Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

Structure theorem for finitely generated modules over Principal Ideal Domains, the Jordan-Hölder theorem and the Extension Problem

Tesi di Laurea in Algebra

Relatrice:
Chiar.ma Prof.ssa
Nicoletta Cantarini

Presentata da:
Lorenzo Ferraiuolo

Anno Accademico 2022-2023

Introduction

This thesis is organized as follows:

- In Chapter 0, we give some preliminary results and definitions, which are fundamental in the following chapters.
- In Chapter 1, we present the structure theorem for finitely generated abelian groups and its generalization to modules over principal ideal domains.
- In Chapter 2, we will prove the Jordan-Hölder Theorem in the case of representations of associative algebras over fields.
- Finally, in Chapter 3, we introduce the theory of group extensions and group cohomology and give some intuition to the first four cohomology groups. Then we prove some results concerning the extension problem of finite groups.

The Structure Theorem for finitely generated abelian groups was proven by Henri Poincaré in 1900 and it is the first step to the complete classification of all finite groups. The Structure Theorem has numerous applications to other branches of mathematics. For instance, in algebraic topology, the n^{th} Betti number of a topological space X is defined as the rank of the n^{th}

homology group of X (when it is finitely generated). The classification of non-finitely generated abelian groups is an open problem. Unlike finitely generated abelian groups where the direct sum decomposition is unique (up to isomorphism), infinitely generated abelian groups can have non-unique direct sum decompositions, further complicating their study. The lack of finiteness conditions on an abelian group means that we allow objects of unrestricted size and complexity. In this setting, many set-theoretic issues (related, for instance, to the theory of infinite cardinals) arise. However, some classes of infinitely generated abelian groups have already been classified, e.g., divisible groups.

The Structure Theorem for finitely-generated abelian groups has one of its natural generalizations into the Structure Theorem for finitely-generated modules over principal ideal domains. This result can be further generalized to Dedekind domains; moreover, the primary decomposition generalizes to finitely generated modules over commutative Noetherian rings.

The Jordan-Hölder Theorem is a more general decomposition result originally stated for finite groups, but it can be generalized for any abelian category. In this generality, one obtains a composition series, rather than a direct sum. From this class of results, two main problems arise: the classification of all the simple (irreducible) objects and the classification of all the possible extensions between them. For instance, the classification of all finite simple groups is a massive result completed in 2004 while the extension problem for finite groups is still open.

The notion of extension varies from subject to subject between two ways in which some structure can be extended, namely, by *embedding* and by *cover-*

ing. In the first case, the extension contains the original space as a subspace and it is usually represented by $1 \to M \to E$ (we say that M is *embedded into* E). In the latter one, the original space is seen as a quotient of the extended space and it is usually represented by $E \to G \to 1$ (we say that E *covers* G). For example, in field theory it is the case that any covering is trivial since any surjective homomorphism of fields is an isomorphism, hence the word extension is usually referred to embeddings of fields. Instead, in group theory any covering naturally induces an embedding (while not every embedding can canonically induce a covering). Concerning group cohomology, the point of view we adopt in this thesis is the general one formulated in 1943-1945 by Eilenberg and MacLane using the derived Ext functor. Long before this formulation of group cohomology, the low dimensional cohomology of groups was already studied in the early 1900s with Shur's works and especially with Shreirer's work on group extensions in 1926.

Contents

Chapter 0

Preliminaries

In this chapter, we will summarize some basic concepts and results (without going into the details of the proofs) that we will need in the sequel.

Definition 0.0.1. *Let R be an integral domain. We say that R is a* **principal ideal domain** (**PID**) *if for every ideal $I \subseteq R$, there exists $a \in I$ such that $I = (a) := \{a \cdot r,\ \text{for every } r \in R\}$.*

Example 0.0.2.

- Every field is (trivially) a PID.
- If $\mathbb{K}$ is a field, then $\mathbb{K}[x]$ is a PID.
- Let $\mathbb{K}$ be a field, then $\mathbb{K}[x, y]$ is not a PID, indeed, the ideal (x, y) is not principal; notice that $\mathbb{K}[x, y]/(xy - 1)$ is a PID (it is called the ring of **Laurent polynomials in one variable over** $\mathbb{K}$).

Definition 0.0.3. *Let R be a unitary ring and M an R-module, then we say that M is a* **finite free** *R-module if $M \cong R^n$ for some $n \in \mathbb{Z}_{>0}$; in this case we say that n is the* **rank** *of M and write $rk(M) = n$.*

Definition 0.0.4. *Let R be a ring and M an R-module; we say that $x \in M$ is a* **torsion element** *if there exists $a \in R^*$ such that $ax = 0$. Moreover, we*

say that M is **torsion-free** *if there are no torsion elements in M different from zero.*

Theorem 0.0.5. *Let R be a PID and M a finitely generated R-module, then M is torsion-free if and only if it is free.*

Proof. Since R is a domain R^n is torsion-free, hence every free R-module is torsion-free. Let us suppose M is torsion-free: since M is finitely generated we can choose a set of generators for M with minimal cardinality, say $\{e_1, \dots, e_n\}$; let us suppose there exists a null linear combination $a_1e_1 + \cdots + a_ne_n = 0$ with $a_i \in R$ for all $i \leq n$ and $a_j \neq 0$ for some $j \leq n$: since R is a PID, the ideal generated by $a_1, \dots, a_n$ is principal so it is generated by only one element of R^*, say a. For every $i \leq n$ there exists $b_i \in R$ such that $a_i = ab_i$ and we can assume $(b_1, \dots, b_n) = (1) = R$, thus $a(b_1e_1 + \cdots + b_ne_n) = 0$ and since M is torsion-free it must be $b_1e_1 + \cdots + b_ne_n = 0$. Moreover for all $i \leq n$ there exists $\alpha_i \in R$ such that $\alpha_1b_1 + \cdots + \alpha_nb_n = 1$; without loss of generality let us suppose that $b_1 \neq 0$ so $\alpha_1(b_1e_1 + \cdots + b_ne_n) = e_1 + \sum_{i=2}^{n} b_i(e_i - \alpha_ie_1) = 0$. Let us define $e_i' := \alpha_ie_1 - e_i$, then $e_1 = \sum_{i=2}^{n} b_ie_i'$, but $\{e_2', \dots, e_n'\}$ is a set of generators for M, thus contradicting the minimality of $\{e_1, \dots, e_n\}$. Therefore $\{e_1, \dots, e_n\}$ is a linear independent set and $M \cong R^n$. □

Remark 0.0.6. In Theorem 0.0.5 it is important that M is finitely generated, indeed as a counter-example we can take the set of rational numbers $\mathbb{Q}$: it is clearly torsion-free but for every $n \in \mathbb{Z}_{>0}$, $\mathbb{Q} \ncong \mathbb{Z}^n$ (see 1.1.15).

Definition 0.0.7. *Let R be an integral domain, we call R a* **euclidean domain** *if there exists a function $\delta : R^* \to \mathbb{Z}_{\geq 0}$ such that for every $a, b \in R$*

there exist $q, r \in R$ such that $b = qa + r$ and either $\delta(r) < \delta(a)$ or $r = 0$.

Proposition 0.0.8. *Every euclidean domain is a principal ideal domain.*

Proof. Let E be a euclidean domain and I be an ideal of E. Then let B be a set of generators for I; if $\max_{x \in B} \delta(x) = 0$ then every $x \in B$ is a unit (i.e. it is an invertible element of the ring), therefore $I = E$. Now, suppose such a maximum does not exist, since for every $x \in E$, $\delta(x) \in \mathbb{Z}_{\geq 0}$, there exists $\min_{x \in B} \delta(x) = \delta(\bar{b}^{(1)})$, $\bar{b}^{(1)} \in B$. Since B is a euclidean domain we know that for every $b \in B$, there exist $q_b, r_b \in R$ such that $b = q_b \bar{b}^{(1)} + r_b$ and either $\delta(r_b) < \delta(\bar{b}^{(1)})$ or $r_b = 0$; thus we can define $B^{(1)} := \{\text{nonzero } r_b, b \in B \setminus \{\bar{b}^{(1)}\}\} \cup \{\bar{b}^{(1)}\}$. Notice that $\max_{x \in B^{(1)}} \delta(x) = \delta(\bar{b}^{(1)})$ and that $B^{(1)}$ is still a generating set for I. Moreover, if $B^{(1)} \setminus \{\bar{b}^{(1)}\}$ is not the empty set, then $\min_{x \in B^{(1)} \setminus \{\bar{b}^{(1)}\}} \delta(x) < \delta(\bar{b}^{(1)})$ otherwise we have $I = (\bar{b}^{(1)})$. We can iterate this process until we end up with either $B^{(n)} = \{\bar{b}^{(n)}\}$ or $\max_{x \in B^{(n)}} \delta(x) = 0$. □

Example 0.0.9. Let $\mathbb{K}$ be a field. Then $\mathbb{K}[X]$ is a euclidean domain with $\delta(f) := deg(f)$, for every $f \in \mathbb{K}[X]^*$.

Definition 0.0.10. *Let G, H be two groups, and $\varphi : G \to Aut(H)$ a homomorphism; we define the* (**outer**) **semidirect product** *of G and H with respect to φ, as the group $G \ltimes_\varphi H$ (or $H \rtimes_\varphi G$) with underlying set $H \times G$ and group multiplication law $(h, g) * (h', g') := (h\varphi(g)(h'), gg')$.*

Example 0.0.11. Let $\mathbb{Z}_2$ acting on $\mathbb{Z}_n$ by the action $\varphi([1]_2)([m]_n) := [-m]_n$; then $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n \cong D_n$, the n^{th} dihedral group.

Definition 0.0.12. *A* **category** $\mathcal{C}$ *consists of:*

- *a collection $Ob_\mathcal{C}$ of* **objects***;*

- *for any pair X, Y of objects, a collection $Hom_{\mathcal{C}}(X, Y)$ of* **morphisms** *from X to Y;*

- *for any pair of morphisms f in $Hom_{\mathcal{C}}(X, Y)$ and $g \in Hom_{\mathcal{C}}(Y, Z)$, a morphism $g \circ f$ in $Hom_{\mathcal{C}}(X, Z)$, called the* **composite** *of f and g;*

- *for any object X, a morphism $id_X \in Hom_{\mathcal{C}}(X, X)$, called the* **identity morphism** *on X;*

such that the following properties are satisfied:

- *for each quadruple X, Y, Z, W of objects, if $f \in Hom_{\mathcal{C}}(X, Y), g \in Hom_{\mathcal{C}}(Z, X), h \in Hom_{\mathcal{C}}(W, Z)$, then $(f \circ g) \circ h = f \circ (g \circ h)$;*

- *for each pair X, Y of objects, if $f \in Hom_{\mathcal{C}}(X, Y)$, then $id_Y \circ f = f = f \circ id_X$.*

We can, moreover, define the **opposite category** *of $\mathcal{C}$ as the category $\mathcal{C}^{op}$ such that $Ob_{\mathcal{C}^{op}} := Ob_{\mathcal{C}}$ and for any X, Y objects $Hom_{\mathcal{C}^{op}}(X, Y) := Hom_{\mathcal{C}}(Y, X)$.*

Example 0.0.13.

- Grp is the category of groups: Ob_{Grp} is the collection of all groups and for any $X, Y \in Ob_{Grp}$, $Hom_{Grp}(X, Y)$ is the set of all group homomorphisms from X to Y.

- Similarly to Grp we can build: Ab, the category of all abelian groups, Ring, the category of all rings, Field, the category of all fields and Set, the category of all sets.

- Let $R \in Ob_{Ring}$, then the left R-modules form the category $RMod$.

- Every group G can be considered as a category with a single object whose morphisms are the elements of G: in this case $Ob_G = \{g\}$ and $Hom(g, g) := G$ (as a group).

Definition 0.0.14. *A* (**covariant**) **functor** F *from a category* $\mathcal{C}$ *to a category* $\mathcal{D}$ *is a map sending each object* $X \in Ob_{\mathcal{C}}$ *to an object* $F(X) \in Ob_{\mathcal{D}}$ *and each morphism* $f \in Hom_{\mathcal{C}}(X, Y)$ *to a morphism* $F(f) : Hom(F(X), F(Y))$, *such that* F *preserves composition* ($F(f \circ g) = F(f) \circ F(g)$) *and identity morphisms* (*for any object* $X \in Ob_{\mathcal{C}}$, $F(id_X) = id_{F(X)}$). *We can also define a* **contravariant functor** *from* $\mathcal{C}$ *to* $\mathcal{D}$ *as a functor from* $\mathcal{C}^{op}$ *to* $\mathcal{D}$.

We will denote a functor F from the category $\mathcal{C}$ to $\mathcal{D}$, $F : \mathcal{C} \to \mathcal{D}$, indeed a functor is a sort of "homomorphism" of categories.

Example 0.0.15.

- We can define a (covariant) functor $\mathcal{P} : Set \to Set$ called the "power set functor" which maps each set I to its power set $\mathcal{P}(I) := \{U \in Set |\ U \subseteq I\}$ and each function $f \in Hom_{Set}(A, B)$ to the map $\mathcal{P}(f) \in Hom_{Set}(\mathcal{P}(A), \mathcal{B})$ such that $\mathcal{P}(f)(U) := f(U)$, for every $U \in \mathcal{P}(X)$.

- Let $B \in Ob_{RMod}$, then we can define the contravariant functor F_B from $RMod$ to $RMod$, where for every $A \in Ob_{RMod}$, $F_B(A) := Hom_{RMod}(A, B) \in RMod$ and $F_B(f)(g) := g \circ f$ for every $A, C \in Ob_{RMod}$, for every $f \in Hom_{RMod}(A, C)$.

- Let G, H be two groups understood as categories as above and $\phi \in Hom_{Grp}(G, H)$, then we can define a functor $\bar{\phi}$ with: $\bar{\phi}(g) := h$ and for every $f \in Hom(g, g)$, $\bar{\phi}(f) := \phi(f)$; this functor is both covariant and contravariant;

Definition 0.0.16. *Let $\mathcal{C}, \mathcal{D}$ two categories and $F, G : \mathcal{C} \to \mathcal{D}$ two functors: we define a* **natural transformation** *between F and G $\phi : F \Rightarrow G$ as a set of maps $\{\phi_A \in Hom_{\mathcal{D}}(F(A), G(A)) |\ A \in Ob_{\mathcal{C}}\}$ such that for every $A, B \in Ob_{\mathcal{C}}$, the diagram:*

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ \downarrow{\scriptstyle \phi_A} & & \downarrow{\scriptstyle \phi_B} \\ G(A) & \xrightarrow{G(f)} & G(B) \end{array}$$

commutes for every $f \in Hom(A, B)$. Furthermore, if for every $A \in Ob_{\mathcal{C}}$ ϕ_A is an isomorphism, then we say that F and G are **naturally isomorphic**.

Chapter 1

Structure theorem for finitely generated modules over a Principal Ideal Domain

Before moving on to the general case of a module over a PID, we will first consider the special case of abelian groups.

1.1 Structure theorem for finitely generated abelian groups

The concepts of **abelian group** and $\mathbb{Z}$-**module** are the same.

Definition 1.1.1. *A ring R is said to be* **noetherian** *if every ideal of R is finitely generated.*

Example 1.1.2.

- By definition a PID (and so a euclidean domain) is a noetherian ring;
- If R is a noetherian ring then so is the polynomial ring $R[x]$, in-

deed: let I be an infinitely generated ideal in $R[x]$ and take a sequence $(p_n)_{n\in\mathbb{Z}_{>0}} \in I$ with the property that f_n is of smallest degree in $I \setminus (p_1, \dots, p_{n-1})$. Moreover, we define $d_n := deg(p_n)$ (notice that $(d_n)_{n\in\mathbb{Z}_{>0}}$ is an increasing sequence) and $(a_n)_{n\in\mathbb{Z}_{>0}} \in R$ where a_n is the leading coefficient of p_n. Let $I_n := (a_1, \dots, a_{n-1})$, since the sequence $(I_n)_{n\in\mathbb{Z}_{>0}}$ is ascending, $I_\infty := \bigcup_{n=1}^{\infty} I_n$ is an ideal. Since R is noetherian, I_∞ is finitely generated with generators all belonging to I_m for some m. Thus $I_\infty = I_m$ and in particular $a_m \in I_m$. Therefore, we have $a_m = a_1b_1 + \dots + a_{m-1}b_{m-1}$ for some $b_1, \dots, b_{m-1}$ in R. Now define $q := p_m - \sum_{i=1}^{m-1} b_i x^{d_m - d_i} p_i \in I \setminus (p_1, \dots, p_{m-1})$, then $deg(q) < d_m$, which is a contradiction;

- Let $\mathbb{K}$ be a field, then the ring $R_n := \mathbb{K}[X_1, \dots, X_n]$, is a noetherian ring, indeed, since $R_n \cong \mathbb{K}[X_1, \dots, X_{n-1}][X_n] =: R_{n-1}[X_n]$ we can conclude by induction on n (for $n = 1$, R_1 is a PID); moreover for every $n > 1$ R_n is not a PID;

- Let $\mathbb{K}$ be a number field, then the set $\mathcal{O}_\mathbb{K} := \{x \in \mathbb{K} \mid$ there exists $p \in \mathbb{Z}[X]$ such that $p(x) = 0$ and p is monic$\}$ (the set of algebraic integers over the field $\mathbb{K}$) is not a noetherian ring, indeed the ideal $(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$ is not finitely generated, othewise $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots$ should all be in a finite field extension of $\mathbb{Q}$.

