, A_*) = 0$ for every $n \geqslant 1$. Now, by the Bézout identity there exists $u, v \in \mathbb{Z}$ such that

$$u \cdot |G| + v \cdot m = 1\,,$$

and hence we have

$$H^n(G, A_*) = 1 \cdot H^n(G, A_*) = u \cdot \underbrace{|G| \cdot H^n(G, A_*))}_{=0} + v \cdot \underbrace{m \cdot H^n(G, A_*)}_{=0} = 0$$

for every $n \geqslant 1$ as $|G| \cdot H^n(G, A_*) = 0$ by Lemma 30.1. Now, because $H^2(G, A_*)$ vanishes, any group extension $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ inducing the given G-action $*$ on A splits by Theorem 24.3. Because $H^1(G, A_*)$ vanishes, all complements of A in E are E-conjugate by Theorem 23.3(b). ■

Theorem 31.2 (*Zassenhaus, 1937*)

Let $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ be an extension of finite groups (where A is not necessarily abelian). If $\big(|A|, |G|\big) = 1$, then the extension splits.

Proof: W.l.o.g. we may assume that $|G| > 1$. Then, we proceed by induction on the order of A.

- If $|A| = 1$ or $|A|$ is a prime number, then A is cyclic, hence abelian. Moreover, $a^{|A|} = 1$ for all $a \in A$. Thus Schur's Theorem applies and yields the result.
- Suppose now that $|A| \in \mathbb{Z}_{\geqslant 2} \backslash \mathbb{P}$. Let $q \in \mathbb{P}$ be a prime number dividing $|A|$, let P be a Sylow q-subgroup of A, and set $N := N_E(P)$ for the normaliser of P in E.

  Claim 1: $E = AN$.
  Indeed, if $e \in E$, then P and ePe^{-1} are Sylow q-subgroups of A, hence A-conjugate, and so there exists $a \in A$ such that $a^{-1}(ePe^{-1})a = P$. Thus $a^{-1}e \in N_E(P) = N$, and therefore $e = a\big(a^{-1}e\big) \in AN$.

  Claim 2: A has a complement in E.
  We split the proof of this claim in two cases:

  Case 1: $N \neq E$.
  In this case, restricting p to N yields the group extension

$$1 \longrightarrow A \cap N \xrightarrow{i|_{A\cap N}} N \xrightarrow{p|_N} G \longrightarrow 1$$

  where $A \cap N \subsetneq A$ because $G \cong E/A = AN/N \cong N/(A \cap N)$. Thus, by the induction hypothesis, this extension splits, and, by Proposition 22.7, there exists a complement H of $A \cap N$ in N. Since $|H| = |G|$ and $\big(|A|, |G|\big) = 1$, we have $H \cap A = \{1\}$, and therefore H is a complement of A in E.

  Case 2: $N = E$.
  Let $Z := Z(P)$ be the centre of P, which is a non-trivial subgroup of P because P is a q-group. Since Z is characteristic in P (i.e. invariant under all automorphisms of P), and since P is normal in N, we deduce that Z is normal in E. Thus, by the universal property of the quotient, p induces a group homomorphism $\overline{p} : E/Z \longrightarrow G, eZ \longrightarrow p(e)$, whose kernel is A/Z. In other words, there is a group extension of the form

$$1 \longrightarrow A/Z \longrightarrow E/Z \longrightarrow G \longrightarrow 1.$$

  Now $|Z| \neq 1$ implies that $|A/Z| < |A|$, hence, by the induction hypothesis again, this extension splits. So let F be a complement of A/Z in E/Z. By the Correspondence Theorem, there exists a subgroup $\widetilde{F} \leqslant E$ containing Z such that $F = \widetilde{F}/Z$. In other words, there is a group extension

$$1 \longrightarrow Z \longrightarrow \widetilde{F} \longrightarrow F \longrightarrow 1\,.$$

  Since $F \cong G$ and $Z \leqslant P \leqslant A$, we have $\big(|Z|, |F|\big) = 1$ and therefore this extension splits by Schur's Theorem. Thus, there is a complement H of Z in $\widetilde{F}$. Again $|H| = |F| = |G|$ and $\big(|A|, |G|\big) = 1$ imply that $H \cap A = 1$, so that H is also a complement of A in E. The second claim is proved.

  Finally, we conclude that the extension splits using Proposition 22.7 . ■

Remark 31.3

(a) Notice that both Schur's and Zassenhaus' Theorems can be stated in terms not involving cohomology, but their proofs rely on cohomological methods.

(b) A variation on the proof of the later theorem yields the following result due to Gaschütz (1952):

Let q be a prime number. Let K be a normal abelian q-subgroup of a finite group G, and let P be a Sylow q-subgroup of G. Then K has a complement in G if and only if K has a complement in P.

32 Burnside's Transfer Theorem

Throughout this section, we let H be a subgroup of G (assumed to be finite!) of index $|G:H| =: r$ and A be a *trivial* $\mathbb{Z}G$-module. Our first aim is to understand the action of the transfer homomorphism on $H^1(G,A)$. So first recall that $H^1(G,A) = Z^1(G,A) = \mathrm{Hom}_{\mathbf{Grp}}(G,A)$ by Example 11, and hence we see the transfer as a homomorphism

$$\mathrm{tr}_H^G : \mathrm{Hom}_{\mathbf{Grp}}(H,A) \longrightarrow \mathrm{Hom}_{\mathbf{Grp}}(G,A)\,.$$

Lemma 32.1

Let $n \in \mathbb{Z}_{\geqslant 0}$ and let $\mathbb{Z}G^{n+1}$ be the n-th term of the bar resolution of $\mathbb{Z}$ seen as the trivial $\mathbb{Z}G$-module. View it as a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}H$-module by restriction. Fix a right transversal $S = \{s_1, \dots, s_r\}$ of H in G. Then the comparison maps between this resolution and the bar resolution of $\mathbb{Z}$ as a $\mathbb{Z}H$-module are given by the canonical inclusions

$$i_n : \mathbb{Z}H^{n+1} \longrightarrow \mathbb{Z}G^{n+1}$$

and by the maps

$$\begin{array}{rccc} \varphi_n : & \mathbb{Z}G^{n+1} & \longrightarrow & \mathbb{Z}H^{n+1} \\ & (g_0, \dots, g_n) & \mapsto & (h_0, \dots, h_n)\,, \end{array}$$

where, for every $0 \leqslant i \leqslant n$, $g_i = h_i s_i$ for some $h_i \in H$ and some $s_i \in S$.

Proof: Thus the Comparison Theorem yields the result, because using the definition of the differential maps of the bar resolution, we see that for each $n \geqslant 1$ there are commutative diagrams

$$\begin{tikzcd} \mathbb{Z}H^{n+1} \arrow[r, "i_n"] \arrow[d, "d_n"] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{Z}G^{n+1} \arrow[d, "d_n"] \\ \mathbb{Z}H^n \arrow[r, "i_{n-1}"'] & \mathbb{Z}G^n \end{tikzcd} \qquad \begin{tikzcd} \mathbb{Z}H \arrow[r, "i_0"] \arrow[d, "\varepsilon"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{Z}G\,, \arrow[d, "\varepsilon"] \\ \mathbb{Z} \arrow[r, "\mathrm{Id}"'] & \mathbb{Z} \end{tikzcd}$$

and

$$\begin{tikzcd} \mathbb{Z}G^{n+1} \arrow[r, "\varphi_n"] \arrow[d, "d_n"] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{Z}H^{n+1} \arrow[d, "d_n"] \\ \mathbb{Z}G^n \arrow[r, "\varphi_{n-1}"'] & \mathbb{Z}H^n \end{tikzcd} \qquad \begin{tikzcd} \mathbb{Z}G \arrow[r, "\varphi_0"] \arrow[d, "\varepsilon"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{Z}H\,, \arrow[d, "\varepsilon"] \\ \mathbb{Z} \arrow[r, "\mathrm{Id}"'] & \mathbb{Z}\,. \end{tikzcd}$$

■

Proposition 32.2

Fix a right transversal $S = \{s_1, \ldots, s_r\}$ of H in G. Then the transfer for H^1 is described as follows:

$$\begin{aligned} \mathrm{tr}_H^G : \mathrm{Hom}_{\mathbf{Grp}}(H, A) &\longrightarrow \mathrm{Hom}_{\mathbf{Grp}}(G, A) \\ f &\longmapsto \left(\mathrm{tr}_H^G(f) : g \longmapsto \sum_{i=1}^{r} f(h_i) \right), \end{aligned}$$

where $s_i g = h_i s_{\sigma(i)}$ with $h_i \in H$ for every $1 \leqslant i \leqslant r$ and $\sigma \in S_r$.

