MH4930: Special Topics in Mathematics Homological Algebra

by Loo Wee Lun

Taken during AY 25/26 at

School of Physical and Mathematical Sciences

Nanyang Technological University

Contents

0 Preface and Disclaimer **2**

1 Module Theory **3**
1.1 Definition and Basic Theory of Modules 3
1.2 Algebras and Module Homomorphisms 4
1.3 Free Module and Tensor Product 9

2 Injective, Projective, and Flat Modules **21**
2.1 Short Exact Sequence and Splitting 21
2.2 Projective Modules and Introduction to Categories 27
2.3 Injective Modules 31
2.4 Flat Modules 37

3 (Co)Homology, Ext Group, and Tor Group **43**
3.1 Basic Theory of (Co)Homology 43
3.2 Ext Group 46
3.3 Tor group 57
3.4 Group Cohomology 60
3.5 Induced Module 65
3.6 Inflation, Restriction, and Corestriction Homomorphisms 68
3.7 Intepretation of First and Second Group Cohomology 74

0 Preface and Disclaimer

This note is written by me, a student who taken the course MH4930: Special Topics in Mathematics under Dr. Lim Kay Jin during academic year 25/26 at the School of Physical and Mathematical Sciences of Nanyang Technological University in Singapore.

I hereby disclaim that the contents of this note are intended solely for my personal use and are not originally produced by me, except for the presentation of the written proofs. I do not take responsibility for any grammatical or mathematical errors in this note. The note may be incomplete, and once the course is finished, I will no longer update it for any reason.

1 Module Theory

1.1 Definition and Basic Theory of Modules

Definition 1.1.1 (Module)**.** Let R be a ring (might be unital or not). A left R-module M is an abelian group $(M,+)$ with binary operation $\cdot : R \times M \to M, (r,m) \mapsto r \cdot m$ such that for every $r,s \in R$ and $m,n \in M$ we have

1. $(r+s)\cdot m = r\cdot m + s\cdot m$
2. $r\cdot(s\cdot m) = (rs)\cdot m$
3. $r\cdot(m+n) = r\cdot m + r\cdot n$

Additionally, if R is unital, then we want $1\cdot m = m$.

One can think of module analogous to "ring action".

Remark 1.1.2. One can define a right R-module in a similar manner. However, the existence of a left module does not necessarily imply the existence of a corresponding right module, where the usual obstruction is the second criteria. Despite that, we describe a general procedure in constructing a right module from a left module.

Suppose $(R,+,\star)$ is a ring. Let $(R^{\text{op}},+,*)$ be a ring where R^{op} is the same set as R but the operation $*$ is defined as $a * b := b \star a$. Then any left R-module $(M,\cdot)$ is a right R^{op} module with operation $\cdot_{\text{op}}$ defined as $m \cdot_{\text{op}} r := r \cdot m$ and vice versa.

Remark 1.1.3. If R is a commutative ring, then any left R-module is a right R-module via the the binary operation $m * r := r \cdot m$.

From now onward, all mentioned module is a left module unless otherwise specified.

Definition 1.1.4 (Sub-module)**.** Let M be an R-module and $N \subseteq M$. We say that N is a sub-module of M if N is also an R-module under the same action.

Remark 1.1.5. If R is a field, then an R-module is a vector space over F. Naturally, a sub-module over a field is a subspace. Thus, the idea of module can be interpreted as a generalization of the theory of vector spaces.

Proposition 1.1.6. *Let M be a group. We have M is abelian if and only if M is a $\mathbb{Z}$-module.*

Proof. ($\Longleftarrow$). This is trivial, since by definition a module must be abelian.

($\Longrightarrow$). For any $n \in \mathbb{Z}$ and $m \in M$, define the operation where

$$n \cdot m \begin{cases} \underbrace{m + \cdots + m}_{n \text{ times}} & , n \geq 0 \\ \underbrace{(-m) + \cdots + (-m)}_{-n \text{ times}} & , n < 0 \end{cases}$$

Then by verifying the axioms (which are omitted here), one can show that M is indeed a $\mathbb{Z}$-module. □

Example 1.1.7. Here, we provide some examples of modules.

1. For any ring R, the trivial module is defined to be $M := \{0\}$ where $r \cdot 0 := 0$ for any $r \in R$
2. For any ring R, the regular R-module is defined to be $M = R$ where $r \cdot m := rm$. To distinguish R as a ring and as a module, we use ${}_R R$ to denote the ring R being a regular module.
3. For any unital ring R, the free R-module is defined to be $M := R^n$ where $r \cdot (v_1, \ldots, v_n) := (rv_1, \ldots, rv_n)$
4. Let $M := \mathbb{R}$, then
   (a) if $R = \mathbb{R}$, then it is a regular module.

(b) if $R = \mathbb{Q}$, then it is a infinite dimensional vector space.

(c) if $R = \mathbb{Z}$, then it is viewed as an abelian group.

5. (Restriction of scalars). Let $\varphi : R \to S$ be a ring homomorphism and $(M, \cdot)$ be an S-module. Then M is an R-module via $r \star m := \varphi(r) \cdot m$.

6. Let $(N, \cdot)$ be an R-module. The annihilator of N is defined to be

$$\mathrm{Ann}_R(N) = \{r \in R : r \cdot n = 0 \ \forall n \in N\}$$

Suppose that $\pi : R \to S$ is a ring epimorphism such that $\ker \pi \subseteq \mathrm{Ann}_R(N)$. Then N is an S-module via $s \star n = r \cdot n$ where $\pi(r) = s$.

7. Let $R = \mathbb{M}_{n\times n}(F)$ where F is some field and $V = \mathbb{M}_{n\times 1}(F)$. Then V is a R-module via left multiplication as the binary operation. We say V is the natural module over the matrix ring R.

Remark 1.1.8. The sub-module of a regular module corresponds to left ideal.

From now onward, all rings are unital unless otherwise specified.

Proposition 1.1.9. *Let M be an R-module, and $x \in N$, $r \in R$. Then we have*

- $0_R \cdot x = 0_M$
- $-1_R \cdot x = -x$

Proof. For the first statement, note that

$$r \cdot m = (0_R + r) \cdot m = 0_R \cdot m + r \cdot m \implies 0_R \cdot m = r \cdot m - r \cdot m = 0_M$$

For the second statement, note that

$$0_M = 0_R \cdot x = (1_R + (-1_R)) \cdot x = 1_R \cdot x + (-1_R \cdot x) = x + (-1_R \cdot x)$$

The statement follows by moving x from LHS to RHS. □

Proposition 1.1.10 (Sub-module criterion)**.** *Let M be a R-module and $N \subseteq M$. We have that N is a sub-module of M if and only if N is non-empty and $x + r \cdot y \in N$ for any $x, y \in N$ and $r \in R$.*

Proof. ($\implies$). If N is a sub-module of M, then N must not be empty since it must contain the identity element. Moreover, since N is a sub-module, thus for any $y \in N$ and $r \in R$ we must have $r \cdot y \in N$ by closure. It is then obvious that $x + r \cdot y \in N$ for any $x, y \in N$ and $r \in R$.

($\impliedby$). Suppose that $N \subseteq M$ is non-empty $x + r \cdot y \in N$ for any $x, y \in N$ and $r \in R$. First note by taking $r = -1$ we see that for any $x, y \in N$ we have $x - y \in N$, thus by the subgroup criterion we see that N is a subgroup of M. Next, since N is non-empty, let $n \in N$ and take $r = -1$. By Proposition 1.1.9 we see that

$$0_M = n - n = n + (-1) \cdot n \in N$$

Finally, by taking $r = 0_R$, we $x = 0_M$ we see that for any $r \in R$ and $y \in N$ we have $r \cdot y \in N$, which establish the closure. This completes the proof. □

Remark 1.1.11. Note that Proposition 1.1.10 can only be used for unital rings. For non-unital rings, we can only prove sub-module via showing that the axioms are true.

1.2 Algebras and Module Homomorphisms

Definition 1.2.1 (R-Algebra)**.** Let R be a commutative (unital) ring. An R-algebra A is a (unital) ring with ring homomorphism $\varphi : R \to A$ such that $\varphi(1_R) = 1_A$ and $\varphi(R) \subset Z(A)$, where $Z(A)$ is the center of the multiplicative group of A.

Example 1.2.2. Let $A = R[X]$ where R is any ID or even a field. Define the ring homomorphism $\varphi : R \to R[X],\ r \mapsto r$. Then $R[X]$ is an R-algebra.

Proposition 1.2.3. *R-algebra A is a R-module via the binary operation $r \cdot a := \varphi(r)\, a$ where φ is the ring homomorphism that embeds R to the center of A.*

Proof. We just have to verify the axioms of modules: for any $r, s \in R$ and $a, b \in A$ we have

1. $(r+s) \cdot a = \varphi(r+s)\, a = (\varphi(r) + \varphi(s))\, a = \varphi(r)\, a + \varphi(s)\, a = r \cdot a + s \cdot a$.
2. $r \cdot (s \cdot a) = \varphi(r)\varphi(s)\, a = \varphi(rs)\, a = (rs) \cdot a$
3. $r \cdot (a+b) = \varphi(r)\,(a+b) = \varphi(r)\, a + \varphi(r)\, b = r \cdot a + r \cdot b$
4. $1_R \cdot a = \varphi(1_R)\, a = 1_A a = a$.

This completes the proof. □

Definition 1.2.4 (Algebra homomorphism)**.** Let $(A, \cdot)$ and $(B, \star)$ be R-algebras and $f : A \to B$ be a ring homomorphism. We then say f is an algebra homomorphism from A to B if $f(1_A) = 1_B$ and $f(r \cdot a) = r \star f(a)$. An algebra isomorphism is then a bijective algebra homomorphism.

Example 1.2.5 (Group algebra)**.** Let G be a group and R be a commutative ring. Define RG (or sometimes $R[G]$) to be the set

$$RG := \left\{ \text{formal finite sum of the form } \sum_{g \in G} r_g g \text{ where } r_g \in R \right\}$$

together with the operating rules

$$\sum r_g g + \sum s_g g = \sum (r_g + s_g)\, g$$

and

$$\left(\sum r_g g\right)\left(\sum s_g g\right) = \sum t_g g,\ t_g := \sum_{h \in G} r_{gh} s_{h^{-1}}$$

Then RG is an R-algebra and is called the group algebra of G over R.

Definition 1.2.6 (Module homomorphism)**.** Let V, W be R-module. The map $\varphi : V \to W$ is a R-module homomorphism if it is a group homomorphism and satisfies $\varphi(r \cdot v) = r \cdot \varphi(v)$ for all $r \in R$ and $v \in V$. An R-module isomorphism is then an R-module homomorphism which is also a group isomorphism.

Example 1.2.7 (Kernel and image)**.** Let $\varphi : V \to W$ be R-module homomorphism. Then we define

$$\ker \varphi := \{v \in V : \varphi(v) = 0\}$$

$$\operatorname{im} \varphi := \{\varphi(v) \in W : v \in V\}$$

Then $\ker \varphi$ and $\operatorname{im} \varphi$ is a sub-module of V and W respectively.

Example 1.2.8. Let V, W be R-module. The hom set from V to W over R is defined to be

$$\operatorname{Hom}_R\{V, W\} := \{R\text{-module homomorphism from } V \text{ to } W\}$$

Example 1.2.9.

1. Let $R := \mathbb{R}[x]$ and define $\varphi : R \to R$ where $\sum a_i x^i \mapsto \sum a_i x^{2i}$. Then φ is a ring homomorphism but not R-module homomorphism. If not, then it must satisfy $\varphi(x \cdot 1) = x$ but $\varphi(x \cdot 1) = \varphi(x) = x^2$.
2. Let $\pi_i : R^n \to R$ where $(r_1, \ldots, r_n) \mapsto r_i$. Then π_i is an R-module homomorphism since

   $$\pi_i(r \cdot (r_1, \ldots, r_n)) = \pi_i(rr_1, \ldots, rr_n) = rr_i = r \cdot \pi_i(r_1, \ldots, r_n)$$

   A partial converse is as follow: let $\tau_i : R \to R^n$ where $x \mapsto (0, \ldots, 0, x, 0, \ldots, 0)$ where x is at the i-th position. Then τ is an R-module homomorphism.
3. For V, W are R-modules, the trivial map is defined to be the R-module homomorphism $\varphi : V \to W$ where $v \mapsto 0_W$.

4. If R is a field, then R-module homomorphism is equivalent to linear transformation.

5. If $R = \mathbb{Z}$, then R-module homomorphism is equivalent to abelian group homomorphism.

Proposition 1.2.10. *Let U, V, W be R-module. We have the following*

1. *$\varphi : U \to V$ is an R-module homomorphism $\iff$ $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $r \in R$ and $x, y \in U$*

2. *$\mathrm{Hom}_R(U, V)$ is an abelian group where for $\varphi, \psi \in \mathrm{Hom}_R(U, V)$ we define $(\varphi + \psi)(u) = \varphi(u) + \psi(u)$ for all $u \in U$. Moreover, if R is commutative, then $\mathrm{Hom}_R(U, V)$ is an R-module with $(r \cdot \varphi)(u) = \varphi(ru)$.*

3. *If $\varphi \in \mathrm{Hom}_R(U, V)$ and $\psi \in \mathrm{Hom}_R(V, W)$, then $\psi \circ \varphi \in \mathrm{Hom}_R(U, W)$.*

4. *$\mathrm{End}_R(U) := \mathrm{Hom}_R(U, U)$ is a unital ring with multiplicative operation defined to be the composition, i.e. $\varphi \circ \psi$. Moreover, if R is commutative, then $\mathrm{End}_R(U)$ is an R-algebra.*

Proof.

1. The forward direction simply follows from the definition, thus omitted. For the backward direction, take $r = 1$ we obtain $\varphi(x + y) = \varphi(x) + \varphi(y)$, showing that it is a homomorphism. Take $y = 0$ we get $\varphi(rx) = r\varphi(x)$, showing that it a R-module homomorphism.

2. Tutorial question.

3. $(\psi \circ \varphi)(ru) = \psi(\varphi(ru)) = \psi(r\varphi(u)) = r\psi(\varphi(u)) = r(\psi \circ \varphi)(u)$

4. We have to prove that it is a unital ring. Let $\varphi, \alpha, \beta, \gamma \in \mathrm{End}_R(U)$,

   - Define map $\mathbb{1} : U \to U$ be the identity map. Clearly $\varphi \circ \mathbb{1} = \mathbb{1} \circ \varphi = \varphi$.
   - $(\alpha + \beta) \circ \gamma(u) = \alpha(\gamma(u)) + \beta(\gamma(u)) = (\alpha \circ \gamma)(u) + (\beta \circ \gamma)(u)$. This shows that $(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma$
   - Similarly for $\alpha \circ (\beta + \gamma) = \alpha \circ \beta + \alpha \circ \gamma$

   To show that it is an R-algebra when R is commutative, define $f : R \to \mathrm{End}_R(U)$ where $r \mapsto r\mathbb{1}$ where $r\mathbb{1} : u \mapsto ru$. It is clear that $r\mathbb{1} = r \cdot \mathbb{1}$. We now show that it is an algebra:

   - $f(r + s) = (r + s)\mathbb{1} = r\mathbb{1} + s\mathbb{1} = f(r) + f(s)$
   - $f(rs) = (rs)\mathbb{1} = (r\mathbb{1})(s\mathbb{1}) = f(r)f(s)$
   - $f(1) = 1 \cdot \mathbb{1} = \mathbb{1}$
   - $(r\mathbb{1}) \circ \varphi(u) = r\varphi(u) = \varphi(ru) = \varphi \circ (r\mathbb{1})(u)$. This shows that $(r\mathbb{1}) \circ \varphi = \varphi \circ (r\mathbb{1})$

   The first and second bullets show that f is indeed a ring homomorphism. The third bullet shows that f preserves identity. The last bullet shows that $f(R) \subseteq Z(\mathrm{End}_R(U))$. Together we conclude that $\mathrm{End}_R(U)$ is indeed an R-algebra.

This completes the proof. □

Remark 1.2.11. Let R, S be rings. An (R, S)-bimodule ${}_RM_S = ({}_RM, M_S)$ where $(rm)s = r(ms)$. Suppose we have ${}_RM_S$ and ${}_RN$. Then $\mathrm{Hom}_R(M, N)$ is an S-module where $(s \cdot \varphi)(m) := \varphi(ms)$.

Example 1.2.12. Let G be a group and F be a field. Consider $R = FG$ and let M be a left R-module. Then the right action defined to be $m * g := g^{-1}m$ makes it a right module.

Proposition 1.2.13. *Let $N \subseteq M$ be R-modules. Then M/N is an R-module where $r \cdot (m + N) := rm + N$. We have a canonical surjective R-module homomorphism $\pi : M \to M/N$.*

Example 1.2.14. Let $V_1, \ldots, V_m$ be submodules of V.

1. $V_1 + \cdots + V_m = \{v_1 + \cdots + v_m : v_i \in V_i\}$ is a submodule of V.

2. Let $A \subseteq V$. We define

$$\langle A \rangle := RA = \left\{ r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R,\ a_1, \ldots, a_n \in A, n \in \mathbb{Z}^+ \right\}$$

Then we say $\langle A \rangle$ is the submodule generated by A, and it is the smallest sub-module of V containing A.

It is clear that $R\emptyset = \{0\}$. Also, if $A = U$ is a submodule of V, then $RU = U$.

Definition 1.2.15 (Finitely generated)**.** Let U be a submodule of V. We say that U is finitely generated as an R-module if there exists a finite set $A \subseteq U$ such that $U = RA$.

Definition 1.2.16 (Cyclic)**.** Let U be a submodule of V. We say that U is cyclic if $U = RA$ where $A = \{a\} \subseteq U$ only contains one element.

Definition 1.2.17 (Minimal generating set)**.** Let V be a finitely generated module. Consider the collection $\mathcal{A}$ of all finite set A that generates V. Notice for all $A \in \mathcal{A}$ we must have $|A|$ is a non-negative integer. We say that a generating set A_0 is a minimal generating set of V if $|A_0| \leq |A|$ for all $A \in \mathcal{A}$.

Remark 1.2.18. In linear algebra, every vector space has a unique dimension. This means that any basis of the fixed vector space has the same cardinality. However, this is not true for the case of module. Therefore, there exists finitely generated module such that its two generating set has different cardinality.

Example 1.2.19.

1. The generating set of $\mathbb{Z}$-module is equivalent to the generating set as abelian group.

2. The cyclic sub-module of a regular module ${}_R R$ is equivalent to a principal left ideal of R. Moreover, if R is a PID, then we have the following chain of equivalence:

$$\text{submodules of } {}_R R \equiv \text{cyclic submodules} \equiv \text{ideals} \equiv \text{principal ideals}$$

3. The submodule of a finitely generated module need not be finitely generated. For example, let F be a field and define $R = F[X_1, X_2, \ldots]$ and $U = \{f \in R : \deg f \geq 1\}$. Note that ${}_R R = R1$ is finitely generated as a regular module. However U is not finitely generated. If not, then there exists $A \subseteq U$ such that $U = RA$ where $|A| < \infty$. But the finiteness of A implies that only finite number of polynomial are chosen, and thus only finite number of variables are involve, contradicting to the fact that there are infinitely many variables in U, since $\{X_1, X_2, \ldots\} \in U$.

4. Let $V = R^n$, then $\Omega := \{e_i = (0, \ldots, 0, 1, 0, \ldots, 0) : 1 \leq i \leq n\}$ is a generating set of V. Additionally, if R is commutative, then Ω is the minimal generating set.

Definition 1.2.20 (Invariant basis number property)**.** Let R be a ring. We say R has the invariant basis number (IBN) property if every finitely generated R-module has a well-defined rank, i.e. any generating set of a finitely generated R-module has the same cardinality.

Theorem 1.2.21 (Isomorphism Theorems of Modules)**.**

1. *Let $\varphi : M \to N$ be R-module homomorphisms. Then $M/\ker\varphi \cong \operatorname{im}\varphi$*

2. *Let U, V be submodules of W. Then $(U+V)/V \cong U/(U \cap V)$.*

3. *Let $U \subseteq V \subseteq W$ be R-modules. Then $W/V = (W/U)/(V/U)$.*

4. *Let $U \subseteq V$ be R-modules. Then there exists an one-to-one correspondence between the following sets:*

$$\{\textit{Submodules of } V \textit{ containing } U\} \longleftrightarrow \{\textit{submodules of } V/U\}$$

The correspondence is given by $W \mapsto \pi(W)$ where π is the canonical map.

Proposition 1.2.22. *Let $N_1, \ldots, N_m$ be sub-modules of an R-module M. TFAE:*

1. *The map $\pi : N_1 \times \cdots \times N_m \to N_1 + \cdots + N_m$ where $(x_1, \ldots, x_m) \mapsto x_1 + \cdots + x_m$ is an isomorphism of R-module.*

2. *For every $j \in \{1, \dots, m\}$ we have*
$$N_j \cap \sum_{i \neq j} N_i = \{0\}$$

3. *For any $x \in N_1 + \cdots + N_m$, there exists a unique $x_i \in N_i$ for every i such that $x = x_1 + \cdots + x_m$.*

Proof. [1 $\implies$ 2]. Suppose not, say there exists non-zero element $x_j \in N_j \cap \sum_{i \neq j} N_i$. So we can express
$$x_j = x_1 + \cdots + x_{j-1} + x_{j+1} + \cdots + x_m \neq 0$$
where $x_i \in N_i$ for all $i = 1, \dots, j-1,\ j+1, \dots, m$. This implies that
$$\pi(\mathbf{0}, x_j, \mathbf{0}) = \pi(x_1, \dots, x_{j-1},\ x_{j+1}, \dots, x_m) \implies \pi(x_1, \dots, x_{j-1}, -x_j,\ x_{j+1}, \dots, x_m) = 0$$
So $(x_1, \dots, x_{j-1}, -x_j,\ x_{j+1}, \dots, x_m) \in \ker \pi$. By assumption π is isomorphism, so it is injective and has trivial kernel, indicating that $(x_1, \dots, x_{j-1}, -x_j,\ x_{j+1}, \dots, x_m) = (0, \dots, 0)$ and thus $x_j = 0$, which is a contradiction.

[2 $\implies$ 3]. It is clear that for $x \in N_1 + \cdots + N_m$ we can write $x = x_1 + \cdots + x_m$ where $x_i \in N_i$ for each i. It remains to show that this representation is unique. Let $x_i \in N_i$ and $y_i \in N_i$ be chosen for all i such that
$$\sum_{i=1}^{m} x_i = \sum_{i=1}^{m} y_i$$
Note that for any j we have
$$N_j \ni x_j - y_j = \sum_{i \neq j} (y_i - x_i) \in \sum_{i \neq j} N_i$$
And so we see that $x_j - y_j$ is a common element of
$$N_j \cap \sum_{i \neq j} N_i = \{0\}$$
and thus implying that $x_j - y_j = 0$, so $x_j = y_j$. Since j is chosen to be arbitrary, we can repeat the procedure and thus showing that the representation is unique.

[3 $\implies$ 1]. Define $\pi : N_1 \times \cdots \times N_m \to N_1 + \cdots + N_m$ such that $(x_1, \dots, x_m) \mapsto x_1 + \cdots + x_m$. It is easy to verify that π is a R-module homomorphism and is surjective. For injectivity, suppose that
$$\pi(x_1, \dots, x_m) = \pi(y_1, \dots, y_m)$$
and so $x_1 + \cdots + x_m = y_1 + \cdots + y_m$. By assumption, the representation is unique, and thus we have $x_i = y_i$ for all $i = 1, 2, \dots, m$. □

Remark 1.2.23 (Internal direct sum)**.** In any cases in Proposition 1.2.22, we say that $\sum_{i=1}^{m} N_i$ is an internal direct sum, or more oftenly and simply, just direct sum. We denote it by
$$\bigoplus_{i=1}^{m} N_i$$

There are several remarks to make regarding direct sum and direct product:

- The first statement of previous proposition actually states that direct product and direct sum are equivalent in the finite case.
- Both direct sum and direct product can be taken over an infinite (possible uncountable) index set.
- The difference of direct sum and direct product is that, direct products contained all possible sequences of elements. However, direct sum requires that only finitely many elements are non-zero. Thus, an immediate example is that, when given infinitely many sub-modules $N_1, N_2, N_3, \dots$, then
$$1 \oplus 1 \oplus 1 \oplus 1 \oplus \dots \notin \bigoplus_{i=1}^{\infty} N_i$$
But we have
$$(1, 1, 1, 1, 1 \dots) \in \prod_{i=1}^{\infty} N_i$$

Of course, direct sum can be further defined for two modules N and M (or more), where by considering $N \times M$ we see that N and M are (isomorphic to some) submodules of $N \times M$. We can then define $N \oplus M$ under the umbrella of $N \times M$.

1.3 Free Module and Tensor Product

Definition 1.3.1 (Free on a subset)**.** Let F be an R-module. We say that F is free on a subset A of F if for every $x \in F$ there exist unique non-zero elements $r_1, \ldots, r_m \in R$ and unique choice of $a_1, \ldots, a_m$ such that

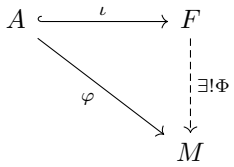
$$x = r_1 a_1 + \cdots + r_m a_m$$

If so, we say that A is a (free) basis of F. Also, when R is unital and commutative, the cardinality $|A|$ of A is well-defined, and we define the rank of F be $|A|$.

Example 1.3.2.

1. ${}_R R$ is free on $\{1\}$ since for every $r \in R$ we have $r = r \cdot 1$.
2. $\bigoplus_R R$ is free on the 'standard free basis' $\{\mathbf{e}_i = (\mathbf{0}, 1_i, \mathbf{0})\}_i$.
3. Let $R = \mathbb{Z}$. Then the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ is not free on $\{\bar{1}\}$ since $\bar{0} = 1 \cdot \bar{0} = 2 \cdot \bar{0} = 4 \cdot \bar{0}$.

Definition 1.3.3 (Free on a set)**.** Let A be a set and F be an R-module. We say that F is free on A if there exists an injective map $\iota : A \to F$ such that for any R-module M and map of set $\varphi : A \to M$, there exists a unique R-module homomorphism $\Phi : F \to M$ such that the the following diagram commutes:



Lemma 1.3.4 (Universal property of free modules)**.** *If F is a free R-module on A a subset of F, then F is free on set A where the map $\iota : A \hookrightarrow F$ is the inclusion map.*

Proof. Let M be an R-module and $\varphi : A \to M$ is a given map of set. Suppose that F is free on a subset $A \subseteq F$, which means that any $x \in F$ has unique representation with respect to A. Write $x = r_1 a_1 + \cdots + r_m a_m$ to denote its unique representation.