Definition 1.1.3. *Let R be a commutative ring. We say that an R-module is* **noetherian** *if each of its submodules is finitely generated.*

Theorem 1.1.4. *Let R be a noetherian ring, then every finitely generated R-module is noetherian.*

Proof. For the moment, let us assume that the statement holds for the free module R^n, for every n and let M be an R-module generated by n generators. Then there exists a surjective morphism $f : R^n \twoheadrightarrow M$; let N be a submodule of M, then there exists a submodule A of R^n such that $f(A) = N$, and since A is finitely generated, also N is finitely generated. We now need to prove the statement for every free module R^n; we will argue by induction on n:

- the case $n = 1$ is clearly true since the ideals of R are precisely its submodules and they are finitely generated since R is noetherian;
- let us suppose, by induction, that every submodule of R^{n-1} is finitely generated. We know that $R^n \cong R \oplus R^{n-1}$ (here we identify R and R^{n-1} as submodules of R^n), then let us define π_1 as the projection onto the first summand. Let us consider a submodule A of R^n and a set of generators $\{a_k\}_{k\in I}$ for A (where I is a generic set of indeces). Then, since R is noetherian, the ideal generated by $\{\pi_1(a_k)\}_{k\in I} \subset R$ is finitely generated, hence there exist $r_1, \dots, r_m \in R$ such that $(r_1, \dots, r_m) = (\pi_1(a_k),\ k \in I)$. For each r_i we can choose an element b_i in $\pi_1^{-1}(r_i) \cap A$; in this way for every element a in A, there exist $\alpha_1, \dots, \alpha_m \in A$ such that $a - \sum_{i=1}^{m} \alpha_i b_i \in \ker(\pi_1) \cap A$. Finally, by induction, since $\ker(\pi_1) \cong R^{n-1}$, $\ker(\pi_1) \cap A$ has to be finitely generated; therefore, let $\{b_{m+1}, \dots, b_{m+h}\}$ be a set of generators for $\ker(\pi_1) \cap A$, we have that A is generated by $\{b_1, \dots, b_{m+h}\}$.

□

Remark 1.1.5. The main idea in the proof of Theorem 1.1.4 can be gener-

alized to prove that if the module M has a submodule N such that N and M/N are noetherian, then M is noetherian.

Theorem 1.1.6. *Let $A \in M_{n\times m}(R)$ where R is an euclidean domain with euclidean valuation function δ. Then there exist $Q \in GL_n(R), P \in GL_m(R)$ such that $\mathcal{A} = QAP^{-1}$ is a diagonal matrix:*

$$\begin{bmatrix} \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_k \end{bmatrix} & \\ & 0 \end{bmatrix}$$

for some $k \in \mathbb{N}$, where for every $i \leq k$, $d_i \neq 0$ and $d_1 \mid d_2 \mid \ldots \mid d_k$, and $0 \in M_{(n-k)\times(m-k)}(R)$.

Proof. Our goal is to use elementary operations (like in the Gaussian elimination) in order to reduce the matrix A to the simpler form: $\begin{pmatrix} d_1 & 0 \\ 0 & B \end{pmatrix}$, where d_1 divides every element of B. Then we will proceed by induction on n. The procedure is divided into three steps:

1. We move one minimal (in the sense of δ) element of A in the first entry;

2. We choose a nonzero element a_{i1} in the first column with $i \neq 1$ (if any); then there exist $r, q \in R$ with $a_{i1} = a_{11}q + r$ and $r = 0 \vee \delta(r) < \delta(a_{11})$, then we replace the i^{th} row with the difference between it and q times the first row; at this point $a_{i1} = r$. Therefore, if $r \neq 0$ we can apply step (1) and move r to a_{11}.

Now, there can be a nonzero element a_{1j} such that $\delta(a_{1j}) < \delta(a_{11})$, so by repeating (1) and (2) (and its analogous for the first row) a finite number of times we can suppose that a_{11} is the only nonzero element in the first row/column; but it may happen that a_{11} does not divide every other element of the matrix.

3. Now, if a_{ij} isn't divided by a_{11} for some $i, j \geq 2$, we can sum the j^{th} column of the matrix to the first; then $a_{i1} = a_{ij}$ for $i > 1$, therefore we can reiterate the steps (2) and (1) which will produce a smaller element in a_{11}.

After a finite number of steps, we arrive to a matrix of the desired form. □

The matrix $\mathcal{A}$ in the previous theorem is said to be the **Smith normal form** (**SNF**) of the matrix A.

Definition 1.1.7. *Let $\mathcal{M}$ be a finitely generated free R-module of rank n and let W be any submodule of $\mathcal{M}$ of rank m. If $v_1, \ldots, v_n$ is a basis of $\mathcal{M}$ and $d_1, \ldots, d_m \in R \setminus \{0\}$ are such that $d_1 v_1, \ldots, d_m v_m$ is a basis of W, then we call such a pair of bases of $\mathcal{M}$ and W* **aligned**.

Definition 1.1.8. *Let R be a PID and $\mathcal{M}$ a finitely generated R-module; let $B \in M_{n\times m}(R)$, we say that B is a* **presentation matrix** *of $\mathcal{M}$ (or equivalently, that B* **presents** *$\mathcal{M}$) if there exists $\phi : R^n \to \mathcal{M}$, a surjective homomorphism, such that $ker(\phi)$ is generated by the columns of B.*

Example 1.1.9. 1. $\begin{pmatrix} -2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ presents $\mathbb{Z}/2 \oplus \mathbb{Z}/3 \oplus \mathbb{Z} \oplus \mathbb{Z}/4$;

2. $\mathbb{Z}$ is presented by $\begin{pmatrix} 1 & -1 \\ 1 & 0 \\ 1 & 2 \end{pmatrix}$ with $\phi : \mathbb{Z}^3 \to \mathbb{Z}$, $\phi(x, y, z) := z + 2x - 3y$.

Remark 1.1.10. From the First Isomorphism Theorem follows $\mathcal{M} \cong R^n / BR^m$.

Now, we want to show that for modules over PIDs any presentation matrix can be equivalently replaced by a diagonal one. For that purpose we need two kinds of transformation of the presentation matrix: replacing relations (null linear combinations) with equivalent ones and change of basis.

Proposition 1.1.11. *Let A be an $m \times n$ presentation matrix of the R-module $\mathcal{M}$. If one of the following holds:*

1. *$\mathcal{A} = QAP^{-1}$, where $Q \in GL_m(R)$ and $P \in GL_n(R)$;*
2. *$\mathcal{A}$ is obtained from A deleting a zero column;*
3. *the j-th column of A is e_i and $\mathcal{A}$ is obtained from A deleting the j-th column and the i-th row;*

then $\mathcal{A}$ and A present the same module.

Proof.

1. $\mathcal{A}$ is obtained from A through a change of basis in R^m and R^n and this does not change the isomorphism class of the quotient R^m / AR^n.
2. A zero column corresponds to the equation $0v_1 + \cdots + 0v_n = 0$ which is trivial and can be omitted.
3. If the j-th column of A is e_i, then we have the equation $v_i = 0$. Hence we can remove v_i from the set of generators. This operation corresponds

to the elimination of the i-th row. Finally, we end up with the j-th column being null, so we can remove it.

□

Notice that in particular, 1.1.11 and 1.1.6 imply that we can consistently diagonalise a presentation matrix in such a way it still presents the same module (eventually respect to another set of generators).

Theorem 1.1.12. *Let G be a free abelian group with $\mathbf{rk}G = n$ and let $S \leq G$. Then there exists a pair of aligned bases $v_1, \ldots, v_n$ and $d_1v_1, \ldots, d_mv_m$ respectively of G and S, such that $d_1 \mid d_2 \mid \ldots \mid d_m$.*

Proof. We start considering a basis $B = \{v_1, \ldots, v_n\}$ of G and a set $\{u_1, \ldots, u_m\}$ of generators for S (notice that this set can be taken with finitely many elements because of 1.1.4). Now we have a matrix A which presents S and by Theorem 1.1.6 we can reduce it to a diagonal matrix $\mathcal{A}$, which presents S respect to a new basis $B' = \{v'_1, \ldots, v'_n\}$ of G and a new set of generators $\{u'_1, \ldots, u'_m\}$ for S such that for every $i \leq \min(m, n)$, $u'_i = d_iv'_i$, for some $d_1, \ldots, d_{min(n,m)} \in \mathbb{Z}^*$. Now, it could be $m > n$, but since $\mathcal{A}$ is diagonal there would be at least $m - n$ zero columns and we can remove them (they correspond to the equations $u'_k = 0$). Finally, we must prove that B' is linearly independent: let us take a generic linear combination $0 = a_1u'_1 + \cdots + a_mu'_m = a_1d_1v'_1 + \cdots + a_md_mv'_m$, then $a_1d_1 = \cdots = a_md_m = 0$ and since for every $i \leq n$, $d_i \neq 0$, it has to be $a_1 = \cdots = a_m = 0$. □

Remark 1.1.13. In the proof, we used the convention $Span\{\varnothing\} = \{0\}$.

Theorem 1.1.14 (Structure Theorem for finitely generated abelian groups)**.** *Let G be a finitely generated abelian group. Then G is the direct sum of*

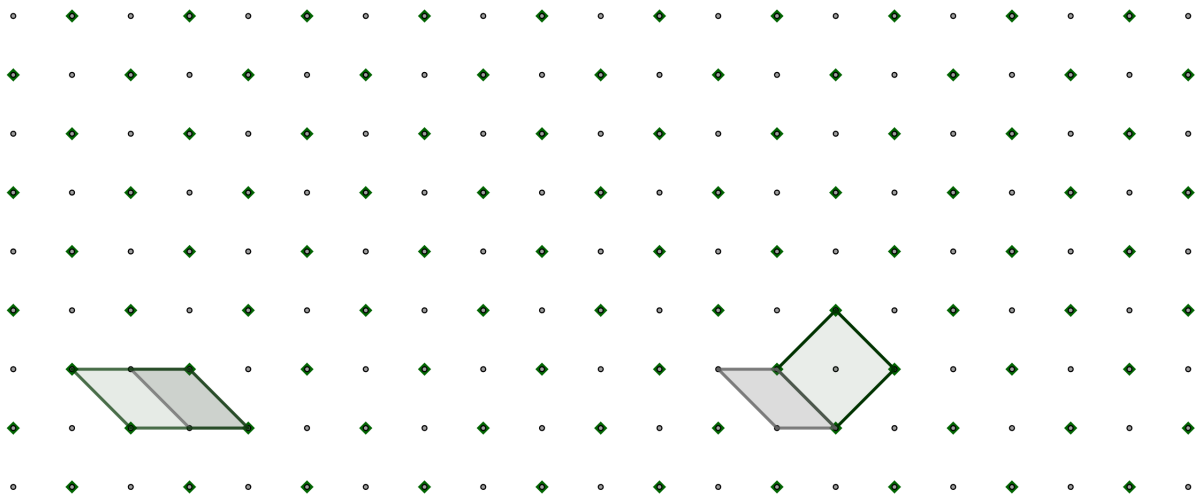


Figure 1.1: On the left, a pair of aligned bases, the given matrix is $\begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix}$; on the right, two non-aligned bases, the given matrix is $\begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix}$.

finite cyclic subgroups $C_{d_1} \oplus \cdots \oplus C_{d_k}$ *(where* d_i *is the order of* C_{d_i}*) and a free abelian group* L*:*

$$\mathcal{V} = C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L \tag{1.1}$$

Moreover for every $i \leq k$*,* $d_i > 1$ *and* $d_1 \mid d_2 \mid \ldots \mid d_k$*.*

Proof. Since $\mathbb{Z}$ is a noetherian ring and G is a finitely generated module over $\mathbb{Z}$, for every set of generators and for every set of relations there exists a presentation matrix that can be reduced to a diagonal matrix:

$$\mathcal{A} := \left[\begin{array}{cccc} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_k \\ \hline & & 0 & \end{array}\right] \in \mathbb{Z}^{n \times k} \tag{1.2}$$

where for every $i \leq k$, $d_i > 1$ and $d_1 \mid d_2 \mid \ldots \mid d_k$.
Therefore $\mathcal{A}$ gives us the following:

$$d_1 v_1 = 0\,,\ d_2 v_2 = 0\,,\ \ldots\ ,\ d_k v_k = 0 \tag{1.3}$$

for some $v_1, \ldots, v_n$ generators of G. Since $\mathcal{A}$ is a presentation matrix for G, every relation between $v_1, \ldots, v_n$ must be a linear combination of relations (1.3) and this implies that $v_{k+1}, \ldots, v_n$ are not involved in any such relation. Therefore, the submodule generated by $v_{k+1}, \ldots, v_n$ has to be free of dimension $n - k$; let us denote it by L.
Let us denote by C_i the subgroup generated by v_i, for every $i \leq k$; we want to show that $G = C_1 \oplus \cdots \oplus C_k \oplus L$ and that d_i is the order of C_i, for every i. It is clear that $G = (C_1 + \cdots + C_k) \oplus L$; moreover, for every $j \leq k$, C_j has clearly order d_j, indeed since $d_j v_j = 0$, we have $|C_j| \leq d_j$, but if $|C_j| < d_j$, there would be an integer $d'_j < d_j$ such that $d'_j v_j = 0$ and this can not be a linear combination of (1.3). Let us take a generic relation $a_1 v_1 + \cdots + a_n v_k = 0$, then this relation must be a linear combination of the columns of $\mathcal{A}$, therefore for every $j \leq k$, $d_j \,|\, a_j$ and so the relation $a_1 v_1 + \cdots + a_n v_k = 0$ is trivial. □

Example 1.1.15. Let us suppose $(\mathbb{Q}, +)$ is finitely generated. Due to Theorem 1.1.14, there exist $m, n \geq 0$ and $d_1 | \ldots | d_m$ with $d_i > 1$ such that $\mathbb{Q} \cong C_{d_1} \oplus \cdots \oplus C_{d_m} \oplus \mathbb{Z}^n$. If $m \geq 1$, then there exists $x \in \mathbb{Q}^*$, such that $d_1 x = 0$ and this is impossible impossible because $\mathbb{Q}$ is a domain. Thus we get $m = 0$ and $\mathbb{Q} \cong \mathbb{Z}^n$. If $n \geq 2$, then there exist $x, y \in \mathbb{Q}^*$ which are linearly independent over $\mathbb{Z}$. But if $x = p/q$ and $y = r/s$, with $p, q, r, s \in \mathbb{Z}$, we have $(qr)x + (-sp)y = 0$, which is a contradiction. So $\mathbb{Q}$ must be cyclic.

Let us suppose that it is generated by a/b with $a, b \in \mathbb{Z}$, $b > 1$. Then $b+1$ can not be written as ka/b for some $k \in \mathbb{Z}$, and again we get a contradiction.

Remark 1.1.16. Using the Chinese Reminder Theorem (CRT) we can go further and split every C_{d_i} in a direct sum of prime-power order cyclic subgroups $C_{d_i} \cong C_{p_{i,1}^{k_1}} \oplus \cdots \oplus C_{p_{i,m_i}^{k m_i}}$.