Proof: On the one hand

$$\mathrm{Hom}_{\mathbf{Grp}}(H, A) = H^1(H, A) \cong H^1\big(\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}H^2, A)\big),$$

via the bar resolution. On the other hand,

$$\mathrm{Hom}_{\mathbf{Grp}}(H, A) = H^1(H, A) \cong H^1\big(\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G^2, A)\big),$$

via the bar resolution for G restricted to H. Now, transfer is defined using the second resolution, therefore, we need to compare these two resolutions. But

$$H^1(H, A) = Z^1(H, A),$$

because $B^1(H, A) = 0$ since H acts trivially on A, and

$$Z^1(H, A) \subseteq C^1(H, A) \cong \mathrm{Hom}_{\mathbb{Z}H}\left(\mathbb{Z}H^2, A\right).$$

If for a given $f \in \mathrm{Hom}_{\mathbf{Grp}}(H, A)$, $\tilde{f}$ denotes the image of f in $\mathrm{Hom}_{\mathbb{Z}H}\left(\mathbb{Z}H^2, A\right)$, then for $h \in H$ set

$$\begin{aligned} \tilde{f} : \mathbb{Z}H^2 &\longrightarrow A \\ (1, h) = [h] &\longmapsto f(h) \end{aligned}$$

and thus for each $k \in H$,

$$\tilde{f}\big((k, kh)\big) = \tilde{f}\big(k \cdot (1, h)\big) = k \cdot f(h) = f(h),$$

because H acts trivially on A, and we extend this map by $\mathbb{Z}$-linearity to the whole of $\mathbb{Z}H^2$. Using the comparison map $\varphi_1 : \mathbb{Z}G^2 \longrightarrow \mathbb{Z}H^2$ of the previous lemma yields $\tilde{f} \circ \varphi_1 : \mathbb{Z}G^2 \longrightarrow A$, which is $\mathbb{Z}H$-linear. Now, computing the transfer using its definition yields for every $x \in \mathbb{Z}G^2$:

$$\mathrm{tr}_H^G\left(\tilde{f} \circ \varphi_1\right)(x) = \sum_{i=1}^{r} s_i^{-1}\big(\tilde{f} \circ \varphi_1\big)(s_i x) = \sum_{i=1}^{r} \big(\tilde{f} \circ \varphi_1\big)(s_i x)$$

because $\left\{s_1^{-1}, \ldots, s_r^{-1}\right\}$ is a left transversal of H in G and A is trivial. We want to view this as a 1-cocycle for G, that is evaluate this on an element $[g] = (1, g) \in G^2 \subset \mathbb{Z}G^2$:

$$\mathrm{tr}_H^G(f)(g) = \mathrm{tr}_H^G\left(\tilde{f} \circ \varphi_1\right)(1, g) = \sum_{i=1}^{r} \big(\tilde{f} \circ \varphi_1\big)(s_i, s_i g) = \sum_{i=1}^{r} \tilde{f}\big(1, h_i\big)$$

because $s_i = 1 \cdot s_i$ and $s_i g = h_i s_{\sigma(i)}$. So we obtain

$$\mathrm{tr}_H^G(f)(g) = \sum_{i=1}^{r} \tilde{f}(1, h_i) = \sum_{i=1}^{r} f(h_i),$$

as required. ■

Lemma 32.3 (*Choice of transversal for a fixed $g \in G$*)

Fix $g \in G$.

(a) There exists a right transversal of H in G of the form

$$S = \{t_1, t_1 g, \dots, t_1 g^{m_1 - 1}, t_2, t_2 g, \dots, t_2 g^{m_2 - 1}, \dots, t_s, t_s g, \dots, t_s g^{m_s - 1}\}$$

with $m_1 + \ldots + m_s = |G : H| = r$ and $t_i g^{m_i} t_i^{-1} \in H$ for all $1 \leqslant i \leqslant s$.

(b) If $f \in \operatorname{Hom}_{\mathbf{Grp}}(H, A)$ and $g \in G$, then $\operatorname{tr}_H^G(f)(g) = \sum_{i=1}^{s} f\big(t_i g^{m_i} t_i^{-1}\big)$.

Proof:

(a) The element g acts on the right on right cosets Hs, via $Hs \longmapsto Hsg$. Decompose the set of right cosets into g-orbits. Let r be the number of g-orbits and let $Ht_1, \dots, Ht_r$ be representatives of the g-orbits. We get all the right cosets of H by applying powers of g to each Ht_i and we suppose that $Ht_i g^{m_i - 1} g = Ht_i$ (that is, m_i is the cardinality of the orbit). With this choice, we obtain a right transversal with the required properties.

(b) Proposition 32.2 together with (a) yield for $1 \leqslant i \leqslant s$:

$$t_i g, t_i g^2, \dots, t_i g^{m_i - 1}$$

belong to the right transversal S, so that $\big(t_i g^k\big) \cdot g = 1 \cdot \big(t_i g^{k+1}\big) \in H \cdot S$ for $0 \leqslant k \leqslant m_i - 2$ and $t_i g^{m_i - 1} g = \big(t_i g^{m_i} t_i^{-1}\big) t_i \in H \cdot S$. Therefore

$$\operatorname{tr}_H^G(f)(g) = \sum_{i=1}^{s} f\big(t_i g^{m_i} t_i^{-1}\big),$$

because all the other elements of H appearing are 1 and $f(1) = 0$. ■

Theorem 32.4 (*Burnside's transfer theorem (or Burnside's normal p-complement theorem), 1911*)

Let G be a finite group, let p be a prime number such that $p \mid |G|$ and let P be a Sylow p-subgroup of G. If P is abelian and $C_G(P) = N_G(P)$, then there exists a normal complement N to P in G, i.e. $G = N \rtimes P$.

Proof:

Claim: If there exist $g \in G$ and $u \in P$ such that $u, gug^{-1} \in P$, then $gug^{-1} = u$.

Indeed: using the assumptions, we have $u \in g^{-1}Pg$, which is abelian, and therefore both P and $g^{-1}Pg$ are Sylow p-subgroups of $C_G(u)$. Thus P and $g^{-1}Pg$ are conjugate in $C_G(u)$, so that there exists $c \in C_G(u)$ such that $cPc^{-1} = g^{-1}Pg$, that is $gcP(gc)^{-1} = P$ and hence $gc \in N_G(P) = C_G(P)$. Finally, $gug^{-1} = (gc)u(gc)^{-1} = u$ because $u \in P$, as required.

Now consider the identity map $\operatorname{Id}_P \in \operatorname{Hom}_{\mathbf{Grp}}(P, P)$ and $\operatorname{tr}_P^G(\operatorname{Id}_P) \in \operatorname{Hom}_{\mathbf{Grp}}(G, P)$. The previous lemma yields for a fixed $u \in P$,

$$\operatorname{tr}_P^G(\operatorname{Id}_P)(u) = \prod_{i=1}^{s} \operatorname{Id}_P\big(\underbrace{t_i u^{m_i} t_i^{-1}}_{\in P}\big)\,.$$

Now using the Claim yields $t_i u^{m_i} t_i^{-1} = u^{m_i}$ for each $1 \leqslant i \leqslant s$, hence

$$\operatorname{tr}_P^G(\operatorname{Id}_P)(u) = \prod_{i=1}^{s} u^{m_i} = u^{|G:P|}.$$

In particular, this proves that $\mathrm{tr}_P^G(\mathrm{Id}_P) : G \twoheadrightarrow P$ is a surjective group homomorphism, because for each $v \in P$, there exists $u \in P$ such that $u^{|G:P|} = v$ by the Bézout identity. (Indeed, Bézout implies that there exist $a, b \in \mathbb{Z}$ such that $a|P| + b|G : P| = 1$, hence $v = v^1 = (v^b)^{|G:P|}$ and we choose $u = v^b$.)

Finally, set $N := \ker\left(\mathrm{tr}_P^G(\mathrm{Id}_P)\right)$, so that we have a group extension

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] & G \arrow[r, "\mathrm{tr}_P^G(\mathrm{Id}_P)"] & P \arrow[r] & 1 \end{tikzcd}$$

with a section given by $\frac{1}{|G:P|} \cdot \iota$, where $\iota : P \longrightarrow G$ is the canonical inclusion. It follows that N is a normal complement of P in G. ■

Corollary 32.1

A finite non-abelian simple group G cannot have a non-trivial cyclic Sylow 2-subgroup.

Proof: Exercise 50 proves that a finite non-abelian group G with a non-trivial cyclic Sylow 2-subgroup possesses a normal 2-complement – as a consequence of Burnside's transfer theorem. It follows that such a group cannot be simple, proving the claim. ■

33 Exercises for Chapter 8

Exercise 47

Let G be a finite group. If A is a $\mathbb{Z}G$-module which is induced from the trivial subgroup, then $H^n(G, A) = 0$ for every $n \geqslant 1$. Deduce that $H^n(G, A) = 0$ for every $n \geqslant 1$ if A is a projective $\mathbb{Z}G$-module.