We define a map $\Phi : F \to M$ such that $x = r_1 a_1 + \cdots + r_m a_m \mapsto r_1 \varphi(a_1) + \cdots + r_m \varphi(a_m)$. We claim that Φ is an R-module homomorphism. Let $y = r'_1 a'_1 + \cdots + r'_m a'_m$ be an element of F. So $x + y = r_1 a_1 + \cdots + r_m a_m + r'_1 a'_1 + \cdots + r'_m a'_m$ and thus

$$\Phi(x + y) = r_1 \varphi(a_1) + \cdots + r_m \varphi(a_m) + r'_1 \varphi(a'_1) + \cdots + r'_m \varphi(a'_m) = \Phi(x) + \Phi(y)$$

Also, let $r \in R$, and so $rx = rr_1 a_1 + \cdots + rr_m a_m$, we have

$$\Phi(rx) = rr_1 \varphi(a_1) + \cdots + rr_m \varphi(a_m) = r(r_1 \varphi(a_1) + \cdots + r_m \varphi(a_m)) = r\varphi(x)$$

This shows that Φ is indeed an R-module homomorphism.

We now check if commutativity holds, i.e. $\Phi \circ \iota = \varphi$. Let $a \in A \subseteq F$, by definition $\iota(a) = a \in F$. Since F is free on the subset A, so the unique representation of a is a. Thus $(\Phi \circ \iota)(a) = \Phi(a) = \varphi(a)$, thus commutativity holds.

To check uniqueness, suppose that $\Psi : F \to M$ is an R-module homomorphism such that $\Psi \circ \iota = \varphi$. But we know that $\Psi \circ \iota = \varphi$, so $\Psi \circ \iota = \Phi \circ \iota$, implying that $\Psi = \Phi$ on $A \subseteq F$. But F is free on the subset A, so the equality of the R-module homomorphisms Ψ and Φ can be extended to the whole F. Thus $\Psi = \Phi$, showing that Φ is indeed unique. This completes the proof. □

Theorem 1.3.5. *Let A be a set and R be a ring. Define*

$$F(A) := \{f : A \to R \mid f(a) \neq 0 \text{ for finitely many } a \in A\}$$

Then $F(A)$ is free on set A with group operation

$$(f+g)(a) = f(a) + g(a)$$

and ring action

$$(r \cdot f)(a) := rf(a)$$

where $\iota : A \to F(A)$ is defined to be $a \mapsto \varepsilon_a$ where

$$\varepsilon_a : b \mapsto \begin{cases} 0 & , b \neq a \\ 1 & , b = a \end{cases}$$

Proof. It is clear that $F(A)$ with the defined group operation and ring action is an R-module. Before the proof, we claim that $F(A)$ is free on the subset $\iota(A)$. To see this, for any $f \in F(A)$ we claim that the unique representation of f over $\iota(A)$ is

$$f(x) = \sum_{a \in A} f(a)\varepsilon_a(x)$$

1. We first show that the declared linear combination is true. Let $x = b \in A$, then

$$\sum_{a \in A} f(a)\varepsilon_a(b) = \sum_{\substack{a \in A \\ a \neq b}} f(a)\varepsilon_a(b) + f(b)\varepsilon_b(b) = 0 + f(b) = f(b)$$

   since $\varepsilon_a(b) = 0$ for all $a \neq b$ and $\varepsilon_b(b) = 1$. This shows that the declared identity holds.

2. We show that it is indeed unique. Suppose we can write f into

$$f(x) = \sum_{a \in A} r_a \varepsilon_a(x)$$

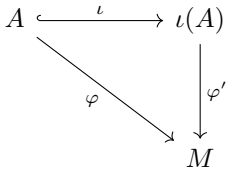
   Then we have

$$f(b) = \sum_{a \in A} r_a \varepsilon_a(b) = r_b \varepsilon_b(b) = r_b$$

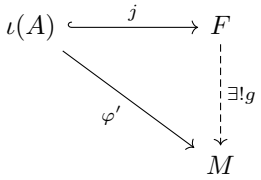
   for any $b \in A$. Thus the declared representation is unique.

This shows that $F(A)$ is free on the subset $\iota(A)$.

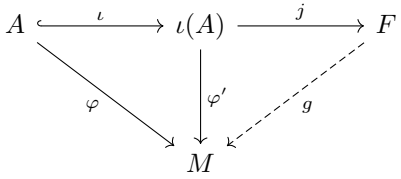
Next, suppose given M is an R-module and $\varphi : A \to M$ is a map of sets. Define $\varphi' : \iota(A) \to M$ where $\varepsilon_a \mapsto \varphi(a)$, then we have the following commutative diagram:



On the other hand, since $F(A)$ is free on the subset $\iota(A)$, so we have the following commutative diagram:



where j is the inclusion map, and the existence of g is ensured by the universal property of free modules. Glueing the two obtained commutative diagram together we get



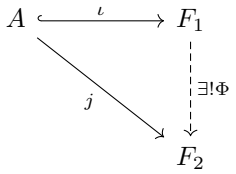
Since $\varphi = \varphi' \circ \iota$ and $\varphi' = g \circ j$, altogether we get $\varphi = g \circ (j \circ \iota)$. This shows that $F(A)$ is free on set A. □

Corollary 1.3.6.

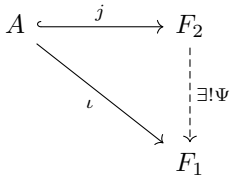
1. *Let F_1 and F_2 be R-modules free on a set A with inclusion maps $\iota : A \to F_1$ and $j : A \to F_2$. Then there exists a unique isomorphism $\Phi : F_1 \to F_2$ such that $\Phi \circ \iota = j$.*

2. *If F is an R-module free on A, then $F \cong F(A)$.*

Proof. Let F_1 and F_2 be R-modules free on a set A with inclusion maps $\iota : A \to F_1$ and $j : A \to F_2$. Consider the following commutative diagram



where the existence of Φ is ensured by the universal property of free module. Similarly we have



Note that $j = \Phi \circ \iota$ and $\iota = \Psi \circ j$. We claim that Ψ and Φ are isomorphisms pair of F_1 and F_2, that is, we show that $\Psi \circ \Phi = \mathrm{id}_{F_1}$ and $\Phi \circ \Psi = \mathrm{id}_{F_2}$. Simply note that

$$\Phi \circ \iota = j \implies \Psi \circ (\Phi \circ \iota) = \Psi \circ j = \iota \implies (\Psi \circ \Phi)(\iota(a)) = \iota(a) \quad \forall a \in A$$

This implies $\Psi \circ \Phi$ fixes $\iota(A) \subseteq F_1$. But since F_1 is free on set A, so it can be extend into whole F_1, thus $\Psi \circ \Phi = \mathrm{id}_{F_1}$. We can use the similar argument to show $\Phi \circ \Psi = \mathrm{id}_{F_2}$, and is thus omitted.

We have proven that $F(A)$ is an R-module that is free on set A. If F is an R-module free on A, it follows directly from the first statement that $F \cong F(A)$. This completes the proof. □

The following definition extends the notion of linear map from linear algebra into the realm of module:

Definition 1.3.7 (R-balanced map)**.** Let ${}_RN, M_R, L$ be abelian groups. Let $\beta : M \times N \to L$ be a map. We say that β is an R-balanced map if it satisfies all the following for any $m, m' \in M$, $n, n' \in N$ and $r \in R$

1. $\beta(m + m', n) = \beta(m, n) + \beta(m', n)$
2. $\beta(m, n + n') = \beta(m, n) + \beta(m, n')$
3. $\beta(mr, n) = \beta(m, rn)$

Definition 1.3.8 (Tensor product)**.** Let M_R and ${}_RN$ be R-module. Let $F(M \times N)$ be the free $\mathbb{Z}$-module on the set $M \times N$. Let H be a subgroup of $F(M \times N)$ generated by elements of the form:

- $(m + m', n) - (m, n) - (m', n)$
- $(m, n + n') - (m, n) - (m, n')$
- $(m \cdot r, n) - (m, r \cdot n)$

for all $m, m' \in M$, $n, n' \in N$ and $r \in R$.

The tensor product of M and N with respect to R is defined to be the quotient group

$$M \otimes_R N := F(M \times N)/H$$

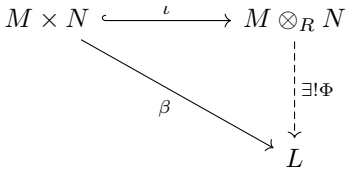
where the tensor product of two elements $m \in M$ and $n \in N$ is defined to be

$$m \otimes n := (m, n) + H$$

Then the map $\iota : M \times N \to M \otimes_R N$ where $(m, n) \mapsto m \otimes n$ is an R-balanced map.

Theorem 1.3.9 (Universal property of tensor product)**.** *Let M_R and ${}_RN$ be R-modules, and consider their tensor product $M \otimes_R N$ with the map $\iota : M \times N \to M \otimes_R N$ where $(m, n) \mapsto m \otimes n$. Then*

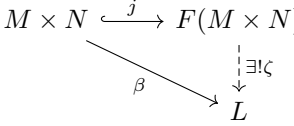
1. *For every abelian group L and every R-balanced map $\beta : M \times N \to L$, there exists a unique group homomorphism $\Phi : M \otimes_R N \to L$ such that the following diagram commutes:*



2. *Conversely, for every abelian group homomorphism $\Phi : M \otimes_R N \to L$, then the map $\beta : M \times N \to L$ where $\beta := \Phi \circ \iota$ is R-balanced. In particular, we have a bijection between the following sets:*

$$\{R\text{-balanced map where } \beta : M \times N \to L\} \leftrightarrow \{\text{group homomorphism } \Phi : M \otimes_R N \to L\}$$

Proof. Let $j : M \times N \to F(M \times N)$ be the inclusion map. Then the universal property of free modules implies the existence of $\zeta : F(M \times N) \to L$ such that $\zeta \circ j = \beta$:

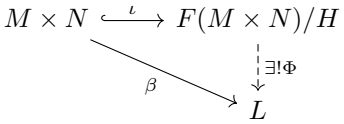


Let H be the subgroup of $F(M \times N)$ as defined in the definition of tensor product. We claim that $H \subseteq \ker \zeta$, specifically we show that all the generators are mapped to 0 by ζ:

$$\begin{aligned}\zeta((m + m', n) - (m, n) - (m', n)) &= (\zeta \circ j)((m + m', n) - (m, n) - (m', n)) \\ &= \beta((m + m', n) - (m, n) - (m', n)) \\ &= 0\end{aligned}$$

where the last equality is because β is an R-balanced maps. Similarly we can show for the other two forms of generators, and thus is omitted here. This shows that $H \subseteq \ker \zeta$.

Thus ζ induces a group homomorphism $\Phi : F(M \times N)/H \to L$ such that $\Phi(m \otimes n) := \zeta(m, n)$.



We check the commutativity:

$$(\Phi \circ \iota)((m, n)) = \Phi(m \otimes n) = \zeta((m, n)) = \zeta(j(m, n)) = (\zeta \circ j)(m, n) = \beta((m, n))$$

This shows that $\Phi \circ \iota = \beta$. Next we show that Φ is uniquely determined. Note that every element of $M \otimes_R N$ takes the form $\sum(m_i \otimes n_i)$. Then

$$\Phi\left(\sum(m_i \otimes n_i)\right) = \sum\left(\Phi(m_i \otimes n_i)\right) = \sum \Phi(\iota((m_i, n_i))) = \sum(\Phi \circ \iota)((m_i, n_i)) = \sum \beta((m_i, n_i))$$

This shows that Φ is determined by β. If we have another group homomorphism Ψ such that $\Psi \circ \iota = \beta$, then again we have

$$\Psi\left(\sum(m_i \otimes n_i)\right) = \sum \beta((m_i, n_i))$$

which implies that $\Phi = \Psi$, showing Φ is indeed uniquely defined.

For the second statement, suppose given an abelian group homomorphism $\Phi : M \otimes_R N \to L$, we check that $\beta := \Phi \circ \iota$ is R-balanced (which is omitted here, since it simply follows from R-balanceness of tensor product). For the correspondence, we claim that the declared map β is a one-to-one correspondence to Φ. Suppose not, then there exists Ψ such that $\Psi \circ \iota = \beta$, but then

$$\Psi \circ \iota = \beta = \Phi \circ \iota \implies \Psi(m \otimes n) = \Phi(m \otimes n) \forall (m, n) \in M \times N$$

This shows that $\Psi = \Phi$. □

Remark 1.3.10. Note that the tensor product $M \otimes_R N$ is defined as a quotient group, and thus any defined map on the tensor product must be examined to be well-defined. This is practically infeasible due to the complicated structure of the quotient group. This is where Theorem 1.3.9 can come useful, since everything, including well-definedness, is already settled in the proof, and the only job remain for us to do is to prove that β is an R-balanced map in order to apply this statement.

Definition 1.3.11 (Bimodule)**.** Let R and S be rings. An (R, S)-bimodule M is both ${}_RM$ and M_S satisfying $(rm)s = r(ms)$, where the ring action notation is dropped for the sake of readability, for every $r, s \in R$ and $m \in M$. In this case, we denote M as ${}_RM_S$.

Example 1.3.12.

1. Let S, T be sub-rings of R. Then ${}_SR_T$ is a bimodule.
2. Let I be an ideal of R. Then ${}_{R/I}(R/I)_R$ is a bimodule.
3. For every R-module M where R is commutative, the induced right action $m * r := r \cdot m$ gives rise to bimodule ${}_RM_R$.
4. Consider modules ${}_RY_S$ and Z_S. We have seen that $M := \mathrm{Hom}_S(Y_S, Z_S)$ is an abelian group where $(\alpha + \beta)(y) := \alpha(y) + \beta(y)$. In fact more can be concluded: M is a R-module with ring action $(\alpha \cdot r)(y) := \alpha(r \cdot y)$
5. Consider ${}_RM$ be a R-module. If S is contained in the center $Z(R)$, then we have bimodule ${}_RM_S$.

Proposition 1.3.13. *If we have modules ${}_SM_R$ and ${}_RN$, then $M \otimes_R N$ is a left S-module.*

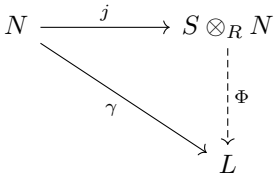
Proof. Define $s(m, n) = (sm, n)$ to be an action of S on $F(M \times N)$. We need to show that $H \subseteq F(M \times N)$ is an S-submodule, which we will omit here. After showing that H is an S-submodule, then by definition

$$M \otimes_R N = F(M \times N)/H$$

and so $M \otimes_R N$ is an S-module. □

Definition 1.3.14 (Extension of scalars)**.** Suppose that M is an R-module and R is a subring of S. The extension of scalar from R to S on M is defined to be $S \otimes_R M$, which is an S-module by previous proposition, since we can view S as ${}_SS_R$.

Theorem 1.3.15 (Universal property of extension of scalar)**.** *Let $\varphi : R \to S$ be a unital ring homomorphism and consider ${}_RN$. Define $j : N \to S \otimes_R N$ where $n \mapsto 1 \otimes n$. For any ${}_SL$ and R-module homomorphism $\gamma : N \to L$, there exists a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ such that the following diagram commutes:*



Proof. We define:

- $\iota : S \times N \to S \otimes_R N$ where $(s, n) \mapsto s \otimes n$
- $\beta : S \times N \to L$ where $(s, n) \mapsto s\gamma(n)$.

We claim that β is R-balanced: First

$$\beta(s, n+n') = s\gamma(n+n') = s\gamma(n) + s\gamma(n') = \beta(s,n) + \beta(s,n')$$

Then:

$$\beta(s+s', n) = (s+s')\gamma(n) = s\gamma(n) + s'\gamma(n) = \beta(s,n) + \beta(s', N)$$

Next, note that since R is a subring of S, we see S as an R-module by $s \cdot r := s\varphi(r)$. We have

$$\beta(s \cdot r, n) = (s \cdot r)\gamma(n) = (s\varphi(r))\gamma(n) = s(\varphi(r)\gamma(n)) = s(r * \gamma(n)) = \beta(s, r * \gamma(n))$$

So β is R-balanced. By the universal property of tensor product there exists a unique group homomorphism $\Phi : S \otimes_R N \to L$ where $\Phi \circ \iota = \beta$.

$$\begin{array}{ccc} S \times N & \xrightarrow{\iota} & S \otimes_R N \\ & \searrow^{\beta} & \downarrow \Phi \\ & & L \end{array}$$

We claim that Φ is an S-module homomorphism:

$$\Phi(s(s' \otimes n)) = \Phi(ss' \otimes n) = ss'\gamma(n) = s(s'\gamma(n)) = s\Phi(s' \otimes n)$$

so Φ is indeed an S-module homomorphism. Finally, we claim that Φ is the required S-module homomorphism such that $\Phi \circ j = \gamma$:

$$(\Phi \circ j)(n) = \Phi(j(n)) = \Phi(1 \otimes n) = 1 \cdot \gamma(n) = \gamma(n)$$

Thus $\Phi \circ j = \gamma$, this completes the proof. □

The following corollary implies that the kernel is the obstruction for N to be embedded in an S-module:

Corollary 1.3.16. *Let $\varphi : R \to S$ be an inclusion map. Let $j : N \to S \otimes_R N$ where $n \mapsto 1 \otimes n$. Then $N/\ker j$ is the unique largest quotient of N such that it can be embedded into an S-module. In particular, N can be embedded into an S-module if $\ker j$ is trivial.*

Proof. We first show that j is an R-module homomorphism: firstly

$$j(n+n') = 1 \otimes (n+n') = 1 \otimes n + 1 \otimes n' = j(n) + j(n')$$

Secondly:

$$j(rn) = 1 \otimes (rn) = (1 \cdot r) \otimes n = \varphi(r) \otimes n = r(1 \otimes n) = rj(n)$$

So j is an R-module homomorphism. Next, consider $K \subseteq N$ such that $\gamma : N/K \to L$ is an injective R-module homomorphism, that is, we are embedding quotient of N into an R-module. Define

- $\pi : N \to N/K$ be the canonical surjection.
- $\beta : N \to L$ defined by $\beta = \gamma \circ \pi$. Note that $\ker \beta = K$.

Since γ and π are R-module homomorphism, so is β. By the universal property of extension of scalar, there exists a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ such that $\Phi \circ j = \beta$:

$$\begin{array}{ccc} N & \xrightarrow{j} & S \otimes_R N \\ & \searrow^{\beta} & \downarrow \Phi \\ & & L \end{array}$$

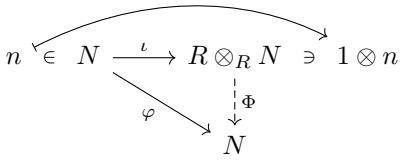
Now let $x \in \ker j$, so $j(x) = 0$, and note that

$$\beta(x) = (\Phi \circ j)(x) = \Phi(j(x)) = \Phi(0) = 0$$

and so $x \in \ker \beta$. This shows that $\ker j \subseteq \ker \beta = K$, thus $N/K = N/\ker \beta \subseteq N/\ker j$. This shows that $N/\ker j$ is the largest possible quotient of N that can be embedded into an S-module. And since j is given, so it must be unique. This completes the proof. □

Example 1.3.17.

1. Consider ${}_RN$ and we claim that $R \otimes_R N \cong N$. To see this, let $\varphi : N \to N$ where $n \mapsto n$ and define $\iota : N \to R \otimes_R N$ where $n \mapsto 1 \otimes n$. It is clear that φ is a R-module homomorphism. We thus have the following diagram



   where by Theorem 1.3.15 $\Phi \circ \iota = \varphi = \mathrm{id}_N$.

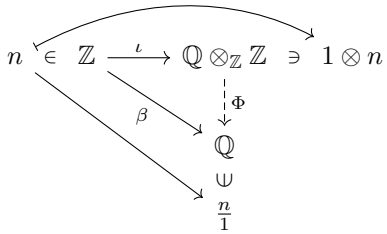
   We claim that ι is an R-module isomorphism. Firstly ι is injective since $\Phi\iota = \mathrm{id}_N$. Next ι is surjective since $r \otimes n = 1 \otimes (rn) = \iota(rn)$. Thus the claim is proved.

2. Let N be a finite abelian group, and so N is a $\mathbb{Z}$-module. We claim that $\mathbb{Q} \otimes_{\mathbb{Z}} N = 0$. To see this, let $\varphi : \mathbb{Z} \to \mathbb{Q}$ and denote $n := |N|$. Note that

$$\frac{r}{s} \otimes x = \frac{r}{sn} \cdot n \otimes x = \frac{r}{sn} \otimes nx = \frac{r}{sn} \otimes 0 = 0$$

   This means that to extend the scalar of N from $\mathbb{Z}$ to $\mathbb{Q}$, the only possible embedding is the zero map. In other words, any quotient of N that can be embedded into a $\mathbb{Q}$-module is the zero quotient.

3. We claim that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Q}$. Similarly to the method in first bullet we have the following commutative diagram:



   We claim that Φ is isomorphism. First to see surjectivity:

$$\frac{n}{m} = \frac{1}{m} \cdot \frac{n}{1} = \frac{1}{m}\beta(n) = \frac{1}{m}\Phi(1 \otimes n) = \Phi\left(\frac{1}{m} \otimes n\right)$$

   To see injectivity, note that an element in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}$ takes the form $\sum (q_i \otimes n_i)$ where $q_i \in \mathbb{Q}$ and $n_i \in \mathbb{Z}$. We can rewrite such element as the following:

$$\sum (q_i \otimes n_i) = \sum (q_i n_i \otimes 1) = \left(\sum (q_i n_i)\right) \otimes 1 =: q \otimes 1$$

   where the last equality is to rename the chunky sum into some element $q \in \mathbb{Q}$. We now prove injectivity by showing that the $\ker \Phi$ is trivial: let $q = a/b$ where $q \otimes 1 \in \ker \Phi$, then

$$\begin{aligned}
\Phi(q \otimes 1) = 0 &\implies b \cdot \Phi(q \otimes 1) = b \cdot 0 \\
&\implies \Phi(a \otimes 1) = 0 \\
&\implies a\Phi(1 \otimes 1) = 0 \\
&\implies a\Phi(\iota(1)) = 0 \\
&\implies a\beta(1) = 0 \\
&\implies a \cdot \frac{1}{1} = 0 \\
&\implies a = 0
\end{aligned}$$

   and thus $q \otimes 1 = 0 \otimes 1 = 0$. This shows that $\ker \Phi$ is trivial, so Φ is injective.

The following definition, as suggested in its name, is the generalization of bi-linearity in linear algebra:

Definition 1.3.18 (R-bilinear)**.** Let R be a commutative ring and let L, M, N be R-modules. A map $\beta : M \times N \to L$ is said to be R-bilinear if all the following holds:

1. $\beta(rm + r'm', n) = r\beta(m, n) + r'\beta(m', n)$
2. $\beta(m, rn + r'n') = r\beta(m, n) + r'\beta(m, n')$

It is immediate from the definition that R-bilinear implies R-balanced. Conversely, if an R-balanced map is, in a sense, 'two-sided R-balanced', then the map is R-bilinear.

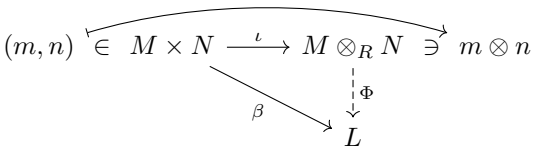
Corollary 1.3.19. *Let R be a commutative ring, M and N be R-modules. Then $M \otimes_R N$ is an R-module and $\iota : M \times N \to M \otimes_R N$ where $(m, n) \mapsto m \otimes n$ is bilinear. Furthermore, if L is an R-module, we have a bijection between the sets:*

$$\{R\text{-bilinear maps } \beta : M \times N \to L\} \longleftrightarrow \{R\text{-module homomorphisms } \Phi : M \otimes_R N \to L\}$$

where the bijection is given by the relation $\Phi \circ \iota = \beta$.

Proof. It has been shown that $M \otimes_R N$ is indeed an R-module by some previous statement. Also, we have proven that ι is a left R-balanced map. Since R is commutative, the same can be concluded that ι is a right R-balanced map. It remains to show that $\Phi : M \otimes_R N \to L$ defined by the relation $\Phi \circ \iota = \beta$ is indeed a R-module homomorphism.

First, note that we have the following commutative diagram:



By Theorem 1.3.9, the map Φ exists and it is a group homomorphism. We show that Φ respects the action of R:

$$\begin{aligned}
\Phi(r(m \otimes n)) &= \Phi(rm \otimes n) \\
&= \Phi(\iota(rm, n)) \\
&= \beta(rm, n) \\
&= r\beta(m, n) \\
&= r\Phi(\iota(m, n) \\
&= r\Phi(m \otimes n)
\end{aligned}$$

This completes the proof. □

Example 1.3.20. Define commutative ring homomorphism $\varphi : R \to S$. We have seen that $S \otimes_R R \cong S$ as a left S-module. In fact we have that $R \otimes_R S \cong S$ as right S-module.