Theorem 1.1.17 (Uniqueness of cyclic decompositions)**.** *Let G be a finite abelian group.*

a) If $G \cong C_{d_1} \oplus \cdots \oplus C_{d_k} \cong C_{d'_1} \oplus \cdots \oplus C_{d'_{k'}}$ with d_i, $d'_j > 1$, $d_i \mid d_{i+1}$ and $d'_j \mid d'_{j+1}$ for every $i < k$, for every $j < k'$, then $k = k'$ and for every $i \leq k$, $d_i = d'_i$. $C_{d_1}, \ldots, C_{d_k}$ are called **invariant factors** *of G.*

b) The same result holds for the prime-power order cyclic groups decomposition; the orders of such groups are called **elementary divisors** *of G.*

Proof. We will show only part (a) of the proof: let f be an automorphism of G and let $v_1, \ldots, v_k$, $v'_1, \ldots, v'_{k'}$ be the generators respectively of the two decompositions of G, then $f(d_{k'} v_k) = d_{k'}(a_1 v'_1 + \cdots + a_{k'} v'_{k'}) = 0 \iff d_{k'} v_k = 0 \Rightarrow d_k \mid d_{k'}$. Similarly $d_{k'} \mid d_k$, therefore $d_{k'} = d_k$. Finally, we can conclude by induction considering the quotient group G/C_{d_k}. □

Remark 1.1.18. If G is a finite abelian p-group of order p^n then $G \cong C_{p^{n_1}} \oplus \cdots \oplus C_{p^{n_k}}$ with $n_1 + \cdots + n_k = n$, and G is determined up to isomorphism by the exponents $n_1, \ldots, n_k$, ignoring their order. Therefore the number of abelian groups of order $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$, up to isomorphisms, equals the product of the numbers of ways k_i can be written as a sum of positive integers (ignoring their order).

Remark 1.1.19 (Reverse Lagrange Theorem). If G is a finite abelian group of order n, for every $k \in \mathbb{N}$, such that $k \mid n$ then there exists $H \leq G$ of order k.

1.2 Structure theorem for finitely generated modules over a Principal Ideal Domain

Theorem 1.2.1. *Let A be a PID. Every finitely generated A-module has the form $F \bigoplus T$ where F is a finite free A-module and T is a finitely generated torsion A-module. Moreover, there exist $a_1, \ldots, a_m \in A^*$ such that $T \cong \bigoplus_{j=1}^{m} A/(a_j)$ and $a_1 \mid a_2 \mid \ldots \mid a_m$.*

We will provide two different proofs of Theorem 1.2.1.
The first is based on the existence of a pair of aligned bases for a finite free module and one of its submodules in a very similar way as for finite free abelian groups.

Definition 1.2.2. *Let A be a ring and M an A-module. Then we define the* **dual module** *of M as $M^\vee := Hom_A(M, A)$, where for every $f, g \in Hom_A(M, A)$, $(f + g)(m) := f(m) + g(m)$ for every $m \in M$ and $(a * f)(m) := af(m)$.*

Notice that if $\phi \in M^\vee$ and M' is a submodule of M, then $\phi(M')$ is a submodule of A, that is, it is an ideal of A.

Theorem 1.2.3. *Let A be a PID, then every pair consisting of a finite free A-module M and a submodule M' of M admits a pair of aligned bases.*

Proof. We divide the proof into five steps:

1. $S := \{\phi(M'),\ \phi \in M^\vee\}$ is not zero and has a maximal (respect to inclusion) member $(a_1) = \psi(M')$;

2. for all $\phi \in M^\vee$, $a_1 \mid \phi(v')$, where $v' \in M'$ is such that $\psi(v') = a_1$;

3. there exists an element $e_1 \in M$ such that $\psi(e_1) = 1$;

4. $M = Ae_1 \oplus \ker(\psi)$ and $M' = Aa_1e_1 \oplus (M' \cap \ker(\psi))$.

Finally, since $\ker(\psi)$ is free and $M' \cap \ker(\psi)$ is a submodule of $\ker(\psi)$ we will conclude by induction on the cardinality of the basis.
Let $B = \{v_1, \ldots, v_n\}$ be a basis of M, then since $ann(M') \neq \{0\}$ there exists an element in the dual basis $B^\vee$ of B, say $v_i^\vee$, which is not identically zero on M', so $S \neq \{0\}$; A is a PID then every nonzero ideal of A is contained only in finitely many ideals of A (indeed, up to unit multiples, every element of A has only a finite number of divisors) therefore S contains a maximal element with respect to inclusion $(a_1) = \psi(M')$. Let v' be an element of M' such that $\psi(v') = a_1$; let us take the ideal $(a_1,\ \phi(v'))$ for some $\phi \in M^\vee$, then since A is a PID $(a_1,\ \phi(v')) = (b)$ for some $b \in A$ and in particular there exist $x, y \in A$ such that $xa_1 + y\phi(v') = b$, but $\psi(v') = a_1$ therefore $b = (x\psi + y\phi)(v')$; this implies that $(a_1) \subseteq (b) \subseteq (x\psi + y\phi)(M')$ hence, by the maximality of (a_1), $(a_1) = (b) = (x\psi + y\phi)(M')$, so $\phi(v') \in (a_1)$.
Now, suppose we have $v' = c_1v_1 + \cdots + c_nv_n$, then $a_1 | c_i$ for every $i \leq n$, indeed $c_i = v_i^\vee(v')$, therefore there exist $b_1, \ldots, b_n \in A$ such that $v' = a_1(b_1v_1 + \cdots + b_nv_n)$; we define $e_1 := b_1v_1 + \cdots + b_nv_n$, hence $v' = a_1e_1$. It is easy to see that $\psi(e_1) = 1$: $a_1 = \psi(v') = \psi(a_1e_1) = a_1\psi(e_1)$, and since $a_1 \neq 0$, $\psi(e_1) = 1$.
For each $v \in M$ we have $v - \psi(v)e_1 \in \ker(\psi)$, moreover $\psi(\alpha e_1) = \alpha$, thus

$Ae_1 \cap \ker(\psi) = \{0\}$ and therefore $M = Ae_1 \oplus \ker(\psi)$; moreover for every $v \in M'$, there exist $b_v \in A$ such that $a_1 b_v = \psi(v)$, hence $v - b_v v' \in M' \cap \ker(\psi)$ and since $v' = a_1 e_1$ we get $M' = Aa_1 e_1 \oplus (M' \cap \ker(\psi))$. □

Remark 1.2.4. Under the hypoteses of Theorem 1.2.3 we can rearrange $a_1, \ldots, a_n$ in such a way that $a_1 \,|\, a_2 \,|\, \ldots \,|\, a_n$; let us see how: if we set $\phi = e_1^\vee + e_2^\vee$ then $a_1 = \phi(v') \in \phi(M')$, so $(a_1) \subseteq \phi(M')$, thus by the maximality of (a_1), $(a_1) = \phi(M')$. Then $a_2 = \phi(a_2 e_2) \in \phi(M') = (a_1)$, so $a_1 \,|\, a_2$; finally by induction we obtain $a_1 \,|\, a_2 \,|\, \ldots \,|\, a_n$.

Now we are ready to give the first proof of the structure theorem:

First proof of Theorem 1.2.1. Let M be a finitely generated A-module, with generators $x_1, \ldots, x_n$. Define $f : A^n \twoheadrightarrow M$ by $f(e_i) = x_i$; f is a surjective linear map therefore M is isomorphic to the quotient $A^n/\ker(f)$. Now, using a pair of aligned bases as in Theorem 1.2.3 and Remark 1.2.4 for A^n and $\ker(f)$, we can write $A^n = \bigoplus_{i=1}^n Av_i$ and $\ker(f) = \bigoplus_{i=1}^m Aa_i v_i$ for some $m \leq n$ and $a_1, \ldots, a_m \in A^*$, with $a_1 \,|\, a_2 \,|\, \ldots \,|\, a_m$. Thus, $M \cong A^n/\ker(f) \cong (\bigoplus_{j=1}^m A/(a_j)) \oplus A^{n-m}$. □

Definition 1.2.5. *Let A be a PID, $a_1, a_2 \in A^*$; we say that $d \in A$ is a* **greatest common divisor** *of a_1 and a_2, and write $d = gcd(a_1, a_2)$, if:*

- *$d \,|\, a_1$, $d \,|\, a_2$;*
- *for every $d' \in A^*$ such that $d' \,|\, a_1$ and $d' \,|\, a_2$, $d' \,|\, d$.*

Remark 1.2.6.

- The notation $d = gcd(a_1, a_2)$ is an abuse. Indeed the greatest common divisor is unique up to unit (i.e. an invertible element) multiplication.

- For every element $a \in A$: $gcd(a, 0) = a$.
- (Bézout's lemma) Let A be a PID, then for every $a, b \in A$, $(a, b) = (gcd(a, b))$.

Lemma 1.2.7. *Let A be a PID and let $r_1, \dots, r_n$, $n \geq 2$, be relatively prime elements of A. Then there is a matrix $B \in GL_n(A)$ which has $(r_1 \dots r_n)$ as its first row.*

Proof. The case $n = 2$ is trivial: $gcd(r_1, r_2) = 1$, so there exist $u, v \in A$ such that $ur_1 - vr_2 = 1$ then we can just set $B = \begin{pmatrix} r_1 & r_2 \\ v & u \end{pmatrix}$ and we are done. Let $d := gcd(r_2, \dots, r_n)$, then there exist $p_2, \dots, p_n \in A$, relatively prime, such that for every $i \geq 2$, $r_i = dp_i$; by induction on n, there exist $B_0 \in GL_{n-1}(A)$ with $(p_2, \dots, p_n)$ as its first row. Since $r_1, \dots, r_n$ are relatively prime, also r_1 and d are relatively prime, therefore there exist $u, v \in A$ such that $ur_1 - vd = \det(B_0)^{-1}$. Now, let us consider the matrices B_0', obtained from B_0 multiplying the first row by u, and

$$B := \begin{pmatrix} r_1 & r_2 & \dots & r_n \\ v & & & \\ 0 & & B_0' & \\ \vdots & & & \\ 0 & & & \end{pmatrix} = \begin{pmatrix} r_1 & dp_2 & \dots & dp_n \\ v & & & \\ 0 & \begin{pmatrix} u & & \\ & I_{n-2} & \end{pmatrix} B_0 & & \\ \vdots & & & \\ 0 & & & \end{pmatrix};$$

thus we have $\det(B) = r_1 u \det B_0 - vd \det B_0 = (r_1 u - vd) \det B_0 = 1$. □

Lemma 1.2.8. *Let A be a PID, let $r_1, \dots, r_n$ be relatively prime elements of A, and let M be a finitely generated A-module. If $\{x_1, \dots, x_n\}$ is a set of generators for M, then there is also a set of generators $\{y_1, \dots, y_n\}$ for M such that $y_1 = r_1 x_1 + \dots + r_n x_n$.*

Proof. By the Lemma 1.2.7 we know that there exists $B \in GL_n(A)$ such that $(r_1 \dots r_n)$ is its first row; then let us consider the image $(y_1 \dots y_n)$ of $(x_1 \dots x_n)$ by B. Then every x_i is a linear combination of $y_1, \dots, y_n$ (so it is a system of generators for M) and in particular $y_1 = r_1x_1 + \dots + r_nx_n$. □

Remark 1.2.9. Let A be a PID and M be an A-module; let $f : A \to M$, $f(a) := ax$, where we have fixed $x \in M$. Then $\mathrm{Im}(f) = Ax$ and $\ker(f) = ann(x) =: (\bar{a})$, so $Ax \cong A/(\bar{a})$.

Definition 1.2.10. *Let A be a PID. We say that two elements $a, b \in A$ are* **associate** *if there exists a unit $u \in A$ such that $b = ua$.*

Second proof of Theorem 1.2.1. Let us suppose that M is generated by n but not by $n-1$ generators; the case $n = 1$ is trivial, so let us suppose $n \geq 2$. Then we can choose a set of generators $\{x_1, \dots, x_n\}$ in such a way that the annihilator of x_1 is generated by an element d with a minimal number of prime factors (counted with multiplicity); our goal is to show that $M = (Ax_1) \oplus (Ax_2 + \dots + Ax_n)$ and then proceed by induction on n. Let us take a generic relation $r_1x_1 + \dots + r_nx_n = 0$ and set $g := gcd(r_1, d)$, then there exist $u, v \in A$ such that $ur_1 + vd = g$, thus we have $gx_1 + ur_2x_2 + \dots + ur_nx_n = 0$; let us consider $\gamma := gcd(g, ur_2, \dots, ur_n)$ hence by Lemma 1.2.8 we can take a new set of generators $y_1, \dots, y_n$ such that $y_1 = (g/\gamma)x_1 + \dots + (ur_n/\gamma)x_n$ (the case $\gamma = 0$ is trivial, indeed $\gamma = 0$ implies $g = ur_2 = \dots = ur_n = 0$, so $r_1 = d = 0$). So $\gamma y_1 = 0$; since the pair (x_1, d) is minimal, γ can not have less prime factors than d, but γ divides g which divides d therefore d and γ have the same number of prime factors i.e. they are associate, moreover γ divides r_1 hence also d divides r_1. Thus

in every relation $r_1x_1 + \cdots + r_nx_n = 0$ it is necessary $r_1x_1 = 0$.
Finally, $Ax_2 + \cdots + Ax_n$ is generated by $n-1$ but not by $n-2$ elements (otherwise M would be generated by $n-1$ elements) so we can conclude by induction on n. It is clear that using the CRT and Remark 1.2.9 we obtain the final result $M \cong (\bigoplus_{j=1}^{m} A/(a_j)) \oplus A^{n-m}$ with $a_1 \mid \ldots \mid a_m$. □

Remark 1.2.11. We point out that in the decomposition $M = F \bigoplus T$, where F is a finite free submodule and T is a torsion submodule, F is not uniquely determined; instead, T is unique: indeed, T is the set of all torsion elements in M, indeed let us consider $v = af + bt$, where $f \in F$, $t \in T$ and $a, b \in A$; then for every $c \in A^*$ the condition $cv = 0$ implies $caf = 0$, but $caf = 0$ if and only if $a = 0$ since f is not a torsion element.

Theorem 1.2.12. *Let A be a PID and let $a_1, \ldots, a_n, b_1, \ldots, b_m \in A$ such that $A/(a_1) \oplus \cdots \oplus A/(a_n) \cong A/(b_1) \oplus \cdots \oplus A/(b_m)$ with $a_1 \mid \ldots \mid a_n$ and $b_1 \mid \ldots \mid b_m$, then $n = m$ and for every $i \leq n$, a_i and b_i are associate.*

Proof. Let $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ be two set of generators such that for every $i \leq n$, $ann(x_i) = (a_i)$, and for every $i \leq m$, $ann(y_i) = (b_i)$. Then there exist $c_1, \ldots, c_n \in A$ such that $y_m = c_1x_1 + \cdots + c_nx_n$, hence $a_ny_m = a_nc_1x_1 + \cdots + a_nc_nx_n = 0$, that is, a_n and b_m are respectively elements of $ann(y_m)$ and $ann(x_n)$. Thus a_n and b_m are associate and in particular $A/(a_n) = A/(b_m)$. Then we conclude by induction on the quotient $A/(a_1) \oplus \cdots \oplus A/(a_{n-1}) \cong (A/(a_1) \oplus \cdots \oplus A/(a_n))/(A/(a_n)) \cong (A/(b_1) \oplus \cdots \oplus A/(b_m))/(A/(b_m)) \cong A/(b_1) \oplus \cdots \oplus A/(b_{m-1})$. □

Remark 1.2.13. Due to Theorem 1.2.12, as in the case of finitely generated abelian groups, we can define the *invariant factors* of a finitely generated

module over a PID and its *elementary divisors*.

An interesting application of the structure theorem is the classification of the linear operators of a vector space. Let V be a finite dimensional $\mathbb{K}$-vector space and $T \in End(V)$. We can think of V as a $\mathbb{K}[x]$-module, where the multiplication by a polynomial is defined as $f * v := f(T)(v)$ (notice that $f * T(v) = fx * v = xf * v = T(f * v)$). Since V has finite dimension as a $\mathbb{K}$-vector space, by Cayley-Hamilton Theorem every operator is a root of its characteristic polynomial. Hence, V is a torsion finitely generated $\mathbb{K}[x]$-module (notice that if v is an eigenvector of T with eigenvalue λ, then $(x - \lambda) * v = 0$). Now, using the structure theorem, we can decompose V into the sum of its invariant factors: $V \cong \mathbb{K}[x]/(s_1) \oplus \cdots \oplus \mathbb{K}[x]/(s_m)$ with $s_1 \,|\, s_2 \,|\, \ldots \,|\, s_m$ (moreover, we can choose the representative s_i with leading coefficient $(-1)^{degs_i}$). Each summand $\mathbb{K}[x]/(s_i)$ is cyclic, therefore there exist $v_1, \ldots, v_m \in V$ such that for every $i \leq m$, $\mathbb{K}[x]v_i \cong \mathbb{K}[x]/(s_i)$ and $V = \bigoplus_{i=1}^{m} \mathbb{K}[x]v_i$. In this case, $(s_i) = \{f \in \mathbb{K}[x] |\ f * v_i = 0\}$. Moreover, every summand is a T-invariant $\mathbb{K}$-vector space of dimension $\deg s_i$, since $T(v) = x * v$.