Exercise 48

Let p be a prime number, let G be a finite group of order divisible by p, and let P be a Sylow p-subgroup of G. If A is an $\mathbb{F}_p G$-module, then the restriction map

$$\mathrm{res}_P^G : H^n(G, A) \longrightarrow H^n(P, \mathrm{Res}_P^G(A))$$

is injective for every $n \geqslant 0$.

Exercise 49

Let p be a prime number. Let G be a finite group of oder divisible by p and let P be a Sylow p-subgroup of G.

(a) Prove that $C_G(P) = Z(P) \times H$, where H is a subgroup of G of order coprime to p.

(b) Prove that $PC_G(P) = P \times H$.

(c) Prove that $N_G(P) = P \rtimes K$, where K is a subgroup of G of order coprime to p, and $H \trianglelefteq K$.

Exercise 50

Let G be a finite group of even order and assume that a Sylow 2-subgroup P of G is cyclic.

(a) Prove that $\mathrm{Aut}(P)$ is a 2-group.

(b) Prove that P has a normal complement in G.

Chapter 9. The Schur Multiplier and Universal Central Extensions

The Schur multiplier is a very important tool of finite group theory and representation theory of finite groups. For an arbitrary group G it is defined as the integral homology group $M(G) := H_2(G, \mathbb{Z})$, which makes it a very important tool of algebraic topology as well. However, when G is a finite group, we have several interpretations of $M(G)$ through cohomology groups. Furthermore, we will see that it has very natural connections with central extensions and projective representations.

Throughout this chapter, unless otherwise stated, G denotes a **finite** group in multiplicative notation and K denotes a field of arbitrary characteristic. As standard, we let $(\mathbb{C}, +, \cdot)$ denote the field of complex numbers, $(\mathbb{C}^\times, \cdot)$ be its multiplicative group of units and we let $\mathbb{S}^1 := \{z \in \mathbb{C}^\times \mid |z| = 1\} \leqslant \mathbb{C}^\times$ for the complex 1-sphere. Moreover, without mention of an explicit G-action, abelian groups are seen as trivial $\mathbb{Z}G$-module.

References:

[CR90] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1990.

[Rot09] J. J. Rotman, *An introduction to the theory of groups. Fourth ed.*, Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[LT17] C. Lassueur and J. Thévenaz, *Universal p'-central extensions*, Expo. Math. **35** (2017), no. 3, 237–251.

34 Definition and Equivalent Characterisations

Definition 34.1 (*Schur multiplier*)

The **Schur multiplier** (or **multiplicator**) of a group G (not necessarily finite) is the abelian group $M(G) := H_2(G, \mathbb{Z})$.

For finite groups, we can further characterise the Schur multiplier in terms of cohomology in different ways as explained below.

We start with a crucial result coming from algebraic topology, which we accept without proof.

Theorem 34.2 (*Integral duality theorem*)

If G is a finite group, then $H^{n+1}(G, \mathbb{Z}) \cong H_n(G, \mathbb{Z})$ whenever $n \geqslant 1$.

Remark 34.3 (*Uniquely divisible groups*)

Recall from group theory that:

- An abelian group $(A, +)$ is said to be **uniquely divisible by an integer** $u \in \mathbb{Z}_{\geqslant 1}$ if for all $a \in A$ there exists a unique $b \in A$ with $a = ub$, or equivalently iff the homomorphism of multiplication by u, i.e. $m_u : A \longrightarrow A, b \mapsto ub$ is an isomorphism. For example, if A is finite and $(|A|, u) = 1$ then A is uniquely divisible by u.
- Moreover, A is said to be **uniquely divisible** if it is uniquely divisible by every positive integer $u \in \mathbb{Z}_{\geqslant 1}$.
  Obviously, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R} \times \mathbb{R}$, ... are uniquely divisible, but $\mathbb{Q}/\mathbb{Z}$ is not uniquely divisible.

Lemma 34.4

Let G be a finite group.

(a) If $(M, +, \cdot)$ is a $\mathbb{Z}G$-module such that the underlying abelian group $(M, +)$ is uniquely divisible by $|G|$, then $H^n(G, M) \cong 0$ for every $n \geqslant 1$.

(b) $H^n(G, \mathbb{C}^\times) \cong H^{n+1}(G, \mathbb{Z}) \cong H^n(G, \mathbb{Q}/\mathbb{Z})$ for all $n \geqslant 1$.

Proof:

(a) Let $n \geqslant 1$ be fixed. By the assumption multiplication by $|G|$, $m_{|G|} : M \longrightarrow M, m \mapsto |G|m$, is an isomorphism, hence so is multiplication by $|G|$, $m_{|G|} : H^n(G, M) \longrightarrow H^n(G, M)$ by functoriality of cohomology. This map being the zero map by Lemma 30.1, it follows that $H^n(G, M) \cong 0$.

(b) Polar coordinates induce a group isomorphism

$$\mathbb{C}^\times \xrightarrow{\cong} \mathbb{R}^\times_{>0} \times \mathbb{S}^1,\ z \mapsto (|z|, e^{i\arg(z)})$$

and $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{S}^1, \cdot), t \mapsto e^{2\pi i t}$ is a surjective group homomorphism with $\ker(\exp) = \mathbb{Z}$, hence it induces a group isomorphism $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$. Therefore, there is a group extension

$$\begin{tikzcd}
\mathcal{E}:\ 1 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{R}^\times_{>0} \times \mathbb{R} \arrow[r, "\mathrm{Id} \times \exp"] & \underbrace{\mathbb{R}^\times_{>0} \times \mathbb{S}^1}_{\cong \mathbb{C}^\times} \arrow[r] & 1\ .
\end{tikzcd}$$

Because the natural logarithm $\ln : (\mathbb{R}^\times_{>0}, \cdot) \longrightarrow (\mathbb{R}, +)$ is a group isomorphism the term in the middle is isomorphic to $\mathbb{R} \times \mathbb{R}$, and hence is uniquely divisible. Thus, it follows from (a) that the long exact sequence in cohomology associated to the extension $\mathcal{E}$ (which we see as a s.e.s. of trivial $\mathbb{Z}G$-modules) has the form

$$\begin{tikzcd}
\cdots \arrow[r] & \underbrace{H^1(G, \mathbb{R}^\times_{>0} \times \mathbb{R})}_{\cong 0} \arrow[r] & H^1(G, \mathbb{C}^\times) \arrow[r] & H^2(G, \mathbb{Z}) \arrow[r] & \underbrace{H^2(G, \mathbb{R}^\times_{>0} \times \mathbb{R})}_{\cong 0} \arrow[r] & \cdots \\
\cdots \arrow[r] & \underbrace{H^n(G, \mathbb{R}^\times_{>0} \times \mathbb{R})}_{\cong 0} \arrow[r] & H^n(G, \mathbb{C}^\times) \arrow[r] & H^{n+1}(G, \mathbb{Z}) \arrow[r] & \underbrace{H^{n+1}(G, \mathbb{R}^\times_{>0} \times \mathbb{R})}_{\cong 0} \arrow[r] & \cdots
\end{tikzcd}$$

Hence, we conclude that $H^n(G, \mathbb{C}^\times) \cong H^{n+1}(G, \mathbb{Z})$ for each $n \geqslant 1$.

Exercise 51: use a similar argument to prove that $H^n(G, \mathbb{Q}/\mathbb{Z}) \cong H^{n+1}(G, \mathbb{Z})$ for all $n \geqslant 1$. ■

Proposition 34.5 (*Alternative descriptions of the Schur multiplier of a finite group*)

If G is a finite group, then $M(G) = H_2(G, \mathbb{Z}) \cong H^3(G, \mathbb{Z}) \cong H^2(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{C}^\times)$.

Proof: The isomorphism $H_2(G, \mathbb{Z}) \cong H^3(G, \mathbb{Z})$ is given by *the integral duality theorem*. The second and the third isomorphisms are given by Lemma 34.4(b). ■

Remark 34.6

In view of Proposition 34.5 and the fact that Schur worked with finite groups, the Schur multiplier of finite group is often defined to be $M(G) = H^2(G, \mathbb{C}^\times)$.

Finally we give a characterisation of $M(G)$ due to Schur, which is known under the name of *Hopf's Formula*, and which we also accept without proof.

Theorem 34.7 (*Hopf's Formula (Schur, 1907)*)

Let G be a finite group which we see as the quotient of a finitely generated free group free group F, i.e. $G \cong F/R$ with $R \trianglelefteq F$. Then, $M(G) \cong (R \cap [F, F])/[F, R]$.

Notice that, in particular, Hopf's formula enables us to recover information about G from a presentation.