Theorem 1.3.21 (Tensor product of R-module homomorphisms)**.** *Let $M_R, M'_R, {}_R N, {}_R N'$ be R-modules. Let $\alpha : M \to M'$ and $\beta : N \to N'$ be R-module homomorphisms. Then we have the following:*

1. *There exists a unique group homomorphism $\alpha \otimes \beta : M \otimes_R N \to M' \otimes_R N'$ where $(\alpha \otimes \beta)(m \otimes n) = \alpha(m) \otimes \beta(n)$.*
2. *If M and M' are (S, R)-bimodule, then $\alpha \otimes \beta$ is a S-module homomorphism.*
3. *Suppose further that we have M''_R and ${}_R N''$ as R-modules. Let $\lambda : M' \to M''$ and $\mu : N' \to N''$ be R-module homomorphisms. Then we have $(\lambda\alpha) \otimes (\mu\beta) = (\lambda \otimes \mu) \circ (\alpha \otimes \beta)$.*

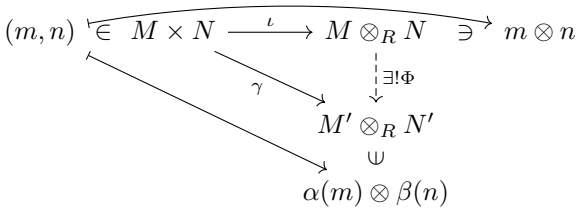
Proof. Let $\gamma : M \times N \to M' \otimes_R N'$ such that $(m, n) \mapsto \alpha(m) \otimes \beta(n)$. We first show that γ is R-balanced. Note

1. $\gamma(mr, n) = \alpha(mr) \otimes \beta(n) = \alpha(m)r \otimes \beta(n) = \alpha(m) \otimes r\beta(n) = \alpha(m) \otimes \beta(rn) = \gamma(m, rn)$

2. $\gamma(m+m',n) = \alpha(m+m') \otimes \beta(n) = (\alpha(m) + \alpha(m')) \otimes \beta(n) = (\alpha(m) \otimes \beta(n)) + (\alpha(m') \otimes \beta(n)) = \gamma(m,n) + \gamma(m',n)$

3. $\gamma(m,n+n') = \alpha(m) \otimes \beta(n+n') = \alpha(m) \otimes (\beta(n) + \beta(n')) = (\alpha(m) \otimes \beta(n)) + (\alpha(m) \otimes \beta(n')) = \gamma(m,n) + \gamma(m,n')$

And thus we obtain the following commutative diagram:



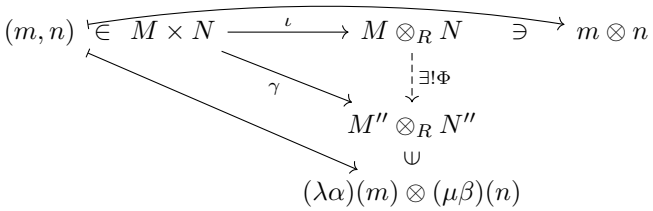
where the existence of the group homomorphism Φ is ensured by Theorem 1.3.9. This proves the first statement.

For the second statement, suppose that M and M' are (S,R)-bimodules. To show that Φ is an S-module homomorphism, we see that

$$\begin{aligned}
\Phi(s(m \otimes n)) &= \Phi(sm \otimes n) \\
&= \Phi(\iota(sm,n)) \\
&= \gamma(sm,n) \\
&= \alpha(sm) \otimes \beta(n) \\
&= s\alpha(m) \otimes \beta(n) \\
&= s(\alpha(m) \otimes \beta(n)) \\
&= s\Phi(m \otimes n)
\end{aligned}$$

This proves the second statement.

For the third statement, note that $\lambda\alpha : M \to M''$ is well-defined, where $m \mapsto \lambda(\alpha(m))$. Similarly we have that $\mu\beta : N \to N''$ is well-defined. Define $\gamma : M \times N \to M'' \times N''$ such that $(m,n) \mapsto (\lambda\alpha)(m) \otimes (\mu\beta)(n)$. We shall prove that γ is R-balanced, but is omitted here for the sake of conciseness. Eventually, we have the following commutative diagram:



We will show that $(\lambda\alpha) \otimes (\mu\beta) = (\lambda \otimes \mu) \circ (\alpha \otimes \beta)$ using the uniqueness of Φ. First note that

$$\Phi(m \otimes n) = \Phi(\iota(m,n)) = \gamma(m,n) = (\lambda\alpha)(m) \otimes (\mu\beta)(n)$$

Next, we see that

$$\begin{aligned}
((\lambda \otimes \mu) \circ (\alpha \otimes \beta))(\iota(m,n)) &= ((\lambda \otimes \mu) \circ (\alpha \otimes \beta))(m \otimes n) \\
&= (\lambda \otimes \mu)(\alpha(m) \otimes \beta(n)) \\
&= \lambda(\alpha(m)) \otimes \mu(\beta(n)) \\
&= (\lambda\alpha \otimes \mu\beta)(m \otimes n) \\
&= (\lambda\alpha \otimes \mu\beta)(\iota(m,n)) \\
&= \Phi(\iota(m,n))
\end{aligned}$$

Since Φ is unique, we see that $(\lambda\alpha) \otimes (\mu\beta) = (\lambda \otimes \mu) \circ (\alpha \otimes \beta)$ must hold. This completes the proof. $\square$

Theorem 1.3.22 (Associativity of tensor product)**.** *Consider the modules $M_{R,R}N_S$ and ${}_SL$. Then there exists a unique module isomorphism such that*

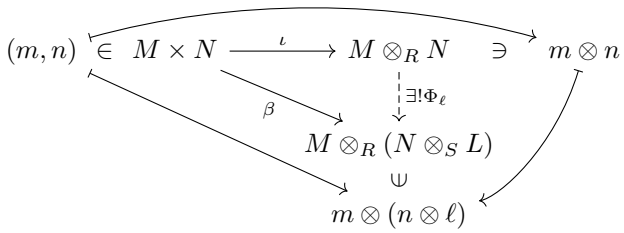
$$(M \otimes_R N) \otimes_S L \cong M \otimes_R (N \otimes_S L)$$

where $\Phi((m \otimes_R n) \otimes_S \ell) = m \otimes_R (n \otimes_S \ell)$. Furthermore, if M is a (T,R)-bimodule, then Φ is a T-module isomorphism.

Proof. Fix $\ell \in L$. Define $\iota : M \times N \to M \otimes_R N$ such that $(m,n) \mapsto m \otimes n$. Also define $\beta : M \times N \to M \otimes_R (N \otimes_S L)$ where $(m,n) \mapsto m \otimes (n \otimes \ell)$. We prove that β is R-balanced:

1. $\beta(mr,n) = mr \otimes (n \otimes \ell) = m \otimes r(n \otimes \ell) = m \otimes (rn \otimes \ell) = \beta(m,rn)$
2. $\beta(m+m',n) = (m+m') \otimes n = (m \otimes n) + (m' \otimes n) = \beta(m,n) + \beta(m',n)$
3. $\beta(m,n+n') = m \otimes (n+n') = (m \otimes n) + (m \otimes n') = \beta(m,n) + \beta(m,n')$

And so we have the following commutative diagram:

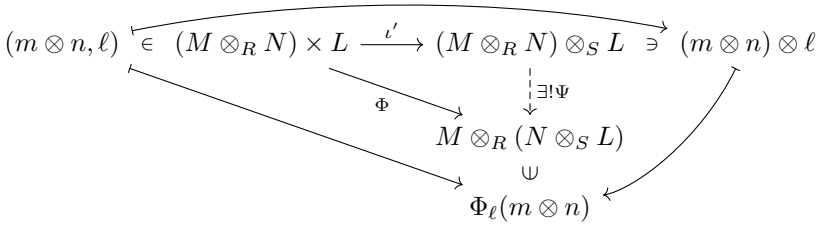


where the existence of the group homomorphism Φ_ℓ is ensured by, again, Theorem 1.3.9. Note that since ℓ is fixed, so Φ_ℓ is with respect to the choice of ℓ.

Next, define $\iota' : (M \otimes_R N) \times L \to (M \otimes_R N) \otimes_S L$ where $(m \otimes n, \ell) \mapsto (m \otimes n) \otimes \ell$. Also, define $\Phi : (M \otimes_R N) \times L \to M \otimes_R (N \otimes_S L)$ where $(m \otimes n, \ell) \mapsto \Phi_\ell(m \otimes n)$. We claim that Φ is an S-homomorphism, since for $s \in S$ we have

$$\Phi((m \otimes n)s, \ell) = \Phi(m \otimes ns, \ell) = \Phi_\ell(m \otimes ns) = m \otimes (ns \otimes \ell) = m \otimes (n \otimes s\ell) = \Phi_{s\ell}(m \otimes n) = \Phi(m \otimes n, s\ell)$$

And thus we obtain the following commutative diagram:



where the existence of the S-module homomorphism Ψ is unique by Theorem 1.3.15. Since the diagram is commutative, we see that

$$\Psi((m \otimes n), \ell) = \Phi_\ell(m \otimes n) = m \otimes (n \otimes \ell)$$

The whole argument can be repeated again, first by fixing $m \in M$ to get $\tilde{\Phi}_m : M \times (N \otimes_S L) \to M \otimes_R (N \otimes_S L)$ such that $(m, n \otimes \ell) \mapsto m \otimes (n \otimes \ell)$, then to obtain an S-module homomorphism $\tilde{\Psi} : M \otimes_R (N \otimes_S L) \to (M \otimes_R N) \otimes_S L$ such that

$$\tilde{\Psi}(m, n \otimes \ell) = \tilde{\Phi}_m(n \otimes \ell) = m \otimes (n \otimes \ell)$$

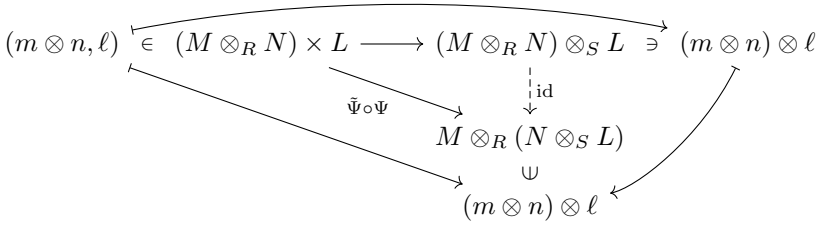
In other words, we now obtain two S-module homomorphisms such that

$$\Psi : (M \otimes_R N) \otimes_S L \rightleftarrows M \otimes_R (N \otimes_S L) : \tilde{\Psi}$$

To show that $(M \otimes_R N) \otimes_S L \cong M \otimes_R (N \otimes_S L)$, it is sufficient to prove that $\tilde{\Psi} \circ \Psi$ and $\Psi \circ \tilde{\Psi}$ are identity maps. We only show that first one. Note that

$$(\tilde{\Psi} \circ \Psi)(m \otimes n, \ell) = \tilde{\Psi}(m \otimes (n \otimes \ell)) = (m \otimes n) \otimes \ell$$

Since $\tilde{\Psi}$ and Ψ are both S-module homomorphism, it is immediate that $\tilde{\Psi} \circ \Psi$ is an S-module homomorphism as well. We thus obtain the following commutative diagram by the universal property of tensor product:



where it is clear that the map id is the only map that takes $(m \otimes n) \otimes \ell$ to itself. By the uniqueness statement in the universal property, we see that $\tilde{\Psi} \circ \Psi = \mathrm{id}$. Similar argument can be used to show that $\Psi \circ \tilde{\Psi} = \mathrm{id}$. This completes the proof. □

The following is an immediate corollary of the previous theorem:

Corollary 1.3.23. *Let R be a commutative ring. Let M, N, L be R-modules. Then $(M \otimes_R N) \otimes_R L \cong M \otimes_R (N \otimes_R L)$*

Theorem 1.3.24 (Distributivity of tensor product)**.** *Let $M_R, M'_R, {}_R N, {}_R N'$ be R-modules. Then there exists a unique module isomorphism Φ such that*

$$M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N')$$

where $\Phi(m \otimes (n, n')) = (m \otimes n, m \otimes n')$. Similarly, there exists a unique module isomorphism Φ' such that

$$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$$

where $\Phi'((m, m') \otimes n) = (m \otimes n, m' \otimes n)$.

Proof. We only prove the second statement, where the arguments are very similar to Theorem 1.3.22, thus some details are omitted. First, obtain the following three diagrams:

Diagram 1:

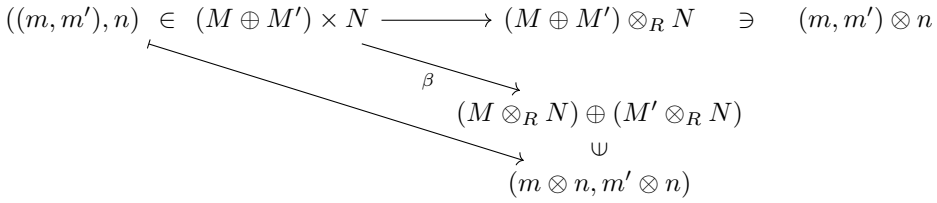


Diagram 2:

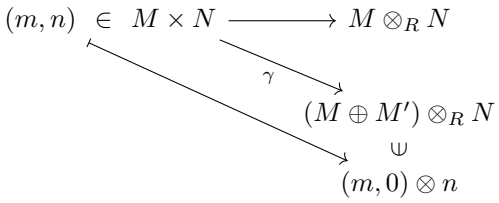
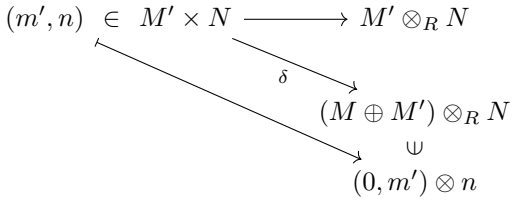


Diagram 3:



Next, prove that all maps β, γ, and δ are R-balanced, which is omitted here due to tedious work. By Theorem 1.3.9, there exists unique group homomorphism Φ, φ, and φ' respectively for diagram 1, 2, and 3 such that all are them are commutative:

Diagram 1:

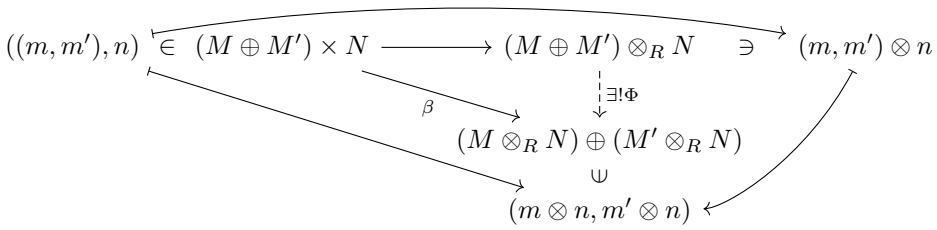


Diagram 2:

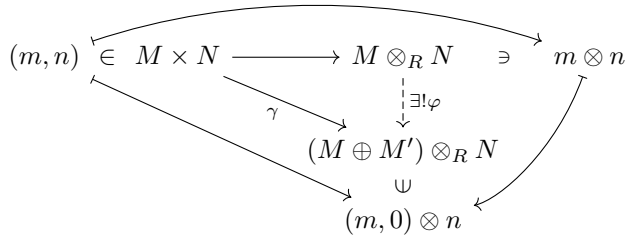
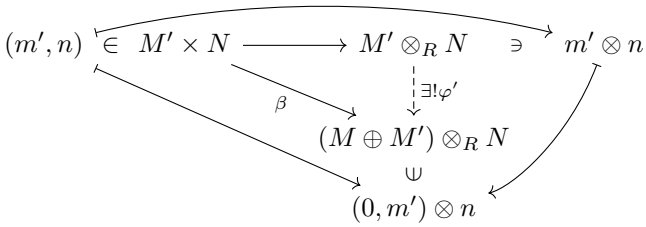


Diagram 3:



We define the map $\Psi : (M \otimes_R N) \oplus (M' \otimes_R N) \to (M \oplus M') \otimes_R N$ such that $((m \otimes n), (m' \otimes n')) \mapsto \varphi(m \otimes n) + \varphi'(m' \otimes n') = (m, 0) \otimes n + (0, m') \otimes n'$. Note both φ and φ' are group homomorphisms, and thus Ψ is a group homomorphism.

Finally, to show that $(M \otimes_R N) \oplus (M' \otimes_R N) \cong (M \oplus M') \otimes_R N$, we need to show that $\Phi \circ \Psi$ and $\Psi \circ \Phi$ are identity maps. We only show one, since another follows with the a similar argument:

$$\Psi(\Phi((m, m') \otimes n)) = \Psi(m \otimes n, m' \otimes n) = (m, 0) \otimes n + (0, m') \otimes n = (m, m') \otimes n$$

This (more or less) completes the proof. □

Corollary 1.3.25. *Let $f : R \to S$ be a ring homomorphism. Then $S \otimes_R R^m \cong S^m$ as a left S-module.*

Proof. Recall that $R^m = \bigoplus_{i=1}^m R$. Observe:

$$S \otimes_R R^m = S \otimes_R \bigoplus_{i=1}^m R \cong \bigoplus_{i=1}^m (S \otimes_R R) \cong \bigoplus_{i=1}^m S = S^m$$

This completes the proof. □

Corollary 1.3.26. *Let R be commutative. Then $R^m \otimes_R R^n \cong R^{mn}$*

Proof. Similar to the previous proof, we note

$$R^m \otimes_R R^n = \left(\bigoplus_m R\right) \otimes \left(\bigoplus_n R\right) = \bigoplus_m \left(R \otimes_R \bigoplus_n R\right) = \bigoplus_m \bigoplus_n (R \otimes_R R) = \bigoplus_m \bigoplus_n R = R^{mn}$$

This completes the proof. □

2 Injective, Projective, and Flat Modules

2.1 Short Exact Sequence and Splitting

Definition 2.1.1 (Exact sequence and complex)**.**

1. A pair of R-module homomorphism
$$X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$$
is said to be exact at Y if $\ker \beta = \operatorname{im} \alpha$, and we say that this sequence is exact.

2. A complex is a chain
$$\ldots \xrightarrow{d_{-2}} X_{-1} \xrightarrow{d_{-1}} X_0 \xrightarrow{d_0} X_1 \xrightarrow{d_1} \ldots$$
where X_i are R-modules, and d_i are R-modules homomorphisms such that $d_{i+1}d_i = 0$ for all i. In other words, we have that $\operatorname{im} d_i \subseteq \ker d_{i+1}$

3. A complex is said to be exact if it is exact at every X_i.

Remark 2.1.2. From the above definition we see that an exact sequence can be made into an exact complex by adding zeroes and zero maps.

Proposition 2.1.3.

1. *The sequence of R-modules $0 \to X \xrightarrow{\alpha} Y$ is exact if and only if α is injective.*

2. *The sequence $Y \xrightarrow{\beta} Z \to 0$ is exact if and only if β is surjective.*

Proof. For the first statement, if the sequence is exact, then $\ker \alpha = \operatorname{im} 0 = \{0\}$, so α is injective. Conversely, if α is injective, then $\ker \alpha = 0$. Since the map from 0 to X is a zero map, so $\operatorname{im} 0 = 0 = \ker \alpha$, thus the sequence is exact.

For the second statement, if the sequence is exact, then $\operatorname{im} \beta = \ker 0$. Note the image of the map $0 : Z \to 0$ is 0, so $\ker 0 = Z$. Together we have $\operatorname{im} \beta = Z$, thus β is surjective. Conversely, if β is surjective, then $\operatorname{im} \beta = Z$. Since the map from Z to 0 is a zero map, so $\ker 0 = Z = \operatorname{im} \beta$, thus the sequence is exact. □

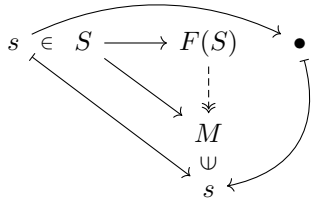
Corollary 2.1.4. *The sequence $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ is exact if and only if α is injective and β is injective and $\operatorname{im} \alpha = \ker \beta$.*

Remark 2.1.5. In this case, we called such sequence a short exact sequence (SES). Moreover, note that
$$Y/\operatorname{im} \alpha \cong Z$$
in the SES.

Example 2.1.6.

1. Let $\varphi : M \to N$ be a R-module homomorphism. Then we have the SES:
$$0 \to \ker \varphi \to M \to \operatorname{im} \varphi \to 0$$

2. Let M be a R-module and S be a generating set of M. Then there exists a surjective R-homomorphism π such that $F(S) \xrightarrow{\pi} M$. This is due to the universal property:



If M is finitely generated, then we can choose S such that $n := |S| < \infty$, and we have
$$\bigoplus_n {}_R R \cong F(S) \xrightarrow{\pi} M$$

An R-module $M \neq 0$ is simple/irreducible if M has only 0 and M as submodule. Let M be simple and $0 \neq m \in M$. Then

$$0 \neq Rm = \{rm : r \in R\} = M$$

due to simplicity of M. This says that $\{m\}$ generates M, and so by above we have that R surjects to M. This tells that simple R-module is quotient of the regular module. In general, every R-module is a quotient of a free module. We then obtain the SES:

$$0 \to \ker \pi \to F(S) \to M \to 0$$

Definition 2.1.7 (Complex homomorphisms)**.** Let $0 \to X \to Y \to Z \to 0$ and $0 \to X' \to Y' \to Z' \to 0$ be SES of R-modules.

1. A homomorphism between the SES's is a collection of R-module homomorphisms $\gamma_1, \gamma_2, \gamma_3$ such that the following is commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} & & \\ 0 & \longrightarrow & X' & \longrightarrow & Y' & \longrightarrow & Z' & \longrightarrow & 0 \end{array}$$

   and we say that the complex homomorphism is an isomorphism if the collection $\gamma_1, \gamma_2, \gamma_3$ are isomorphisms.

2. The SES $0 \to X \to Y \to Z \to 0$ and $0 \to X \to Y' \to Z \to 0$ are said to be equivalent if there exists an R-module isomorphism $g : Y \to Y'$ such that the following commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & X & \longrightarrow & Y' & \longrightarrow & Z & \longrightarrow & 0 \end{array}$$

Example 2.1.8. Since there is no isomorphism between $\mathbb{Z}$ and $\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, thus the following SES must not be equivalent:

$$0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}/n\mathbb{Z} \to 0$$

and

$$0 \to \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

Proposition 2.1.9 (Five Lemma)**.** *Suppose we have the following commutative diagram and suppose that each of the following rows are exact:*

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{g_1} & M_2 & \xrightarrow{g_2} & M_3 & \xrightarrow{g_3} & M_4 & \xrightarrow{g_4} & M_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ N_1 & \xrightarrow{h_1} & N_2 & \xrightarrow{h_2} & N_3 & \xrightarrow{h_3} & N_4 & \xrightarrow{h_4} & N_5 \end{array}$$

and f_i are R-module homomorphisms. Then we have that:

1. *If f_5 is injective and f_2, f_4 are surjective, then f_3 is surjective.*
2. *If f_1 is surjective and f_2, f_4 are injective, then f_3 is injective.*

Proof. We first show surjectivity. Suppose as assumed in the first statement. Let $n \in N_3$. Then $h_4(h_3(n)) = 0 \in N_5$. Since f_4 is surjective, there exists $m \in M_4$ such that $f_4(m) = h_3(n) \in N_4$. Sending m along two routes we have

$$f_5(g_4(m)) = h_4(f_4(m)) = h_4(h_3(n)) = 0 \in N_5$$

Since f_5 is injective, we have $g_4(m) = 0 \in M_5$, implying that $m \in \ker g_4$. Due to the exactness we have that $m \in \operatorname{im} g_3$, so there exists $a \in M_3$ such that $g_3(a) = m \in M_4$. Again, sending $a \in M_3$ along two routes we have

$$h_3(f_3(a)) = f_4(g_3(a)) = f_4(m) = h_3(m)$$

And thus $h_3(f_3(a)-m)=0$, implying that $f_3(a)-m \in \ker h_3 = \operatorname{im} h_2$, and so there is $b \in N_2$ such that $h_2(b) = f_3(a)-m \in N_3$. Note f_2 is surjective, so there exists $c \in M_2$ such that $f_2(c)=b \in N_2$. Sending $c \in M_2$ along two different routes we have

$$f_3(h_2(c)) = h_2(f_2(c)) = h_2(b) = f_3(a) - m \in N_3$$

Rearranging the equation we get $f_3(a-h_2(c)) = m$. This proves that f_3 is surjective.

We now show injectivity. Suppose as assumed in the second statement. It suffices to show that $\ker f_3$ is trivial. Let $m \in M_3$ such that $f_3(m)=0$. Sending $m \in M_3$ along two routes we get

$$f_4(g_3(m)) = h_3(f_3(m)) = h_3(0) = 0 \in N_4$$

Since f_4 is injective, so $g_3(m)=0 \in M_4$. This implies that $m \in \ker g_3 = \operatorname{im} g_2$, so there exists $a \in M_2$ such that $g_2(a)=m \in M_3$. Sending $a \in M_2$ along two routes, we have

$$h_2(f_2(a)) = f_3(g_2(a)) = f_3(m) = 0$$

So $f_2(a) \in \ker h_2 = \operatorname{im} h_1$, implying that there exists $n \in N_1$ such that $h_1(n) = f_2(a) \in N_2$. Since f_1 is surjective, so there exists $b \in M_1$ such that $f_1(b)=n$. Sending $b \in M_1$ along two routes we have

$$f_2(g_1(b)) = h_1(f_1(b)) = h_1(n) = f_2(a)$$

Rearranging the equation we get $f_2(g_1(b)-a)=0 \in N_2$. Since f_2 is injective, so $g_1(b)-a=0 \in N_2$, which by rearranging we have $g_1(b)=a$. Lastly, send $b \in M_1$ to M_3 via compositing g_1 and g_2, which we get a zero map:

$$g_2(g_1(b)) = 0 \in M_3$$

Since $g_1(b)=a$, we have that $g_2(a)=0 \in M_3$. Recall that $g_2(a)=m \in M_3$, so together we have that $m=0 \in M_3$. This shows that $\ker f_3$ is trivial. □

Definition 2.1.10 (Splitting sequence)**.** A SES $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ splits if there exists a submodule $Y' \subseteq Y$ such that $Y = Y' \oplus \alpha(X)$.

Remark 2.1.11. Note that if a SES splits, then we have that

$$Y' \cong Y/\alpha(X) = Y/\operatorname{im}\alpha = Y/\ker\beta \cong Z$$

Moreover, since α is injective, so $\alpha(X) \cong X$ and we have $Y \cong X \oplus Z$. To conclude, a SES splits implies that $Y \cong X \oplus Z$. However, the converse is not true.

Proposition 2.1.12. *Let $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ be a SES. TFAE:*

1. *The SES splits.*
2. *$\exists \gamma : Z \to Y$ is an R-module homomorphism such that $\beta \circ \gamma = \mathrm{id}_Z$*
3. *$\exists \delta : Y \to X$ is an R-module homomorphism such that $\delta \circ \alpha = \mathrm{id}_X$*
4. *$\exists \varphi : Y \to X \oplus Z$ such that $\varphi \circ \alpha = \iota : X \to X \oplus Z$ is the inclusion map and $\beta \circ \varphi^{-1} = \pi : X \oplus Z \to Z$ is the canonical map.*

Proof. The logic chain of the proof is 1. $\implies$ 2. $\implies$ 3. $\implies$ 4. $\implies$ 1..