Now, picking bases B_i for each V_i yields a basis B of V in which the matrix $M_B(T)$ is block-diagonal. Let us denote every $M_{B_i}(T_{|V_i})$ by M_i. Notice that for every $i \leq m$, $v_i, x * v_i, \ldots, x^{dimV_i - 1} * v_i$ is a basis of V_i. Indeed, it is clearly a generating set, moreover if there exist $\alpha_0, \ldots, \alpha_{dimV_i - 1} \in \mathbb{K}$ such that $0 = \alpha_0 v_i + \cdots + \alpha_{dimV_i - 1} x^{dimV_i - 1} * v_i$, then $0 = (\alpha_0 + \alpha_1 x + \cdots + \alpha_{dimV_i - 1} x^{dimV_i - 1}) * v_i =: q * v_i$. But $\deg q < \deg s_i$, hence it has to be $q = 0$, that is $\alpha_0 = \cdots = \alpha_{dimV_i - 1} = 0$. Thus, we can choose $B_i := \{v_i, x * v_i, \ldots, x^{dimV_i - 1} * v_i\}$.

With these choices of B_i, the matrices M_i take the form:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -\alpha_0^{(i)} \\ 1 & 0 & \cdots & 0 & -\alpha_1^{(i)} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -\alpha_{degs_i-1}^{(i)} \end{pmatrix}$$

where $\alpha_0^{(i)} + \alpha_1^{(i)}x + \cdots + \alpha_{degs_i-1}^{(i)}x^{degs_i-1} + x^{degs_i} = (-1)^{degs_i}s_i$ (M_i is said to be the **companion matrix** of s_i, indeed its characteristic polynomial is precisely s_i).

The resulting form of $M_B(T)$ is

$$\begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & M_m \end{pmatrix},$$

and it is called the **Rational Canonical Form** (or **Frobenius Normal Form**) of the endomorphism T.

Using the same module structure on V, we can proceed analogously by decomposing V with the elementary divisor decomposition. In this case, we have $V \cong \mathbb{K}[x]/(p_1^{k_1}) \oplus \cdots \oplus \mathbb{K}[x]/(p_n^{k_n})$, where $p_1, \ldots, p_n \in \mathbb{K}[x]$ are irreducible (as before we can suppose the leading coefficient of p_i to be $(-1)^{degp_i}$). As above there exist $v_1, \ldots, v_n \in V$ such that for every $i \leq n$, $V_i := \mathbb{K}[x]v_i \cong \mathbb{K}[x]/(p_i^{k_i})$ and every V_i is T-invariant. Let $d_i :=$degp_i, for every $i \leq n$, then consider $B_i := \{(x^j p_i^l) * v_i\}_{0 \leq j < d_i, 0 \leq l < k_i}$. B_i is clearly a generating set since for every $0 \leq d < d_i k_i$ there is exactly one polynomial

of degree d in B_i. Moreover, as above, B_i is clearly linear independent, thus it is a basis. Notice that $x(x^{d_i-1}p_i^l) = p_i^{l+1} - (a_0 + a_1x + \cdots + a_{d_i-1}x^{d_i-1})p_i^l$, hence $T((x^{d_i-1}p_i^l) * v_i) = (p_i^{l+1} - (a_0 + a_1x + \cdots + a_{d_i-1}x^{d_i-1})p_i^l) * v_i$ and in particular $T((x^{d_i-1}p_i^{k_i-1}) * v_i) = -((a_0 + a_1x + \cdots + a_{d_i-1}x^{d_i-1})p_i^{k_i-1}) * v_i$, where $a_0 + a_1x + \cdots + a_{d_i-1}x^{d_i-1} + x^{d_i} = (-1)^{d_i}p_i$. Therefore, we can write $M_B(T)$ as a block-diagonal matrix, with blocks of the form

$$\begin{pmatrix} D_i & 0 & \cdots & \cdots & 0 \\ Y_i & D_i & 0 & \cdots & \vdots \\ 0 & Y_i & D_i & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & Y_i & D_i \end{pmatrix} \in M_{d_ik_i \times d_ik_i}(\mathbb{K}),$$

where D_i is the companion matrix of the polynomial p_i and $Y_i = e_1e_{d_i}^\top \in M_{d_i \times d_i}(\mathbb{K})$. Finally, if $\mathbb{K}$ is algebraically closed, then for every $i \leq n$, $p_i(x) = \lambda_i - x$ for some $\lambda_i \in \mathbb{K}$. Hence, for every $i \leq n$, $D_i = \lambda_i$ and $Y_i = 1$. Thus, each block is of the form

$$\begin{pmatrix} \lambda_i & 0 & \cdots & \cdots & 0 \\ 1 & \lambda_i & 0 & \cdots & \vdots \\ 0 & 1 & \lambda_i & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & \lambda_i \end{pmatrix} \in M_{k_i \times k_i}(\mathbb{K}).$$

This form of the matrix $M_B(T)$ is called the **Jordan Canonical Form** of T.

Chapter 2

The Jordan-Hölder theorem

The name **Jordan-Hölder theorem** usually refers to a wide class of uniqueness results in abstract algebra and category theory concerning maximal chains of subobjects; they are very useful theorems because they relate the structure of an object to that of simpler ones and serves as a kind of unique factorization theorem. In this chapter, we will focus on representations of algebras and modules and we will state the theorem for these structures.

Definition 2.0.1. *Let $\mathbb{K}$ be a field, we define a* $\mathbb{K}$**-algebra** *A as a $\mathbb{K}$-vector space endowed with a bilinear binary map $\cdot : A \times A \to A$. We say that A is* **associative** *(respectively* **commutative** *and* **unitary***) if $\cdot$ is associative (respectively commutative and unitary). If A and A' are two $\mathbb{K}$-algebras, we define a* **homomorphism** *of $\mathbb{K}$-algebras from A to A' as a map $p : A \to A'$ such that p is a linear map and for every $a, b \in A$, $p(ab) = p(a)p(b)$.*

Remark 2.0.2. An associative algebra is both a vector space and a ring.

Example 2.0.3.
- Every field $\mathbb{K}$ is a $\mathbb{K}$-algebra.

- $\mathbb{K}[x]$ is an infinite dimensional $\mathbb{K}$-algebra.

- $\mathbb{R}^3$ equipped with the vector product $\times$ form a non-associative, anti-commutative $\mathbb{R}$-algebra.

- The space $M_n(\mathbb{K})$ of all $n \times n$ matrices with coefficients in a field $\mathbb{K}$ is an associative, non-commutative algebra (so we can also consider the corresponding structure on $\mathrm{End}(V)$, where V is a finite-dimensional $\mathbb{K}$-vector space).

- The set of self-adjoint matrices over a field with the product $A \cdot B := \frac{1}{2}(AB + BA)$ is a non-associative algebra.

- If G is a group, we can consider the vector space $\mathbb{K}G := \{\sum_{g \in I} a_g g$ such that $I \subseteq G$, $|I| < \infty$ and for every $g \in I$, $a_g \in \mathbb{K}\}$ endowed with the product induced by the product law in G, then $\mathbb{K}G$ is an associative unitary algebra over $\mathbb{K}$ called the **group algebra** of G.

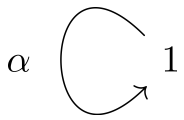
- Let $Q := (V, A)$ be a quiver (where V is the set of vertices and A the set of arrows) and let us consider the set of paths $P_Q := \{a_1 \dots a_n \,|\, n \in \mathbb{N}$ and $s(a_i) = t(a_{i+1})$, $a_i \in A \cup V$, for every $1 \leq i < n\}$; here t is the "target" map i.e. $t(a)$ is the vertex pointed by a and s is the "start" map i.e. s is the map which associates a with its starting vertex; then the vector space $\mathbb{K}Q := \{\sum_{i \leq n} \alpha_i v_i \mid n \in \mathbb{N}, \alpha_i \in \mathbb{K}, v_i \in P_Q$ for every $i \leq n\}$ endowed with the vector product induced by the following

product law in P_Q:

$$p \cdot q := \begin{cases} p \text{ , if } s(p) = q \\ q \text{ , if } p = t(q) \\ pq \text{ , if } s(p) = t(q) \\ 0 \text{ , otherwise} \end{cases} \qquad \forall p, q \in P_Q;$$

in this way $\mathbb{K}Q$ is a $\mathbb{K}$-algebra called the **path algebra** of Q over $\mathbb{K}$, in particular if $|V| < \infty$ then $\mathbb{K}Q$ is unitary, indeed the element $\sum_{p \in V} p$ is the multiplicative identity element.

- Let L be the 1-loop quiver:



then we have $\mathbb{K}L \cong \mathbb{K}[T]$.

Throughout this chapter $\mathbb{K}$ will be a field and, unless specified, A will be an associative and unitary $\mathbb{K}$-algebra.

Definition 2.0.4. *Let V be a $\mathbb{K}$-vector space and $\rho : A \to End(V)$ a homomorphism of algebras, then we say that (V, ρ) is a* **representation** *of A.*

Example 2.0.5.

- If $A = \mathbb{K}$, then every $\mathbb{K}$-vector space V, with $\rho(\lambda)(v) := \lambda v$, $\lambda \in \mathbb{K}$, $v \in V$, is a representation of A;
- every algebra A has the trivial representations ($V = 0$, $\rho = 0$) and ($V = A$, $\rho(a)(v) := av$);
- let us consider the algebra $\mathbb{R}S^1$: then define $\rho : \mathbb{R}S^1 \to \mathrm{End}(\mathbb{R}^2)$, $\rho(e^{i\theta}) := \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$, then $(\mathbb{R}^2, \rho)$ is a representation for $\mathbb{R}S^1$.

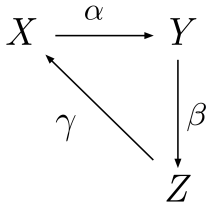
We will usually write V instead of (V, ρ) to denote the representation.

Definition 2.0.6. *Let V be a nonzero representation of A; a subspace $\mathcal{U} \subset V$ which is invariant under the action of $\rho(a)$, for every $a \in A$, is said to be a* **subrepresentation** *of V. Moreover, we say that V is* **irreducible** (*or* **simple**) *if its only subrepresentations are the trivial one and $\mathcal{V}$ itself.*

Example 2.0.7.

- Let us denote by $C_2 := \{e, g\}$, the cyclic group of order 2 and let $\rho : \mathbb{K}C_2 \to \mathrm{End}(\mathbb{K})$, $\rho(\alpha_0 e + \alpha_1 g)(\lambda) := (\alpha_0 + \alpha_1)\lambda$, for $\alpha_0, \alpha_1, \lambda \in \mathbb{K}$; then $(\mathbb{K}, \rho)$ is an irreducible representation of $\mathbb{K}C_2$.

- Let us consider the quiver Q:



  and define $\rho : \mathbb{K}Q \to M_3(\mathbb{K})$ over the generator set $\{X, Y, Z, \alpha, \beta, \gamma\}$:

  - $\rho(X) := e_1 e_1^T$;
  - $\rho(\alpha) := e_2 e_1^T$;
  - $\rho(Y) := e_2 e_2^T$;
  - $\rho(\beta) := e_3 e_2^T$;
  - $\rho(Z) := e_3 e_3^T$;
  - $\rho(\gamma) := e_1 e_3^T$;

  then $(\mathbb{K}^3, M_C^{-1} \circ \rho)$ is an irreducible representation of $\mathbb{K}Q$. Indeed, let U be a subrepresentation of Q and let $0 \neq v \in U$. Then it must be either $\rho(X)v \neq 0$ or $\rho(Y)v \neq 0$ or $\rho(Z)v \neq 0$, that is, either $e_1 \in U$ or $e_2 \in U$ or $e_3 \in U$. Without loss of generality, let us suppose $e_1 \in U$. Then, we have $e_2 = \rho(\alpha)e_1 \in U$ and $e_3 = \rho(\beta)e_2 \in U$, that is, $U = \mathbb{K}^3$.

Remark 2.0.8. If (V, ρ) is a representation of A, then V is equivalently a left A-module. Indeed the action of A on V is defined as follows: for $a \in A$,

$a * v := \rho(a)(v)$. Vice versa we can induce naturally a structure of $\mathbb{K}$-vector space on V defining: $\lambda * v := (\lambda e) * v$, for every $\lambda \in \mathbb{K}$, for every $v \in V$, where e is some fixed element in A; moreover we can define $\rho : A \to \mathrm{End}(V)$, $\rho(a)(v) := a * v$, for every $a \in A$, $v \in V$. Finally (V, ρ) is a representation of A.

Definition 2.0.9. *Let V_1, V_2 be two representations of A and $\phi : V_1 \to V_2$; we say that ϕ is a* **homomorphism of representations** *(or an* **intertwining operator***) if ϕ is linear and commutes with the action of A, i.e. $\phi(a \cdot v) = a \cdot \phi(v)$, for every $a \in A$, for every $v \in V_1$.*

Definition 2.0.10. *Let $\mathcal{V}$ be a representation of A; we define a* **filtration** *of $\mathcal{V}$ as a finite chain of subrepresentations $0 = V_0 \subset V_1 \subset \cdots \subset V_n = \mathcal{V}$. Moreover we call* **factors** *the successive quotients V_{i+1}/V_i, for every $i < n$.*

Remark 2.0.11.

- Let V be a representation of A and $W \subset V$ be a subrepresentation, then the quotient V/W is a representation of A; indeed since W is closed under the action of $\rho(\alpha)$, for every $\alpha \in A$, the map $[\rho] : A \to \mathrm{End}(V/W)$, $[\rho](\alpha)([v]) := [\rho(\alpha)(v)]$, for $\alpha \in A$ and $v \in V$, is well defined.

- Let us consider a filtration $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ and the filtration $0 = V_1/V_1 \subset V_2/V_1 \subset \cdots \subset V_n/V_1 = V/V_1$, then by the Third Isomorphism Theorem they have the same factors (except for V_1).

We are interested in a particular kind of filtrations, i.e., those whose factors are simple, but not all representations admit such filtrations. For instance let us consider $A = \mathbb{K}\mathbb{Z}$, with the trivial representation $\mathcal{V} = \mathbb{K}\mathbb{Z}$;

suppose $0 = V_0 \subset V_1 \subset \cdots \subset V_n = \mathcal{V}$ is a filtration, then every V_i must be of the form $\mathbb{K}d_i\mathbb{Z}$, with $d_i \mid d_{i-1}$. Since $V_0 = 0$ the only possible value for d_0 is 0. Notice that for every $i > 1$, $V_i/V_{i-1} \cong \mathbb{K}\frac{d_{i-1}}{d_i}\mathbb{Z}$, therefore if we want the factors to be irreducible, it must be $d_{i-1} = d_i p_{i-1}$, where p_{i-1} is prime; but in this case $V_1/V_0 \cong V_1 \cong \mathbb{K}p_1 \cdot \ldots \cdot p_n\mathbb{Z}$ and for $n > 1$, $p_1 \cdot \ldots \cdot p_n$ is not prime. Hence A does not admit a finite filtration with irreducible factors.

Lemma 2.0.12. *Any finite dimensional representation $\mathcal{V}$ of A admits a finite filtration $0 = V_0 \subset V_1 \subset \cdots \subset V_n = \mathcal{V}$ such that the successive quotients V_i/V_{i-1} are irreducible.*

Proof. We proceed by induction on $q :=\dim V$. The case $q = 0$ is trivial; Let us take an irreducible subrepresentation $V_1 \subseteq V$, and consider the representation $U := V/V_1$. Then by the induction hypothesis there exists a filtration $0 = U_0 \subset U_1 \subset \cdots \subset U_{n-1} = U$ of U such that for every $1 \leq i \leq n$, U_i/U_{i-1} is irreducible. Let us consider $\pi_U : V \twoheadrightarrow U$ the canonical projection, then for all $i \geq 2$ define $V_i := \pi_U^{-1}(U_{i-1})$, in particular $V_{i+1}/V_i \cong (V_{i+1}/V_1)/(V_i/V_1) \cong U_i/U_{i-1}$ for all $i = 1, \ldots, n$. Therefore $0 = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = V$ is a filtration of V with the desired property. □

Example 2.0.13.

- If $A = \mathbb{K}$ and $\mathcal{V}$ is a representation of A of dimension n, then if $B = \{v_1, \ldots, v_n\}$ is a basis of $\mathcal{V}$, $0 \subset \langle v_1 \rangle \subset \cdots \subset \langle v_1, \ldots, v_n \rangle$ is a filtration with irreducible factors.