Remark 34.8

Hopf proved in 1942 that an aspherical topological space X has the property that its homology groups are completely determined by its fundamental group $\pi_1(X)$. More precisely, he proved that $H_2(X) \cong (R \cap [F, F])/[F, R]$, where F is a group and $R \trianglelefteq F$ are such that $\pi_1(X) \cong F/R$. Schur had already proved this formula in the special case of finite groups, hence the terminology! In fact, comparison of Hopf's Formula with Schur's Theorem from 1907 lead Eilenberg and Mac Lane to the creation of the *Cohomology of Groups*.

Remark 34.9

In the ATLAS of Finite Groups the Schur multiplier is one of the first piece of information which is listed at the top of the page corresponding to a simple group. We will see in the next sections how it relates to central extensions of simple groups.

35 Numerical Properties

Lemma 35.1

If G is a finite group, then $M(G)$ is a finite abelian group such that $\exp(M(G)) \mid |G|$.
In particular, if p is a prime number and G is a finite p-group, then so is $M(G)$.

Proof: This is a special case of Proposition 30.2. ■

Remark 35.2

In fact it can be proved that $\exp(M(G))^2 \mid |G|$. This was already proved by Schur in 1904 in specific cases. A proof in the general case requires the notion of a *representation group* (or *covering group*) which we will introduce in the next section. Moreover, Jon Alperin and Kuo Tzee-Nan proved in 1967 that $\exp(M(G)) \cdot \exp(G) \mid |G|$.

Lemma 35.3

If G is a finite cyclic group then $M(G) \cong \{1\}$.

Proof: Exercise 52. ∎

Theorem 35.4

Let p be a prime number and let $P \in \mathrm{Syl}_p(G)$. Then $\mathrm{res}^G_P|_{M(G)_p} : M(G)_p \longrightarrow M(P)$ is an injective group homomorphism.

Proof: By Proposition 27.3, $\mathrm{tr}^G_P \circ \mathrm{res}^G_P : M(G) = H^2(G, \mathbb{C}^\times) \longrightarrow H^2(G, \mathbb{C}^\times) = M(G)$ is multiplication by $|G : P|$. Restriction of this multiplication to $M(G)_p$ is an automorphism since $(|G : P|, p) = 1$. This proves that $\mathrm{res}^G_P|_{M(G)_p}$ is an injective map. ∎

Corollary 35.5

If for every prime number p such that $p \mid |G|$ the Sylow p-subgroups of G are cyclic, then $M(G) \cong \{1\}$.

Proof: Assume p is a prime number such that $p \mid |M(G)|$. Then $p \mid |G|$ by Lemma 35.1. So let $P \in \mathrm{Syl}_p(G)$. Then $M(P) \cong \{1\}$ by Lemma 35.3. Therefore, $M(G)_p \cong \{1\}$ since it is isomorphic to a subgroup of $M(P)$ by Theorem 35.4(b). The claim follows. ∎

Example 13

Corollary 35.5 implies for example that:

(a) the Schur multiplier of the symmetric group $\mathfrak{S}_3$ is trivial because $|\mathfrak{S}_3| = 6$ and $\mathfrak{S}_3$ has Sylow 2-subgroups isomorphic to C_2 and a unique Sylow 3-subgroup isomorphic to C_3;

(b) the Schur multiplier of the dihedral group D_{10} is trivial because $|D_{10}| = 10 = 2 \cdot 5$ so the Sylow p-subgroups must be isomorphic to C_p for each $p \in \{2, 5\}$.

36 Projective Representations

Definition 36.1 (*Projective representation*)

A **projective representation** of a finite group G over a field K, with 2-cocycle $\alpha : G \times G \longrightarrow K^\times$ is a map $T : G \longrightarrow \mathrm{GL}(V)$ where V is a finite-dimensional K-vector space and such that

$$T(g)T(h) = \alpha(g, h)T(gh) \qquad \forall\, g, h \in G\,.$$

Remark 36.2

(a) Notice that a projective representation is not in general a group homomorphism. Nevertheless, if $\pi_V : \mathrm{GL}(V) \longrightarrow \mathrm{PGL}(V) := \mathrm{GL}(V)/(K^\times \cdot \mathrm{Id}_V)$ denotes the quotient morphism, then clearly a projective representation $T : G \longrightarrow \mathrm{GL}(V)$ gives rise to a group homomorphism

$$\theta : G \xrightarrow{T} \mathrm{GL}(V) \xrightarrow{\pi_V} \mathrm{PGL}(V)\,,$$

explaining the terminology.

However, we emphasise *projective representations* in the sense of Definition 36.1 are not the same as the *K-representations associated to projective KG-modules* in the sense of Remark 14(a).

(c) Two projective representations $S : G \longrightarrow \mathrm{GL}(W)$ and $T : G \longrightarrow \mathrm{GL}(V)$, with 2-cocycles β and α resp., and are called **equivalent** if there exists a K-isomorphism $X : W \longrightarrow V$ and a 1-cochain (= a map) $\mu : G \longrightarrow K^\times$ such that

$$\mu(g) \cdot X \circ S(g) = T(g) \circ X \qquad \forall g \in G\,.$$

When this occurs, β and α differ by the 2-coboundary $d^*(\mu)$.

(d) Since $K^\times \cdot \mathrm{Id}_V = Z(\mathrm{GL}(V))$ there is a natural central extension

$$1 \longrightarrow K^\times \cdot \mathrm{Id}_V \longrightarrow \mathrm{GL}(V) \xrightarrow{\pi_V} \mathrm{PGL}(V) \longrightarrow 1\,.$$

Notation 36.3

Given a central extension of groups $1 \longrightarrow Z \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ (i.e. with $Z = \ker \pi \leqslant Z(E)$) in order to shorten the notation will often say that the pair (E, π) is a *central extension of G*.

Definition 36.4 (*Projective lifting property*)

A central extension (E, π) of G is said to have the **projective lifting property (relative to K)** if, for every finite-dimensional K-vector space V, every group homomorphism $\theta : G \longrightarrow \mathrm{PGL}(V)$ can be completed to a commutative diagram of group homomorphisms:

$$\begin{tikzcd}
1 \arrow[r] & Z \arrow[r] \arrow[d, "\lambda|_Z"'] & E \arrow[r, "\pi"] \arrow[d, "\lambda"'] & G \arrow[r] \arrow[d, "\theta"'] & 1 \\
1 \arrow[r] & K^\times \cdot \mathrm{Id}_V \arrow[r] & \mathrm{GL}(V) \arrow[r, "\pi_V"] & \mathrm{PGL}(V) \arrow[r] & 1
\end{tikzcd}$$

When this can be done, we say that θ can be **lifted** to the K-representation λ of E and λ is called a **lift** or a **lifting** of θ.

Remark 36.5

(a) In general, the homomorphism λ is not uniquely determined. However, by commutativity of the diagram, if $\lambda, \lambda' : E \longrightarrow \mathrm{GL}(V)$ are two liftings of θ to E, then there exists a degree one representation $\mu : E \longrightarrow \mathrm{GL}(K)$ such that $\lambda' = \lambda \otimes \mu$.

(b) Practically speaking, if a central extension (E, π) of G has the projective lifting property and $T : G \longrightarrow \mathrm{GL}(V)$ is any projective representation of G, then there exists a K-representation $\lambda : E \longrightarrow \mathrm{GL}(V)$ of E, such that T is equivalent (as a projective representation) to the projective representation inducing $\lambda \circ u : G \longrightarrow \mathrm{PGL}(V)$ where $u : G \longrightarrow E$ is a set-theoretic section for π.

37 Central Extensions and Universality

We now want to establish connections between central extensions, the projective lifting property and the Schur multiplier. To achieve this aim, we need to introduce further concepts.

Definition 37.1 (***B-universal central extensions***)

Let B be an abelian group. A central extension $1 \longrightarrow Z \longrightarrow E \xrightarrow{\nu} G \longrightarrow 1$ is called B-**universal** if, for any central extension of groups $1 \longrightarrow B \longrightarrow X \xrightarrow{\pi} G^* \longrightarrow 1$ with kernel B and any group homomorphism $\theta : G \longrightarrow G^*$, there exists a group homomorphism $\widetilde{\theta} : E \longrightarrow X$ such that the following diagram commutes:

$$\begin{tikzcd}
1 \arrow[r] & Z \arrow[r] \arrow[d, "\widetilde{\theta}|_Z"'] & E \arrow[r, "\nu"] \arrow[d, "\exists\, \widetilde{\theta}"'] & G \arrow[r] \arrow[d, "\theta"'] & 1 \\
1 \arrow[r] & B \arrow[r] & X \arrow[r, "\pi"] & G^* \arrow[r] & 1
\end{tikzcd}$$

Remark 37.2

Any $K^\times$-universal central extension of groups has the projective lifting property.