[1. $\implies$ 2.]. Suppose that the SES splits, so let $Y' \subseteq Y$ be such that $Y = Y' \oplus \alpha(X)$. We define the map $\gamma : Z \to Y$ where $z \mapsto \gamma(z)$ such that $\gamma(z)$ is defined via the following procedure

- Since $\operatorname{im}\beta = \ker 0 = Z$, so there exists $y \in Y$ such that $\beta(y) = z$.
- Since $Y = Y' \oplus \alpha(X)$, we can write $y = a + b$ by some $a \in Y'$ and $b \in \alpha(X)$.
- Then we define $\gamma(z) := a$.

We first claim that γ is well-defined. Suppose that $\beta(y') = z = \beta(y)$ for some other $y' \in Y$ where $y' = a' + b'$ where $a' \in Y'$ and $b' \in \alpha(X)$. Note $\beta(y - y') = 0$, so $y - y' \in \ker\beta = \operatorname{im}\alpha = \alpha(X)$. We can write

$$y - y' = (a - a') + (b - b')$$

Since $y - y' \in \alpha(X)$, so $a - a'$ must be the zero element, which shows that $a = a'$. This implies that $\gamma(z) = a = a'$, so γ is well-defined. Next, we show that γ is an R-module homomorphism, i.e. we show that $\gamma(rz) = r\gamma(z)$. Let $\beta(y) = z$. Note that

$$\beta(ry) = r\beta(y) = rz$$

On the other hand, we have $ry = r(a + b) = ra + rb$. Since Y' and $\alpha(X)$ are R-modules, so $ra \in Y'$ and $rb \in \alpha(X)$, implying that $ry \in Y' \oplus \alpha(X)$. Therefore

$$\gamma(rz) = ra = r\gamma(z)$$

This shows that γ is an R-module homomorphism. Lastly, we check the requirement: for any $z \in Z$, let $\gamma(z) = a$, then

$$\beta(\gamma(z)) = \beta(a) \overset{(*)}{=} \beta(y) = z$$

where the stared equality is achieved as followed: since $y \in Y = Y' \oplus \alpha(X)$, so we can write $y = a + b$ such that $a \in Y'$ and $b \in \alpha(X)$. Let $b = \alpha(x)$. Together, we see

$$\beta(y) = \beta(a + b) = \beta(a) + \beta(b) = \beta(a) + \beta(\alpha(x)) = \beta(a)$$

since $\beta \circ \alpha$ is zero map due to exactness. This shows that $\beta \circ \gamma = \mathrm{id}_Z$.

[2. $\implies$ 3.]. Suppose that we have an R-module homomorphism $\gamma : Z \to Y$ such that $\beta \circ \gamma = \mathrm{id}_Z$. We define $\delta : Y \to X$ such that $y \mapsto \delta(y)$ where $\delta(y)$ is defined as follow:

- Note that $\beta(y - \gamma(\beta(y))) = \beta(y) - \beta(\gamma(\beta(y))) = \beta(y) - \beta(y) = 0$
- It implies that $y - \gamma(\beta(y)) \in \ker\beta = \operatorname{im}\alpha$, so there exists $x \in X$ such that $\alpha(x) = y - \gamma(\beta(y))$.
- We then define $\delta(y) := x$.

We first show that δ is well-defined. Note that by exactness we have $\ker\alpha = \operatorname{im} 0 = 0$, so α is injective. Since δ is defined via α, so consequently δ must be injective. Next we show that δ is an R-module homomorphism. To compute $\delta(ry)$, consider:

$$ry - \gamma\left(\beta\left(ry\right)\right) = r(y - \gamma\left(\beta(y)\right)) = r\alpha(x) = \alpha(rx)$$

So $\delta(ry) = rx = r\delta(y)$. This shows that δ is an R-module homomorphism. Lastly, we check the requirement: to compute $\delta(\alpha(x))$, consider:

$$\alpha(x) - \gamma(\beta(\alpha(x))) = \alpha(x) - \gamma(0) = \alpha(x)$$

due to the exactness. So $\delta(\alpha(x)) = x$. This shows that $\delta \circ \alpha = \mathrm{id}_X$.

[3. $\implies$ 4.]. Suppose we have an R-module homomorphism $\delta : Y \to X$ such that $\delta \circ \alpha = \mathrm{id}_X$. Define $\varphi : Y \to X \oplus Z$ such that $y \mapsto (\delta(y),\ \beta(y))$. We have then have the following diagram:

$$\begin{array}{ccccccccc}
 & & & \overset{\delta}{\curvearrowleft} & & & & & \\
0 & \xrightarrow{0} & X & \xrightarrow[\alpha]{} & Y & \xrightarrow[\beta]{} & Z & \xrightarrow{0} & 0 \\
\uparrow\downarrow{\scriptstyle \mathrm{id}} & & \uparrow\downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \varphi} & & \uparrow\downarrow{\scriptstyle \mathrm{id}} & & \uparrow\downarrow{\scriptstyle \mathrm{id}} \\
0 & \xrightarrow{0} & X & \xrightarrow{\iota} & X \oplus Z & \xrightarrow{\pi} & Z & \xrightarrow{0} & 0
\end{array}$$

where $\iota : X \to X \oplus Z$ is the inclusion map $x \mapsto (x, 0)$ and π is the canonical map onto Z. We examine the two requirements. For the first one:

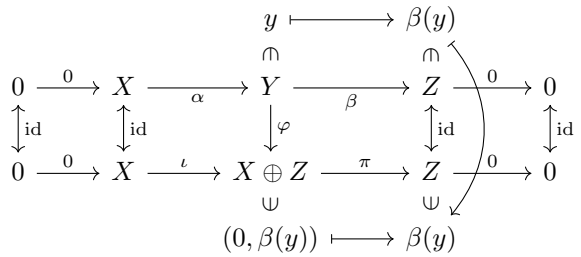
$$\varphi(\alpha(x)) = (\delta(\alpha(x)), \beta(\alpha(x))) = (x, 0) = \iota(x)$$

For the second one:

$$\pi(\varphi(y)) = \pi(\delta(y), \beta(y)) = \beta(y)$$

This shows $\pi \circ \varphi = \beta$, and thus $\beta \circ \varphi^{-1} = \pi$.

[4. $\implies$ 1.]. Suppose as assumed in the given condition. We have the following diagram:



To show that the SES splits, define $Y' = \varphi^{-1}(0 \oplus Z)$. Since 0 and Z are modules, and φ is module homomorphism, so Y' is a module, and is thus a submodule of Y. We claim that $Y = Y' \oplus \operatorname{im} \alpha$. By assumption $\varphi \circ \alpha = \iota$, so $\alpha = \varphi^{-1} \circ \iota$. Next, note that $\varphi^{-1} : X \oplus Z \to Y$, so

$$Y' = \varphi^{-1}(X \oplus 0) \oplus \varphi^{-1}(0 \oplus Z) = \varphi^{-1}(\iota(X)) \oplus Y' = \alpha(X) \oplus Y'$$

This completes the proof. □

Proposition 2.1.13. *Let X, Y and V be R-modules. Let $\alpha : X \to Y$ be an R-module homomorphism. The map $\alpha_* : \operatorname{Hom}_R(V, X) \to \operatorname{Hom}_R(V, Y)$ where $f \mapsto \alpha \circ f$ is as abelian group homomorphism. Furthermore, if α is injective, then so is α_*. In other words, the SES*

$$0 \to X \xrightarrow{\alpha} Y$$

implies that we have the SES

$$0 \to \operatorname{Hom}_R(V, X) \xrightarrow{\alpha_*} \operatorname{Hom}_R(V, Y)$$

Proof. The proof for α_* being an abelian group homomorphism is left as an tutorial. Suppose α is injective. Let $f \in \operatorname{Hom}_R(V, X)$ such that $\alpha \circ f = 0$ for every $v \in V$. Then for any $v \in V$ we have

$$(\alpha \circ f)(v) = 0 \implies \alpha(f(v)) = 0 \implies f(v) = 0$$

since α is injective. This shows that f is a zero map, so α_* is injective. □

Remark 2.1.14. In general α_* is not surjective even if α is surjective.

Theorem 2.1.15. *Let V, X, Y, Z be R-modules and*

$$0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \tag{1}$$

be a short sequence where α and β are R-module homomorphisms.

1. *If the above short sequence 1 is exact, then the following is exact:*

$$0 \to \operatorname{Hom}_R(V, X) \xrightarrow{\alpha_*} \operatorname{Hom}_R(V, Y) \xrightarrow{\beta_*} \operatorname{Hom}_R(V, Z)$$

2. $0 \to \operatorname{Hom}_R(V, X) \xrightarrow{\alpha_*} \operatorname{Hom}_R(V, Y) \xrightarrow{\beta_*} \operatorname{Hom}_R(V, Z)$ *is exact for all V if and only if $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is exact.*

Proof. For the first statement, suppose that the short sequence 1 given exists. Then α is injective, and thus α_* is injective by Proposition 2.1.13. We now prove that $\operatorname{im} \alpha_* = \ker \beta_*$. Firstly, let $f \in \operatorname{Hom}_R(V, X)$. Since

$$(\beta_* \circ \alpha_*)(f) = \beta \circ \alpha \circ f = 0 \circ f = 0$$

This implies that $\operatorname{im} \alpha_* \subseteq \ker \beta_*$. Next, to show $\ker \beta_* \subseteq \operatorname{im} \alpha_*$, let $g \in \ker \beta_*$, so for any $v \in V$ we have

$$(\beta_*(g))(v) = \beta(g(v)) = 0$$

Note it implies that $g(v) \in \ker \beta = \operatorname{im} \alpha$ due to the exactness of SES 1. So there exists $x_v \in X$ such that $\alpha(x_v) = g(v)$. Next, define the map $f : V \to X$ such that $v \mapsto x_v$. The map f is well-defined since α is

injective by assumption. We claim that f is a R-module homomorphism. Indeed, for any $v, v' \in V$, let $\alpha(x_v) = g(v)$ and $\alpha(x_{v'}) = g(v')$. Then

$$\alpha(x_v + x_{v'}) = \alpha(x_v) + \alpha(x_{v'}) = g(x_v) + g(x_{v'}) = g(x_v + x_{v'})$$

This proves that $f(v+v) = x_{v+v'} = x_v + x_{v'} = f(v) + f(v')$. Next, let $r \in R$, then

$$\alpha(rx_v) = r\alpha(x_v) = rg(v) = g(rv)$$

This proves that $f(rv) = x_{rv} = rx_v = rf(v)$, and so f is really an R-module homomorphism. Finally, note that

$$(\alpha_*(f))(v) = (\alpha \circ f)(v) = \alpha(f(v)) = \alpha(x_v) = g(v)$$

Since $v \in V$ is arbitrary, we conclude that $\alpha_*(f) = g$. This proves that $\ker \beta_* \subseteq \operatorname{im} \alpha_*$, which also proved the first statement.

For the second statement, note that the backward direction is equivalent to the first statement, which we have proven it to be true. For the forward direction, suppose that

$$0 \to \operatorname{Hom}_R(V, X) \xrightarrow{\alpha_*} \operatorname{Hom}_R(V, Y) \xrightarrow{\beta_*} \operatorname{Hom}_R(V, Z)$$

is exact for all V. Consider taking $V = R$, since we have that $\operatorname{Hom}_R(R, X) \cong X$ where the isomorphism is given by $f \mapsto f(1)$. This is similar for Y and Z. Thus we have the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Hom}_R(R,X) & \xrightarrow{\alpha_*} & \operatorname{Hom}_R(R,Y) & \xrightarrow{\beta_*} & \operatorname{Hom}_R(R,Z) & \longrightarrow & 0 \\
 & & \updownarrow & & \updownarrow & & \updownarrow & & \\
0 & \longrightarrow & X & \xrightarrow[\alpha]{} & Y & \xrightarrow[\beta]{} & Z & \longrightarrow & 0
\end{array}$$

where the double-sided arrows between both sequences represent the isomorphisms defined above. We claim that the diagram is commutative. We only prove the commutativity between $\operatorname{Hom}_R(R, X) - \operatorname{Hom}_R(R, Y) - Y - X$, i.e. the first square. Let $f \in \operatorname{Hom}_R(R, X)$. Sending f along the upper path we get $(\alpha_*(f))(1) = (\alpha \circ f)(1) = \alpha(f(1))$. On the other hand, sending f along the lower path we get $\alpha(f(1))$. This shows commutativity in the first square. Same argument can be applied to show commutativity in the second square.

We need to show that $\operatorname{im} \alpha = \ker \beta$. We first show $\operatorname{im} \alpha \subseteq \ker \beta$. Let $x \in X$, so there exists $f_x \in \operatorname{Hom}_R(R, X)$ such that $f_x(1) = x$. Sending f_x along the first row, and due to exactness we have that

$$(\beta_* \circ \alpha_*)(f_x) = 0 \implies \beta \circ \alpha \circ f_x = 0$$

Therefore $(\beta \circ \alpha \circ f_x)(1) = \beta(\alpha(f_x(1))) = \beta(\alpha(x)) = 0$. This proves that $\alpha(x) \in \ker \beta$, implying that $\operatorname{im} \alpha \subseteq \ker \beta$.

Next, to show $\ker \beta \subseteq \operatorname{im} \alpha$, let $y \in \ker \beta$, i.e. $\beta(y) = 0$. Then there exists $f_y \in \operatorname{Hom}_R(R, Y)$ such that $f_y(1) = y$. Note that

$$(\beta_*(f_y))(1) = \beta(f_y(1)) = \beta(y) = 0 \in Z$$

But $\beta_*(f_y) \in \operatorname{Hom}_R(R, Z)$, and there is an isomorphism between $\operatorname{Hom}_R(R, Z)$ and Z. Since $(\beta_*(f_y))(1) = 0 = 0(1)$, we see that $\beta_*(f_y)$ must be the zero map due to the injectivity of the isomorphism. This further implies that $f_y \in \ker \beta_*$, and by exactness in first row we get $f_y \in \operatorname{im} \alpha_*$. So, there exists $g_x \in \operatorname{Hom}_R(R, X)$ where $g_x(1) := x$ such that $\alpha_*(g_x) = f_y$. Thus

$$(\alpha_*(g_x))(1) = f_y(1) \implies (\alpha \circ g_x)(1) = y \implies \alpha(g_x(1)) = \alpha(x) = y$$

Therefore $y \in \operatorname{im} \alpha$, which proves that $\ker \beta \subseteq \operatorname{im} \alpha$. This completes the proof. □

Proposition 2.1.16. *Let X, Y, Z be R-module. Then*

1. $\operatorname{Hom}_R(X, Y \oplus Z) \cong \operatorname{Hom}_R(X, Y) \oplus \operatorname{Hom}_R(X, Z)$
2. $\operatorname{Hom}_R(X \oplus Y, Z) \cong \operatorname{Hom}_R(X, Z) \oplus \operatorname{Hom}_R(Y, Z)$

Proof. We only prove the first statement. Consider a map from $\mathrm{Hom}_R(X, Y \oplus Z)$ to $\mathrm{Hom}_R(X, Y) \oplus \mathrm{Hom}_R(X, Z)$ such that

$$f \mapsto (\pi_Y \circ f, \pi_Z \circ f)$$

This is an isomorphism of abelian groups. The details are left as an exercise. □

Remark 2.1.17. The above can be generalized to infinite direct sum, where we have that

$$\mathrm{Hom}_R\left(\bigoplus_{i\in I} X_i, Y\right) \cong \prod_{i\in I} \mathrm{Hom}_R(X_i, Y)$$

This is one of the tutorial question.

2.2 Projective Modules and Introduction to Categories

Proposition 2.2.1 (Equivalent Condition of Projective Module)**.** *Let P be an R-module. TFAE:*

1. ***Any** SES $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ gives rise to a SES*

$$0 \to \mathrm{Hom}_R(P, X) \xrightarrow{\alpha_*} \mathrm{Hom}_R(P, Y) \xrightarrow{\beta_*} \mathrm{Hom}_R(P, Z) \to 0$$

2. *For any surjective R-module homomorphism $\beta : Y \to Z$ and any R-module homomorphism $f : P \to Z$, there exists R-module homomorphism $g : P \to Y$, which is called a lift, such that $\beta \circ g = f$, i.e.*

$$\begin{array}{ccccc} & & & & P \\ & & \overset{\exists g}{\swarrow} & & \downarrow f \\ Y & \xrightarrow[\beta]{} & Z & \longrightarrow & 0 \end{array}$$

3. *Every SES $0 \to X \to Y \to P \to 0$ splits. In this case P is a direct summand of Y, that is there exists an R-module Y' such that $Y \cong Y' \oplus P$. We write $P \mid Y$.*

4. *P is a direct summand of a free R-module.*

If P satisfies any of these equivalent conditions, we call P a projective module.

Proof. [1. $\implies$ 2.] Consider the SES

$$0 \to \ker\beta \to Y \xrightarrow{\beta} Z \to 0$$

By assumption this gives rise the folliowing SES:

$$0 \to \mathrm{Hom}_R(P, \ker\beta) \to \mathrm{Hom}_R(P, Y) \xrightarrow{\beta_*} \mathrm{Hom}_R(P, Z) \to 0$$

where $\beta_* : g \mapsto \beta \circ g$. Note by second statement of Theorem 2.1.15 says that β_* is surjective. Thus for any $f \in \mathrm{Hom}_R(P, Z)$ there exists a $g_f \in \mathrm{Hom}_R(P, Y)$ such that $\beta_*(g) = \beta \circ g = f$.

[2. $\implies$ 3.] Suppose as stated by the statement. Consider the following diagram:

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \overset{\exists g}{\swarrow} & \uparrow \downarrow \mathrm{id}_P & & \\ 0 & \longrightarrow & X & \xrightarrow{\iota} & Y & \xrightarrow{\pi} & P & \longrightarrow & 0 \end{array}$$

where the existence of g is ensure by the assumption and that $\pi \circ g = \mathrm{id}_P$. By the second statement of Proposition 2.1.12, the existence of g implies that the SES splits.

[3. $\implies$ 4.] Suppose as stated in the statement. Since every R-module is a quotient of a free module, define $F(S)$ be a free module such that $F(S)$ surjects to P via map π. Then consider the SES

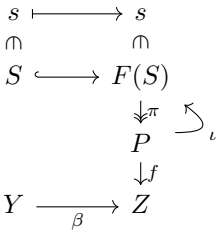
$$0 \to \ker\pi \to F(S) \xrightarrow{\pi} P \to 0$$

By the assumption, the above SES splits, and thus $F(S) = \ker \pi \oplus P$, showing that $P \mid F(S)$.

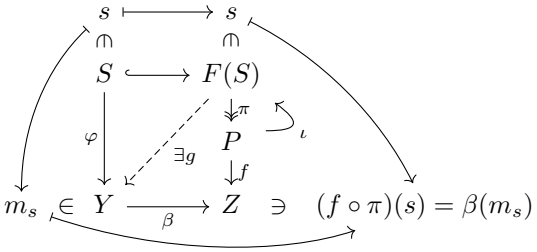
[4. $\implies$ 1.]. Suppose as stated in the statement. Assume that we have an SES $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$, and consider the short sequence

$$0 \to \mathrm{Hom}_R(P, X) \xrightarrow{\alpha_*} \mathrm{Hom}_R(P, Y) \xrightarrow{\beta_*} \mathrm{Hom}_R(P, Z) \to 0$$

Immediately by Theorem 2.1.15 we have that $\ker \alpha_* = 0$ and $\operatorname{im} \alpha_* = \ker \beta_*$, so it suffices to show that β_* is surjective. Take $f \in \mathrm{Hom}_R(P, Z)$. By assumption $F(S) \cong P \oplus P'$ for some free module $F(S)$ and $P' \subseteq F(S)$ is an R-module. Consider the following diagram:



where π is the canonical map from $F(S)$ to P and ι is the inclusion map from P to $F(S)$. Note that $\pi \circ \iota = \mathrm{id}_P$. Next, define the map $\varphi : S \to Y$ where $s \mapsto m_s$ if $\beta(m_s) = (f \circ \pi)(s)$. The map φ is indeed well-defined since β is surjective. Thus we now have the following diagram:

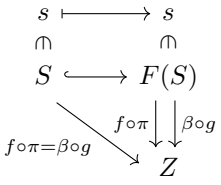


where the existence of g follows from the universal property of free module. In the diagram, the upper-triangular part is commutative, and we claim that the lower-triangular part is also commutative, i.e. $\beta \circ g = f \circ \pi$.

We first show that $\beta \circ g = f \circ \pi$ when restricted to S, or more precisely, the image of S in $F(S)$. This is easy, since for any $s \in S$ we have

$$(\beta \circ g)(s) = \beta(g(s)) = \beta(\varphi(s)) = \beta(m_s) = (f \circ \pi)(s)$$

Next, consider the following commutative diagram:



where the commutativity follows from the proven statement that $\beta \circ g = f \circ \pi$ when restricted on S. Then, by the uniqueness of the universal property of free module $F(S)$, we must have that $\beta \circ g = f \circ \pi$ on $F(S)$. This proves our claim.

Recall that we need to prove that β_* is surjective, in particular we have been given $f \in \mathrm{Hom}_R(P, Z)$ and we want to look for its pre-image under β_*. Consider $g \circ \iota : P \to Y$, so $g \circ \iota \in \mathrm{Hom}_R(P, Y)$. Then

$$\beta_*(g \circ \iota) = \beta \circ g \circ \iota \overset{(*)}{=} f \circ \pi \circ \iota \overset{(**)}{=} f \circ \mathrm{id}_P = f$$

where in $(*)$ we use the fact that $\beta \circ g = f \circ \pi$ and in $(**)$ we use the fact that $\pi \circ \iota = \mathrm{id}_P$. We have shown that $g \circ \iota$ is the pre-image of f under β_*, thus showing that β_* is surjective. The proof is then completed. $\square$

Remark 2.2.2. As shown and stated previously in Proposition 2.1.13, if $\alpha : X \to Y$ is injective, then $\alpha_* : \mathrm{Hom}_R(V, X) \to \mathrm{Hom}_R(V, Y)$ is injective for any V, but this statement need not holds when we replace injectivity with surjectivity. In particular, we have the statement:

Let V be an R-module. Then TFAE

- *V is projective.*
- *the SES $Y \xrightarrow{\beta} Z \to 0$ gives rise to the SES $\mathrm{Hom}_R(V, Y) \xrightarrow{\beta*} \mathrm{Hom}_R(V, Z) \to 0$.*

which is a direct consequence of the first statement of Proposition 2.2.1.

Corollary 2.2.3.

1. *Free modules are projective.*
2. *A (finitely generated) R-module is projective if and only if it is a direct summand of a (finitely generated) free module.*
3. *Direct sum of projective module is projective.*
4. *Every module is a quotient of projective module.*

Proof. For the first statement, if F is a free module, since $F \cong F \oplus 0$, so F is projective.

For the second statement, the statement is true by Proposition 2.2.1(4.). We check the finitely generated part. Suppose that P is finitely generated, then there exists S finite cardinality such that $F(S)$ surjects onto P, so $P \mid F(S)$. For the converse, if $P \mid F(S)$ where S has finite cardinality, then $F(S)$ surjects to P by the canonical map, π, so P is finitely generated by the image of $\pi(S)$.

Third statement is a tutorial question.

For fourth statement, every module is a quotient of free module, and is thus a quotient of projective module. □

Remark 2.2.4. Projective module is nice. One of the reasons is that, according to Proposition 2.2.1, for a projective module P, it suffices to only discuss on its Hom set, i.e. we only have to talk about maps. It might seems complicated, but this provides us a huge space to carry out abstraction. In fact, this is the central theme of category theory. In the light of this, we introduce some basic categorical notation.

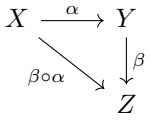
Definition 2.2.5 (Category)**.** A category $\mathcal{C}$ consists of the following:

1. A class of objects $\mathrm{Obj}(\mathcal{C})$
2. For any two objects X and Y, we have a class of morphisms (i.e. maps) $\mathrm{Mor}_{\mathcal{C}}(X, Y)$
3. For any objects X, Y, and Z, we have a binary operation $\mathrm{Mor}_{\mathcal{C}}(X, Y) \times \mathrm{Mor}_{\mathcal{C}}(Y, Z) \to \mathrm{Mor}_{\mathcal{C}}(X, Z)$ such that $(f, g) \mapsto g \circ f$, such that
   - the operation is associative
   - $\mathrm{Mor}_{\mathcal{C}}(X, X)$ contains an identity 1_X such that for any $g \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$ and $h \in \mathrm{Mor}_{\mathcal{C}}(Z, X)$, we have $g \circ 1_X = g$ and $1_X \circ h = h$

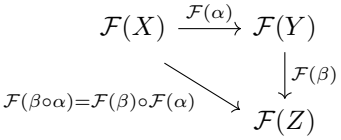
Definition 2.2.6 (Covariant functor)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be a categories. A covariant functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ consists of the following things:

1. For any object $X \in \mathrm{Obj}(\mathcal{C})$, we have an object $\mathcal{F}(X) \in \mathcal{D}$
2. For any morphism $\alpha : X \to Y$ of $\mathcal{C}$, we have a morphism $\mathcal{F}(\alpha) : \mathcal{F}(X) \to \mathcal{F}(Y)$ of $\mathcal{D}$ such that the following holds:
   - $\mathcal{F}(1_X) = 1_{\mathcal{F}(X)}$

- If we have the commutative diagram

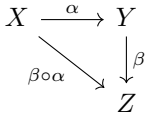


  then we have the commutative diagram:

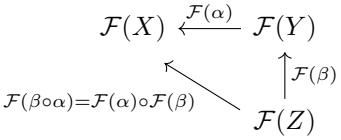


Definition 2.2.7 (Contravariant functor)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be a categories. A contravariant functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ consists of the following things:

1. For any object $X \in \mathrm{Obj}(\mathcal{C})$, we have an object $\mathcal{F}(X) \in \mathcal{D}$
2. For any morphism $\alpha : X \to Y$ of $\mathcal{C}$, we have a morphism $\mathcal{F}(\alpha) : \mathcal{F}(Y) \to \mathcal{F}(X)$ of $\mathcal{D}$ such that the following holds:
   - $\mathcal{F}(1_X) = 1_{\mathcal{F}(X)}$
   - If we have the commutative diagram



     then we have the commutative diagram:



Corollary 2.2.8. *For any R-module V the following*

$$\mathcal{F} := \mathrm{Hom}_R(V, -) : R\text{-}mod \to Ab$$

is a left exact covariant functor. Moreover, the functor is exact if and only if V is projective.