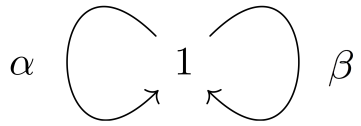
Now we are ready to present the main theorem of this chapter:

Theorem 2.0.14 (Jordan-Hölder)**.** *Let V be a finite dimensional representation of A, and let $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$, $0 = V_0' \subset \cdots \subset$*

$V'_m = V$ be filtrations of V, such that the representations $W_i := V_i/V_{i-1}$ and $W'_i := V'_i/V'_{i-1}$ are irreducible for all i. Then $n = m$, and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that W_i is isomorphic to $W'_{\sigma(i)}$ for each $i = 1, \dots, n$.

Proof. We will prove the theorem by induction on $q :=$dim$V$. If $q = 0$ then the theorem is clearly true. Therefore let us suppose the theorem holds for every representation of dimension $k < q$: by induction hypothesis if $V_1 = V'_1$ (as subspaces), then we can conclude considering the quotient filtration on V/V_1. So assume $V_1 \neq V'_1$. Since V_1, V'_1 are irreducible $V_1 \cap V'_1 = 0$, therefore let $U := V/(V_1 \oplus V'_1)$. By Lemma 2.0.12 there exists $0 = U_0 \subset U_1 \subset \cdots \subset U_p = U$ a filtration of U with irreducible quotients $Z_i := U_i/U_{i-1}$. Moreover V/V_1 has a filtration with successive quotients $W_1, Z_1, \dots, Z_p$ and another filtration with successive quotients $W_2, \dots, W_n$, instead V/V'_1 has a filtration with successive quotients $W'_1, Z_1, \dots, Z_p$ and another filtration with successive quotients $W'_2, \dots, W'_n$. Finally, we can conclude by induction on these filtrations. □

Example 2.0.15. Let Q be the quiver with one vertex and two loops:



with the path algebra $\mathbb{K}Q$. Let us consider $A, B \in M_n(\mathbb{K})$ and $\rho : \mathbb{K}Q \to End(\mathbb{K}^n)$, $\rho(\alpha^{j_1}\beta^{k_1} \dots \alpha^{j_m}\beta^{k_m}) = A^{j_1}B^{k_1} \dots A^{j_m}B^{k_m}$, for $m \in \mathbb{Z}_{\geq 0}$, and $j_1, \dots, j_m$, $k_1, \dots, k_m \in \mathbb{Z}_{\geq 0}$ (we define ρ only on the set of paths P_Q and then extend it by linearity), so $(\mathbb{K}^n, \rho)$ is a representation of $\mathbb{K}Q$; it is

clear that every subspace of $\mathbb{K}^n$ is a subrepresentation of $\mathbb{K}^n$ if and only if $AW \subseteq W$ and $BW \subseteq W$. For example if $\mathbb{K} = \mathbb{R}$, $n = 2$, $B = I_2$ and $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, then $(\mathbb{R}^2, \rho)$ is irreducible; on the contrary, if $\mathbb{K} = \mathbb{R}$, $n = 3$, $B = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ and $A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, then $0 \subset \langle e_1, e_2 \rangle \subset \mathbb{R}^3$ and $0 \subset \langle e_3 \rangle \subset \mathbb{R}^3$ are two filtrations of $(\mathbb{R}^3, \rho)$ with irreducible factors.

Now, taking into account Remark 2.0.8, we introduce some related definitions that will enable us to reformulate Jordan-Hölder Theorem for modules.

Definition 2.0.16. *Let M be an A-module, we say that M is* **irreducible** (*or* **simple**) *if its only submodules are 0 and M.*

If M is an irreducible A-module and $m \in M \setminus \{0\}$, then for every $x \in M$ there exists $a \in A$ such that $x = a \cdot m$; so, we will write $M = (m)$.

Definition 2.0.17. *Let M be an A-module, we call* **composition series of length n** *a finite chain of submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ such that for every $i < n$, M_{i+1}/M_i is irreducible.*

Let M be an A-module, then, with the construction of Remark 2.0.8 in mind, it is easy to see that there is a natural correspondence between the submodules of M and its subrepresentations. In particular, every A-module is irreducible if and only if it is irreducible as a representation of A and that every composition series of M as on A-module is a filtration where the factors are irreducible.

Corollary 2.0.18 (Jordan-Hölder Theorem for modules)**.** *Let M be an A-module, then for any two composition series $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ and $0 = M'_0 \subset \cdots \subset M'_m = M$: $n = m$ and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that M_i/M_{i-1} is isomorphic to $M'_{\sigma(i)}/M'_{\sigma(i)-1}$ for each $i = 1, \ldots, n$.*

Theorem 2.0.19 (Schur's Lemma)**.** *Let V_1, V_2 be representations of A. Let $\phi : V_1 \to V_2$ be a nonzero homomorphism of representations. Then:*

1) if V_1 is irreducible, ϕ is injective;

2) if V_2 is irreducible, ϕ is surjective.

Thus, if both V_1 and V_2 are irreducible, ϕ is an isomorphism.

Proof. See [4, Theorem 3.33]. □

Remark 2.0.20. If A is a finite dimensional algebra, let $M = (m)$ be a simple A-module, then we can consider $\phi : A \to M$, $\phi(a) := a \cdot m$; by Theorem 2.0.19 ϕ is a surjective homomorphism of A-modules, hence $M \cong A/\ker(\phi)$. Therefore completing the series $\ker(\phi) \subset A$ to a composition series, by Corollary 2.0.18 M is a factor of A, so A has only a finite number of irreducible modules (and thus irreducible representations), up to isomorphisms.

As a consequence of Theorem 2.0.18 we can give a natural generalization of the concept of vector space dimension which permits the extension of some properties from linear algebra.

Definition 2.0.21. *Let M be an A-module, then if there exists a finite composition series, we set $\ell(M)$ as the length of the composition series; otherwise, we set $\ell(M) := \infty$. We call $\ell(M)$ the* **length** *of M.*

Remark 2.0.22. By induction on the length, it is easy to prove that every A-module M with finite length is finitely generated, in particular, the module can be generated by exactly $\ell(M)$ elements.

Finally, we state the Jordan-Hölder Theorem for Groups and some of its applications. We recall that a simple group is a group with no non-trivial normal subgroups.

Theorem 2.0.23 (Jordan-Hölder Theorem for Groups)**.** *Let G be a finite group. Let $0 \lhd H_1 \lhd \cdots \lhd H_n = G$ and $0 \lhd K_1 \lhd \cdots \lhd K_m = G$ be two normal series of G such that H_i/H_{i-1} and K_j/K_{j-1} are simple, for every $i \leq n$, and $j \leq m$. Then, $n = m$ and there exists $\sigma \in \mathfrak{S}_n$ such that $H_i/H_{i-1} \cong K_{\sigma(i)}/K_{\sigma(i)-1}$.*

Proof. See [12, Theorem 5.12]. □

Definition 2.0.24. *Let G be a group. We say that G is* **solvable** *if there exists a subnormal series $0 \lhd K_1 \lhd \cdots \lhd K_m \lhd G$ such that every quotient K_i/K_{i-1} is abelian.*

Remark 2.0.25. Using Theorem 2.0.23 and Theorem 1.1.14 it is easy to see that every finite solvable group is completely determined by its order: indeed let $0 \lhd K_1 \lhd \cdots \lhd K_m \lhd G$ be a subnormal series with abelian factors, then by the structure theorem there exist $p_1, \ldots, p_k \in \mathbb{Z}_{>0}$ primes and $n_1, \ldots, n_k \in \mathbb{Z}_{>0}$ such that $G/K_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$; without loss of generality we can suppose $n_1 > 0$, so there exists a subgroup of G/K_m, say H/K_m, such that $H/K_m \cong \mathbb{Z}_{p_1^{n_1-1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$. Such group H must be a normal subgroup of G (since H/K_m was normal in G/K_m) and contains K_m as a normal subgroup, so we can extend our initial subnormal series

to obtain $0 \lhd K_1 \lhd \cdots \lhd K_m \lhd H \lhd G$ and in particular $G/H \cong (G/K_m)/(H/K_m) \cong \mathbb{Z}_{p_1}$, then we can conclude by induction on H, since every subgroup of a solvable group is solvable.

Example 2.0.26 (**Fundamental theorem of arithmetic**). Applying the Jordan-Hölder Theorem to finite cyclic groups we can prove the fundamental theorem of arithmetic. Indeed, the only simple cyclic finite groups are C_p, where p is a prime. Hence, since the quotient of a cyclic group is cyclic, a decomposition series of C_n must have as factors $\{C_{p_1}, \ldots, C_{p_m}\}$ (with multiplicities), where $p_1, \ldots, p_m$ are primes; these factors are unique by Theorem 2.0.23. Finally, if p is a prime and p divides n, then $|\langle [p] \rangle| = n/p$; Therefore, $C_n/\langle [p] \rangle \cong C_p$. Hence, C_p is a decomposition factor of C_n, that is, we can uniquely write n as a product of primes (ignoring the order).

Example 2.0.27. Let $D_6 := \langle r, s \mid r^6 = s^2 = (sr)^2 = e \rangle$ be the 6^{th} dihedral group, then $0 \lhd \langle r^2 \rangle \lhd \langle r \rangle \lhd D_6$ and $0 \lhd \langle r^3 \rangle \lhd \langle r \rangle \lhd D_6$ are two composition series for D_6.

The composition factors and the length of a representation/A-module/ finite group are isomorphism invariants which can tell us a lot about the structure of the algebra/module/group; however, they do not permit us to completely classify them. For instance, let us take the finite groups D_4 and the quaternion group Q_8. They have the same composition factors ($\mathbb{Z}/2$ with multiplicity 3) but they are not isomorphic (Q_8 does not have an element of order 4).

Thus, a problem arising from the Jordan-Hölder theorem is the following: let V and W be two simple representations of A, who are (up to isomorphism) the representations M of A such that V is a subrepresentation of M and

$W \cong M/V$? This problem is called the **extension problem** (it can be equivalently rephrased for groups and modules) and it is a central, still open, problem in modern abstract algebra.

Chapter 3

The Extension Problem

As we have mentioned at the end of Chapter 2, the Jordan-Hölder Theorem is of great relevance in the theory of finite groups. Due to this theorem, a finite group uniquely determines a family of simple groups, that is, its composition factors. This provides motivation for the **Hölder's program**:

1) Classify up to isomorphisms all finite simple groups.

2) For every two groups G and M, determine all groups E which contain a normal subgroup isomorphic to M and such that the quotient group E/M is isomorphic to G. This is the extension problem.

The first step has been officially completed in 2004, while the second is still an open problem. The accomplishment of these two points would allow us to completely classify all finite groups. Indeed, if $G_1, \ldots, G_n$ is an ordered family of simple groups, then, knowing the solution to the extension problem, we are able to construct all finite groups whose composition factors are the G_i. In fact, as a first step, we can determine all the groups E_2 containing a normal subgroup isomorphic to G_1 and such that $E_2/G_1 \cong G_2$.

Then we will end up with a certain number of series: $1 \triangleleft G_1 \triangleleft E_2$ whose factors are G_2 and G_1. Iterating this process, we find all the composition series $1 \triangleleft G_1 \triangleleft E_2 \triangleleft \cdots \triangleleft E_n =: E$ having $G_1, \ldots, G_n$ as composition factors. However, the same group may be found several times among these E, as we will see.
In this Chapter, we will adopt the notation $X \in \mathcal{C}$ instead of $X \in Ob_{\mathcal{C}}$, when $\mathcal{C}$ is a category.

3.1 Extensions of Groups

Definition 3.1.1. *Let $M, E, G \in Grp$, then we define a* **short exact sequence** *as a sequence $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ such that $ker(\pi) = Im(i)$, i is injective and π is surjective. Moreover, we will say that the short exact sequence is* **right split** *if there exists a group homomorphism $s : G \to E$ such that $\pi \circ s = id_G$, in this case s is called a (group-theoretic)* **section** *of π; analogously we can define a* **left split** *sequence. If a short exact sequence is both right and left split we simply say it is* **split** *or that it* **splits**.

In particular, if $M, E, G \in Ab$ and $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ is right split, then it is also left split.

Definition 3.1.2. *Let $G, M \in Grp$, an* **extension of G by M** *is a short exact sequence $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$. In case $M \in Ab$, we say that the extension is* **abelian**.

Example 3.1.3.
- Let $G := \mathbb{Z}_2 \times \mathbb{Z}_2$, $M := \mathbb{Z}_2$, $E := Q_8$, $i : M \to E$ with $i([1]) := -1$ and $\pi : E \to G$ with $\pi(i) := ([1], [0])$ and $\pi(j) := ([0], [1])$, then $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ is an abelian extension.

- Let us consider an action φ of G on M, then the semidirect product $E := M \rtimes_\varphi G$ with $i(m) := (m, e_G)$ and $\pi(m, g) := g$ is always an extension of G by M. In particular, this extension splits.

Definition 3.1.4. *Let $M, G \in Grp$, we say that two extensions $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ and $0 \to M \xrightarrow{i'} E' \xrightarrow{\pi'} G \to 1$ of G by M are* **equivalent** *if there exists an isomorphism (an "equivalence map") $\phi : E \to E'$ such that the diagram:*

$$\begin{array}{ccccccc} & & & & E & & & \\ & & & \overset{i}{\nearrow} & \downarrow \phi & \overset{\pi}{\searrow} & & \\ 0 & \longrightarrow & M & & & & G & \longrightarrow & 1 \\ & & & \underset{i'}{\searrow} & & \underset{\pi'}{\nearrow} & & \\ & & & & E' & & & \end{array} \tag{3.1}$$

commutes.

Example 3.1.5. Let $M := \mathbb{Z}_2$, $G := \mathbb{Z}_2 \times \mathbb{Z}_2$ and $E := \mathbb{Z}_4 \times \mathbb{Z}_2 =: \langle x, y \rangle$, where $x := ([1]_4, [0]_2)$ and $y := ([0]_4, [1]_2)$. Let $i([1]_2) := ([2]_4, [0]_2)$ and let $\pi_1(x) := ([1]_2, [0]_2)$, $\pi_1(y) := ([0]_2, [1]_2)$ and $\pi_2(x) := ([0]_2, [1]_2)$, $\pi_2(y) := ([1]_2, [1]_2)$. Then $0 \to M \xrightarrow{i} E \xrightarrow{\pi_1} G \to 1$, $0 \to M \xrightarrow{i} E \xrightarrow{\pi_2} G \to 1$ are extensions of $\mathbb{Z}_2 \times \mathbb{Z}_2$ by $\mathbb{Z}_2$ and, with a simple calculation it can be shown that they are not equivalent.

Remark 3.1.6. By the Five Lemma, in order to prove that two extensions are equivalent it is sufficient to prove the existence of a homomorphism ϕ between E and E' such that diagram (3.1) commutes.

Definition 3.1.7. *Let $G \in Grp$, $M \in Ab$ and $\rho \in Hom(G, Aut(M))$. Then we say that (M, ρ) is a representation of G on M or, equivalently, that M is a* $\mathbf{G-module}$ *and we will usually simply denote it by M.*

Remark 3.1.8.
- G-modules form a category that we will denote by $GMod$;

- the notion of G-module is equivalent to that of $\mathbb{Z}[G]$-module since every abelian group is also a $\mathbb{Z}$-module.

Let $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ be an abelian extension of G by M, then we can induce a structure of G-module on M: take any set-theoretic section s of G in E (i.e. a function $s : G \to E$ such that $\pi \circ s = id_G$) we define $g * m \equiv \rho(g)(m) := i^{-1}(s(g)i(m)s(g)^{-1})$. This map is well defined, indeed let $h, k \in \pi^{-1}(g)$ then $h^{-1}k \in i(M)$, therefore $i^{-1}(hi(m)h^{-1}ki(m)^{-1}k^{-1}) = i^{-1}(hi(m)i(m)^{-1}h^{-1}kk^{-1}) = e$, so $i^{-1}(hi(m)h^{-1}) = i^{-1}(ki(m)k^{-1})$.

Remark 3.1.9.
- Equivalent extensions induce the same action on M: let $\varphi : E \to E'$ be an equivalence map, then $i'(g *_{E'} m) = \varphi(i(g *_E m)) = \varphi(s(g)i(m)s(g)^{-1}) = \varphi(s(g))i'(m)\varphi(s(g))^{-1}$ but $\pi = \pi' \circ \varphi$ so, $g = \pi(s(g)) = \pi'(\varphi(s(g))) =: s'(g)$; therefore $\varphi(s(g))i'(m)\varphi(s(g))^{-1} = s'(g)i'(m)s'(g)^{-1} = i'(g *_{E'} m)$, hence $g *_E m = g *_{E'} m$, for every $(g, m) \in G \times M$.