Remark 37.3 (***The Hochschild-Serre 5-term exact sequence***)

To each central extension $1 \longrightarrow Z \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ and each abelian group $(B, \cdot)$ (seen with trivial action of Z, E and G) can be associated a *5-term exact sequence*

$$1 \longrightarrow \mathrm{Hom}(G,B) \xrightarrow{\mathrm{Inf}_G^E} \mathrm{Hom}(E,B) \xrightarrow{\mathrm{Res}_Z^E} \mathrm{Hom}(Z,B) \xrightarrow{\mathrm{tr}} H^2(G,B) \xrightarrow{\mathrm{Inf}_G^E} H^2(E,B)$$

called the *Hochschild-Serre exact sequence* in the literature, because it arises from the low degree terms in the Hochschild-Serre spectral sequence associated to the given central extension (see [Wei94, Section 6.8]). The first homomorphism Inf_G^E is the inflation of homomorphisms, which is defined by

$$\mathrm{Inf}_G^E(\psi) = \psi \circ \pi \qquad \forall\, \psi \in \mathrm{Hom}(G,B)\,,$$

and is clearly injective. The homomorphism Res_Z^E denotes the ordinary restriction of maps from E to Z. The last homomorphism Inf_G^E is the inflation in cohomology, which is defined as follows: given a class $[\alpha] \in H^2(G,B)$ represented by a 2-cocycle $\alpha \in Z^2(G,B)$, the element $\mathrm{Inf}_G^E([\alpha]) \in H^2(E,B)$ is the cohomology class represented by the 2-cocycle $\beta \in Z^2(E,B)$ defined by

$$\beta(u,v) := \alpha(\pi(u),\pi(v)),\ \forall\, u,v \in E\,.$$

Finally, the homomorphism tr is called *transgression* and is defined as follows: given $\varphi \in \mathrm{Hom}(Z,B)$, then

$$\mathrm{tr}(\varphi) := [\varphi \circ \alpha] \in H^2(G,B)\,,$$

where $\alpha \in Z^2(G,Z)$ is a 2-cocycle representing the cohomology class corresponding to the central extension (E,π).

For ease of notation we often simply write Inf for the inflation maps and Res for the restriction map. In the case in which $B = K^\times$, writing $\mathrm{Hom}(G,K^\times) =: X(G)$, the 5-term exact sequence is

$$1 \longrightarrow X(G) \xrightarrow{\mathrm{Inf}} X(E) \xrightarrow{\mathrm{Res}} X(Z) \xrightarrow{\mathrm{tr}} H^2(G,K^\times) \xrightarrow{\mathrm{Inf}} H^2(E,K^\times)\,.$$

Proposition 37.4

A central extension $1 \longrightarrow Z \longrightarrow E \xrightarrow{v} G \longrightarrow 1$ is B-universal if and only if the transgression homomorphism $\mathrm{tr} : \mathrm{Hom}(Z, B) \longrightarrow H^2(G, B)$ is surjective.

Proof: The necessary condition is left as an exercise. See Exercise 53.
Conversely, assume that $\mathrm{tr} : \mathrm{Hom}(Z, B) \longrightarrow H^2(G, B)$ is surjective. Let $1 \longrightarrow B \longrightarrow X \xrightarrow{\pi} G^* \longrightarrow 1$ be a central extension of groups and let $\theta : G \longrightarrow G^*$ be a group homomorphism. Let $u : G \longrightarrow E$, $v : G^* \longrightarrow X$ be set-theoretic sections for v and π, respectively, and let $f : G \times G \longrightarrow Z$ and $g : G^* \times G^* \longrightarrow B$ be the associated 2-cocycles, respectively. Then

$$g_\theta : G \times G \xrightarrow{\theta\times\theta} G^* \times G^* \xrightarrow{f} B$$

is a 2-cocycle in $Z^2(G, B)$ (because f is and θ is a group homomorphism). Since tr is surjective, there exists $\varphi \in \mathrm{Hom}(Z, B)$ such that $\mathrm{tr}(\varphi) = [\varphi \circ f] = [g_\theta] \in H^2(G, B)$. Thus $\varphi \circ f$ and g_θ differ by a 2-coboundary, so there exists a 1-cochain $\tau : G \longrightarrow B$ such that $\tau(1) = 1$ and

$$\varphi f(x, y) = g(\theta(x), \theta(y))\tau(x)\tau(y)\tau(xy)^{-1} \qquad \forall\, x, y \in G\,.$$

Since any element of E may be written as $zu(x)$ with $z \in Z$ and $x \in G$, define

$$\lambda : E \longrightarrow E^*, zu(x) \mapsto \varphi(z)\tau(x)v(\theta(x))\,.$$

It is then easily verified that λ is the required homomorphism. ■

Lemma 37.5

If G is a finite group and $K = \overline{K}$ is an algebraically closed field of characteristic $p > 0$, then $p \nmid |H^2(G, K^\times)|$.

Proof: Let $c \in H^2(G, K^\times)$ and write $c = [\alpha]$ with $\alpha \in Z^2(G, K^\times)$. Write $o(c) = p^a \cdot m$ where $(m, p) = 1$. We must prove that $a = 0$. Since $c^{o(c)}$ is trivial in $H^2(G, K^\times)$, we have

$$\alpha(x, y)^{o(c)} = \mu(x)\mu(y)\mu(xy)^{-1} \quad \forall\, x, y \in G$$

for some 1-cochain $\mu : G \longrightarrow K^\times$. Since K is algebraically closed each of its elements has a unique p^a-th root of unity and we can write

$$(\alpha(x, y)^m)^{p^a} = \left(\mu(x)^{\frac{1}{p^a}}\mu(y)^{\frac{1}{p^a}}\mu(xy)^{\frac{-1}{p^a}}\right)^{p^a}$$

and it follows that

$$\alpha(x, y)^m = \mu(x)^{\frac{1}{p^a}}\mu(y)^{\frac{1}{p^a}}\mu(xy)^{\frac{-1}{p^a}}$$

which contradicts the assumption that c has order $p^a \cdot m$, unless $p^a = 1$, as required. ■

Theorem 37.6

Let G be a finite group and let $K = \overline{K}$ be an algebraically closed field. Then the following assertions hold:

(a) There exists a central extensions $1 \longrightarrow Z \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ with kernel $Z \cong H^2(G, K^\times)$ and having the projective lifting property relative to K.

(b) Any central extension (E, π) of G with the projective lifting property relative to K is $K^\times$-universal.

Proof:

(a) By Remark 37.2 and Proposition 37.4 it suffices to construct a central extension

$$1 \longrightarrow H^2(G, K^\times) \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$$

such that the associated transgression homomorphism

$$\mathrm{tr} : \mathrm{Hom}\left(H^2(G, K^\times), K^\times\right) \longrightarrow H^2(G, K^\times)$$

is surjective. Since by Proposition 30.2 the group $H^2(G, K^\times)$ is a finite abelian group, we may express it as a finite product of finite cyclic groups

$$H^2(G, K^\times) = \langle c_1 \mid c_1^{e_1} = 1\rangle \times \cdots \times \langle c_d \mid c_d^{e_d} = 1\rangle$$

where by Lemma 37.5, $\mathrm{char}(K) \nmid e_i =: o(c_i)$ for each $1 \leqslant i \leqslant d$. Now, as $K = \overline{K}$, for each $1 \leqslant i \leqslant d$, we there exists an e_i-th primitive root of unity $\zeta_i \in K$ (these need not be distinct). Then, by Exercise 54, for each $1 \leqslant i \leqslant d$ there exists $\alpha_i \in Z^2(G, K^\times)$ such that $c_i = [\alpha_i]$ and

$$\alpha_i(x, y) = \zeta_i^{a_i(x,y)} \qquad \forall\, x, y \in G$$

where the exponents $a_i(x, y)$ are uniquely determined integers such that $0 \leqslant a_i(x, y) < e_i$. Next, for each $(x, y) \in G \times G$, let

$$a(x, y) := c_1^{a_1(x,y)} \cdot \cdots \cdot c_d^{a_d(x,y)}\,.$$

The 2-cocycle identity

$$\alpha_i(y, z)\alpha_i(x, yz) = \alpha_i(xy, z)\alpha_i(x, y) \qquad \forall\, x, y, z \in G,\ \forall\, 1 \leqslant i \leqslant d$$

implies then that

$$a_i(y, z) + a_i(x, yz) \equiv a_i(xy, z)a_i(x, y) \pmod{e_i} \qquad \forall\, x, y, z \in G,\ \forall\, 1 \leqslant i \leqslant d$$

and since c_i has order e_i for each $1 \leqslant i \leqslant d$, it follows that $a : G \times G \longrightarrow H^2(G, K^\times)$ satisfies the 2-cocycle identity and defines a 2-cocycle. Therefore, by Theorem 24.3 (and its proof), there exists a central extension

$$1 \longrightarrow H^2(G, K^\times) \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$$

associated to $[a] \in H^2(G, H^2(G, K^\times))$ and it remains to prove that the associated transgression map is surjective. So let $b \in H^2(G, K^\times)$ and write

$$b = (c_1^{b_1}, \ldots, c_d^{b_d}) \in \langle c_1 \mid c_1^{e_1} = 1\rangle \times \cdots \times \langle c_d \mid c_d^{e_d} = 1\rangle$$

with $1 \leqslant b_i \leqslant e_d$ for each $1 \leqslant i \leqslant d$. Then $b = [\beta]$ for the 2-cocycle $\beta \in Z^2(G, K^\times)$ defined by

$$\beta(x, y) := \prod_{i=1}^{d} \zeta_i^{b_i a_i(x,y)} \quad \forall\, x, y \in G\,.$$

Then, there exists a well-defined $\varphi \in \mathrm{Hom}\left(H^2(G, K^\times), K^\times\right)$ defined by

$$\varphi(c_i) := \zeta_i^{b_i} \qquad \forall\, 1 \leqslant i \leqslant d$$

and which is such that

$$\varphi(a(x, y)) = \beta(x, y) \quad \forall\, x, y \in G\,.$$

Hence, $\mathrm{tr}(\varphi) = b$, completing the proof of (a).