Proof. Let X be an R-module and consider $\mathrm{Hom}_R(V, X)$. Let $\alpha : X \to Y$ be an R-module homomorphism and denote $\mathcal{F}(\alpha) = \alpha_* : \mathrm{Hom}_R(V, X) \to \mathrm{Hom}_R(V, Y)$. We prove the axiom for a covariant functor. Suppose we have $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$, and so we have $\beta \circ \alpha : X \to Z$. As shown previously, this gives the following sequence:

$$\mathrm{Hom}_R(V, X) \xrightarrow{\alpha_*} \mathrm{Hom}_R(V, Y) \xrightarrow{\beta_*} \mathrm{Hom}_R(V, Z)$$

where clearly $\beta_* \circ \alpha_* = (\beta \circ \alpha)_*$. This proves the second axiom. Next, for the first axiom, define $\mathrm{id}_X : X \to X$ be the identity map of X. Then $(\mathrm{id}_X)_* : f \mapsto \mathrm{id} \circ f = f$, which shows that $(\mathrm{id}_X)_* = \mathrm{id}_{\mathrm{Hom}_R(X,X)}$. Therefore $\mathcal{F}$ is a covariant functor.

For the second part of the statement, it follows directly from the definition of projective modules. This completes the proof. □

Example 2.2.9.

1. Let F be a field, an F-module V is a vector space over F and hence V has a basis, i.e. $B \subseteq V$ such that V is free on B. So V is then projective, since free implies projective. In particular, all F-module are free and projective.

2. Let V be a $\mathbb{Z}$-module. Suppose that V consists an non-zero element x of finite order n. We claim that V is not free. Suppose not, then V is free on a set $B \subseteq V$, then

$$x = r_1 b_1 + \ldots, + r_m b_m$$

where $r_i \in \mathbb{Z}$ and $b_i \in B$. But since order of x is n, so we have

$$x = (n+1)x = x = r_1(n+1)b_1 + \cdots + r_m(n+1)b_m$$

Note $(n+1)r_i \neq r_i$ in $\mathbb{Z}$, so this gives non-unique representation of x. Since projective $\mathbb{Z}$-module are direct summand of free $\mathbb{Z}$-modules, any projective $\mathbb{Z}$-module does not contain non-zero element of finite order.

3. The previous example shows that all finite abelian groups are not projective.

4. The $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is torsion, i.e. for any $x \in \mathbb{Q}/\mathbb{Z}$, there exists $n \in \mathbb{Z}$ such that $nx = 0$. In particular, if $x = r/s + \mathbb{Z}$, take $n = s$ and we have

$$s\left(\frac{r}{s} + \mathbb{Z}\right) = r + \mathbb{Z} = \mathbb{Z}$$

So $\mathbb{Q}/\mathbb{Z}$ is not projective by the first example. From the characterization of projective modules, the SES

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

does not split. If not, then $\mathbb{Q}/\mathbb{Z}$ is a direct summand of $\mathbb{Q}$. Since $\mathbb{Q}/\mathbb{Z}$ contains non-zero element of finite order, it implies that so is $\mathbb{Q}$, which is clearly contradiction.

5. $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module. This follows from the fact that, if R is an integral domain, then torsion implies not projective. Since $\mathbb{Z}$ is an integral domain and $\mathbb{Q}$ is torsion, so $\mathbb{Q}$ is not projective as a $\mathbb{Z}$-module.

6. Following previous example, if R is not an integral domain, we can have R-module that is torsion yet projective. Consider $R = \mathbb{Z}/6\mathbb{Z}$ as the regular module. Clearly R is not an integral domain since $\bar{2} \cdot \bar{3} = 0$. Also $\mathbb{Z}/6\mathbb{Z}$ is clearly torsion, since for every $\bar{x}$ we have $6 \cdot \bar{x} = 0$. Lastly, we see that $R = R\{1\}$, so R is free of rank 1. Free implies projective, so $\mathbb{Z}/6\mathbb{Z}$ is an example of torsion module that is projective.

7. A finitely generated module over a $\mathbb{Z}$ is projective if and only if it is free. Free implies projective is clear. Assuming that it is projective. By the Classification of Finitely Generated Module over PID, an finitely generated $\mathbb{Z}$-module M is isomorphic with

$$\mathbb{Z}^n \bigoplus \text{ direct sum of finite copies of finite cyclic groups}$$

The direct sum of finite cyclic groups part contains elements of finite order. By assumption M is projective, so there must be no non-zero elements of finite order in M, implying that the direct sum of finite cyclic groups must be 0. This shows that

$$M \cong \mathbb{Z}^n$$

So M is free.

2.3 Injective Modules

Theorem 2.3.1. *Let V be an R-module and consider the sequence*

$$X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$$

If the above sequence is exact, then the following sequence is also exact:

$$0 \to \mathrm{Hom}_R(Z, V) \xrightarrow{\beta^*} \mathrm{Hom}_R(Y, V) \xrightarrow{\alpha^*} \mathrm{Hom}_R(X, V)$$

where $\beta^* : f \mapsto f \circ \beta$ and $\alpha^* : f \mapsto f \circ \alpha$. Furthermore, the sequance $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ is exact if and only if the following

$$0 \to \mathrm{Hom}_R(Z, V) \xrightarrow{\beta^*} \mathrm{Hom}_R(Y, V) \xrightarrow{\alpha^*} \mathrm{Hom}_R(X, V)$$

is exact for every V.

Proof. Suppose that $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ is exact. We first show that β^* is injective. Let $f \in \ker \beta^*$, so $\beta^*(f) = f \circ \beta = 0$ is the zero map, i.e. for all $y \in Y$ we have $f(\beta(y)) = 0$. By assumption β is surjective, thus for all $z \in Z$, let $y_z \in Y$ be such that $\beta(y_z) = z$, and so $f(z) = f(\beta(y)) = 0$. This shows that f must be a zero map, so $\ker \beta^*$ is trivial.

Next, we show that $\operatorname{im} \beta^* \subseteq \ker \alpha^*$. This is simple, simply follow:

$$\alpha^*(\beta^*(f)) = \alpha^*(f \circ \beta) = f \circ \beta \circ \alpha = f \circ (\beta \circ \alpha) \overset{(*)}{=} f \circ (0) = 0$$

where at $(*)$ we apply the assumption that $\beta \circ \alpha = 0$ given by exactness.

Then, we show that $\ker \alpha^* \subseteq \operatorname{im} \beta^*$. Let $g \in \ker \alpha^*$, i.e. $\alpha^*(g) = g \circ \alpha = 0$ is the zero map. Note that β is surjective, so for every $z \in Z$ we let $y_z \in Y$ be such that $\beta(y_z) = z$. Then, we define $f : Z \to V$ such that $z \mapsto g(y_z)$. We claim that $\beta^*(f) = g$.

- First we show f is well-defined. Suppose given z, let $y_z, y_z' \in Y$ be such that $\beta(y_z') = z = \beta(y_z)$. This implies $\beta(y_z - y_z') = 0$ and so $y_z - y_z' \in \ker \beta = \operatorname{im} \alpha$. So let $x \in X$ such that $\alpha(x) = y_z - y_z'$. Recall that $g \circ \alpha$ is the zero map by assumption, thus $g(y_z - y_z') = g(\alpha(x)) = 0$. This shows that $g(y_z) = g(y_z')$, showing that f is indeed well-defined.

- Next we show that f is an R-module homomorphism. Let $z, z' \in Z$ and let $y_z, y_{z'} \in Z$ such that $\beta(y_z) = z$ and $\beta(y_{z'}) = z'$, implying that $\beta(y_z + y_{z'}) = z + z'$. Therefore, by definition of the map f, we have $f(z) = g(y_z)$ and $f(z') = g(y_{z'})$. To show additivity:

  $$f(z + z') = g(y_z + y_{z'}) \overset{(**)}{=} g(y_z) + g(y_{z'}) = f(z) + f(z')$$

  where at $(**)$ it is valid to split since by assumption g is R-module homomorphism. Next, let $r \in R$. Note $\beta(ry_z) = r\beta(y_z) = rz$, so

  $$f(rz) = g(ry_z) = rg(y_z) = f(z)$$

  This shows that f is a R-module homomorphism.

- Lastly, suppose again given z, let $y_z \in Y$ be such that $\beta(y_z) = z$. So $(\beta^*(f))(y_z) = f(\beta(y_z)) = f(z) = g(y)$. This shows that $\beta^*(f) = g$.

This proves the first statement.

For the second statement, the forward direction is immediate from the first statement, so it suffices to show the backward direction is true. Suppose as assumed in the statement. First we show that β is surjective. Consider

$$V := \operatorname{coker} \beta = Z / \operatorname{im} \beta$$

Let $\pi : Z \to V$ be the canonical surjection. Then $\beta^*(\pi) = \pi \circ \beta$, so $(\beta^*(\pi))(y) = (\pi \circ \beta)(y) = \pi(\beta(y))$. Since $\beta(y) \in \operatorname{im} \beta$. so $(\beta^*(\pi))(y) = \overline{0}$. This means that $\beta^*(\pi) = 0$. Since β^* is injective, so $\pi = 0$ which means that $V = 0$, and so $Z = \operatorname{im} \beta$. This shows that β is surjective.

Next, we show that $\operatorname{im} \alpha \subseteq \ker \beta$. Take $V = Z$, and let id_Z be the identical map of Z. By the assumption of exactness $\alpha^* \circ \beta^*$ is zero map. So

$$(\alpha^* \circ \beta^*)(\operatorname{id}_Z) = 0 \implies \beta \circ \alpha \circ \operatorname{id}_Z = 0 \implies \beta \circ \alpha = 0$$

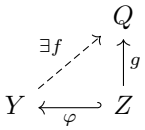
This shows that $\operatorname{im} \alpha \subseteq \ker \beta$.

Lastly, we show that $\ker \beta \subseteq \operatorname{im} \alpha$. Let $V = \operatorname{coker} \alpha = Y / \operatorname{im} \alpha$. Let $\pi : Y \to V$ be the canonical surjection. Similar to previous argument, we see that $\alpha^*(\pi) = \pi \circ \alpha = 0$ is the zero map, so $\pi \in \ker \alpha^* = \operatorname{im} \beta^*$ due to exactness. Let $g \in \operatorname{Hom}_R(Z, V)$ such that $\beta^*(g) = g \circ \beta = \pi$. Then for every $y \in \ker \beta$, we see that

$$(g \circ \beta)(y) = \pi(y) \implies g(\beta(y)) = \pi(y) \implies g(0) = \pi(y) \implies \pi(y) = 0$$

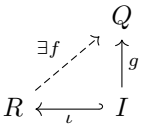
By definition of canonical surjection π, we have that $y \in \operatorname{im} \alpha$. So $\ker \beta \subseteq \operatorname{im} \alpha$. The proof is completed. □

Definition 2.3.2 (Injective modules)**.** Let Q be an R-module. We say that Q is injective if for any injective R-module homomorphism $\varphi : Z \to Y$ and R-module homomorphism $g : Z \to Q$, there exists $f : Y \to Q$ such that $f \circ \varphi = g$, i.e. we have the following commutative diagram



Proposition 2.3.3. *Let Q be an R-module.*

1. *(Baer's Criterion) The module Q is injective if and only if for every left ideal I of R and any R-module homomorphism $g : I \to Q$, there exists R-module homomorphism $f : R \to Q$ such that $g = f \circ \iota$, where $\iota : I \hookrightarrow R$ is the inclusion map.*



2. *If R is a PID, then Q is injective if and only if Q is divisible (i.e. for every $r \in R$ is non-zero, we have $rQ = Q$). When R is a PID, quotients of injective R-modules are injective.*

Proof. The forward direction simply follows from the definition of injective module, thus we are done. To prove the backward statement, suppose as stated in the condition, and we want to show that module Q is injective.

First, let $\alpha : Z \hookrightarrow Y$ be the inclusion map, and let $\beta : Z \to Q$ be a R-module homomorphism. Define

$$\Omega = \{(f', Y') : \operatorname{im}\alpha \subseteq Y' \subseteq Y \text{ and } f' : Y' \to Q \text{ s.t. } f' \circ \alpha = \beta, f' \text{ is } R\text{-module homomorphism}\}$$

Note that Ω is non-empty since we can check that $(\beta \circ \alpha^{-1}, \operatorname{im}\alpha) \in \Omega$. We now impose a partial order to Ω, where we define the partial order

$$(f', Y') \leq (f'', Y'') \iff Y' \subseteq Y'' \text{ and } f''\,|_{Y'} = f'$$

We show that it is indeed a partial order:

- Firstly, it is clear that $(f', Y') = (f', Y')$.
- Next, suppose that $(f', Y') \leq (f'', Y'')$ and $(f'', Y'') \leq (f', Y')$. This says that $Y' \subseteq Y'' \subseteq Y'$, so $Y' = Y''$. Also, we see that $f' = f''\,|_{Y'} = f''\,|_{Y''} = f''$. This concludes that $(f', Y') = (f'', Y'')$.
- Lastly, suppose that $(f', Y') \leq (f'', Y'') \leq (f''', Y''')$. Then we have $Y' \subseteq Y'' \subseteq Y'''$, implying that $Y' \subseteq Y'''$. Also, note that $f' = f''\,|_{Y'} = (f'''\,|_{Y''})\,|_{Y'} = f'''\,|_{Y'}$. This shows that $(f', Y') \leq (f''', Y''')$.

Therefore the relation $\leq$ is indeed a partial order. (As part of a tutorial question) we see Ω satisfies the hypothesis for applying Zorn's Lemma, and thus Ω has a maximum element, say (f, Y').

We claim that $Y' = Y$. Suppose not, then $Y' \subsetneq Y$, and let $m \in Y \setminus Y'$. Define $I = \{r \in R : rm \in Y'\}$. This is clearly an ideal of R. Let $g : I \to Q$ such that $g(r) = f(rm)$. We show that it is an R-module homomorphism:

- First, note $g(r + r') = f((r + r')m) = f(rm + r'm) = f(rm) + f(r'm) = g(r) + g(r')$.
- Next, let $s \in R$, we have $g(sr) = f((sr)m) = f(s(rm)) = sf(rm) = sg(r)$.

So g is an R-module homomorphism. By assumption, the exists an R-module homomorphism $h : R \to Q$ such that $h \circ \iota = g$, where $\iota : I \to R$ is the inclusion map.

Define the map $\gamma : Y' + Rm \to Q$ by $\gamma(m' + rm) = f(m') + h(r)$ where $m' \in Y'$ and $r \in R$. We show that $(\gamma, Y' + Rm) \in \Omega$

- We first show that γ is well-defined. Let $m_1' + r_1 m = m_2' + r_2 m$. Then $(r_2 - r_1)m = m_1' - m_2' \in Y'$, implying that $(r_2 - r_1) \in I$. Recall that $h \circ \iota = g$, so we have

$$h(r_2 - r_1) = (h \circ \iota)(r_2 - r_1) = g(r_2 - r_1) = f((r_2 - r_1)m) = f(m_1' - m_2')$$

and thus $h(r_2) - h(r_1) = h(r_2 - r_1) = f(m_1' - m_2') = f(m_1') - f(m_2')$. By rearranging we see that γ is well-defined.

- We show that γ is R-module homomorphism. Note

$$\begin{aligned}\gamma((m_1' + r_1 m) + (m_2' + r_2 m)) &= \gamma((m_1' + m_2') + (r_1 + r_2)m) \\ &= f(m_1' + m_2') + h(r_1 + r_2) \\ &= f(m_1') + f(m_2') + h(r_1) + h(r_2) \\ &= \gamma(m_1' + r_1 m) + \gamma(m_2' + r_2 m)\end{aligned}$$

and also

$$\begin{aligned}\gamma(s(m' + rm)) &= \gamma(sm' + (sr)m) \\ &= f(sm') + h(sr) \\ &= sf(m') + sh(r) \\ &= s(f(m') + h(r)) \\ &= s\gamma(m' + rm)\end{aligned}$$

This shows that γ is an R-module homomorphism.

- Lastly, we show that $\gamma \circ \alpha = \beta$. Since $(f, Y') \in \Omega$, by definition it satisfies $\operatorname{im}\alpha \subseteq Y' \subseteq Y$ and $f \circ \alpha = \beta$. Note $\alpha : Z \to Y$, so for all $z \in Z$ we have $\alpha(z) \in \operatorname{im}\alpha \subseteq Y'$, thus we can express $\alpha(z) = m' + 0m$ for $m' \in Y'$ and $0 \in R$. Therefore

$$\gamma(\alpha(z)) = \gamma(m' + 0m) = f(m') + h(0) = f(m') = f(\alpha(z)) = (f \circ \alpha)(z) = \beta(z)$$

We claim that $(\gamma, Y' + Rm)$ is strictly larger than the maximal element (f, Y') obtained from the Zorn's Lemma. Clearly $Y' \subsetneq Y' + Rm$. Also, note $\gamma \mid_{Y'} = f$. This contradicts to the maximality of (f, Y'), thus $Y' = Y$, and we have obtained an extended map $f : Y \to Q$. This completes the proof for the first statement.

For the second statement, we first show the forward direction: let Q be injective. Let $r \in R$ be non-zero. It is clear that $rQ \subseteq Q$, so we want to show that $rQ \subseteq Q$. For any $m \in Q$, define $g : (r) \to Q$ where $r \mapsto m$ and so $sr \mapsto sm$. By Baer's criterion, since Q is injective, there exists $f : R \to Q$ such that $f \circ \iota = g$ where $\iota : (r) \hookrightarrow R$ is the inclusion map. In particular $f(r) = (f \circ \iota)(r) = g(r) = m$. Note f is an R-module homomorphism, so $m = f(r) = rf(1) \in rQ$, implying that $m \in rQ$. This shows that Q is divisible.

For the backward direction, suppose that Q is divisible, and we want to show that Q is injective. Let $I \triangleleft R$ and $g : I \to Q$ be an R-module homomorphism. Since R is PID, so $I = (r)$ for some $r \in I$. If $r = 0$, then take $f : R \to Q$ is the zero map, and we have $f \circ \iota = 0 = g$. So the statement holds for when $r = 0$. Next, assume $r \neq 0$, since Q is divisible we have $rQ = Q$. We want to construct $f : R \to Q = rQ$ such that $f \circ \iota = g$. Note $g(r) \in Q = rQ$, so let $g(r) = rm$ for some $m \in Q$, and we define $f : R \to Q$ where $1 \mapsto m$. This implicitly defines for other $s \in R$ where $s \mapsto sm$. Note f is certainly well-defined, and we now show that f is a R-module homomorphism:

- $f(s + s') = (s + s')m = sm + s'm = f(s) + f(s')$.
- $f(s \cdot s') = f(ss') = (ss')m = s(s'm) = sf'(s)$.

So f is a R-module homomorphism. Lastly, see that $(f \circ \iota)(r) = f(r) = rm = g(r)$. Since $I = (r)$, so it implies $f \circ \iota = g$. By definition of injective modules, we have shown that Q is injective.

Finally, let Q be an injective R-module, and $Q' \subseteq Q$. Let $r \in R$ is non-zero element, observe that

$$r\,(Q/Q') = rQ/Q' = Q/Q'$$

Since R is PID and Q/Q' is divisible, we have that Q/Q' is injective. This completes the whole proof. $\square$

Example 2.3.4.

1. Over any ring R, any injective R-module is divisible.
2. Note $\mathbb{Z}$ is a PID. Applying the previous proposition, $\mathbb{Q}$ is an injective $\mathbb{Z}$-module because $\mathbb{Q}$ is divisible. However $\mathbb{Z}$ is not an injective $\mathbb{Z}$-module because $2\mathbb{Z} \neq \mathbb{Z}$. Also, since $\mathbb{Z}$ is PID, so quotients of injective $\mathbb{Z}$-module are injective, thus $\mathbb{Q}/\mathbb{Z}$ is injective. Recall we have seen that $\mathbb{Q}/\mathbb{Z}$ is not projective.
3. Let F be a field. Then any F-module is injective.

Corollary 2.3.5. *Any $\mathbb{Z}$-module is a sub-module of an injective $\mathbb{Z}$-module.*

Proof. Let M be a $\mathbb{Z}$-module and let $F(A)$ surjects onto M via π. This induces an isomorphism φ such that

$$F(A)/\ker\pi \overset{\varphi}{\cong} M$$

Let $Q = \bigoplus_{a\in A} \mathbb{Q}$ be a free $\mathbb{Z}$-module, where we consider $\mathbb{Q}$ as a $\mathbb{Z}$-module. For any $n \in \mathbb{Z}\setminus\{0\}$ and $\left(\frac{r_a}{s_a}\right)_{a\in A} \in Q$, we have

$$\left(\frac{r_a}{s_a}\right)_{a\in A} = n\left(\frac{r_a}{ns_a}\right)_{a\in A}$$

So Q is divisible, and thus Q is an injective $\mathbb{Z}$-module.

Next, observe that $\ker\pi \subseteq F(A) \cong \bigoplus_{a\in A}\mathbb{Z}$ and we can embed $F(A) \cong \bigoplus_{a\in A}\mathbb{Z}$ into Q via the following inclusion map

$$\iota : (n_a)_{a\in A} \mapsto \left(\frac{n_a}{1}\right)_{a\in A}$$

Since Q is injective, so $Q/\ker\pi$ is injective by the second statement of Proposition 2.3.3 (note $\mathbb{Z}$ is PID). Together, we see that

$$M \cong \frac{F(A)}{\ker\pi} \overset{\iota'}{\hookrightarrow} \frac{Q}{\ker\pi}$$

where the inclusion ι' is induced by ι. This proves that M, as a $\mathbb{Z}$-module, is a submodule of an injective $\mathbb{Z}$-module $Q/\ker\pi$ □

Theorem 2.3.6. *Any R-module is a sub-module of an injective R-module.*

Proof. Let M be an R-module. By treating M as a Z-module, by Corollary 2.3.5, it is a sub-module of an injective $\mathbb{Z}$-module, say Q. Note that $\mathrm{Hom}_Z(R,M) \subseteq \mathrm{Hom}_Z(R,Q)$ due to the following arguments:

- Since $M \subseteq Q$, we have the exact sequence $0 \to M \xrightarrow{\iota} Q \xrightarrow{\pi} Q/M$.
- This gives rise to the exact sequence $0 \to \mathrm{Hom}_{\mathbb{Z}}(R,M) \xrightarrow{\iota_*} \mathrm{Hom}_{\mathbb{Z}}(R,Q) \xrightarrow{\pi_*} \mathrm{Hom}_{\mathbb{Z}}(R,Q/M)$.
- This shows that $\mathrm{Hom}_{\mathbb{Z}}(R,M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R,Q)$.

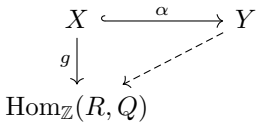
On the other hand, recall that $\mathrm{Hom}_R(R,M) \cong M$. Also it is clear that $\mathrm{Hom}_R(R,M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R,M)$. Altogether, we have the following:

$$M \cong \mathrm{Hom}_R(R,M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R,M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R,Q)$$

which summarizes into $M \subseteq \mathrm{Hom}_{\mathbb{Z}}(R,Q)$. We now show that $\mathrm{Hom}_{\mathbb{Z}}(R,Q)$ is an injective R-module.

Firstly , note we can view $\mathrm{Hom}_{\mathbb{Z}}(R,Q)$ as an R-module via the R-action $(r\cdot\varphi)(x) = \varphi(xr)$, which is valid since we can impose the $(\mathbb{Z},R)$-bimodule structure to R.

Next, to show that $\mathrm{Hom}_{\mathbb{Z}}(R,Q)$ is injective, let X and Y be any R-modules. Let $\alpha : X \hookrightarrow Y$ be an injective R-module homomorphism, and let $g : X \to \mathrm{Hom}_{\mathbb{Z}}(R,Q)$ be an R-module homomorphism. We want to show that there exists a R-module homomorphism that commutes the following diagram:



Define $g' : X \to Q$ where $x \mapsto (g(x))(1)$. We claim that g' is a $\mathbb{Z}$-module homomorphism:

- It suffices to show that it is an abelian group homomorphism. By definition X and Q are abelian groups. Note then $g'(x + x') = (g(x + x'))(1) = (g(x) + g(x'))(1) = (g(x))(1) + (g(x'))(1) = g'(x) + g'(x')$. Thus g' is a $\mathbb{Z}$-module homomorphism.

Since Q is an injective $\mathbb{Z}$-module, so there exists a $\mathbb{Z}$-module homomorphism f' such that the following diagram commutes:

$$\begin{array}{ccc} X & \xhookrightarrow{\alpha} & Y \\ {\scriptstyle g'}\downarrow & \swarrow_{\exists f'} & \\ Q & & \end{array}$$

i.e. $f' \circ \alpha = g'$. Define $f : Y \to \mathrm{Hom}_{\mathbb{Z}}(R, Q)$ by $y \mapsto f_y$ such that f_y is defined to be the map $f_y : r \mapsto f'(ry)$. We show that f is an R-module homomorphism:

- We claim f is well-defined, i.e. $f_y \in \mathrm{Hom}_{\mathbb{Z}}(R, Q)$. It suffices to show that f_y is an abelian group homomorphism. Note $f_y(r + r') = f'((r + r')y) = f'(ry + r'y) = f'(ry) + f(r'y) = f_y(r) + f_y(r')$. Thus $f(y) = f_y$ is indeed a $\mathbb{Z}$-module homomorphism.
- To show additivity: $(f(y + y'))(r) = f_{y+y'}(r) = f'(r(y + y')) = f'(ry + ry') = f'(ry) + f'(ry') = f_y(r) + f_{y'}(r) = (f_y + f_{y'})(r) = (f(y) + f(y'))(r)$.
- To show it respect R-action: $(s \cdot f(y))(r) = (s \cdot f_y)(r) = f_y(rs) = f'(rsy) = f'(r(sy)) = f_{sy}(r) = (f(sy))(r)$.

Lastly, we show that $f \circ \alpha = g$, i.e. we want to show that $((f \circ \alpha)(x))(r) = (g(x))(r)$ where $x \in X$ and $r \in R$. Note

$$\begin{aligned} ((f \circ \alpha)(x))(r) &= (f(\alpha(x)))(r) \\ &= f_{\alpha(x)}(r) \\ &= f'(r\alpha(x)) \\ &= f'(\alpha(rx)) \\ &= (f' \circ \alpha)(rx) \\ &= g'(rx) \\ &= (g(rx))(1) \\ &= (r \cdot g(x))(1) \\ &= (g(x))(1 \cdot r) \\ &= (g(x))(r) \end{aligned}$$

In other words, we have establish the following commutative diagram:

$$\begin{array}{ccc} X & \xhookrightarrow{\alpha} & Y \\ {\scriptstyle g}\downarrow & \swarrow_{\exists f} & \\ \mathrm{Hom}_{\mathbb{Z}}(R, Q) & & \end{array}$$

Therefore $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module. This completes the proof. □

Proposition 2.3.7. *Let I be an R-module. TFAE:*

1. *I is injective.*
2. *For any SES $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$, we have SES*

$$0 \to \mathrm{Hom}_R(X, I) \xrightarrow{\beta^*} \mathrm{Hom}_R(Y, I) \xrightarrow{\alpha^*} \mathrm{Hom}_R(X, I) \to 0$$

3. *Let Y be a R-module. If I is isomorphic to a submodule of Y, then the following SES splits:*

$$0 \to I \xhookrightarrow{\iota} Y \xrightarrow{\pi} \!\!\!\rightarrow Y/I \to 0$$

And hence $I \mid Y$. Consequently $Y \cong I \oplus Y/I$.