- Let $\rho \in Hom(G, Aut(M))$ be an action of G on M, then there always exists an extension having ρ as induced action: it is enough to consider the sequence $0 \to M \xrightarrow{i} G \ltimes_\rho M \xrightarrow{\pi} G \to 1$; indeed, if we set $s(g) := (0, g)$, we have $g * m = i^{-1}(s(g)i(m)s(g)^{-1}) = i^{-1}((0, g)(m, e_G)(0, g^{-1})) = i^{-1}((\rho(g)(m), g)(0, g^{-1})) = i^{-1}((\rho(g)(m), e_G)) = \rho(g)(m)$.

3.2 Group Cohomology

Definition 3.2.1. *A* **cochain complex** *is a pair of sequences* $(C^{\cdot}, \partial^{\cdot})$*, with* $C^n \in Ab$*,* $\partial^n \in Hom_{Ab}(C^{n-1}, C^n)$ *such that* $\partial^{n+1} \circ \partial^n = 0$*, for any* $n \in \mathbb{Z}$*. We say that any element of* $ker(\partial^n)$ *is a* $\mathbf{n-cochain}$ *and any element of* $Im(\partial^{n-1})$ *is a* $\mathbf{n-coboundary}$*. Finally we define the* $\mathbf{n^{th}-cohomology\ group}$*,* $H^n(C^{\cdot}) := ker(\partial^{n+1})/Im(\partial^n)$*.*

Definition 3.2.2. *A* **chain complex** *is a pair of sequences* $(C_{\cdot}, \partial_{\cdot})$*, with* $C_n \in Ab$*,* $\partial_n \in Hom_{Ab}(C_n, C_{n-1})$ *such that* $\partial_n \circ \partial_{n+1} = 0$*, for any* $n \in \mathbb{Z}$*. We say that any element of* $ker(\partial_n)$ *is a* $\mathbf{n-chain}$ *and any element of* $Im(\partial^{n+1})$ *is a* $\mathbf{n-boundary}$*. Finally we define the* $\mathbf{n^{th}-homology\ group}$*,* $H_n(C_{\cdot}) := ker(\partial_n)/Im(\partial_{n+1})$*.*

We will denote a chain complex with the diagram: $\cdots \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} C_{-1} \xrightarrow{\partial_{-1}} \cdots$ and analogously for cochain complexes. Furthermore, we will say that a chain complex is **exact at** k if $H_k(C_{\cdot}) = 0$, we will say that the complex is **exact** if it is exact for any $k \in \mathbb{Z}$.
From now on, G will be a group and M a G-module.

Definition 3.2.3. *We define a* **free resolution of** M **over** $\mathbb{Z}[G]$ *as an exact chain complex of* $\mathbb{Z}[G]$*-modules* $\cdots E_2 \xrightarrow{\partial_2} E_1 \xrightarrow{\partial_1} E_0 \xrightarrow{\partial_0} M \to 0$ *such that for every* $n \geq 0$*,* E_n *is free.*

Example 3.2.4.
- (**Bar resolution**) let $M = \mathbb{Z}$ with G acting trivially on it (i.e., $g * n = n$, for every $n \in \mathbb{Z}$); let us consider the complex $\cdots \xrightarrow{\partial_3} \bigoplus_{g,h \in G} R\langle g|h\rangle \xrightarrow{\partial_2} \bigoplus_{g \in G} R\langle g\rangle \xrightarrow{\partial_1} R\langle\rangle \xrightarrow{\partial_0} \mathbb{Z} \to 0$, where $R := \mathbb{Z}[G]$ and $\langle * \rangle$ denotes the generator of the cyclic left R-module

$R\langle * \rangle \cong R$. In this case $\partial_0(\langle\rangle) := 1$, $\partial_1(\langle g\rangle) := g\langle\rangle - \langle\rangle$, $\partial_2(\langle g|h\rangle) := g\langle h\rangle - \langle gh\rangle + \langle g\rangle$, and in general $\partial_n(\langle g_1|\dots|g_n\rangle) := g_1\langle g_2|\dots|g_n\rangle - \sum_{k=2}^{n}(-1)^k\langle g_1|\dots|g_{k-1}g_k|\dots|g_n\rangle + (-1)^n\langle g_1|\dots|g_{n-1}\rangle$, for every $n \geq 2$. This complex is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$.

- Let $G = \mathbb{Z}_n = \langle [1]_n \rangle$, $M = \mathbb{Z}$ and let G act on M trivially; consider the chain complex $\cdots \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$, where $\epsilon([1]_n) := 1$, $D([1]_n) := [1]_n - [0]_n$, $N([1]_n) := [0]_n + \cdots + [n-1]_n$, $\partial_{2k} := N$ and $\partial_{2k-1} := D$, for every $k \geq 1$. It is easy to see that this is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[\mathbb{Z}_n]$.

Remark 3.2.5. let $R \in Ring$, $A, B \in RMod$; consider two free resolutions $\cdots A_2 \xrightarrow{\partial_2} A_1 \xrightarrow{\partial_1} A_0 \xrightarrow{\partial_0} A \to 0$ and $\cdots B_2 \xrightarrow{\partial_2} B_1 \xrightarrow{\partial_1} B_0 \xrightarrow{\partial_0} B \to 0$ and $\phi \in Hom(A, B)$. Then we can lift ϕ uniquely up to 0-boundaries to a map in $Hom(A_0, B_0)$ in such a way that the diagram

$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{\partial_3^A} & A_2 & \xrightarrow{\partial_2^A} & A_1 & \xrightarrow{\partial_1^A} & A_0 & \xrightarrow{\partial_0^A} & A & \longrightarrow & 0 \\
 & & & & & & \downarrow{\scriptstyle \phi^{(1)}} & & \downarrow{\scriptstyle \phi} & & \\
\cdots & \xrightarrow{\partial_3^B} & B_2 & \xrightarrow{\partial_2^B} & B_1 & \xrightarrow{\partial_1^B} & B_0 & \xrightarrow{\partial_0^B} & B & \longrightarrow & 0
\end{array}$$

commutes, that is: $\partial_0^B \circ \phi^{(1)} = \phi \circ \partial_0^A$. Indeed, take two such morphisms $\tilde{\phi}, \bar{\phi}$, then $\partial_0^B(\tilde{\phi} - \bar{\phi}) = 0$, hence $\tilde{\phi} - \bar{\phi} = \partial_1^B \circ h$ for some $h \in Hom(A_0, B_1)$. We point out that since A_0, B_0 are free, such morphism always exists: fix a basis of A_0, then for every basis element α fix an element in $(\partial_0^B)^{-1}(\phi(\partial_0^A(\alpha)))$, call it $\phi^{(1)}(\alpha)$. Repeating the process for every $n > 1$ we can induce uniquely (up to n-boundaries) from ϕ a morphism of complexes $\phi^{(\cdot)}$; the morphisms $\phi^{(\cdot)}$ are called **liftings** of ϕ.

Definition 3.2.6. *Let $R \in Ring$ and $B \in RMod$, then, for any $n \in$*

$\mathbb{Z}$, we define the contravariant functor $Ext^n_R(-,B) : RMod \to Ab$, with $Ext^n_R(A,B) := H^n(Hom_R(F^A_\cdot, B))$ where $F^A_\cdot$ is a free resolution of A, for any $A \in RMod$ and for every $f \in Hom(A,C)$, $Ext^n_R(f)([c]) := [c \circ f^{(n+1)}]$, for every $A, C \in RMod$.

The above definition assumes that a choice of free resolution of every R-module has been made. Let us prove that $Ext^n_R(-,B)$ is well defined, i.e., that it does not depend on the choice of the free resolutions:

Proposition 3.2.7. *Let $R \in Ring$, $\cdots E_2 \xrightarrow{\partial_2} E_1 \xrightarrow{\partial_1} E_0 \xrightarrow{\partial_0} A \to 0$ and $\cdots E'_2 \xrightarrow{\partial'_2} E'_1 \xrightarrow{\partial'_1} E'_0 \xrightarrow{\partial'_0} A \to 0$ be two free resolutions of $A \in RMod$ and $F^n, \bar{F}^n : RMod \to Ab$ the Ext^n functors defined above using respectively the first and the second family of resolutions, then $F^n, \bar{F}^n$ are naturally isomorphic, for every $n \in \mathbb{Z}_{>0}$.*

Proof. Consider the diagram:

$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{\partial_3} & E_2 & \xrightarrow{\partial_2} & E_1 & \xrightarrow{\partial_1} & E_0 & \xrightarrow{\partial_0} & A & \longrightarrow & 0 \\
 & & & & & & & & \downarrow{\scriptstyle id_A} & & \\
\cdots & \xrightarrow{\partial'_3} & E'_2 & \xrightarrow{\partial'_2} & E'_1 & \xrightarrow{\partial'_1} & E'_0 & \xrightarrow{\partial'_0} & A & \longrightarrow & 0
\end{array}$$

and for every $n \in \mathbb{Z}_{>0}$, the n^{th} lifting $\varphi^{(n)}$ of id_A. Every lifting induces a map between the cochain complexes:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Hom(E_0,B) & \xrightarrow{\partial^1} & Hom(E_1,B) & \xrightarrow{\partial^2} & Hom(E_2,B) & \xrightarrow{\partial^3} & \cdots \\
 & & {\scriptstyle \phi^{(1)}}\uparrow & & {\scriptstyle \phi^{(2)}}\uparrow & & {\scriptstyle \phi^{(3)}}\uparrow & & \\
0 & \longrightarrow & Hom(E'_0,B) & \xrightarrow{\bar{\partial}^1} & Hom(E'_1,B) & \xrightarrow{\bar{\partial}^2} & Hom(E'_2,B) & \xrightarrow{\bar{\partial}^3} & \cdots
\end{array},$$

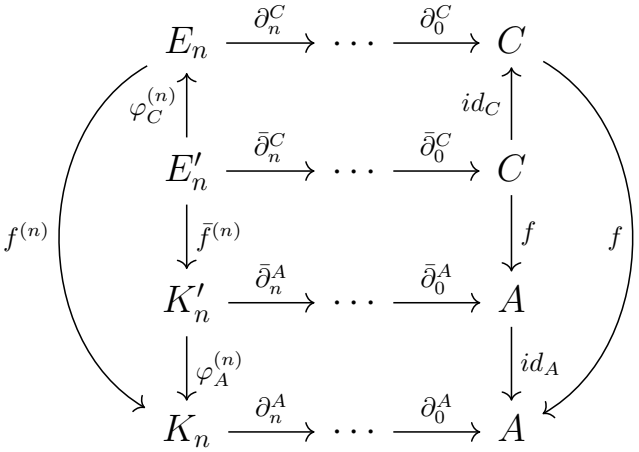
in particular, for every $n \in \mathbb{Z}_{>0}$, $\phi^{(n)}(a) := a \circ \varphi^{(n)}$. Since $\partial^n \circ \phi^{(n)} = \phi^{(n+1)} \circ \bar{\partial}^n$, every $\phi^{(n)}$ induces in cohomology the map $[\phi^{(n)}]([a]) := [\phi^{(n)}(a)]$.

Let us show that $[\phi^{(n)}]$ is an isomorphism for every $n \in \mathbb{Z}_{>0}$: in order to prove it we will construct its inverse. Consider the liftings $\vartheta^{(\cdot)}$ of id_A in the diagram:

$$\begin{array}{ccccccccccc} \cdots & \xrightarrow{\partial_3} & E_2 & \xrightarrow{\partial_2} & E_1 & \xrightarrow{\partial_1} & E_0 & \xrightarrow{\partial_0} & A & \longrightarrow & 0 \\ & & & & & & & & \uparrow{\scriptstyle id_A} & & \\ \cdots & \xrightarrow{\partial'_3} & E'_2 & \xrightarrow{\partial'_2} & E'_1 & \xrightarrow{\partial'_1} & E'_0 & \xrightarrow{\partial'_0} & A & \longrightarrow & 0 \end{array}$$

now, as before, we can apply the Hom functor to the diagram and obtain $\theta^{(\cdot)}$; therefore it is sufficient to prove that $[\phi^{(n)}] \circ [\theta^{(n)}] = [id_{Hom(E_{n-1},B)}] \equiv id_{H^n(Hom(E.,B))}$ and by the symmetry of this construction, we have done. Let $[a] \in H^n(Hom(E., B))$, then $[\phi^{(n)}] \circ [\theta^{(n)}]([a]) - [a] = [a \circ (\vartheta^{(n)} \circ \varphi^{(n)} - id_{E_{n-1}})]$, but $\vartheta^{(n)} \circ \varphi^{(n)}$ is a lifting of $id_{E_{n-1}}$ therefore their difference is a n-boundary, hence $[a \circ (\vartheta^{(n)} \circ \varphi^{(n)} - id_{E_{n-1}})] = [a \circ \partial_n \circ \alpha] = 0$ (here α is just a function, not necessarily a morphism).

It remains to prove that $[\phi^{(n)}]$ is actually a natural transformation, so, let us take $f \in Hom(A, C)$ and consider the diagram:



where $f^{(n)}, \bar{f}^{(n)}$ are liftings of f and $\varphi_A^{(n)}, \varphi_C^{(n)}$ liftings of id_A, id_C. Then $\varphi_A^{(n)} \circ \bar{f}^{(n)}$ and $f^{(n)} \circ \varphi_C^{(n)}$ are liftings of f, then they differ by n-boundaries,

so, as before, they induce the same morphism in cohomology. Therefore, $F(f) \circ [\phi_A^{(n)}] = [\phi_C^{(n)}] \circ F'(f)$. □

Finally, we define the **n^{th}-cohomology group of G with coefficients in M** as $H^n(G, M) := Ext^n_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Remark 3.2.8. Let $G \in Grp$, then $H^n(G, 0) = 0$, for every $n \in \mathbb{Z}_{\geq 0}$.

3.3 Cohomology groups and group extensions

In what follows, unless specified, M will be a G-module.

3.3.1 The 0^{th} cohomology group

For $n = 0$, we have $H^0(G, M) = \{f \in Hom(R\langle\rangle, M) |\ g * f(\langle\rangle) - f(\langle\rangle) = 0$, for every $g \in G\} \cong \{m \in M |\ g * m = m$, for every $g \in G\} =: M^G$.

3.3.2 The first cohomology group

Let $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ be an extension, then we define: $Inn_M(E) := \{\phi \in Aut(E) |$ there exists $m \in M$ with $\phi(h) = i(m)hi(m)^{-1}$, for every $h \in E\}$ and $Aut_{G,M}(E) := \{\phi \in Aut(E) |\ \phi_{|M} \equiv id_M$ and $\pi \circ \phi = \pi\}$.