(b) Let $1 \longrightarrow Z \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ be a central extension of G with the projective lifting property relative to K. Let $u : G \longrightarrow E$ be a set-theoretic section for π and let $f : G \times G \longrightarrow Z$ be the associated 2-cocycle. By Proposition 37.4, it suffices to prove that the transgression map $\mathrm{tr} : \mathrm{Hom}(Z, K^\times) \longrightarrow H^2(G, K^\times)$ is surjective. So let $c \in H^2(G, K^\times)$ and write $c = [\alpha]$ with $\alpha \in Z^2(G, K^\times)$. Then, there exists a projective representation $T : G \longrightarrow \mathrm{GL}(V)$ with associated 2-cocycle α and we let $\theta := \pi_V \circ T : G \longrightarrow \mathrm{PGL}(V)$ be the induced group homomorphism to $\mathrm{PGL}(V)$ as in Remark 36(b). Then, by the projective lifting property, there exists a K-represenentation $\lambda : E \longrightarrow \mathrm{GL}(V)$ such that the diagram

$$\begin{tikzcd}
1 \arrow[r] & Z \arrow[r] \arrow[d, "\lambda|_Z"'] & E \arrow[r, "\pi"] \arrow[d, "\lambda"'] & G \arrow[r] \arrow[d, "\theta"'] & 1 \\
1 \arrow[r] & K^\times \cdot \mathrm{Id}_V \arrow[r] & \mathrm{GL}(V) \arrow[r, "\pi_V"] & \mathrm{PGL}(V) \arrow[r] & 1
\end{tikzcd}$$

commutes. Moreover, from the fact that for every $x, y \in G$ we have

$$u(x)u(x) = f(x, y)u(xy)$$

follows that

$$\lambda(u(x))\lambda(u(y)) = \lambda|_Z(f(x, y))\lambda(u(xy)) .$$

Therefore $\mathrm{tr}(\lambda|_Z) = c$, proving the surjectivity of the transgression, as required. ■

We can now eventually connect central extensions to the Schur multiplier.

Definition 37.7

Assume $K = \mathbb{C}$. A **representation group** of a finite group G is a central extension (E, π) of G of minimal order with the projective lifting property relative to $\mathbb{C}$.

Theorem 37.8

Let G be a finite group. Then, representations groups of G exist. Furthermore, a central extension $1 \longrightarrow Z \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ is a representation group of G if and only if $Z \leqslant [E, E]$ and $|Z| = |H^2(G, \mathbb{C}^\times)|$, and if these two conditions are satisfied, then $Z \cong H^2(G, \mathbb{C}^\times)$.

Proof: To begin with representation groups of finite groups exist by Theorem 37.6(a) and one of them has kernel $H^2(G, \mathbb{C}^\times)$.

Next, assuming that (E, π) is a representation group of G, then (E, π) is $\mathbb{C}^\times$-universal by Theorem 37.6(b) and thus the transgression $\mathrm{tr} : \mathrm{Hom}(Z, \mathbb{C}^\times) \longrightarrow H^2(G, \mathbb{C}^\times)$ is surjective by Proposition 37.4. Therefore,

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

since $|\mathrm{Hom}(Z, \mathbb{C}^\times)| = |Z|$ because Z is abelian and $\mathrm{Hom}(Z, \mathbb{C}^\times)$ is the group of linear characters of Z. So by minimality of (E, π) we must have

$$|Z| = |H^2(G, \mathbb{C}^\times)| \qquad \text{and} \qquad \mathrm{tr} \text{ is an isomorphism.}$$

Therefore $\ker(\mathrm{tr}) = \{1\}$ and $Z \leqslant [E, E]$ by Exercise 55.

Conversely, assume $1 \longrightarrow Z \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ is a central extension such that $Z \leqslant [E, E]$ and $|Z| = |H^2(G, \mathbb{C}^\times)|$. Again, to prove that (E, π) is a representation group of G, it suffices to prove that the transgression $\mathrm{tr} : \mathrm{Hom}(Z, \mathbb{C}^\times) \longrightarrow H^2(G, \mathbb{C}^\times)$ is surjective. Since $Z \leqslant [E, E]$, Exercise 55(a) yields

$$\ker(\mathrm{tr}) = (Z \cap [E, E])^\perp = Z^\perp = \{1\}$$

so tr is injective. This and the assumption yield $|Z| = |H^2(G, \mathbb{C}^\times)| \geqslant |\mathrm{Hom}(Z, \mathbb{C}^\times)| = |Z|$ and so in fact equality holds, proving that tr is surjective. ■

38 Exercises for Chapter 9

Exercise 51

Prove that $H^n(G, \mathbb{Q}/\mathbb{Z}) \cong H^{n+1}(G, \mathbb{Z})$ for all $n \geqslant 1$ using an argument similar to the one used in the proof of Lemma 34.4.

Exercise 52

Prove that $M(G)$ is trivial if G is a finite cyclic group.

Exercise 53

Let B be an abelian group. Prove that if a central extension $1 \longrightarrow Z \longrightarrow E \xrightarrow{\nu} G \longrightarrow 1$ is B-universal, then the transgression homomorphism $\mathrm{tr} : \mathrm{Hom}(Z, B) \longrightarrow H^2(G, B)$ is surjective.

Exercise 54

Let G be a finite group and $K = \overline{K}$ be an algebraically closed field of characteristic $p \geqslant 0$. Prove that any cohomology class $c \in H^2(G, K^\times)$ can be represented by a 2-cocycle $\alpha : G \times G \longrightarrow K^\times$ whose values are $o(c)$-th roots of unity in K.

Exercise 55

Assume $K = \mathbb{C}$ and let $1 \longrightarrow Z \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ be a central extension of finite groups. Prove that:

(a) $\ker(\mathrm{tr}) = (Z \cap [E, E])^\perp =: \{\varphi \in \mathrm{Hom}(Z, \mathbb{C}^\times) \mid Z \cap [E, E] \leqslant \ker(\varphi)\}$; and

(b) $Z \leqslant [E, E]$ if and only if the transgression $\mathrm{tr} : \mathrm{Hom}(Z, \mathbb{C}^\times) \longrightarrow H^2(G, \mathbb{C}^\times) = M(G)$ is injective.

Exercise 56

Assume $K = \mathbb{C}$ and let $1 \longrightarrow Z \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ be a central extension of finite groups. Prove that if $Z \leqslant [E, E]$, then the transgression $\mathrm{tr} : \mathrm{Hom}(Z, \mathbb{C}^\times) \longrightarrow H^2(G, \mathbb{C}^\times) = M(G)$ is injective.

Appendix: The Language of Category Theory

This appendix provides a short introduction to some of the basic notions of category theory used in this lecture.

References:

[McL98] S. Mac Lane, *Categories for the working mathematician*, second ed., Graduate Texts in Mathematics, vol. 5, Springer-Verlag, New York, 1998.

[Wei94] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

A Categories

Definition A.1 (*Category*)

A **category** $\mathcal{C}$ consists of:

- a class $\mathrm{Ob}\,\mathcal{C}$ of **objects**,
- a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of **morphisms** for every ordered pair (A, B) of objects, and
- a **composition function**

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) & \longrightarrow & \mathrm{Hom}_{\mathcal{C}}(A,C) \\ (f,g) & \mapsto & g \circ f \end{array}$$

  for each ordered triple (A, B, C) of objects,

satisfying the following axioms:

(C1) **Unit axiom**: for each object $A \in \mathrm{Ob}\,\mathcal{C}$, there exists an **identity morphism** $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ such that for every $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ for all $B \in \mathrm{Ob}\,\mathcal{C}$,

$$f \circ 1_A = f = 1_B \circ f\,.$$

(C2) **Associativity axiom**: for every $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ and $h \in \mathrm{Hom}_{\mathcal{C}}(C, D)$ with $A, B, C, D \in \mathrm{Ob}\,\mathcal{C}$,

$$h \circ (g \circ f) = (h \circ g) \circ f\,.$$

Let us start with some remarks and examples to enlighthen this definition:

Remark A.2

(a) $\operatorname{Ob}\mathcal{C}$ need not be a set!