Corollary 2.3.8. *Let V be an R-module. Then*

$$\mathcal{F} := \mathrm{Hom}_R(-, V) : R\text{-}mod \to Ab$$

is a left exact contravariant functor, i.e. the SES $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ gives rise to the exact sequence

$$0 \to \mathrm{Hom}_R(Z, V) \xrightarrow{\beta^*} \mathrm{Hom}_R(Y, V) \xrightarrow{\alpha^*} \mathrm{Hom}_R(X, V)$$

Furthermore, the functor $\mathcal{F}$ is exact if and only if V is injective.

Proof. The proofs of previous proposition and corollary are left as tutorial questions. □

2.4 Flat Modules

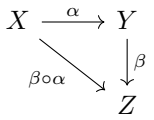
Let D be a right R-module. The operation

$$\mathcal{F} := D \otimes_R - : R\text{-mod} \to \mathrm{Ab}$$

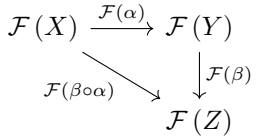
where ${}_RX \mapsto D \otimes_R X$ such that $(\alpha : X \to Y) \mapsto ((1 \otimes \alpha) : D \otimes_R X \to D \otimes_R Y, d \otimes x \mapsto d \otimes \alpha(x))$. The functor $\mathcal{F}$ is a covariant functor.

To see this, we show all the axioms of a covariant functor hold:

- For any R-module X, it is clear that $D \otimes_R X$ is well-defined and is an abelian group, which lies in the category Ab of abelian group.
- Define $\mathbb{1}_X : X \to X$ be the identity map on X. By definition $\mathcal{F}(\mathbb{1}_X) = 1 \otimes \mathbb{1}_X$ such that $1 \otimes \mathbb{1}_X : D \otimes_R X \to D \otimes_R X$ defined by $d \otimes x \mapsto d \otimes x$. Clearly we see that $\mathcal{F}(\mathbb{1}_X)$ is the identity map on $\mathcal{F}(X)$. This shows that $\mathcal{F}(\mathbb{1}_X) = \mathbb{1}_{\mathcal{F}(X)}$.
- Suppose we have commutative diagram

  Then we have that

  and we examine that it is commutative. By following definition we see

  $$\mathcal{F}(\beta \circ \alpha) = 1 \otimes (\beta \circ \alpha) = (1 \circ 1) \otimes (\beta \circ \alpha) = (1 \otimes \beta) \circ (1 \otimes \alpha) = \mathcal{F}(\beta)\mathcal{F}(\alpha)$$

  This shows that the diagram is commutative.

Moreover, if D is a (S, R)-bimodule, then $\mathcal{F} : X \mapsto D \otimes_R X$ is a functor that maps from category of R-mod to category of S-mod.

Theorem 2.4.1. *Let D be an (S, R)-bimodule and X, Y, Z be left R-module. If $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ is exact, then*

$$D \otimes_R X \xrightarrow{1\otimes\alpha} D \otimes_R Y \xrightarrow{1\otimes\beta} D \otimes_R Z \to 0 \tag{2}$$

is exact. Moreover $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ is exact if and only if (2) is exact for all D.

Proof. Assume as supposed in the statement. For the first statement we show the following:

1. $(1 \otimes \beta)$ is surjective. Let $d \otimes z \in D \otimes_R Z$. By assumption β is surjective, so there exists $y \in Y$ such that $\beta(y) = z$. Observe then that $(1 \otimes \beta)(d \otimes y) = d \otimes \beta(y) = d \otimes z$.

2. $\operatorname{im}(1\otimes\alpha) \subseteq \ker(1\otimes\beta)$. First observe that by definition $\beta\circ\alpha = 0$. Thus $(1\otimes\beta)(1\otimes\alpha) = 1\otimes(\beta\circ\alpha) = 1\otimes 0 = 0$. This shows that $\operatorname{im}(1\otimes\alpha) \subseteq \ker(1\otimes\beta)$.

3. $\ker(1\otimes\beta) \subseteq \operatorname{im}(1\otimes\alpha)$. To prove this, recall we have proved that $\operatorname{im}(1\otimes\alpha) \subseteq \ker(1\otimes\beta)$, this implies that we have the surjection:

$$\pi : (D\otimes_R Y)/\operatorname{im}(1\otimes\alpha) \twoheadrightarrow (D\otimes_R Y)/\ker(1\otimes\beta) \cong D\otimes_R Z$$

Our goal is to show that π is injective. First, by assumption β is surjective, so for each $z\in Z$ we define $y_z \in Z$ be such that $\beta(y) = z$. Next define the map $\gamma : D\times Z \to (D\otimes_R Y)/\operatorname{im}(1\otimes\alpha)$ where $(d,z)\mapsto (d\otimes y_z) + \operatorname{im}(1\otimes\alpha) =: \overline{d\otimes y_z}$.

- We claim that π is well-defined. Let y' and y be such that $\beta(y') = z = \beta(y)$. Note then $y - y' \in \ker\beta = \operatorname{im}\alpha$ due to exactness. Thus $d\otimes y - d\otimes y' = d\otimes(y-y') \in \operatorname{im}(1\otimes\alpha)$. This shows that regardless of the choice of y_z is y or y', we always have that

$$\overline{d\otimes y} = \gamma(d,z) = \overline{d\otimes y'}$$

- Next we show that γ is R-balanced. If $\beta(y_z) = z$, then $\beta(ry_z) = rz$, and so $y_{rz} = ry_z$. Thus

$$\gamma(d,rz) = \overline{d\otimes y_{rz}} = \overline{d\otimes ry_z} = \overline{dr\otimes y_z} = \gamma(dr,z)$$

For the second axiom, simply prove that

$$\gamma(d+d',z) = \overline{(d+d')\otimes y_z} = \overline{d\otimes y_z + d'\otimes y_z} = \overline{d\otimes y_z} + \overline{d'\otimes y_z} = \gamma(d,z) + \gamma(d',z)$$

For the third axiom, if $\beta(y_z) = z$ and $\beta(y_{z'}) = z'$, then $\beta(y_z + y_{z'}) = z + z'$, so $y_{z+z'} = y_z + y_{z'}$. Thus

$$\gamma(d,z+z') = \overline{d\otimes y_{z+z'}} = \overline{d\otimes(y_z+y_{z'})} = \overline{d\otimes y_z} + \overline{d\otimes y_{z'}} = \gamma(d,z) + \gamma(d,z')$$

This shows that γ is R-balanced.

Therefore, by the Universal Property of Tensor Product, there exists $\pi' : D\otimes_R Z \to (D\otimes_R Y)/\operatorname{im}(1\otimes\alpha)$ where $d\otimes z \mapsto \overline{d\otimes y_z}$.

Define $\varphi : (D\otimes_R Y)/\operatorname{im}(1\otimes\alpha) : D\otimes_R Z$ by $d\otimes y \mapsto d\otimes\beta(y)$. We show that $\pi'\circ\varphi$ and $\varphi\circ\pi'$ are identity maps (on respective domain).

- $(\pi'\circ\varphi)(\overline{d\otimes y}) = \pi'(d\otimes\beta(y)) = \overline{d\otimes y}$
- $(\varphi\circ\pi')(d\otimes z) = \varphi(\overline{d\otimes y_z}) = d\otimes\beta(y_z) = d\otimes z$

This shows that φ and π are inverses of each other, implying that they are isomorphisms. This shows that $\operatorname{im}(1\otimes\alpha) = \ker(1\otimes\beta)$.

For the second statement, the forward direction is proved, so supposed that (2) is exact for all (S,R)-bimodule D. Take $D = R$. Recall $R\otimes_R X \cong X$ and this holds similarly for Y and Z. We then have the following diagram:

$$\begin{array}{ccccccc} R\otimes_R X & \xrightarrow{1\otimes\alpha} & R\otimes_R Y & \xrightarrow{1\otimes\beta} & R\otimes_R Z & \longrightarrow & 0 \\ \updownarrow & & \updownarrow & & \updownarrow & & \\ X & \xrightarrow{\alpha} & Y & \xrightarrow{\beta} & Z & \longrightarrow & 0 \end{array}$$

where the isomorphism between $R\otimes_R X$ and X is given by $1\otimes x \mapsto x$ (similarly for Y and Z). We show that we have commutativity in the first and second square. First, let $1\otimes x \in R\otimes_R X$, then sending along the upper route to Y we obtain

$$1\otimes x \overset{1\otimes\alpha}{\mapsto} 1\otimes\alpha(x) \mapsto \alpha(x)$$

If sending along the lower route to Y we obtain

$$1\otimes x \mapsto x \overset{\alpha}{\mapsto} \alpha(x)$$

This shows we have commutativity in the first square. Similarly we have comutativity in the second square. This gives commutativity in the whole diagram. Since the first row is commutative and we have isomorphisms map, we conclude that the second row is commutative. This completes the proof. □

Example 2.4.2. $\mathbb{Z} \overset{\alpha}{\hookrightarrow} \mathbb{Q}$. Take $D = \mathbb{Z}/2Z$. Then $D \otimes_{\mathbb{Z}} \mathbb{Z} \cong D = \mathbb{Z}/2\mathbb{Z}$. But $D \otimes_{\mathbb{Z}} \mathbb{Q} \cong 0$, since

$$x \otimes \frac{r}{s} = x \otimes \frac{2r}{2s} = 2x \otimes \frac{r}{2s} = 0$$

since $2x = 0$ in D.

Proposition 2.4.3. *Let D be a right R-module. TFAE:*

1. *If we have SES $0 \to X \to Y \to Z \to 0$, then we have $0 \to D \otimes_R X \to D \otimes_R Y \to D \otimes_R Z \to 0$ is exact.*
2. *if $0 \to X \to Y$ is exact, then $0 \to D \otimes_R X \to D \otimes_R Y$ is exact.*

In any of these cases, we say that D is a flat R-module.

Corollary 2.4.4. *Let D be a right R-module. The functor $\mathcal{F} : D \otimes_R - : R\text{-}mod \to Ab$ is right exact covariant. Moreover $\mathcal{F}$ is exact if and only if D is flat. If D is a (S, R)-bimodule, then $\mathcal{F} : D \otimes_R -$ is a functor that sends from R-module to S-module.*

Theorem 2.4.5. *Projective (and hence free) modules are flat.*

Proof. We first prove the special case for free modules. Let F be a free R-module and $\alpha : X \to Y$ be an injective R-module homomorphism. To show that F is flat, by Proposition 2.4.3 we show that if $0 \to X \overset{\alpha}{\to} Y$ is exact, then $0 \to D \otimes_R X \overset{1\otimes\alpha}{\longrightarrow} D \otimes_R Y$ is exact. This is equivalent to showing that the injection $\alpha : X \to Y$ implies $1 \otimes \alpha : F \otimes_R X \to F \otimes_R Y$ is injective.

First, since F is free, so we can write $F \cong \bigoplus_{a\in A} R$ where F is free on a subset $A \subseteq F$. Next, in tutorial, we have seen that $(\bigoplus R) \otimes_R X \cong \bigoplus(R \otimes_R X)$. We have also seen previously that $R \otimes_R X \cong X$. Altogether we obtain the following commutative diagram:

$$\begin{array}{ccccccc}
 & & F \otimes_R X & \xrightarrow{1\otimes\alpha} & F \otimes_R Y & & \\
 & & \updownarrow & & \updownarrow & & \\
\sum(\mathbb{1}_a \otimes x_a) & \in & (\bigoplus R) \otimes_R X & \longrightarrow & (\bigoplus R) \otimes_R Y & \ni & \sum(\mathbb{1}_a \otimes \alpha(x_a)) \\
\uparrow\downarrow & & \updownarrow & & \updownarrow & & \downarrow\uparrow \\
\sum(1 \otimes x_a) & \in & \bigoplus(R \otimes_R X) & \longrightarrow & \bigoplus(R \otimes_R Y) & \ni & \sum(1 \otimes \alpha(x_a)) \\
\uparrow\downarrow & & \updownarrow & & \updownarrow & & \downarrow\uparrow \\
\sum x_a & \in & \bigoplus_{a\in A} X & \xrightarrow{\varphi} & \bigoplus_{a\in A} Y & \ni & \sum \alpha(x_a)
\end{array}$$

where $\mathbb{1}_a$ denotes the direct sum indexed by A which takes value 1 at the a-th position and 0 otherwise. If $\sum x_a \in \ker\varphi$, then $\sum \alpha(x_a) = 0$. Since this is a direct sum, we must have $\alpha(x_a) = 0$ for all a. By assumption α is injective, so $x_a = 0$ for all a. Therefore $\sum x_a = 0$. This shows that φ is injective, and thus $1 \otimes \alpha$ is injective, showing that any free R-module is flat.

Next, let P be a projective R-module. Then $P \oplus P' = F$ for some free R-module F. Note $(P \oplus P') \otimes_R X \cong (P \otimes_R X) \oplus (P' \otimes_R X)$. We have the following commutative diagram:

$$\begin{array}{ccccccc}
a \otimes x & \in & F \otimes_R X & \xrightarrow{1\otimes\alpha} & F \otimes_R Y & \ni & a \otimes \alpha(x) \\
\uparrow & & \updownarrow & & \uparrow & & \downarrow \\
(a + 0) \otimes x & \in & (P \oplus P') \otimes_R X & & & & \\
\uparrow & & \updownarrow & & \downarrow & & \\
(a \otimes x, 0) & \in & (P \otimes_R X) \oplus (P' \otimes_R X) & \longrightarrow & (P \otimes_R Y) \oplus (P' \otimes_R Y) & \ni & (a \otimes \alpha(x), 0)
\end{array}$$

By the previous settled special case, since F is free, so $1 \otimes \alpha$ is injective. By restricting $1 \otimes \alpha$ to $P \otimes_R X$ (and thus is mapped to $P \otimes_R Y$) it is also injective. □

Example 2.4.6.

1. $\mathbb{Z}/2\mathbb{Z}$ is not flat, since $\mathbb{Z}$ injects to $\mathbb{Q}$ yet $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong 0$, so no injective map is possible after tensoring.

2. $\mathbb{Q}$ is not projective but it is flat. Let $\alpha : X \hookrightarrow Y$ be a $\mathbb{Z}$-module homomorphism. Consider $1 \otimes \alpha : \mathbb{Q} \otimes_{\mathbb{Z}} X \to \mathbb{Q} \otimes_{\mathbb{Z}} Y$. Note for an element in $\mathbb{Q} \otimes_{\mathbb{Z}} X$ takes the form and can be rewriten into

$$\begin{aligned}\frac{r_1}{s_1} \otimes x_1 + \cdots + \frac{r_m}{s_m} \otimes x_m &= \frac{r_1'}{s} \otimes x_1 + \cdots + \frac{r_m'}{s} \otimes x_m \\ &= \frac{1}{s} \otimes r_1' x_1 + \cdots + \frac{1}{s} \otimes r_m' x_m \\ &= \frac{1}{s} \otimes x\end{aligned}$$

   where $s = \operatorname{lcm}(s_1, \ldots, s_m)$. So $1 \otimes \alpha$ is injective, and $\mathbb{Q}$ is flat.

3. We have seen that $\mathbb{Q}/\mathbb{Z}$ is injective. We claim that it is not flat. Let $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Z}$ be defined $n \mapsto 2n$. Recall that $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}$. Then note

$$(1 \otimes \varphi)\left(\overline{\frac{1}{2}} \otimes 1\right) = \overline{\frac{1}{2}} \otimes \varphi(1) = \overline{\frac{1}{2}} \otimes 2 = \overline{\frac{1}{2}} \cdot 2 \otimes 1 = \overline{1} \otimes 1 = 0$$

   since $\overline{1} \in \mathbb{Z}$, which is quotiened out in $\mathbb{Q}/\mathbb{Z}$.

Remark 2.4.7. All previous statements and examples sums up the relation of free, projective, and flat module as follow:

$$\text{Free modules} \implies \text{Projective modules} \implies \text{Flat modules}$$

We provide examples for each of the class of modules:

- Free modules: Direct sum of R-modules.
- Projective modules that are not free. Let K be a field, and consider the ring $R = K \times K$. Note R itself is free as a regular R-module. Take $P = K \times 0$, then P is projective since

$$R = (K \times 0) \oplus (0 \times K)$$

  However P is not free. To see this, suppose to the contrary that P is a free R-module, then

$$P \cong \bigoplus_{i=1}^{n} R$$

  for some n. Note $R = K \times K$ is a vector space over K, so $\dim R$ is well-defined. In particular we see $\dim R = 2 \dim K$. Similarly, since P is isomorphic to K, we have $\dim R = \dim K$. The isomorphism suggests that

$$\dim K = n(2 \dim K) \implies (2n-1) \dim K = 0 \implies 2n - 1 = 0$$

  This gives $n = 1/2$, which is absurd, so P is not a free R-module.

- Flat module that is not projective. $\mathbb{Q}$ as a $\mathbb{Z}$-module is not projective, but it is flat.

Definition 2.4.8 (Functor adjunction)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be categories. Let $X \in \operatorname{Obj}(\mathcal{C})$ and $Z \in \operatorname{Obj}(\mathcal{D})$. Let $\mathcal{L} : \mathcal{C} \to \mathcal{D}$ and $\mathcal{R} : \mathcal{D} \to \mathcal{C}$ be two functors. We say that $(\mathcal{L}, \mathcal{R})$ is a pair of adjoint functor if $\operatorname{Mor}_{\mathcal{D}}(\mathcal{L}(X), Z) \cong \operatorname{Mor}_{\mathcal{C}}(X, \mathcal{R}(Z))$.

Theorem 2.4.9 (Tensor-Hom Adjunction)**.** *Let X be a right R-module, Y be a (R, S)-bimodule, and Z be a right S-module. Then $(- \otimes_R Y,\ \operatorname{Hom}_S(Y, -))$ is a pair of adjunct functors. In other words, we have an isomorphism of abelian group:*

$$\operatorname{Hom}_S(X \otimes_R Y, Z) \cong \operatorname{Hom}_R(X, \operatorname{Hom}_S(Y, Z))$$

Proof. Define $f : \operatorname{Hom}_S(X \otimes_R Y, Z) \to \operatorname{Hom}_R(X, \operatorname{Hom}_S(Y, Z))$ where

$$f : \varphi \mapsto \tilde{\varphi} : X \to \operatorname{Hom}_S(Y, Z)$$

and $\tilde{\varphi}$ is defined by $x \mapsto \tilde{\varphi}_x(y) := \varphi(x \otimes y)$. Our goal is to construct a map g and show that $f \circ g$ and $g \circ f$ are identity maps on their respective domain, which shows that they are isomorphisms.

We first show that f is well-defined, which will be broken down into several steps. First, we show that $f(\varphi)$ is an R-module homomorphism. It is easy to check that additivity holds, thus omitted. For any $r \in R$, $x \in X$, and $y \in Y$, we have

$$\begin{aligned}((f(\varphi))(xr))(y) &= (\tilde{\varphi}(xr))(y) \\ &= \tilde{\varphi}_{xr}(y) \\ &= \varphi(xr \otimes y) \\ &= \varphi(x \otimes ry) \\ &= \tilde{\varphi}_x(ry) \\ &= (\tilde{\varphi}_x \cdot r)(y) \\ &= ((f(\varphi))(x) \cdot r)(y)\end{aligned}$$

This shows $f(\varphi)$ respects R-action. Next show that $(f(\varphi))(x) = \tilde{\varphi}_x$ is really a S-module homomorphism. Similar we omit the proof for additivity. For any $s \in S$, we have

$$\begin{aligned}((f(\varphi))(x))(ys) &= \tilde{\varphi}_x(ys) \\ &= \varphi(x \otimes ys) \\ &= \varphi(x \otimes y)s \\ &= \tilde{\varphi}_x(y)s \\ &= ((f(\varphi))(x))(y)s\end{aligned}$$

This shows that $(f(\varphi))(x) = \tilde{\varphi}_x$ respect S-action.

Suppose given $\psi \in \mathrm{Hom}_R(X, \mathrm{Hom}_S(Y, Z))$. We define $\beta : X \times Y \to Z$ by

$$\beta : (x, y) \mapsto (\psi(x))(y)$$

We claim that β is R-balanced, where one just have to verify all the axioms for R-balanced:

$$\beta(xr, y) = (\psi(xr))(y) = (\psi(x) \cdot r)(y) = (\psi(x))(ry) = \beta(x, ry)$$

and

$$\beta(x + x', y) = (\psi(x + x'))(y) = (\psi(x) + \psi(x'))(y) = (\psi(x))(y) + (\psi(x'))(y) = \beta(x, y) + \beta(x', y)$$

and

$$\beta(x, y + y') = (\psi(x))(y + y') = (\psi(x))(y) + (\psi(x))(y') = \beta(x, y) + \beta(x, y')$$

Since $\beta : X \times Y \to Z$ is an R-balanced map, by the universal property of tensor product, there exists R-homomorphism $\psi' : X \otimes_R Y \to Z$ such that $x \otimes y \mapsto (\psi(x))(y)$. Thus, for all $\psi \in \mathrm{Hom}_R(X, \mathrm{Hom}_S(Y, Z))$ we are able to get a corresponding $\psi' \in \mathrm{Hom}_S(X \otimes_R Y, Z)$ according to the described procedure.

We then define $g : \mathrm{Hom}_R(X, \mathrm{Hom}_S(Y, Z)) \to \mathrm{Hom}_S(X \otimes_R Y, Z)$ where

$$g : \psi \mapsto \psi'$$

where $\psi' : x \otimes y \mapsto \psi'(x \otimes y) = (\psi(x))(y)$. We claim that f and g are invserses of each other. To see this, we first show $(f \circ g)(\psi) = \psi$. For the sake of readability, we write $(f \circ g)(\psi) = f(g(\psi)) = f(\psi') = \tilde{\psi'}$

$$(((f \circ g)(\psi))(x))(y) = (\tilde{\psi'}(x))(y) = \psi'_x(y) = \psi'(x \otimes y) = (\psi(x))(y)$$

Next, we have to show $(g \circ f)(\varphi) = \varphi$.

$$((g \circ f)(\varphi))(x \otimes y) = (f(\varphi))'(x \otimes y) = ((f(\varphi))(x))(y) = \tilde{\varphi}_x(y) = \varphi(x \otimes y)$$

Thus we have shown that f and g are isomorphisms. This completes the proof. □

Remark 2.4.10. The intuition of the defined map f is as follow: for f, a homomorphism φ that initially maps $x \otimes y$ to $\varphi(x \otimes y)$, is separated into stages: first an element x of X determines the image map, then it takes all y to $\varphi(x \otimes y)$.

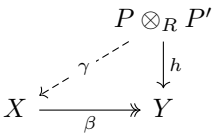
$$f : \varphi \mapsto (x \mapsto (y \mapsto \varphi(x \otimes y)))$$

For g, a homomorphism ψ works as follow: given an $x \in X$, it defines another homomorphism $\psi(x)$, and this homomorphism sends y to $(\psi(x))(y)$. This is exactly the image of $x \otimes y$ mapped by g.

$$\psi \mapsto (x \otimes y \mapsto (\psi(x))(y))$$

Corollary 2.4.11. *Let R be a commutative ring. Then the tensor product of two projective R-module is projective.*

Proof. Let R be a commutative ring. Let P and P' be projective R-modules. By definition of projective modules, suppose we have X and Y are R-modules, let $\beta : X \twoheadrightarrow Y$ and $h : P \otimes_R P' \to Y$ be R-module homomorphisms where β is surjective. We want to construct a map $\gamma : P \otimes_R P' \to X$ such that $h = \gamma \circ \gamma$:



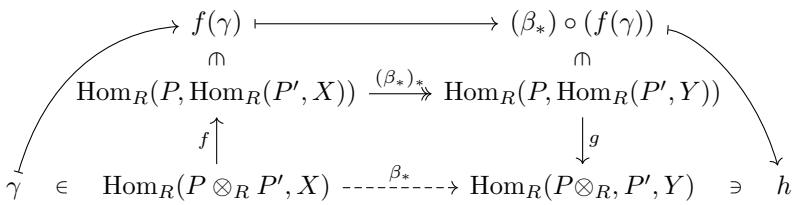
First, note that β induces the following surjective map

$$\beta_* : \mathrm{Hom}_R(P', X) \twoheadrightarrow \mathrm{Hom}_R(P', Y),\ \alpha \mapsto \beta \circ \alpha$$

This further induces a surjective map

$$(\beta_*)_* : \mathrm{Hom}_R(P, \mathrm{Hom}_R(P', X)) \twoheadrightarrow \mathrm{Hom}_R(P, \mathrm{Hom}_R(P', Y)),\ \varphi \mapsto \beta_* \circ \varphi$$

With this, due to tensor-hom adjunction, we have



where f and g are as defined in Theorem 2.4.9. Here the element γ is explicit defined according to the following procedure:

- Due to tensor-hom adjunction, there must be an isomorphic copy of h in $\mathrm{Hom}_R(P, \mathrm{Hom}_R(P', Y))$.
- Since $(\beta_*)_*$ is surjective, there must be a pre-image of the isomorphic copy of h.
- Again, due to tensor-hom adjunction, there must be an isomorphic copy of the pre-image of isomorphic copy of h. We define it to be γ.