Theorem 3.3.1. *Let $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ be an extension, then $H^1(G, M) \cong Aut_{G,M}(E)/Inn_M(E) =: Out(G, M)$.*

Proof. Let s be a section and define $\sigma : Aut_{G,M}(E) \to H^1(G, M)$, $\sigma(\phi) := [f_\phi]$, where f_ϕ is the unique element of $Hom_{\mathbb{Z}[G]}(\bigoplus_{g \in G} \mathbb{Z}[G], M)$ such that $f_\phi(\langle g\rangle) := i^{-1}(\phi(s(g))s(g)^{-1}) \in M$; σ is well defined, indeed, since π

$(s(g)s(h)) = \pi(s(gh))$, there exists $m \in M$ such that $s(g)s(h) = i(m)s(gh)$, therefore: $f_\phi(\langle gh \rangle) =$

$$i^{-1}(\phi(s(gh))s(gh)^{-1}) = i^{-1}(\phi(i(m)^{-1}s(g)s(h))s(h)^{-1}s(g)^{-1}i(m)) =$$
$$-m + i^{-1}(\phi(s(g))f_\phi(\langle h \rangle)s(g)^{-1}) + m = f_\phi(\langle g \rangle) + g * f_\phi(\langle h \rangle),$$

so $f_\phi \in ker(\partial^2)$. We now have to prove that σ is surjective and that $ker(\sigma) = Inn_M(E)$; we have $\phi \in ker(\sigma) \iff$ there exists $m \in M$: for every $g \in G$, $\phi(s(g))s(g)^{-1} = i(g*m-m) = i(m)^{-1}i(g*m) \iff$ there exists $m \in M$: for every $g \in G$, $\phi(s(g))s(g)^{-1} = i(-m)s(g)i(m)s(g)^{-1} \iff$ there exists $m \in M$ such that for every $g \in G$, $\phi(s(g)) = i(-m)s(g)i(-m)^{-1} \iff$ $\phi \in Inn_M(E)$. Now, let $[f] \in H^1(G, M)$, then define $\phi(s(g)) := f(\langle g \rangle)s(g)$, then $\phi \in Aut_{G,M}(E)$ and $\sigma(\phi) = [f]$. □

3.3.3 The second cohomology group

Let $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ be an extension; consider a set-theoretic section s with $s(e_G) = e_E$ (a **normalized** section), then define the map $f : G \times G \to M$, $f(g, h) := i^{-1}(s(g)s(h)s(gh)^{-1})$ which measures the difference of s from being an homomorphism. Notice that since s is normalized, $f(e_G, g) = f(g, e_G) = e_M$. Furthermore, define $\ell : M \times G \to E$, $\ell(m, g) := i(m)s(g)$ (in particular, ℓ is a bijection); therefore, $\ell(m_1, g_1)\ell(m_2, g_2) = i(m_1)s(g_1)i(m_2)s(g_2) = i(m_1)i(g_1 * m_2)i(f(g_1, g_2))s(g_1g_2) = \ell(m_1 + g_1 * m_2 + f(g_1, g_2), g_1g_2)$. Hence the group law in E is completely determined by the group laws of G and M, by the action of G on M (i.e., by the G-module

structure on M) and by f. Using the associativity in E we obtain:

$$((m_1,g_1)(m_2,g_2))(m_3,g_3) = (m_1 + g_1 * m_2 + f(g_1,g_2), g_1g_2)(m_3,g_3)$$
$$= (m_1 + g_1 * m_2 + f(g_1,g_2) + g_1g_2 * m_3 + f(g_1g_2,g_3), g_1g_2g_3)$$
$$(m_1,g_1)((m_2,g_2)(m_3,g_3)) = (m_1,g_1)(m_2 + g_2 * m_3 + f(g_2,g_3), g_2g_3)$$
$$= (m_1 + g_1 * m_2 + g_1g_2 * m_3 + g_1 * f(g_2,g_3) + f(g_1,g_2g_3), g_1g_2g_3)$$

therefore, $((m_1,g_1)(m_2,g_2))(m_3,g_3) = (m_1,g_1)((m_2,g_2)(m_3,g_3)) \iff$ $f(g_1,g_2) + f(g_1g_2,g_3) - f(g_1,g_2g_3) - g_1f(g_2,g_3) = 0$. Considering the bar complex wedefine $\bar{f} \in Hom(\bigoplus_{g,h\in G} R\langle g|h\rangle, M)$ as $\bar{f}(\langle g|h\rangle) := f(g,h)$, then $\bar{f}$ is a 2-cocycle. So we have associated a 2-cocycle to every pair $((E,i,\pi),s)$. The following result improves this correspondence:

Proposition 3.3.2. *Let s, s_0 be two different normalized sections of $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$, then the corresponding 2-cocycles differ by a 2-coboundary.*

Proof. Since, for every $g \in G$, $s(g)$ and $s_0(g)$ lie in the same coset of M, there exists an element $\alpha(g) \in M$ such that $s_0(g) = \alpha(g)s(g)$. Therefore:

$$f_0(g,h) = \alpha(g)s(g)\alpha(h)s(h)s(gh)^{-1}\alpha(gh)^{-1} =$$
$$= \alpha(g) + s(g)\alpha(h)s(g)^{-1} + s(g)s(h)s(gh)^{-1} - \alpha(gh) =$$
$$= f(g,h) + g * \alpha(h) - \alpha(gh) + \alpha(g).$$

So, we have $(\bar{f}_0 - \bar{f})(\langle g|h\rangle) = \partial^1\bar{\alpha}$. □

In the end, $[f]$ does not depend on the choice of the section therefore, it is a property of the extension. When there's no ambiguity we will denote it by $[f_E]$ and we will call it the **factor system** of E. Now we prove that it is also invariant under equivalence of extensions:

Proposition 3.3.3. *Let* $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ *and* $0 \to M \xrightarrow{i'} E' \xrightarrow{\pi'} G \to 1$ *be two extensions of* G *by* M *with* $[f_E] = [f_{E'}]$*; then the two extensions are equivalent.*

Proof. It is sufficient to prove that there exists a morphism $\varphi : E \to E'$ such that $i' = \varphi \circ i$ and $\pi = \pi' \circ \varphi$. Every element h of E can be written uniquely in the form $h = i(m)s(g) \equiv (m, g)_E$ with s some fixed section of E; so we can define $\varphi(s(g)) := i'(\alpha(g))s'(g)$ (where s' is some fixed section of E' and α is a map such that $f_E(g, h) - f_{E'}(g, h) = g * \alpha(h) - \alpha(gh) + \alpha(g))$, and $\varphi(i(m)) := i'(m)$ (in particular $\varphi(e_E) = \varphi(i(0)) = i'(0) = e_{E'}$) and so, $\varphi(h) := i'(m + \alpha(g))s'(g)$. This map is an homomorphism: indeed, $\varphi((m, g)_E(m', g')_E) = \varphi((m + g * m' + f_E(g, g'), gg')_E) = i'(m + g * m' + f_E(g, g') + \alpha(gg'))s'(gg') = (m + g * m' + f_E(g, g') + \alpha(gg'), gg')_{E'} = (m + g * m' + f_{E'}(g, g') + \alpha(g) + g * \alpha(g'), gg')_{E'} = (m + \alpha(g), g)_{E'}(m' + \alpha(g'), g')_{E'} = \varphi((m, g)_E)\varphi((m', g')_E)$. □

Viceversa, if we take $[f] \in H^2(G, M)$ we can consider the extension $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ where $E := M \times G$ endowed with the multiplicative law: $(m, g)(m', g') := (m + g * m' + f(g, g'), gg')$. Since $\bar{f} \in ker(\partial^2)$ this law is associative, the identity element is $(0, e_G)$ and $(m, g)^{-1} = (-g^{-1} * (m + f(g, g^{-1})), g^{-1})$ since $f(g, g^{-1}) = -g * f(g^{-1}, g)$. Finally, if we set $i(m) := (m, e_G)$, $\pi(m, g) := g$, $s(g) := (0, g)$ we have $f(g, h) = i^{-1}(s(g)s(h)s(gh)^{-}1)$.
Therefore, there is a bijection between $H^2(G, M)$ and the extensions of G by M (**Shreirer's Theorem**, 1926).

Remark 3.3.4. Let us consider the extension where $E := M \ltimes_\varphi G$ and

$\varphi(g)(m) := g * m$ and i (respectively π) is the canonical embedding (respectively projection). In this case we can choose s in such a way that $f = 0$; therefore, if $H^2(G, M) = 0$ then there is only one extension of G by M, so it must be exactly $G \ltimes_\varphi M$.

Definition 3.3.5. *Let $M \in Ab$, $G \in Grp$, $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ an extension, then we say that this extension is* **central** *if $i(M) \subseteq Z(E)$, where $Z(E)$ is the center of E.*

Example 3.3.6. The extension $0 \to \mathbb{Z}_2 \xrightarrow{i} Q_8 \xrightarrow{\pi} \mathbb{Z}_2 \times \mathbb{Z}_2 \to 0$, where $i([1]) := -1$, $\pi(i) := ([1], [0])$, $\pi(j) := ([0], [1])$ is a central extension.

Notice that in the case of a central extension, the induced action of G on M must be trivial; the converse is also true: $(m_2, g)(m_1, e_G) = (m_2 + g * m_1 + f(g, e_G), g) = (m_1 + m_2, g) = (m_1, e_G)(m_2, g)$, that is, every element in E commutes with element in $i(M)$. Therefore central extensions of a group G by an abelian group M are classified by the second cohomology group $H^2(G, M)$, where here M is understood as a G-module with the trivial G-action.
Finally, it is easy to see that a split central extension is necessarily a direct product since in this case $f = 0$ and the action of G on M is trivial.

3.3.4 The third cohomology group

The third cohomology group arises naturally from considering generic extensions, that is, extensions where M can be nonabelian. In particular, we will start from the same strategies as those in Section 3.3.3, but in the most general setting. To this purpose, let us consider an extension $1 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$, where $M, E, G \in Grp$ and let us take a

set-theoretic section s of G. Then for any $g \in G$ we can induce an automorphism on M, say ω_g, such that $\omega_g(m) = i^{-1}(s(g)i(m)s(g)^{-1})$. In case M is nonabelian, this function $\omega : G \to Aut(M)$ is not an action, indeed it is not a morphism: as in the previous paragraph, we can consider the function $f(g,h) := i^{-1}(s(g)s(h)s(gh)^{-1})$, then we have $\omega_{gh} = \phi_{f(g,h)^{-1}} \circ \omega_g \circ \omega_h$. Moreover, we point out that as in the previous paragraph, due to the associativity in E, f satisfies a "generalized cocycle condition": $f(g,h) = \omega_g(f(h,k))f(g,hk)f(gh,k)^{-1}$, for every $g,h,k \in G$.

Definition 3.3.7. *Let $G \in Grp$ and $\phi : G \to Aut(G)$ such that $\phi(g)$ is the conjugation by g, then we define:*

- *the group of* **inner** *automorphisms as $Inn(G) := Im(\phi)$;*
- *the group of* **outer** *automorphisms as $Out(G) := Aut(G)/Inn(G)$.*

Remark 3.3.8.

- Definition 3.3.7 is well-posed, indeed $Inn(G)$ is normal in $Aut(G)$: let $\sigma \in Aut(G)$ and $a \in G$, then we have $\sigma \circ \phi_a \circ \sigma^{-1} = \phi_{\sigma(a)} \in Inn(G)$.
- $Z(G) = ker(\phi)$, hence $Inn(G) \cong G/Z(G)$.
- The sequence $1 \to Z(G) \hookrightarrow G \xrightarrow{\phi} Aut(G) \twoheadrightarrow Out(G) \to 1$ is exact.
- $f : Out(G) \to Aut(Z(G))$, $f([\varphi]) := \varphi_{|Z(G)}$ is a well-defined injective homomorphism, indeed since for every $\theta \in Inn(G)$, $\theta_{|Z(G)} = id_{Z(G)}$, then if $[\varphi^1] = [\varphi^2] \in Out(G)$, there exists $\theta \in Inn(G) : \theta \circ \varphi^1 = \varphi^2$, thus $\varphi^2_{|Z(G)} = (\theta)_{|Z(G)} \circ (\varphi^1)_{|Z(G)} = \varphi^1_{|Z(G)}$.

- Since every inner automorphism fixes element-wise $Z(M)$ and $Z(M)$ is characteristic in M, we can see a morphism from G to $Out(M)$ as an action of G on $Z(M)$, in this way $Z(M)$ is a G-module.

Therefore ω can be understood as a morphism from G to $Out(M)$; thus from now on we denote by ω the morphism sending $g \in G$ to $[\omega_g]$. Furthermore, these functions depend on the choice of the section s, namely, if s' is another set-theoretic section of G, then we can define a function $\alpha : G \to M$ in such a way that $s'(g) = i(\alpha(g))s(g)$, for every $g \in G$; thus, $\omega'_g = \phi_{\alpha(g)} \circ \omega_g$ where $\phi_{\alpha(g)} \in Aut(M)$ is the conjugation by $\alpha(g)$, and $f'(g,h) = \alpha(g)\omega_g(\alpha(h))f(g,h)\alpha(gh)^{-1}$. Then we can define en equivalence relation of pairs $(\omega,\ f)$ where $\omega \in Hom(G, Out(M))$ and f is a function from $G \times G$ to M satisfying the generalized cocycle condition: $(\omega,\ f) \sim (\omega',\ f')$ if and only if there exists $\alpha : G \to M$ such that $\omega'(g) = \phi_{\alpha(g)} \circ \omega(g)$ and $f'(g,h) = \alpha(g)\omega_g(\alpha(h))f(g,h)\alpha(gh)^{-1}$, for every $g, h \in G$. We call such equivalence classes of pairs **generalized cocycles**. By similar arguments as those used in section 3.3.3, we can establish an injective correspondence between equivalence classes of extensions of G by M and generalized cocycles $[(\omega,\ f)]$.

Now, we want to figure out when there exists an extension inducing a fixed morphism $\omega \in Hom(G, Out(M))$: for every $g \in G$, fix some representative of $\omega(g)$, say ω_g (in particular we choose $\omega_{e_G} = id_M$); then we have $\omega_g\omega_h\omega_{gh}^{-1} \in Inn(M)$, since $[\omega_g\omega_h\omega_{gh}^{-1}] = [\omega_g] + [\omega_h] - [\omega_{gh}] = 0$. Thus we can define a function $f : G \times G \to M$ such that $\omega_g\omega_h\omega_{gh}^{-1} = \phi_{f(g,h)}$, for every $g, h \in G$ (we choose $f(g, e_G) = f(e_G, h) = e_M$, for every $g, h \in G$). In general, the pair (ω, f) is not a generalized cocycle, thus we can not induce

an extension as we have done before. Indeed, all we can say is that:

$$\phi_{f(g,h)f(gh,k)} = \phi_{f(g,h)} \circ \phi_{f(gh,k)} = \omega_g\omega_h\omega_{gh}^{-1}\omega_{gh}\omega_k\omega_{ghk}^{-1} =$$
$$= \omega_g\omega_h\omega_k\omega_{ghk}^{-1} = \omega_g\omega_h\omega_k\omega_{hk}^{-1}\omega_g^{-1}\omega_g\omega_{hk}\omega_{ghk}^{-1} =$$
$$= \phi_{\omega_g(f(h,k))} \circ \phi_{f(g,hk)} = \phi_{\omega_g(f(h,k))f(g,hk)}.$$

Therefore, it must be $\bar{c}(g,h,k) := f(g,h)f(gh,k)(\omega_g(f(h,k))f(g,hk))^{-1} \in Z(M)$. In particular, it can be proven that the function $c : \bigoplus_{g,h,k\in G} \mathbb{Z}[G]\langle g|h|k\rangle \to Z(M)$ with $c(\langle g|h|k\rangle) := \bar{c}(g,h,k)$ is a 3-cocycle in cohomology of G with coefficients in $Z(M)$ (seen as a G-module with the action induced by ω). We will show only a part of the proof since the remaining calculations are analogous (see [11] Lemma 3.5, pg. 35 for the full process).
We need to prove: $\omega_g(\bar{c}(h,k,l)) - \bar{c}(gh,k,l) + \bar{c}(g,hk,l) - \bar{c}(g,h,kl) + \bar{c}(g,h,k) = 0$ that is $\omega_g(\bar{c}(h,k,l)) + \bar{c}(g,h,k) + \bar{c}(g,hk,l) = \bar{c}(g,h,kl) + \bar{c}(gh,k,l)$, for every $g,h,k,l \in G$. We have:

$$\bar{c}(g,h,kl) + \bar{c}(gh,k,l) =$$
$$= f(g,h)f(gh,kl)(\omega_g(f(h,kl))f(g,hkl))^{-1}f(gh,k)f(ghk,l)(\omega_{gh}(f(k,l))$$
$$f(gh,kl))^{-1} = f(g,hkl)^{-1}\omega_g(f(h,kl))^{-1}f(g,h)f(gh,kl)f(gh,kl)^{-1}$$
$$\omega_{gh}(f(k,l))^{-1}f(gh,k)f(ghk,l) = \omega_g(f(h,kl))^{-1}f(g,h)f(gh,kl)f(gh,kl)^{-1}$$
$$\omega_{gh}(f(k,l))^{-1}f(gh,k)f(ghk,l)f(g,hkl)^{-1} = \omega_g(f(h,kl))^{-1}f(g,h)$$
$$\omega_{gh}(f(k,l))^{-1}f(gh,k)f(ghk,l)f(g,hkl)^{-1}.$$

Proposition 3.3.9. *If c is the 3-cocycle defined earlier, then there exists an extension of G by M inducing the morphism ω if and only if c is a 3-coboundary.*

Proof. We have already seen that an extension $1 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ induces a generalized cocycle $[(\omega, f)]$, hence in this case $\bar{c}(g,h,k) = e_M$, for all $g,h,k \in G$, that is $c = 0$ in $H^3(G, Z(M))$. Now, if c is a 3-coboundary, then it must be: $\bar{c}(g,h,k) = g * (a_{h,k}) - a_{gh,k} + a_{g,hk} - a_{g,h}$, for every $g,h,k \in G$, where $g*(a_{h,k}) \equiv \omega_g(a_{h,k})$ and $a_{g,h} \in Z(M)$, for every $g,h \in G$. We define $f'(g,h) := f(g,h)a_{g,h}^{-1}$, notice that $\phi_{f'(g,h)} = \phi_{f(g,h)}$; therefore, by definition of f, we can simply consider f' instead. It is easy to see that in this way the pair $[(\omega, f')]$ is a generalized cocycle, so we can construct an extension as before with $E := M \times G$, the group law $(m,g) * (m',g') := (m \cdot g * m' \cdot f(g,g'), gg')$ and i, π respectively the canonical inclusion of M in $M \times G$ and the canonical projection of $M \times G$ onto G. □

Theorem 3.3.10. *Let $\omega \in Hom(G, Out(M))$ and consider $Z(M)$ as a G-module with the action induced by ω; if there exists some extension of G by M inducing ω, then they are classified by $H^2(G, Z(M))$.*

Proof. We are assuming that an extension exists, so let $[(\omega, f_0)]$ be the generalized cocycle induced by that extension; from now on we will consider $Z(M)$ as a G-module with G acting on $Z(M)$ by ω. We define the map $\theta : H^2(G, Z(M)) \to \{$generalized cocycles induced by extensions of G by $Z(M)\}$, $\theta([c]) := [(\omega, cf_0)]$. This map is well defined, indeed if $[c] = [c']$, then $c'(g,h) = \bar{\alpha}(g,h)c(g,h)$ where $\bar{\alpha}$ is a 2-coboundary, hence $c'(g,h)f_0(g,h) = (\omega_g(\alpha(h)) - \alpha(gh) + \alpha(g))c(g,h)f_0(g,h) = \alpha(g)\omega_g(\alpha(h))$ $c(g,h)f_0(g,h)\alpha(gh)^{-1}$. Moreover, it is easy to see that $[(\omega, cf_0)]$ is a generalized cocycle. Now we need to prove that this map is a bijection:

- surjectivity: let $[\omega, f]$ be a generalized cocycle, then $\phi_{f(g,h)} = \omega_g\omega_h\omega_{gh}^{-1} = \phi_{f_0(g,h)}$; so there exists an element $c(g,h) \in Z(M)$ such that $f(g,h) =$

$c(g,h)f_0(g,h)$, for every $g,h \in G$. In order to conclude it is sufficient to prove that $c(g,h)$ is a 2-cocycle, this follows easily from the fact that $c(g,h) \in Z(M)$ and f, f_0 satisfy the generalized cocycle condition;

- injectivity: let $[\omega, cf_0] = [\omega, c'f_0]$, then by definition for every $g \in G$, there exists $a_g \in M$ such that:

$$\omega_g = \phi_{a_g}\omega_g$$
$$c'(g,h)f_0(g,h) = a_g\omega_g(a_h)c(g,h)f_0(g,h)a_{gh}^{-1}$$

that is, $a_g \in Z(M)$ and so $c(g,h)^{-1}c'(g,h) = a_g\omega_g(a_h)a_{gh}^{-1} \in Z(M)$, hence $[c] = [c']$ in $H^2(G, Z(M))$.