(b) The only requirement on $\operatorname{Hom}_{\mathcal{C}}(A, B)$ is that it be a set, and it is allowed to be empty.

(c) It is common to write $f : A \longrightarrow B$ or $A \xrightarrow{f} B$ instead of $f \in \operatorname{Hom}_{\mathcal{C}}(A, B)$, and to talk about *arrows* instead of *morphisms*. It is also common to write "$A \in \mathcal{C}$" instead of "$A \in \operatorname{Ob}\mathcal{C}$".

(d) The identity morphism $1_A \in \operatorname{Hom}_{\mathcal{C}}(A, A)$ is uniquely determined: indeed, if $f_A \in \operatorname{Hom}_{\mathcal{C}}(A, A)$ were a second identity morphisms, then we would have $f_A = f_A \circ 1_A = 1_A$.

Example A.3

(a) $\mathcal{C} = \mathbf{1}$: category with one object and one morphism (the identity morphism):

$$\begin{tikzcd}
\bullet \arrow[loop right, "1_\bullet"]
\end{tikzcd}$$

(b) $\mathcal{C} = \mathbf{2}$: category with two objects and three morphism, where two of them are identity morphisms and the third one goes from one object to the other:

$$\begin{tikzcd}
A \arrow[loop left, "1_A"] \arrow[r] & B \arrow[loop right, "1_B"]
\end{tikzcd}$$

(c) A group G can be seen as a category $\mathcal{C}(G)$ with one object: $\operatorname{Ob}\mathcal{C}(G) = \{\bullet\}$, $\operatorname{Hom}_{\mathcal{C}(G)}(\bullet, \bullet) = G$ (notice that this is a set) and composition is given by multiplication in the group.

(d) The $n \times m$-matrices with entries in a field k for n, m ranging over the positive integers form a category $\mathbf{Mat}_k$: $\operatorname{Ob}\mathbf{Mat}_k = \mathbb{Z}_{>0}$, morphisms $n \longrightarrow m$ from n to m are the $m \times n$-matrices, and compositions are given by the ordinary matrix multiplication.

Example A.4 (*Categories and algebraic structures*)

(a) $\mathcal{C} = \mathbf{Set}$, the *category of sets*: objects are sets, morphisms are maps of sets, and composition is the usual composition of functions.

(b) $\mathcal{C} = \mathbf{Vec}_k$, the *category of vector spaces over the field k*: objects are k-vector spaces, morphisms are k-linear maps, and composition is the usual composition of functions.

(c) $\mathcal{C} = \mathbf{Top}$, the *category of topological spaces*: objects are topological spaces, morphisms are continous maps, and composition is the usual composition of functions.

(d) $\mathcal{C} = \mathbf{Grp}$, the *category of groups*: objects are groups, morphisms are homomorphisms of groups, and composition is the usual composition of functions.

(e) $\mathcal{C} = \mathbf{Ab}$, the *category of abelian groups*: objects are abelian groups, morphisms are homomorphisms of groups, and composition is the usual composition of functions.

(f) $\mathcal{C} = \mathbf{Rng}$, the *category of rings*: objects are rings, morphisms are homomorphisms of rings, and composition is the usual composition of functions.

(g) $\mathcal{C} =_R \mathbf{Mod}$, the *category of left R-modules*: objects are *left* modules over the ring R, morphisms are R-homomorphisms, and composition is the usual composition of functions.

(g') $\mathcal{C} = \mathbf{Mod}_R$, the *category of left R-modules*: objects are *right* modules over the ring R, morphisms are R-homomorphisms, and composition is the usual composition of functions.

(g") $\mathcal{C} =_R \mathbf{Mod}_S$, the *category of* (R,S)*-bimodules*: objects are (R,S)-bimodules over the rings R and S, morphisms are (R,S)-homomorphisms, and composition is the usual composition of functions.

(h) Examples of your own ...

Definition A.5 (*Monomorphism/epimorphism*)

Let $\mathcal{C}$ be a category and let $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ be a morphism. Then f is called

(a) a **monomorphism** iff for all morphisms $g_1, g_2 : C \longrightarrow A$,

$$f \circ g_1 = f \circ g_2 \Longrightarrow g_1 = g_2 \,.$$

(b) an **epimorphism** iff for all morphisms $g_1, g_2 : B \longrightarrow C$,

$$g_1 \circ f = g_2 \circ f \Longrightarrow g_1 = g_2 \,.$$

Remark A.6

In categories, where morphisms are set-theoretic maps, then injective morphisms are monomorphisms, and surjective morphisms are epimorphisms.
In module categories (${}_R\mathbf{Mod}$, $\mathbf{Mod}_R$, ${}_R\mathbf{Mod}_S$, ...), the converse holds as well, but:

Warning: It is not true in general, that all monomorphisms must be injective, and all epimorphisms must be surjective.

For example in **Rng**, the canonical injection $\iota : \mathbb{Z} \longrightarrow \mathbb{Q}$ is an epimorphism. Indeed, if C is a ring and $g_1, g_2 \in \mathrm{Hom}_{\mathbf{Rng}}(\mathbb{Q}, C)$

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\iota"] & \mathbb{Q} \arrow[r, shift left, "g_2"] \arrow[r, shift right, "g_1"'] & C \end{tikzcd}$$

are such that $g_1 \circ \iota = g_2 \circ \iota$, then we must have $g_1 = g_2$ by the universal property of the field of fractions. However, ι is clearly not surjective.

B Functors

Definition B.1 (*Covariant functor*)

Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A **covariant functor** $F : \mathcal{C} \longrightarrow \mathcal{D}$ is a collection of maps:

- $F : \mathrm{Ob}\,\mathcal{C} \longrightarrow \mathrm{Ob}\,\mathcal{D}, X \mapsto F(X)$, and
- $F_{A,B}\; : \mathrm{Hom}_{\mathcal{C}}(A, B) \mapsto \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$,

satisfying:

(a) If $A \xrightarrow{f} B \xrightarrow{g} C$ are morphisms in $\mathcal{C}$, then $F(g \circ f) = F(g) \circ F(f)$; and

(b) $F(1_A) = 1_{F(A)}$ for every $A \in \mathrm{Ob}\,\mathcal{C}$.

Definition B.2 (*Contravariant functor*)

Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A **contravariant functor** $F : \mathcal{C} \longrightarrow \mathcal{D}$ is a collection of maps:

- $F : \mathrm{Ob}\,\mathcal{C} \longrightarrow \mathrm{Ob}\,\mathcal{D}, X \mapsto F(X)$, and
- $F_{A,B}\; : \mathrm{Hom}_{\mathcal{C}}(A, B) \mapsto \mathrm{Hom}_{\mathcal{D}}(F(B), F(A))$,

satisfying:

(a) If $A \xrightarrow{f} B \xrightarrow{g} C$ are morphisms in $\mathcal{C}$, then $F(g \circ f) = F(f) \circ F(g)$; and

(b) $F(1_A) = 1_{F(A)}$ for every $A \in \mathrm{Ob}\,\mathcal{C}$.

Remark B.3

Often in the literature functors are defined only on objects of categories. When no confusion is to be made and the action of functors on the morphism sets are implicitely obvious, we will also adopt this convention.

Example B.4

Let $Q \in \mathrm{Ob}({}_R\mathbf{Mod})$. Then

$$\begin{array}{rccc} \mathrm{Hom}_R(Q, -): & {}_R\mathbf{Mod} & \longrightarrow & \mathbf{Ab} \\ & M & \mapsto & \mathrm{Hom}_R(Q, M)\,, \end{array}$$

is a covariant functor, and

$$\begin{array}{rccc} \mathrm{Hom}_R(-, Q): & {}_R\mathbf{Mod} & \longrightarrow & \mathbf{Ab} \\ & M & \mapsto & \mathrm{Hom}_R(M, Q)\,, \end{array}$$

is a contravariant functor.

Exact Functors.

We are now interested in the relations between functors and exact sequences in categories where it makes sense to define exact sequences, that is categories that behave essentially like module categories such as ${}_R\mathbf{Mod}$. These are the so-called **abelian categories**. It is not the aim, to go into these details, but roughly speaking abelian categories are categories satisfying the following properties:

- they have a zero object (in ${}_R\mathbf{Mod}$: the zero module)
- they have products and coproducts (in ${}_R\mathbf{Mod}$: products and direct sums)
- they have kernels and cokernels (in ${}_R\mathbf{Mod}$: the usual kernels and cokernels of R-linear maps)
- monomorphisms are kernels and epimorphisms are cokernels (in ${}_R\mathbf{Mod}$: satisfied)

Definition B.5 (*Pre-additive categories/additive functors*)

(a) A category $\mathcal{C}$ in which all sets of morphisms are abelian groups is called **pre-additive**.