We claim that the above diagram commutes, i.e. we want to show $\beta_*(\gamma) = \beta \circ \gamma = h$. We want to show that for any $s \in P$ and $t \in P'$, we must have $(\beta \circ \gamma)(s \otimes t) = h(s \otimes t)$. Note that

$$\begin{aligned}
h(s \otimes t) &= (g(\beta_* \circ f(\gamma)))(s \otimes t) \\
&= (g(\beta_* \circ \tilde{\gamma}))(s \otimes t) \\
&= (\beta_* \circ \tilde{\gamma})'(s \otimes t) \\
&= ((\beta_* \circ \tilde{\gamma})(s))(t) \\
&= (\beta_*(\tilde{\gamma}_s))(t) \\
&= (\beta \circ \tilde{\gamma}_s)(t) \\
&= \beta(\tilde{\gamma}_s(t)) \\
&= \beta(\gamma(s \otimes t)) \\
&= (\beta \circ \gamma)(s \otimes t)
\end{aligned}$$

This shows that $h = \beta \circ \gamma$, and thus we have shown that $P \otimes_R P$ is projective. □

3 (Co)Homology, Ext Group, and Tor Group

3.1 Basic Theory of (Co)Homology

Definition 3.1.1 (Chain complex and cochain complex)**.** A chain complex is a sequence

$$\mathcal{C} := (X_\bullet, d_\bullet) : \cdots \to X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} X_{-1} \xrightarrow{d_{-1}} X_{-2} \to \dots$$

where X_i are R-modules and d_i are R-module homomorphism, such that $d_{n-1} \circ d_n = 0$. In other words $\operatorname{im} d_n \subseteq \ker d_{n-1}$.

Similarly, a cochain complex is a sequence

$$\mathcal{D} := (X^\bullet, d^\bullet) : \dots \leftarrow X^1 \xleftarrow{d^1} X^0 \xleftarrow{d^0} X^{-1} \xleftarrow{d^{-1}} X^{-2} \leftarrow \dots$$

where X^i are R-modules and d^i are R-module homomorphism, such that $d^n \circ d^{n-1} = 0$. In other words $\operatorname{im} d^{n-1} \subseteq \ker d^n$.

Definition 3.1.2 (Boundedness)**.** A chain complex is said to be bounded above if there exists $N \in \mathbb{Z}$ such that $X_m = 0$ for all $m < N$. Similarly, a cochain complex is said to be bounded below if there exists $M \in \mathbb{Z}$ such that $X^m = 0$ for all $m < M$

Definition 3.1.3 (Homology)**.** Suppose given a chain complex $\mathcal{C} := (X_\bullet, d_\bullet)$. The n-th homology is defined to be the quotient group

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

Definition 3.1.4 (Cohomology)**.** Suppose given a cochain complex $\mathcal{D} := (X^\bullet, d^\bullet)$. The n-th cohomology is defined to be the quotient group

$$H^n(\mathcal{D}) := \frac{\ker d^{n+1}}{\operatorname{im} d^n}$$

Remark 3.1.5 ((Co)homology and exactness)**.** (Co)homology detects failure of exactness in (co)chain complex. In particular, the n-th (co)homology is 0 if and only if the n-th position of the (co)chain complex is exact. A (co)chain complex is said to be exact if it is exact at every term. It should be clear that, thus, a (co)chain complex is exact if and only if the (co)homology is always exact.

Definition 3.1.6 (Homomorphism of (co)chain complexes)**.** Let $(X^\bullet, d^\bullet)$ and $(Y^\bullet, \delta^\bullet)$ be two (co)chain complexes. The homomorphism from $X^\bullet$ to $Y^\bullet$ is a collection of module homomorphism $\varphi : X^\bullet \to Y^\bullet$ where for all n we have $\varphi_n : X^n \to Y^n$ such that the following diagram commutes:

$$\begin{array}{ccccccccc}
\dots & \xrightarrow{d^{n-1}} & X^{n-1} & \xrightarrow{d^n} & X^n & \xrightarrow{d^{n+1}} & \dots \\
 & & \downarrow{\scriptstyle \varphi_{n-1}} & & \downarrow{\scriptstyle \varphi_n} & & \\
\dots & \xrightarrow{\delta^{n-1}} & Y^{n-1} & \xrightarrow{\delta^n} & Y^n & \xrightarrow{\delta^{n+1}} & \dots
\end{array}$$

Proposition 3.1.7. *Let $\varphi : X^\bullet \to Y^\bullet$ be a homomorphism of cochain complex. Then it induces an R-module homomorphism $\alpha^* : H^n(X) \to H^n(Y)$, one for each n, given by $\overline{x} \mapsto \overline{\varphi(x)}$. The statement holds similarly for chain complexes.*

Proof. Suppose as stated in the statement. The argument splits into two parts: showing that the claimed map is well-defined, and showing that it is indeed an R-module homomorphism. Note by definition of complexes homomorphism have the following commutative diagram:

$$\begin{array}{ccccccccc}
\dots & \longrightarrow & X^n & \xrightarrow{d^{n+1}} & X^{n+1} & \longrightarrow & \dots \\
 & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n+1}} & & \\
\dots & \longrightarrow & Y^n & \xrightarrow{\delta^{n+1}} & Y^{n+1} & \longrightarrow & \dots
\end{array}$$

Let $x \in \ker d_{n+1}$. Since the diagram is commutative, we must have

$$\delta_{n+1}(\varphi_n(x)) = \varphi_{n+1}(d_{n+1}(x)) = \varphi_{n+1}(0) = 0$$

So $\varphi_n(x) \in \ker \delta_{n+1}$. Thus an element $\overline{x} \in H^n(X)$ means that $x \in \ker d_n$, implying that $\varphi_n(x) \in \ker \delta_{n+1}$, and thus $\overline{\varphi_n(x)} \in H^{n+1}(X)$. So the claimed map is valid.

To show that the map is well-defined, consider elements $\overline{x}$ and $\overline{x'}$ from $H^n(X)$. This implies that $x, x' \in \ker d_n$. Consequently $x - x' \in \ker d_{n+1} \subseteq \operatorname{im} d_n$ by the definition of complexes, so let $x'' \in X^{n-1}$ such that $d_n(x'') = x - x'$. Observe that

$$\varphi_n(x) - \varphi_n(x') = \varphi_n(x - x') = \varphi_n(d_n(x'')) = \delta_n(\varphi_{n-1}(x''))$$

Thus $\varphi(x) - \varphi(x') \in \operatorname{im} \delta_n$, i.e. $\overline{(\varphi(x))} = \overline{(\varphi(x'))}$.

Lastly, to show that the map α^* is R-module homomorphism:

$$\begin{aligned}
\alpha^n(\overline{x} + \overline{x'}) &= \alpha^n(\overline{x + x'}) \\
&= \overline{\varphi(x + x')} \\
&= \overline{\varphi(x) + \varphi(x')} \\
&= \overline{\varphi(x)} + \overline{\varphi(x')} \\
&= \alpha^n(\overline{x}) + \alpha^n(\overline{x'})
\end{aligned}$$

and

$$\alpha^n(r\overline{x}) = \alpha^n(\overline{rx}) = \overline{\varphi(rx)} = \overline{r\varphi(x)} = r\ \overline{\varphi(x)}$$

This completes the proof. □

Theorem 3.1.8 (Long Exact Sequence in Cohomology)**.** *Let $(X^\bullet, d_X^\bullet), (Y^\bullet, d_Y^\bullet), (Z^\bullet, d_Z^\bullet)$ be cochain complexes. Let $0 \to X^\bullet \xrightarrow{\alpha} Y^\bullet \xrightarrow{\beta} Z^\bullet \to 0$ be a SES of cochain complex bounded below by 0 (i.e. $X^{-n} = 0$ for all $n > 0$), that is, to say that for every n we have*

$$0 \to X^n \xrightarrow{\alpha_n} Y^n \xrightarrow{\beta_n} Z^n \to 0$$

Then, we have a long exact sequence (LES) given by

$$0 \to H^0(X) \xrightarrow{\alpha_0^*} H^0(Y) \xrightarrow{\beta_0^*} H^0(Z) \xrightarrow{\delta_0} H^1(X) \xrightarrow{\alpha_1^*} H^1(Y) \xrightarrow{\beta_1^*} H^1(Z) \xrightarrow{\delta_1} \cdots$$

where for each n

- *α_n^* sends $\overline{x}$ to $\overline{\alpha_n(x)}$*
- *β_n^* sends $\overline{y}$ to $\overline{\beta_n(y)}$*
- *$\delta_n : H^n(Z) \to H^{n+1}(X)$ where $\overline{z} \mapsto \delta_n(z)$ is defined as follow*
  1. *Let $y \in Y^n$ such that $\beta_n(y) = z$.*
  2. *Let $x \in X^{n+1}$ such that $\alpha_{n+1}(x) = d_Y^{n+1}(y)$.*
  3. *Let $\overline{x} \in H^{n+1}(X)$ be represented by x.*
  4. *We thus define $\delta_n(z)$ to be $\overline{x}$.*

Here, each δ_n is called the connecting homomorphism.

Furthermore, if any two of the complexes are exact, then the third is exact.

Proof. The well-definedness of connecting homomorphisms is left as a tutorial problem, thus is omitted here.

We first check that exactness occurs at

$$H^n(X) \xrightarrow{\alpha_n^*} H^n(Y) \xrightarrow{\beta_n^*} H^n(Z)$$

that is, we show that $\operatorname{im} \alpha_n^* = \ker \beta_n^*$. First, to show $\operatorname{im} \alpha_n^* \subseteq \ker \beta_n^*$, let $\overline{x} \in H^n(X)$. By assumption $\beta_n \circ \alpha_n$ is zero map due to exactness. Thus

$$\beta_n^*(\alpha_n^*(\overline{x})) = \beta_n^*(\overline{\alpha_n(x)}) = \overline{\beta_n(\alpha_n(x))} = \overline{0}$$

Thus $\operatorname{im}\alpha_n^* \subseteq \ker\beta_n^*$. Next, to show that $\ker\beta_n^* \subseteq \operatorname{im}\alpha_n^*$, let $\overline{y} \in H^n(Y)$ such that $\beta_n^*(\overline{y}) = \overline{\beta_n(y)} = \overline{0} \in H^n(Z)$, thus $\beta_n(y) \in \operatorname{im} d_Z^n$, so let $z \in Z^{n-1}$ such that $d_Z^n(z) = \beta_n(y)$. Note β_{n-1} is surjective, so let $y' \in Y^{n-1}$ such that $\beta_{n-1}(y') = z$. Altogether we have

$$\beta_n(y) = d_Z^n(z) = d_Z^n(\beta_{n-1}(y')) = \beta_n(d_Y^n(y'))$$

This implies $\beta_n(y - d_Y^n(y')) = 0$, so $y - d_Y^n(y') \in \ker\beta_n = \operatorname{im}\alpha_n$. Let $x \in X^n$ such that $\alpha_n(x) = y - d_Y^n(y')$, and thus

$$d_Y^{n+1}(\alpha_n(x)) = d_Y^{n+1}(y - d_Y^n(y')) = d_Y^{n+1}(y) - d_Y^{n+1}(d_Y^n(y')) = d_Y^{n+1}(y) + 0$$

Note that by commutativity of the diagram, LHS can be written as $\alpha_{n+1}(d_X^{n+1}(x))$. Also, for RHS, recall that $\overline{y} \in H^n(Y)$, where by definition

$$H^n(Y) = \frac{\ker d_Y^{n+1}}{\operatorname{im} d_Y^n}$$

and thus $y \in \ker d_Y^{n+1}$, which implies that $d_Y^{n+1}(y) = 0$. Altogether we have $\alpha_{n+1}(d_X^{n+1}(x)) = 0$. By assumption on exactness we see α_{n+1} is exact, so $d_X^{n+1}(x) = 0$, i.e. $x \in \ker d_X^{n+1}$. Again, by definition of cohomology, we see that $\overline{x} \in H^n(X)$. We claim that $\overline{x}$ is the pre-image of $\overline{y}$ under α_n^*:

$$\alpha_n^*(\overline{x}) = \overline{\alpha_n(x)} = \overline{y - d_Y^n(y')} \in H^n(Y) = \frac{\ker d_Y^{n+1}}{\operatorname{im} d_Y^n}$$

By definition of cohomology $H^n(Y)$ we see that $\overline{y - d_Y^n(y')} = \overline{y}$ since the image of d_Y^n is quotiented away in $H^n(Y)$. This shows that $\alpha_n^*(\overline{x}) = \overline{y}$, thus $y \in \operatorname{im}\alpha_n^*$.

We now check exactness occurs at

$$H^n(Y) \xrightarrow{\beta_n^*} H^n(Z) \xrightarrow{\delta_n} H^{n+1}(X)$$

First, to show $\operatorname{im}\beta_n^* \subseteq \ker\delta_n$, let $\overline{y} \in H^n(Y)$. By definition $\beta_n^*(\overline{y}) = \overline{\beta_n(y)}$. For convenience let $z = \beta(y)$, so $\beta_n^*(\overline{y}) = \overline{z}$, and we want to show $\delta_n(\overline{z}) = 0$. By definition of δ_n, if $\alpha_n(x) = d_Y^n(y)$, then $\delta_n(\overline{(z)}) = \overline{x}$. Note that by our assumption $\overline{y} \in H^n(Y)$ implies that $y \in \ker d_Y^n$, so $\alpha_n(x) = d_Y^n(y) = 0$. But provided the SES, we note $\ker\alpha_n = 0$, so α_n is injective, and thus $x = 0$. This implies that

$$\delta_n(\beta_n^*(\overline{y})) = \delta_n(\overline{\beta(y)}) = \delta_n(\overline{z}) = \overline{x} = \overline{0}$$

Thus $\operatorname{im}\beta_n^* \subseteq \ker\delta_n$. Next to show that $\ker\delta_n \subseteq \operatorname{im}\beta_n^*$, let $\overline{z} \in H^n(Z)$ such that $\delta_n(\overline{z}) = \overline{x} = 0 \in H^{n+1}(X)$, i.e. $x \in \operatorname{im} d_X^{n+1}$, where by definition of the connecting homomorphisms we have some y such that $\beta_n(y) = z$ and $\alpha_{n+1}(x) = d_Y^{n+1}(y)$. Let $x = d_X^{n+1}(x')$. Then

$$d_Y^{n+1}(y) = \alpha_{n+1}(x) = \alpha_{n+1}(d_X^{n+1}(x')) \overset{(*)}{=} d_Y^n((\alpha_n)(x'))$$

where $(*)$ is due to the commutativity of the diagram. Together, the above implies that $y - \alpha_n(x') \in \ker d_Y^{n+1}$, and we claim that this is the pre-image of $\overline{z}$ under β_n^*:

$$\beta_n^*(\overline{y - \alpha_n(x')}) = \overline{\beta_n(y - \alpha_n(x'))} = \overline{\beta_n(y)} - \overline{\beta_n(\alpha_n(x'))} = \overline{z} - 0 = \overline{z}$$

where note $\beta_n \circ \alpha_n$ is the zero map due to exactness in the assumption.

For the second statement, recall that exactness of a complex is equivalent to the trivialness of cohomology. From the first statement we obtained the LES:

$$0 \to H^0(X) \xrightarrow{\alpha_0^*} H^0(Y) \xrightarrow{\beta_0^*} H^0(Z) \xrightarrow{\delta_0} H^1(X) \xrightarrow{\alpha_1^*} H^1(Y) \xrightarrow{\beta_1^*} H^1(Z) \xrightarrow{\delta_1} \cdots$$

Case 1: if $X^\bullet$ and $Y^\bullet$ are trivial, we have

$$0 \to 0 \xrightarrow{\alpha_0^*} 0 \xrightarrow{\beta_0^*} H^0(Z) \xrightarrow{\delta_0} 0 \xrightarrow{\alpha_1^*} 0 \xrightarrow{\beta_1^*} H^1(Z) \xrightarrow{\delta_1} \cdots$$

This forces α_n^*, β_n^*, and δ_n to be zero maps. Specifically, note that $\ker\delta_n = H^n(Z)$. Due to exactness, we see that $0 = \operatorname{im}\beta_n^* = \ker\delta_n = H^n(Z)$, and thus $Z^\bullet$ must be exact.

Case 2: If $Y^\bullet$ and $Z^\bullet$ are trivial, we have

$$0 \to H^0(X) \xrightarrow{\alpha_0^*} 0 \xrightarrow{\beta_0^*} 0 \xrightarrow{\delta_0} H^1(X) \xrightarrow{\alpha_1^*} 0 \xrightarrow{\beta_1^*} 0 \xrightarrow{\delta_1} \cdots$$

This forces α_n^*, β_n^*, and δ_n to be zero maps. Specifically, note that $\ker \alpha_n^* = H^n(X)$. Due to exactness, we see that $0 = \operatorname{im} \delta_n^* = \ker \delta_{n+1} = H^{n+1}(X)$. Similarly $H^0(X)$ it is also 0. This shows that $X^\bullet$ must be exact.

Case 3: If $X^\bullet$ and $Z^\bullet$ are trivial, we have

$$0 \to 0 \xrightarrow{\alpha_0^*} H^0(Y) \xrightarrow{\beta_0^*} 0 \xrightarrow{\delta_0} 0 \xrightarrow{\alpha_1^*} H^1(Y) \xrightarrow{\beta_1^*} 0 \xrightarrow{\delta_1} \cdots$$

This forces α_n^*, β_n^*, and δ_n to be zero maps. Specifically, note that $\ker \beta_n^* = H^n(Y)$. Due to exactness, we see that $0 = \operatorname{im} \alpha_n^* = \ker \beta_n^* = H^n(Y)$. This shows that $Y^\bullet$ must be exact.

The proof is thus completed. □

3.2 Ext Group

Definition 3.2.1 (Projective resolution)**.** Let V be an R-module. A projective resolution of V is an exact complex

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} V \to 0 \to 0 \to \dots$$

such that each P_i is projective R-module. In shorthand notation we write $P_\bullet \twoheadrightarrow V$ to denote a free resolution of V.

Remark 3.2.2. Similarly we can define a free resolution, where we replace projective by free.

Proposition 3.2.3. *Every R-module has a projective resolution.*

Proof. Let V be an R-module. By previous result there exists projective R-module P_0 such that $P_0 \overset{\varepsilon}{\twoheadrightarrow} V$. Consider $\ker \varepsilon$, and there exists a projective R-module P_1 such that P_1 surjects to $\ker \varepsilon$ via d_1. Suppose we have, inductively, that

$$P_n \xrightarrow{d_n} \dots \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} V$$

Let ε be d_0, and by our construction we observe that P_n surjects to $\ker d_{n-1}$ via d_n, i.e.

$$P_n \twoheadrightarrow \ker d_{n-1}$$

and thus this shows that $\operatorname{im} d_n = \ker d_{n-1}$. This completes the proof. □

A similar statement on free resolution can be proven:

Proposition 3.2.4. *Every R-module has a free resolution.*

Remark 3.2.5. If V is a projective R-module, then we have a projective resolution

$$\cdots \to 0 \to V \xrightarrow{\mathrm{id}} V \to 0 \to 0 \dots$$

Also, projective resolution is not unique, where the following

$$0 \to V \xrightarrow{\alpha} V \oplus V \xrightarrow{\beta} V \to 0 \to \dots$$

where $\alpha : v \mapsto (v, 0$ and $\beta : (v, w) \mapsto w$, is also a projective module of V

Definition 3.2.6 (Ext group)**.** Let $P_\bullet \twoheadrightarrow V$ be a projective resolution of V and W be an R-module. We get a complex (of abelian group)

$$\mathcal{C} := 0 \to \operatorname{Hom}_R(P_0, W) \xrightarrow{d_1^*} \operatorname{Hom}_(P_1, W) \xrightarrow{d_2^*} \operatorname{Hom}_R(P_2, W) \xrightarrow{d_3^*} \dots$$

where V is forgetted. It is indeed a complex since

$$d_{n+1}^* \circ d_n^* = (d_n \circ d_{n+1})^* = 0$$

Note that this complex is usually not exact.

The n-th cohomology group derived from the left exact contravariant functor $\operatorname{Hom}_R(-, W)$ is

$$\operatorname{Ext}_R^n(V, W) := H^n(\mathcal{C}) = \frac{\ker d_{n+1}^*}{\operatorname{im} d_n^*}$$

Clearly $\operatorname{Ext}_R^0(V, W) = \ker d_1^*$.

Proposition 3.2.7. *Let V and W be R-modules. Then*

$$\mathrm{Ext}^0_R(V,W) \cong \mathrm{Hom}_R(V,W)$$

Proof. We extract the following exact sequence from the projective resolution $P_\bullet \twoheadrightarrow V$:

$$P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} V \to 0$$

Recall that $\mathrm{Hom}_R(-,W)$ is a left contravariant functor, so we have the exact sequence

$$0 \xrightarrow{0} \mathrm{Hom}_R(V,W) \xrightarrow{\varepsilon^*} \mathrm{Hom}_R(P_0,W) \xrightarrow{d_1^*} \mathrm{Hom}_R(P_1,W)$$

By 1st isomorphism theorem on ε^* we get

$$\frac{\mathrm{Hom}_R(V,W)}{\ker \varepsilon^*} \cong \mathrm{im}\, \varepsilon^* = \ker d_1^*$$

Note that $\ker \varepsilon^* = \mathrm{im}\, 0 = 0$ due to exactness. On the other hand, by exactness we have $\mathrm{im}\, \varepsilon^* = \ker d_1^*$. By definition of Ext we have that $\mathrm{Ext}^0_R(V,W) = \ker d_1^*$. Altogether, we see

$$\mathrm{Hom}_R(V,W) \cong \mathrm{Ext}^0_R(V,W)$$

This completes the proof. □

Example 3.2.8.

1. We compute $\mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$ for any abelian group D, where $m \geq 2$. From previous proposition we know

   $$\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$$

   Let $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$. By definition

   $$m(\varphi(\overline{1})) = \varphi(\overline{m}) = 0$$

   Thus we know

   $$\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \{d \in D : m \cdot d = 0\}$$

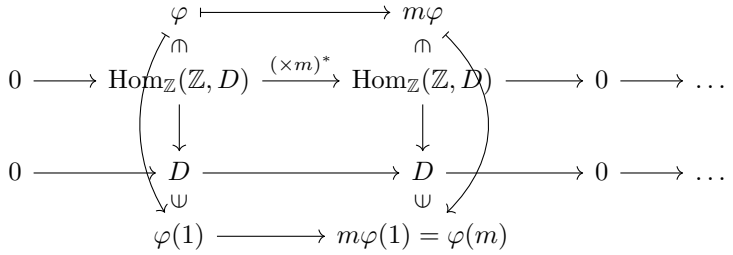
   where we will denote it as ${}_mD$. To investigate the general case, we have to come up with the projective resolution:

   $$\cdots \to 0 \to \mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \xrightarrow{\mathrm{mod}\ m} \mathbb{Z}/m\mathbb{Z} \to 0$$

   This is indeed a free resolution of $\mathbb{Z}/m\mathbb{Z}$ (one can verify the exactness easily). Thus taking hom we get

   $$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \xrightarrow{(\times m)^*} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \to 0 \to \dots$$

   And it is clear that $\mathrm{Ext}^2_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) = 0$ for all $n \geq 2$. We compute the Ext^1 as follow: note $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \cong D$ with isomorphism given by $\varphi \mapsto \varphi(1)$. Thus:

   and $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong D/mD$.

2. If $\mathbb{Z}/m\mathbb{Z}$ is a $(\mathbb{Z}/d\mathbb{Z})$-module for some d, then $d \cdot \overline{1} = \overline{0}$, implying that $\overline{d} = \overline{0}$, so $m \mid d$. We now compute $\mathrm{Ext}_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$ where D is a $\mathbb{Z}/d\mathbb{Z}$-module. To come up with a free resolution of $\mathbb{Z}/m\mathbb{Z}$, note we must start from

   $$\dots \xrightarrow{\mathbb{Z}} /d\mathbb{Z} \xrightarrow{\beta} \mathbb{Z}/d\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}/d\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/m\mathbb{Z} \to 0$$

where π is the canonical surjection. We have to determine what is α and β. Note we must have $\operatorname{im}\alpha = \ker\pi$. This says that α is the operation $\times m$. Similarly, one can derive that β is the operation $\times\frac{d}{m}$. Thus we obtain the free resolution of $\mathbb{Z}/m\mathbb{Z}$:

$$\ldots \xrightarrow{\times\frac{d}{m}} \mathbb{Z}/d\mathbb{Z} \xrightarrow{\times m} \mathbb{Z}/d\mathbb{Z} \xrightarrow{\mathbb{Z}} /d\mathbb{Z} \xrightarrow{\times\frac{d}{m}} \mathbb{Z}/d\mathbb{Z} \xrightarrow{\times m} \mathbb{Z}/d\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/m\mathbb{Z} \to 0$$

Next, perform similar action as in the first example: to compute the Ext group, take hom and remove the first entry we have

$$0 \to \operatorname{Hom}_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, D) \xrightarrow{(\times m)^*} \operatorname{Hom}_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, D) \xrightarrow{(\times\frac{d}{m})^*} \operatorname{Hom}_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, D) \xrightarrow{(\times m)^*} \ldots$$

We have verified previously that the 0-th Ext group is isomorphic to $\operatorname{Hom}_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$. Let $\varphi \in \operatorname{Hom}_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$. It suffices to see $d := \varphi(\overline{1})$. Note $\overline{0} = \varphi(\overline{m}) = m\varphi(\overline{1}) = md$. This says that

$$\operatorname{Ext}^0_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \{d \in D : m \cdot d = 0\}$$

Next, since the maps of the complex alternates, all odd-order Ext groups are the same, simialrly for even-order. Direct computation says that if n is odd

$$\operatorname{Ext}^n_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \frac{\left\{x \in D : \frac{d}{m} \cdot x = 0\right\}}{\{mx : x \in D\}}$$

and if n is even

$$\operatorname{Ext}^n_{\mathbb{Z}/d\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \frac{\{x \in D : m \cdot x = 0\}}{\left\{\frac{d}{m} \cdot x : x \in D\right\}}$$

Remark 3.2.9. The above example is not rigorous enough, in the sense that, we cannot assume that we still get the same result if starting from another projective resolution. In fact, we have that the result obtained is independent of the projective resolution.

Proposition 3.2.10 (Comparison Theorem)**.** *Let $f : V \to V'$ be an R-module homomorphism and $P_\bullet \twoheadrightarrow V$ be a projective resolution of V and $P'_\bullet \twoheadrightarrow V'$ be an exact complex, where it need not to be a projective resolution of V'. Then there exists $f_n : P_n \to P'_n$ such that the following commute:*

$$\begin{array}{ccccccccccccc}
\ldots & \longrightarrow & P_3 & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{d_0} & V & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} & & \downarrow \\
\ldots & \longrightarrow & P'_3 & \xrightarrow[\delta_3]{} & P'_2 & \xrightarrow[\delta_2]{} & P'_1 & \xrightarrow[\delta_1]{} & P'_0 & \xrightarrow[\delta_0]{} & V' & \longrightarrow & 0
\end{array}$$

Futhermore, given two such maps $f_n : P_n \to P'_n$ and $g_n : P_n \to P'_n$, there exists $s_n : P_n \to P'_{n+1}$ such that $f_n - g_n = \delta_{n+1}s_n + s_{n-1}d_n$.