□

3.3.5 Higher dimension cohomology groups

Proposition 3.3.11. *If G is a finite group, then every element of $H^n(G,M)$, $n \in \mathbb{Z}_{>0}$, has finite order which divides $|G|$.*

Proof. Let $[a] \in H^{n+1}(G,M)$, then $\partial^{n+1}(a) = 0$ if and only if $a \circ \partial_{n+1} = 0$, therefore for every $g_1, \ldots, g_n, g_{n+1} \in G$, $0 = a(\partial_{n+1}(\langle g_1| \ldots |g_{n+1}\rangle)) = g_1 a(\langle g_2| \ldots |g_{n+1}\rangle) - \sum_{k=2}^{n+1}(-1)^k a(\langle g_1| \ldots |g_{k-1}g_k| \ldots |g_{n+1}\rangle) + (-1)^{n+1}a(\langle g_1| \ldots |g_n\rangle)$; since G is finite, we can sum over g_{n+1}:

$$\sum_{k=2}^{n+1}(-1)^k a\Big(\sum_{g_{n+1}\in G}\langle g_1| \ldots |g_{k-1}g_k| \ldots |g_{n+1}\rangle\Big) =$$
$$g_1 a\Big(\sum_{g_{n+1}\in G}\langle g_2| \ldots |g_{n+1}\rangle\Big) + (-1)^{n+1}a\Big(\sum_{g_{n+1}\in G}\langle g_1| \ldots |g_n\rangle\Big).$$

Then, if we set $f(\langle g_1|\dots|g_{n-1}\rangle) := a(\sum_{g\in G}\langle g_1|\dots|g_{n-1}|g\rangle)$, we obtain:

$$0 = g_1 f(\langle g_2|\dots|g_n\rangle) - \sum_{k=2}^{n}(-1)^k f(\langle g_1|\dots|g_{k-1}g_k|\dots|g_n\rangle)+$$
$$(-1)^n f(\langle g_1|\dots|g_{n-1}\rangle) + (-1)^{n+1}|G|a(\langle g_1|\dots|g_n\rangle) =$$
$$\partial^n(f)(\langle g_1|\dots|g_n\rangle) + (-1)^{n+1}|G|a(\langle g_1|\dots|g_n\rangle).$$

Therefore, $0 = [(-1)^n\partial^n(f)] = [|G|a] = |G|[a]$. □

Corollary 3.3.12. *Let G be a finite group and M be a finite G-module, then every element in $H^n(G,M)$ has finite order dividing $gcd(|G|,|M|)$.*

Proof. The result follows directly from Proposition 3.3.11, from the fact that every element in $Hom(K,M)$ has finite order which divides by $|M|$ and from the definition of the greatest common divisor. □

Remark 3.3.13. Let G be a finite group and M be a finite G-module such that $gcd(|G|,|M|) = 1$. Then $H^n(G,M) = 0$ for all $n \in \mathbb{Z}_{>0}$.

Proposition 3.3.14. *If G is a finite group and M is a finitely generated G-module then $H^n(G,M)$ is finitely generated for all n.*

Proof. Consider the bar complex $F_\cdot \to \mathbb{Z} \to 0$. Then for every $n \in \mathbb{Z}_{\geq 0}$ F_n is finitely generated since G is finite (in particular, it is generated by $|G|^n$ elements), therefore $Hom_{\mathbb{Z}[G]}(F_n, M)$ is finitely generated. Indeed, consider a finite set of generators of M, say A: then, a map in $Hom_{\mathbb{Z}[G]}(F_n,M)$ is uniquely determined by the images of basis elements of F_n; therefore, fix a basis B of F_n and take $C := \{\delta_b^a \in Hom_{\mathbb{Z}[G]}(F_n,M)|\ a \in A, \in B\}$ where δ_b^a is the unique map such that $\delta_b^a(b') = 0$, for every $b' \in B \setminus \{b\}$ and $\delta_b^a(b) = a$.

Then, it is clear that C generates $Hom_{\mathbb{Z}[G]}(F_n, M)$. Finally, since $H^n(G, M)$ is a quotient of $Hom_{\mathbb{Z}[G]}(F_n, M)$ it is finitely generated too. □

Corollary 3.3.15. *If G is a finite group and M is a finitely generated G-module then $H^n(G, M)$ is finite for all n and its order divides $|G|$.*

Proof. The proof follows easily from Propositions 3.3.11 and 3.3.14 and the structure theorem of finitely generated abelian groups (Theorem 1.1.14). □

3.4 Some results on classifications

Theorem 3.4.1. *Let $n \in \mathbb{Z}_{>0}$ and $M \in \mathbb{Z}_n Mod$. We define ${}_{\bar{N}}M := \{x \in M |\ \bar{N}(x) = 0\}$, where $\bar{N}$ is the multiplication by $[0] + \cdots + [n-1]$. Then, for every $m \geq 1$,*

$$H^0(\mathbb{Z}_n, M) \cong M^{\mathbb{Z}_n}$$
$$H^{2m-1}(\mathbb{Z}_n, M) \cong {}_{\bar{N}}M/\bar{D}M$$
$$H^{2m}(\mathbb{Z}_n, M) \cong M^{\mathbb{Z}_n}/\bar{N}M$$

where $\bar{D}$ is the multiplication by $[1] - [0]$.

Proof. Consider the free resolution of $\mathbb{Z}$ defined in Example 3.2.4. In this case we have for every $n \geq 0$, $f \in Hom(\mathbb{Z}[\mathbb{Z}_n], M)$, $d^{2n+1}(f) = f \circ D = \bar{D} \circ f$ and $d^{2n}(f) = f \circ N = \bar{N} \circ f$. Let $f \in Hom(\mathbb{Z}[\mathbb{Z}_n], M)$, then $f \in \ker(d^{2n+1})$ if and only if $([0] - [1]) * f([0]) = 0$, that is $f([0]) \in M^{\mathbb{Z}_n}$; moreover $f \in \mathrm{Im}(d^{2n+1})$ if and only if $f([0]) \in \bar{D}M$. Since $Hom(\mathbb{Z}[\mathbb{Z}_n], M) \cong M$ as modules we have: $\ker(d^{2n+1}) \cong M^{\mathbb{Z}_n}$, $\mathrm{Im}(d^{2n+1}) \cong \bar{D}M$, $\ker(d^{2n} \cong {}_{\bar{N}}M$ and $\mathrm{Im}(d^{2n} \cong \bar{N}M$. Finally, the result follows from the definition of $H^k(\mathbb{Z}_n, M)$. □

Definition 3.4.2. *Let G be a finite group of order $p^n m$ where p is a prime, $n > 0$ and m is not divisible by p, then a* **Sylow $\mathbf{p-}$subgroup** *of G is a subgroup of order p^n (a maximal p-subgroup).*

Definition 3.4.3. *Let G be a finite group, then a* **Hall subgroup** *H of G is a subgroup such that $gcd(|H|, [G : H]) = 1$.*

Definition 3.4.4. *Let G be a finite group and $H \leq G$ then we define the* **normalizer** *of H in G as the group $N_G(H) := \{g \in G |\ gHg^{-1} = H\}$.*

Example 3.4.5.
- Let $N \trianglelefteq G$ then $N_G(N) = G$.
- Let $H := \{e, (1\,2)\} \leq \mathfrak{S}_n$, then $N_G(N) = \{\alpha \in \mathfrak{S}_n |\ \alpha \cdot (1\ 2) = (1\ 2) \cdot \alpha\}$.

Remark 3.4.6. $N_G(H)$ is the largest subgroup of G in which H is normal and in particular if $H \leq K \leq G$, then $K \cap N_G(H) = N_K(H)$.

Lemma 3.4.7 (Frattini Argument)**.** *Let G be a finite group, $K \trianglelefteq G$ and P a Sylow p-subgroup of K (for some prime p), then $G = KN_G(P)$.*

Proof. Let $g \in G$, then $gPg^{-1} \leq gKg^{-1} = K$; hence gPg^{-1} is a Sylow p-subgroup of K, so by the second Sylow Theorem there exists $k \in K$ such that $kPk^{-1} = gPg^{-1}$. Therefore, $P = (k^{-1}g)P(k^{-1}g)^{-1}$, that is $k^{-1}g \in N_G(P)$. Thus we can write $g = k(k^{-1}g)$. □

Definition 3.4.8. *Let G be a group and $H \leq G$; H is* **characteristic** *in G if $\phi(H) = H$ for every $\phi \in Aut(G)$.*

Notice that since every conjugation by an element of G is an automorphism of any normal subgroup K of G, then if we take $H \leq K$ characteristic in K, then H is fixed by the conjugation, that is, H is normal in G.

Example 3.4.9. The center $Z(G)$ is always a characteristic subgroup of G.

Theorem 3.4.10 (Schur-Zassenhaus, 1937)**.** *If $n, m \in \mathbb{Z}_{>0}$ are relatively prime, then any extension $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ of a group M of order m by a group G of order n is right split.*

Proof. If M is abelian, the result follows directly from 3.3.13. For the general case it is sufficient to prove that for every finite group E of order mn which has M as a normal subgroup, there exists a subgroup $H \leq E$ of order n. Indeed, since $gcd(n, m) = 1$, it must be $H \cap M = e_E$, thus $E = HM$ and by the second isomorphism theorem $G \cong E/M = HM/M \cong H/(H \cap M) \cong H$. Moreover every element in E can be written in a unique way as product of an element in H and an element in M: indeed, if $g = hk = \bar{h}\bar{k}$ then $\bar{h}^{-1}h = \bar{k}k^{-1} \in H \cap M = \{e_E\}$ hence $k = \bar{k}$ and $h = \bar{h}$, for every $g \in E$. Thus, $E \cong G \ltimes_\phi M$ with $\phi(g)(k) = g^{-1}kg$. Furthermore, $\pi = p \circ f$, where $f(gk) := (g, k)$ and $p((g, k)) := g$, and $i \circ f = i'$ that is $0 \to M \xrightarrow{i} E \xrightarrow{\pi} G \to 1$ and $0 \to M \xrightarrow{i'} G \ltimes_\phi M \xrightarrow{p} G \to 1$ are equivalent where f is the equivalence map.

We will proceed by induction on m. The base case $m = 1$ is trivial; now let us divide the induction step into two cases:

- suppose M has a proper nontrivial subgroup T normal in E. Then, $M/T \lhd E/T$ and $(E/T)/(M/T) \cong E/M$ which has order n, hence M/T is a Hall subgroup of E/T and has order strictly less than m; therefore by induction hypothesis there exists a subgroup of E/T with order n, say H/T. Moreover, since T is a Hall subgroup also for H, by induction hypothesis on H, there exists a subgroup of H (and so, of E) which has order n.

- Now, suppose the only subgroup of M normal in E is the trivial one; let p be a prime divisor of m and P be a Sylow p-subgroup of M. Therefore, we have $E = KN_E(P)$ (since the Frattini argument 3.4.7); moreover, by the second isomorphism theorem we have: $G \cong E/M = MN_E(P)/M \cong N_E(P)/(M \cap N_E(P)) = N_E(P)/N_M(P)$. Now, if $|N_E(P) < nm|$, then $|N_M(P)| < m$, so by induction hypothesis $N_E(P)$ (and so, also E) has a subgroup of order n. Thus we can now suppose $N_E(P) = E$, that is $P \trianglelefteq E$; therefore it must be $P = M$. As we have seen above, since $Z(M)$ is characteristic in M, $Z(M)$ is normal in E, therefore it must be either $Z(M) = e_E$ or $Z(M) = M$; but, M is a p-group hence its center can not be trivial: indeed, from the class equation $|M| = |Z(M)| + \sum_{x \notin Z(M)} [M : C(x)]$ (where $C(x) := \{y \in M | xy = yx\}$ is the centralizer of x); for every $x \notin Z(M)$, has to be $p|[M : C(x)]$ and this imply $p|(|M| - \sum_{x \notin Z(M)} [M : C(x)]) = |Z(M)|$, therefore $|Z(M)| \neq 1$.

□

Bibliography

[1] Artin, M.: Algebra, Bollati Boringhieri, 1997, PROGRAMMA DI MATEMATICA FISICA, ISBN: 9788833955865.

[2] Burde, D.: Cohomology of Groups and Algebras, Lecture Notes 2023; available at: https://homepage.univie.ac.at/dietrich.burde/papers/burde_76_coho.pdf.

[3] Conrad, K.: Modules over a PID; available at: https://kconrad.math.uconn.edu/blurbs/linmultialg/modulesoverPID.pdf.

[4] Erdmann, K., Holm, T.: Algebras and Representation Theory. Springer, Berlin (2018).

[5] Etingof, P., Gerovitch, S., Golberg, O., Hensel, S., Liu, T., Schwendner, A., Vaintrob, D., Yudovina, E.: Introduction to representation theory, American Mathematical Society, Providence, Rhode Island, UK, ISBN 9780821853511 (2011).

[6] Ho, R.: Classification of Group Extensions and H^2; available at: https://math.uchicago.edu/ may/VIGRE/VIGRE2011/REUPapers/Ho.pdf.

[7] Morandi, P.: Group Extensions and H^3; available at: https://drive.google.com/file/d/1DRRHEV2LBK68-wksxqfkQ_h1vqGWtfCG/view?usp=drive_link.

[8] Schedler, T.: Fundamental theorem of modules over a PID and applications; available at: https://math.uchicago.edu/∼womp/2007/PIDmod2007.pdf.

[9] Schreier, O.: Über die Erweiterung von Gruppen I. Monatsh. f. Mathematik und Physik 34, 165-180 (1926).

[10] Spindler, K.: A short and elementary proof of the structure theorem for finitely generated modules over PIDs. Elemente der Mathematik, 2018, 73.3: 136-138.

[11] Rotman, J.: An Introduction to Homological Algebra. Springer Science & Business Media, second edition, 2008.

[12] Rotman, J.: An Introduction to the Theory of Groups, Vol. 148 of Graduate Texts in Mathematics, 4th Edition, Springer, 1995.

[13] Tao, T.: Some notes on group extensions, 2010; available at: https://terrytao. wordpress.com/2010/01/23/some-notes-on-group-extensions/.

[14] Zhang, C.: Classifying group extensions with not necessarily abelian kernel; available at: https://pnp.mathematik.uni-stuttgart.de/lexmath/kuenzer/bachelor_zhang.pdf.