(b) A functor $F : \mathcal{C} \longrightarrow \mathcal{D}$ between pre-additive categories is called **additive** iff the maps $F_{A,B}$ are homomorphisms of groups for all $A, B \in \operatorname{Ob}\mathcal{C}$.

Definition B.6 (*Left exact/right exact/exact functors*)

Let $F : \mathcal{C} \longrightarrow \mathcal{D}$ be a covariant (resp. contravariant) additive functor between two abelian categories, and let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a s.e.s. of objects and morphisms in $\mathcal{C}$. Then F is called:

(a) **left exact** if $0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$ (resp. $0 \longrightarrow F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A)$)) is an exact sequence.

(b) **right exact** if $F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0$ (resp. $F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A)) \longrightarrow 0$) is an exact sequence.

(c) **exact** if $0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0$ (resp. $0 \longrightarrow F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A)) \longrightarrow 0$) is a short exact sequence.

Example B.7

The functors $\operatorname{Hom}_R(Q, -)$ and $\operatorname{Hom}_R(-, Q)$ of Example B.4 are both left exact functors. Moreover $\operatorname{Hom}_R(Q, -)$ is exact if and only if Q is projective, and $\operatorname{Hom}_R(-, Q)$ is exact if and only if Q is injective.

Bibliography

[Bro94] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994, Corrected reprint of the 1982 original.

[CR90] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1990, With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication.

[Eve91] L. Evens, *The cohomology of groups*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1991.

[Hum96] J. F. Humphreys, *A course in group theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1996.

[Joh90] D. L. Johnson, *Presentations of groups*, London Mathematical Society Student Texts, vol. 15, Cambridge University Press, Cambridge, 1990.

[LT17] C. Lassueur and J. Thévenaz, *Universal p'-central extensions*, Expo. Math. **35** (2017), no. 3, 237–251.

[ML98] S. Mac Lane, *Categories for the working mathematician*, second ed., Graduate Texts in Mathematics, vol. 5, Springer-Verlag, New York, 1998.

[Rot95] J. J. Rotman, *An introduction to the theory of groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[Rot09] Joseph J. Rotman, *An introduction to homological algebra*, second ed., Universitext, Springer, New York, 2009.

[Rot10] J. J. Rotman, *Advanced modern algebra. 2nd ed.*, Providence, RI: American Mathematical Society (AMS), 2010.

[Wei94] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

Index of Notation

General symbols

$\mathbb{C}$	field of complex numbers
$\mathbb{F}_q$	finite field with q elements
Id_M	identity map on the set M
$\mathrm{Im}(f)$	image of the map f
$\ker(\varphi)$	kernel of the morphism φ
$\mathbb{N}$	the natural numbers without 0
$\mathbb{N}_0$	the natural numbers with 0
$\mathbb{P}$	the prime numbers in $\mathbb{Z}$
$\mathbb{Q}$	field of rational numbers
$\mathbb{R}$	field of real numbers
$\mathbb{Z}$	ring of integer numbers
$\mathbb{Z}_{\geqslant a}, \mathbb{Z}_{>a}, \mathbb{Z}_{\leqslant a}, \mathbb{Z}_{<a}$	$\{m \in \mathbb{Z} \mid m \geqslant a$ (resp. $m > a, m \geqslant a, m < a)\}$
$\lvert X \rvert$	cardinality of the set X
δ_{ij}	Kronecker's delta
$\bigcup$	union
$\coprod$	disjoint union
$\bigcap$	intersection
$\sum$	summation symbol
$\prod, \times$	cartesian/direct product
$\rtimes$	semi-direct product
$\oplus$	direct sum
$\otimes$	tensor product
$\varnothing$	empty set
$\forall$	for all
$\exists$	there exists
$\cong$	isomorphism
$a \mid b \ , \ a \nmid b$	a divides b, a does not divide b
(a, b)	gcd of a and b
$f\rvert_S$	restriction of the map f to the subset S
$\hookrightarrow$	injective map
$\twoheadrightarrow$	surjective map

Group theory

$\mathrm{Aut}(G)$	automorphism group of the group G
$\mathrm{Aut}_{A,G}(E)$	automorphism the group G inducing the identity on A and G
$\mathfrak{A}_n$	alternating group on n letters
C_m	cyclic group of order m in multiplicative notation
$C_G(x)$	centraliser of the element x in G
$C_G(H)$	centraliser of the subgroup H in G
D_{2n}	dihedral group of order $2n$
$\mathrm{End}(A)$	endomorphism ring of the abelian group A
$\mathcal{E}(G, A_*)$	set of equivalence classes of group extensions
	$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$ inducing the G-action $*$
G/N	quotient group G modulo N
$\mathrm{GL}_n(K)$	general linear group over K
$\mathrm{PGL}_n(K)$	projective general linear group over K
$H \leqslant G$, $H < G$	H is a subgroup of G, resp. a proper subgroup
$N \trianglelefteq G$	N is a normal subgroup G
$N_G(H)$	normaliser of H in G
$N \rtimes_\theta H$	semi-direct product of N by H w.r.t. θ
$\mathrm{PGL}_n(K)$	projective linear group over K
Q_8	quaternion group of order 8
Q_{2^n}	generalised quaternion group of order 2^n
$\mathfrak{S}_n$	symmetric group on n letters
SD_{2^n}	semi-dihedral group of order 2^n
$\mathrm{SL}_n(K)$	special linear group over K
$\mathbb{Z}/m\mathbb{Z}$	cyclic group of order m in additive notation
${}^x g$	conjugate of g by x, i.e. gxg^{-1}
$\langle g \rangle \subseteq G$	subgroup of G generated by g
$G = \langle X \mid R \rangle$	presentation for the group G
$\lvert G : H \rvert$	index of the subgroup H in G
$\overline{x} \in G/N$	class of $x \in G$ in the quotient group G/N
$\{1\}$, 1, $\mathbb{1}$	trivial group

Module theory

$\mathrm{Hom}_R(M, N)$	R-homomorphisms from M to N
$\mathrm{End}_R(M)$	R-endomorphism ring of the R-module M
KG	group algebra of the group G over the ring K
$\varepsilon : KG \longrightarrow K$	augmentation map
IG	augmentation ideal
M^G	G-fixed points of the module M
M_G	G-cofixed points of the module M
$M\downarrow^G_H$, $\mathrm{Res}^G_H(M)$	restriction of M from G to H
$\mathrm{Ind}^G_H(M)$	induction of M from H to G
res^G_H	restriction from G to H in cohomology
tr^G_H	transfer from H to G

Homological algebra

$B_n(C_\bullet)$	n-boundaries of $C_\bullet$
$B^n(C^\bullet)$	n-coboundaries of $C^\bullet$
$B^n(G, A)$	n-coboundaries with coeff. in A rel. to the bar resolution
$(C_\bullet, d_\bullet)$, $C_\bullet$	chain complex
$(C^\bullet, d^\bullet)$, $C^\bullet$	cochain complex
$C^n(G, A)$	n-cochains with coeff. in A rel. to the bar resolution
$\mathrm{Ext}_R^n(M, N)$	n-th Ext-group of M with coefficients in N
$H_n(C_\bullet)$	n-th homology group/module of $C_\bullet$
$H_n(G, M)$	n-th homology group of the group G with coeff. in M
$H^n(C^\bullet)$	n-th cohomology group/module of $C^\bullet$
$H^n(G, M)$	n-th cohomology group of the group G with coeff. in M
$P_\bullet \twoheadrightarrow M$	projective resolution of the module M
$\mathrm{Tor}_n^R(M, N)$	n-th Tor-group of M with coefficients in N
$Z_n(C_\bullet)$	n-cycles of $C_\bullet$
$Z^n(C^\bullet)$	n-cocycles of $C^\bullet$
$Z^n(G, A)$	n-cocycles with coeff. in A rel. to the bar resolution
$[g_1 \vert g_2 \vert \ldots \vert g_n]$	bar notation

Category Theory

$\mathrm{Ob}\,\mathcal{C}$	objects of the category $\mathcal{C}$
$\mathrm{Hom}_{\mathcal{C}}(A, B)$	morphisms from A to B
$\mathbf{Set}$	the category of sets
$\mathbf{Vec}_k$	the category of vector spaces over the field k
$\mathbf{Top}$	the category of topological spaces
$\mathbf{Grp}$	the category of groups
$\mathbf{Ab}$	the category of abelian groups
$\mathbf{Rng}$	the category of rings
${}_R\mathbf{Mod}$	the category of left R-modules
$\mathbf{Mod}_R$	the category of left R-modules
${}_R\mathbf{Mod}_S$	the category of (R, S)-bimodules

Index