Proof. The idea of the proof is to get the required map from the definition of projective module, and we will be performing induction on the length of the projective resolution.

First, for the base case, suppose that we have

$$\begin{array}{ccccc}
P_0 & \xrightarrow{d_0} & V & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \\
P'_0 & \xrightarrow{\delta_0} & V' & \longrightarrow & 0
\end{array}$$

Note δ_0 is surjective. Also P_0 get maps to V' via $f \circ d_0$. We thus have the following commutative diagram:

$$\begin{array}{ccc}
 & & P_0 \\
 & \overset{\exists f_0}{\swarrow} & \downarrow{\scriptstyle f\circ d_0} \\
P'_0 & \xrightarrow[\delta_0]{} & \operatorname{im}\delta_0 = V'
\end{array}$$

where the existence of f_0 is ensured by the definition of projective module. This proves the base case.

Next, suppose we have constructed $f_{n-1} : P_{n-1} \to P'_{n-1}$. The following is a part of the commutative diagram:

$$\begin{array}{ccccc} P_n & \xrightarrow{d_n} & P_{n-1} & \xrightarrow{d_{n-1}} & P_{n-2} \\ & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_{n-2}} \\ P'_n & \xrightarrow{\delta_n} & P_{n-1} & \xrightarrow{\delta_{n-1}} & P'_{n-2} \end{array}$$

Similarly, consider $f_{n-1} \circ d_n$ that maps P_n to $\operatorname{im} \delta_n$. Note we have to check for the condition on applying the lift of the map in the definition of projective modules, which is true, since

$$\delta_{n-1} \circ (f_{n-1} \circ d_n) = (\delta_{n-1} \circ f_{n-1}) \circ d_n = f_{n-2} \circ d_{n-1} \circ d_n = 0$$

Thus we have

$$\begin{array}{ccc} & & P_n \\ & \overset{\exists f_n}{\swarrow} & \downarrow{\scriptstyle f_{n-1} \circ d_n} \\ P'_{n-1} & \xrightarrow{\delta_n} & \operatorname{im} \delta_n = \ker \delta_{n-1} \end{array}$$

where existence of f_n is ensured by the definition of projectivce modules. This proves the first part of the statement.

For the second part of the statement, we use the similar trick to compute the desired maps $s_\bullet$. First define $s_{-2} : 0 \to V'$ where $s_{-2} = 0$ and $s_{-1} : V \to P'_0$ where $s_{-1} = 0$. It is clear that the required condition is satisfied, simply check that $f - f = 0 \cdot 0 + \delta_0 \cdot 0 = 0$.

Next, for the construction of s_0, consider the map $f_0 - g_0 - s_{-1} d_0$ that maps P_0 to $\operatorname{im} \delta_1$. We first check that

$$\delta_0 \circ (f_0 - g_0 - s_{-1} \circ d_0) = f \circ d_0 - f \circ d_0 = 0$$

Thus we have the following commutative diagram

$$\begin{array}{ccc} & & P_0 \\ & \overset{\exists s_0}{\swarrow} & \downarrow{\scriptstyle f_0 - g_0 - s_{-1} d_0} \\ P'_1 & \xrightarrow{\delta_1} & \operatorname{im} \delta_1 = \ker \delta_0 \end{array}$$

where existence of s_0 is ensured by the definition of projective module. We see that the required condition $f_0 - g_0 = s_{-1} d_0 + \delta_1 s_0$ holds since the commutativity of the diagram says that $f_0 - g_0 - s_{-1} \circ d_0 = \delta_1 s_0$. For the inductive steps, suppose we have constructed $s_{n-1} : P_{n-1} \to P'_n$. We consider $f_n - g_n - s_{n-1} d_n$ †hat maps P_n to $\operatorname{im} \delta_{n+1}$. We check that

$$\begin{aligned} \delta_n (f_n - g_n - s_{n-1} d_n) &= f_{n-1} d_n - g_{n-1} d_n - \delta_n s_{n-1} d_n \\ &= (f_{n-1} - g_{n-1} - \delta_n s_{n-1}) d_n \\ &= (s_{n-1} d_{n-1}) d_n \\ &= 0 \end{aligned}$$

Thus, by the definition of projective modules we have the followng commutative diagram:

$$\begin{array}{ccc} & & P_n \\ & \overset{\exists s_n}{\swarrow} & \downarrow{\scriptstyle f_n - g_n - s_{n-1} d_n} \\ P'_{n+1} & \xrightarrow{\delta_{n+1}} & \operatorname{im} \delta_{n+1} = \ker \delta_n \end{array}$$

where the existence of s_n is ensured by the definition on projective module in lifting of maps. This concludes the proof. □

Definition 3.2.11 (Homotopic and homotopy equivalence)**.**

1. Let $f, g : X^\bullet \to Y^\bullet$ be morphisms of complexes. We say that f and g are homotopic, denoted by $f \simeq g$, if there exists $s_\bullet$ be a collection of map where $s_n : X^n \to Y^{n+1}$ such that $f - g = ds + sd$.

2. The complexes $X^\bullet$ and $Y^\bullet$ are homotopy equivalent if there exists $f : X^\bullet \to Y^\bullet$ and $f' : Y^\bullet \to X^\bullet$ such that $f \circ f' \simeq \mathrm{id}_{Y^\bullet}$ and $f' \circ f \simeq \mathrm{id}_{X^\bullet}$.

Proposition 3.2.12.

1. *Suppose that $f, g : X^\bullet \to Y^\bullet$ are homotopic. We have*
$$f^* = g^* : H^n(X^\bullet) \to H^n(Y^\bullet)$$
2. *If $X^\bullet$ and $Y^\bullet$ are homotopy equivalent, then $H^n(X^\bullet) \cong H^n(Y^\bullet)$.*

Proof. The map $f : X^\bullet \to Y^\bullet$ induces $f^* : H^n(X^\bullet) \to H^n(Y^\bullet)$ where $[x] \mapsto [f(x)]$. This is similar for g. Since f and g are homotopic, there exists some map $s_n : X^n \to Y^{n+1}$ such that $f - g = ds + sd$. Observe that

$$\begin{aligned} f^*([x]) &= [f(x)] \\ &= [g(x) + ds(x) + sd(x)] \\ &= [g(x)] + [ds(x)] \\ &= [g(x)] + 0 \\ &= g^*([x]) \end{aligned}$$

This proves the first statement.

For the second statement, if $X^\bullet$ and $Y^\bullet$ are homotopy equivalent, it means having $f : X^\bullet \to Y^\bullet$ and $f' : Y^\bullet \to X^\bullet$ such that $f \circ f' \simeq \mathrm{id}_{Y^\bullet}$ and $f' \circ f \simeq \mathrm{id}_{X^\bullet}$. These maps induces $f^* : H^n(X^\bullet) \to H^n(Y^\bullet)$ and $f'^* : H^n(Y^\bullet) \to H^n(X^\bullet)$. Note

$$(f'^* \circ f^*)([x]) = (f' \circ f)^*([x]) = (\mathrm{id}_{X^\bullet})^*([x]) = [x]$$

Thus $f'^* \circ f^* = \mathrm{id}_{H^n(X^\bullet)}$. Similarly one can show that $f^* \circ f'^* = \mathrm{id}_{H^n(Y^\bullet)}$. This shows that f^* is an isomorphism, and so $H^n(X^\bullet)$ and $H^n(Y^\bullet)$ are isomorphic. □

Theorem 3.2.13. *The n-th cohomology group $\mathrm{Ext}^n_R(V, W)$ is independent, up to isomorphism, of the choice of the projective resolution of V.*

Proof. Let $P_\bullet \twoheadrightarrow V$ and $P'_\bullet \twoheadrightarrow V$ be two projective resolution of V. We thus have the following commutative diagram by Comporison Theorem:

$$\begin{array}{ccccccccccccc} \dots & \longrightarrow & P_2 & \xrightarrow{d} & P_1 & \xrightarrow{d} & P_0 & \xrightarrow{d} & V & \longrightarrow & 0 & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \updownarrow & & & & \\ \dots & \longrightarrow & P'_2 & \xrightarrow{d} & P'_1 & \xrightarrow{d} & P'_0 & \xrightarrow{d} & V & \longrightarrow & 0 & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_0} & & \updownarrow & & & & \\ \dots & \longrightarrow & P_2 & \xrightarrow{d} & P_1 & \xrightarrow{d} & P_0 & \xrightarrow{d} & V & \longrightarrow & 0 & \longrightarrow & \dots \end{array}$$

First, by removing V and taking $\mathrm{Hom}_R(-, W)$ we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_R(P_0, W) & \xrightarrow{d^*} & \mathrm{Hom}_R(P_1, W) & \xrightarrow{d^*} & \mathrm{Hom}_R(P_2, W) & \longrightarrow & \dots \\ & & \uparrow{\scriptstyle f_0^*} & & \uparrow{\scriptstyle f_1^*} & & \uparrow{\scriptstyle f_2^*} & & \\ 0 & \longrightarrow & \mathrm{Hom}_R(P'_0, W) & \xrightarrow{d^*} & \mathrm{Hom}_R(P'_1, W) & \xrightarrow{d^*} & \mathrm{Hom}_R(P'_2, W) & \longrightarrow & \dots \\ & & \uparrow{\scriptstyle g_0^*} & & \uparrow{\scriptstyle g_1^*} & & \uparrow{\scriptstyle g_2^*} & & \\ 0 & \longrightarrow & \mathrm{Hom}_R(P_0, W) & \xrightarrow{d^*} & \mathrm{Hom}_R(P_1, W) & \xrightarrow{d^*} & \mathrm{Hom}_R(P_2, W) & \longrightarrow & \dots \end{array}$$

On the other hand, note that $g_n \circ f_n$ is a map from P_n to itself. We can construct the following commutative diagram:

$$\begin{array}{ccccccccccc} \dots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{d_0} & V & \longrightarrow & 0 \\ & & {\scriptstyle 1}\downarrow\downarrow{\scriptstyle g_2 f_2} & & {\scriptstyle 1}\downarrow\downarrow{\scriptstyle g_1 f_1} & & {\scriptstyle 1}\downarrow\downarrow{\scriptstyle g_0 f_0} & & \updownarrow & & \\ \dots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{d_0} & V & \longrightarrow & 0 \end{array}$$

By the second part of the Comparison Theorem, there exists $s_n : P_n \to P_{n+1}$ such that $gf - 1 = ds + sd$.

Back to the diagram with hom, see that

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_R(P_0, W) & \xrightarrow{d_1^*} & \mathrm{Hom}_R(P_1, W) & \xrightarrow{d_2^*} & \mathrm{Hom}_R(P_2, W) & \xrightarrow{d_3^*} & \dots \\
 & & \uparrow{\scriptstyle 1^*} & \nwarrow{\scriptstyle (g_0 f_0)^*} & \uparrow{\scriptstyle 1^*} & \nwarrow{\scriptstyle (g_1 f_1)^*} & \uparrow{\scriptstyle 1^*} & & \\
0 & \longrightarrow & \mathrm{Hom}_R(P_0, W) & \xrightarrow{d_1^*} & \mathrm{Hom}_R(P_1, W) & \xrightarrow{d_2^*} & \mathrm{Hom}_R(P_2, W) & \xrightarrow{d_3^*} & \dots
\end{array}$$

where note $(g_n f_n)^* = f_n^* g_n^*$. Note that the relation $gf - 1 = ds + sd$ implies that $f^* g^* - 1^* = s^* d^* + d^* s^*$. By definition this is saying that $f^* \circ g^* \simeq \mathrm{id}_X$. Similarly, one can repeat all the arguments above to conclude that $g^* \circ f^* \simeq \mathrm{id}_Y$. Therefore the two complexes involving hom induces from $P_\bullet \twoheadrightarrow V$ and $P'_\bullet \twoheadrightarrow V$ are homotopy equivalent. Previous proposition says that the cohomologies computed from these two complexes are isomorphic, and thus the Ext group are independent of the choice of the starting projective resolution. □

Theorem 3.2.14 (Snake Lemma)**.** *Suppose we have a commutative diagram below with exact rows:*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X & \xrightarrow{\alpha} & Y & \xrightarrow{\beta} & Z & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & X' & \xrightarrow{\alpha'} & Y' & \xrightarrow{\beta'} & Z' & \longrightarrow & 0
\end{array}$$

We then have an exact sequence

$$0 \to \ker f \xrightarrow{\alpha} \ker g \xrightarrow{\beta} \ker h \xrightarrow{\delta} \mathrm{coker}\, f \xrightarrow{\alpha'} \mathrm{coker}\, g \xrightarrow{\beta'} \mathrm{coker}\, h \to 0$$

where cokernel of a map $\phi : A \to B$ is defined as the quotient $\mathrm{coker}\, \phi = B / \mathrm{im}\, \phi$.

Proof. Left as tutorial exercise. □

Theorem 3.2.15 (Horseshoe Lemma)**.** *Let $0 \to X \to Y \to Z \to 0$ be a SES of R-modules and $P_\bullet \twoheadrightarrow X$, $Q_\bullet \twoheadrightarrow Z$ be projective resolutions of X, Z respectively. Then we have an exact commutative diagram:*

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{d_0} & X & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & P_2 \oplus Q_2 & \longrightarrow & P_1 \oplus Q_1 & \longrightarrow & P_0 \oplus Q_0 & \longrightarrow & Y & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_0} & & \downarrow & & \\
\dots & \longrightarrow & Q_2 & \xrightarrow[\delta_2]{} & Q_1 & \xrightarrow[\delta_1]{} & Q_0 & \xrightarrow[\delta_0]{} & Z & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & 0 & &
\end{array}$$

In particular, we denote the second non-zero row as $P_\bullet \oplus Q_\bullet$, and it is a projective resolution of Y.

Proof. Left as tutorial exercise. □

Theorem 3.2.16. *Let $0 \to X \to Y \to Z \to 0$ be a SES of R-modules. Then we have a LES of abelian groups*

$$0 \to \mathrm{Hom}_R(Z, D) \to \mathrm{Hom}_R(Y, D) \to \mathrm{Hom}_R(X, D)$$
$$\to \mathrm{Ext}^1_R(Z, D) \to \mathrm{Ext}^1_R(Y, D) \to \mathrm{Ext}^1_R(X, D) \to \mathrm{Ext}^2_R(Z, D) \to \dots$$

Proof. Take projective resolution $P_\bullet \twoheadrightarrow X$ and $Q_\bullet \twoheadrightarrow Z$. By Horseshoe Lemma, we get the diagram

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{d_0} & X & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & P_2 \oplus Q_2 & \longrightarrow & P_1 \oplus Q_1 & \longrightarrow & P_0 \oplus Q_0 & \longrightarrow & Y & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_0} & & \downarrow & & \\
\dots & \longrightarrow & Q_2 & \xrightarrow[\delta_2]{} & Q_1 & \xrightarrow[\delta_1]{} & Q_0 & \xrightarrow[\delta_0]{} & Z & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & 0 & &
\end{array}$$

Taking $\mathrm{Hom}_R(-, D)$ we get

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathrm{Hom}_R(P_0, D) & \xrightarrow{d_1^*} & \mathrm{Hom}_R(P_1, D) & \xrightarrow{d_2^*} & \mathrm{Hom}_R(P_2, D) & \longrightarrow & \dots \\
 & & \uparrow{\scriptstyle \iota_0^*} & & \uparrow{\scriptstyle \iota_0^*} & & \uparrow{\scriptstyle \iota_0^*} & & \\
0 & \longrightarrow & \mathrm{Hom}_R(P_0 \oplus Q_0, D) & \xrightarrow{\gamma_1^*} & \mathrm{Hom}_R(P_1 \oplus Q_1, D) & \xrightarrow{\gamma_2^*} & \mathrm{Hom}_R(P_2 \oplus Q_2, D) & \longrightarrow & \dots \\
 & & \uparrow{\scriptstyle \pi_0^*} & & \uparrow{\scriptstyle \pi_0^*} & & \uparrow{\scriptstyle \pi_0^*} & & \\
0 & \longrightarrow & \mathrm{Hom}_R(Q_0, D) & \xrightarrow{\delta_1^*} & \mathrm{Hom}_R(Q_1, D) & \xrightarrow{\delta_2^*} & \mathrm{Hom}_R(Q_2, D) & \longrightarrow & \dots \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where we shall refer to the second, third, and fourth row of complexes, which are non-zero, as $C^\bullet, B^\bullet$, and $A^\bullet$ respectively. Note $\mathrm{Hom}_R(P \oplus Q, D) \cong \mathrm{Hom}_R(P, D) \oplus \mathrm{Hom}_R(Q, D)$ via the following pairs of maps:

$$\begin{array}{rccc}
 & \alpha\pi_P \oplus \beta\pi_Q & \xleftarrow{\quad g \quad} & (\alpha,\ \beta) \\
 & \cap & & \cap \\
f: & \mathrm{Hom}_R(P \oplus Q, D) & \rightleftarrows & \mathrm{Hom}_R(P, D) \oplus \mathrm{Hom}_R(Q, D) \qquad : g \\
 & \cup & & \cup \\
 & \varphi & \xmapsto{\quad f \quad} & (\varphi \circ \iota_P,\ \varphi \circ \iota_Q)
\end{array}$$

It is easy to verify that they are indeed isomorphism pairs, and is omitted here. This says that $\mathrm{Hom}_R(P \oplus Q, D)$ splits, and thus we get a SES of complexes

$$0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$$

Lastly, by theorem regarding LES on cohomology, we have

$$0 \to H^0(A^\bullet) \to H^0(B^\bullet) \to H^0(C^\bullet) \to H^1(A^\bullet) \to H^1(B^\bullet) \to H^1(C^\bullet) \to \dots$$

where they the respective Ext groups of X, Y, and Z with D. Additionally, the 0-th Ext group is simply the hom set. Thus reexpressing the above LES we obtain

$$0 \to \mathrm{Hom}_R(Z, D) \to \mathrm{Hom}_R(Y, D) \to \mathrm{Hom}_R(X, D)$$

$$\to \mathrm{Ext}^1_R(Z, D) \to \mathrm{Ext}^1_R(Y, D) \to \mathrm{Ext}^1_R(X, D) \to \mathrm{Ext}^2_R(Z, D) \to \dots$$

which completes the proof. □

Remark 3.2.17. Note that since $\mathrm{Hom}_R(X, D) \cong \mathrm{Ext}^0_R(X, D)$, thus the whole LES above is a LES of ext groups.

Theorem 3.2.18. *Let Q be a R-module. TFAE:*

1. *Q is injective.*

2. *$\mathrm{Ext}^1_R(A, Q) = 0$ for all R-module A*

3. *$\mathrm{Ext}^n_R(A, Q) = 0$ for all R-module A and $n \in \mathbb{Z}^+$.*

Proof.

[3. $\implies$ 2.] Trivial.

[2. $\implies$ 1.] Suppose given SES $0 \to X \to Y \to Z \to 0$, we have LES on the Ext group

$$0 \to \mathrm{Hom}_R(Z, Q) \to \mathrm{Hom}_R(Y, Q) \to \mathrm{Hom}_R(X, Q) \to \mathrm{Ext}^1_R(Z, D) = 0 \to \dots$$

This reduces into a SES

$$0 \to \mathrm{Hom}_R(Z, Q) \to \mathrm{Hom}_R(Y, Q) \to \mathrm{Hom}_R(X, Q) \to 0$$

So Q is injective.

[1. $\implies$ 3.] Let $P_\bullet \twoheadrightarrow A$ be a projective resolution fo A and Q be an injective module. Taking $\mathrm{Hom}_R(-, Q)$ we have the following complex:

$$0 \to \mathrm{Hom}_R(A, Q) \xrightarrow{d_0^*} \mathrm{Hom}_R(P_0, Q) \xrightarrow{d_1^*} \mathrm{Hom}_R(P_1, Q) \xrightarrow{d_2^*} \mathrm{Hom}_R(P_2, Q) \xrightarrow{d_3^*} \dots$$

and we claim that it is a LES. Firstly, it is clear that $\mathrm{im}\, d_n^* \subseteq \ker d_{n+1}^*$ since $d_{n+1}^* d_n^* = (d_n d_{n+1})^* = 0$.

On the other hand, let $\phi \in \ker d_{n+1}^*$, so $\phi : P_n \to Q$ such that $\phi \circ d_{n+1} = 0$. This implies that $\mathrm{im}\, d_{n+1} \subseteq \ker \phi$. Since projective resolution is exact, thus $\ker d_n \subseteq \ker \phi \subseteq P_n$. Define $\tilde{d_n} : P_n/\ker d_n \to P_{n-1}$ by $[x] \mapsto d_n(x)$. Clearly $\tilde{d_n}$ is injective. Define also $\tilde{\phi} : P_n/\ker d_n \to Q$ by $[x] \mapsto \phi(x)$. We thus have the following commutative diagram by the definition of Q being injective:

$$\begin{array}{ccc} & & Q \\ & \overset{\tilde{\phi}}{\nearrow} & \uparrow \exists\varphi \\ P_n/\ker d_n & \xhookrightarrow[\tilde{d_n}]{} & P_{n-1} \end{array}$$

where existence of φ is ensured by the definition of injective module. Lastly, we check that $d_n^*(\varphi) = \phi$. The commutative diagram implies $\varphi \circ \tilde{d_n} = \tilde{\phi}$, so

$$(\varphi \circ \tilde{d_n})([x]) = \tilde{\phi}([x]) \implies \varphi(d_n(x)) = \phi(x) \implies (d_n^*(\varphi))(x) = \phi(x)$$

Thus $d_n^*(\varphi) = \phi$, implying that $\phi \in \mathrm{im}\, d_n^*$. Thus the complex obtained is indeed exact, and thus its cohomologies, i.e. all the Ext groups, are trivial. This completes the proof. □

Theorem 3.2.19. *Let $0 \to U \xrightarrow{\alpha} V \xrightarrow{\beta} W \to 0$ be a SES of R-modules and D be any R-module. Then we have a LES*

$$0 \to \mathrm{Hom}_R(D, U) \to \mathrm{Hom}_R(0, V) \to \mathrm{Hom}_R(D, W)$$
$$\to \mathrm{Ext}^1_R(D, U) \to \mathrm{Ext}^1_R(D, V) \to \mathrm{Ext}^1_R(D, W) \to \mathrm{Ext}^2_R(D, U) \to \dots$$

Proof. Take a projective resolution $P_\bullet \twoheadrightarrow D$ of D. Taking $\mathrm{Hom}_R(-, U), \mathrm{Hom}_R(-, V)$, and $\mathrm{Hom}_R(-, W)$ we obtain

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_R(P_0, U) & \xrightarrow{d_1^*} & \mathrm{Hom}_R(P_1, U) & \xrightarrow{d_2^*} & \mathrm{Hom}_R(P_2, U) & \xrightarrow{d_3^*} & \dots \\
 & & \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle \alpha_*} & & \\
0 & \longrightarrow & \mathrm{Hom}_R(P_0, V) & \xrightarrow{d_1^*} & \mathrm{Hom}_R(P_1, V) & \xrightarrow{d_2^*} & \mathrm{Hom}_R(P_2, V) & \xrightarrow{d_3^*} & \dots \\
 & & \downarrow{\scriptstyle \beta_*} & & \downarrow{\scriptstyle \beta_*} & & \downarrow{\scriptstyle \beta_*} & & \\
0 & \longrightarrow & \mathrm{Hom}_R(P_0, W) & \xrightarrow{d_1^*} & \mathrm{Hom}_R(P_1, W) & \xrightarrow{d_2^*} & \mathrm{Hom}_R(P_2, W) & \xrightarrow{d_3^*} & \dots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where the columns are exact, since P_0 is projective. This implies that we get a SES of complexes

$$0 \to \mathrm{Hom}_R(P_\bullet, U) \to \mathrm{Hom}_R(P_\bullet, V) \to \mathrm{Hom}_R(P_\bullet, W) \to 0$$

We shall denote this SES as $0 \to X_\bullet \to Y_\bullet \to Z_\bullet \to 0$. This induces a LES on the cohomology, i.e.

$$0 \to H^1(X_\bullet) \to H^1(Y_\bullet) \to H^1(Z_\bullet) \to H^2(X_\bullet) \to H^2(Y_\bullet) \to H^2(Z_\bullet) \to \dots$$

where each cohomology represents their respective Ext groups on either U, V, or W. Recall also that the 0-th Ext group is isomorphic to the hom set. Thus rewriting the above LES gives us

$$0 \to \mathrm{Hom}_R(D, U) \to \mathrm{Hom}_R(0, V) \to \mathrm{Hom}_R(D, W)$$
$$\to \mathrm{Ext}^1_R(D, U) \to \mathrm{Ext}^1_R(D, V) \to \mathrm{Ext}^1_R(D, W) \to \mathrm{Ext}^2_R(D, U) \to \dots$$

as required. □

Remark 3.2.20. Similarly, note that since $\mathrm{Hom}_R(X, D) \cong \mathrm{Ext}^0_R(X, D)$, thus the whole LES above is a LES of Ext groups.

Remark 3.2.21. Since $\mathrm{Hom}_R(D, -)$ is a left exact covariant functor, we obtained a right covariant derived functor $\mathrm{Ext}^m_R(D, -) : \text{R-mod} \to \text{Ab}$. This is 'dual' to that the relation between $\mathrm{Hom}_R(-, D)$ and $\mathrm{Ext}^n_R(-, D)$.

Theorem 3.2.22. *Let P be an R-module. TFAE:*

1. *P is projective.*
2. *$\mathrm{Ext}^1_R(P, B) = 0$ for all R-module B.*
3. *$\mathrm{Ext}^n_R(P, B) = 0$ for all $n \geq 1$ and R-module B.*

Proof. The proof is left as a tutorial question. □

Example 3.2.23.

1. For any free R-module F, we have $\mathrm{Ext}^n_R(F, B) = 0$ for any $n \geq 1$ and R-module B. In particular $\mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}^m, B) = 0$ for all $n \geq 1$ and $m \geq 1$.
2. We compute $\mathrm{Ext}^n_{\mathbb{Z}}(A, B)$ when A is finitely generated $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a PID, by the classification of finitely generated module over PID, we have

   $$A \cong \mathbb{Z}^m \oplus (\mathbb{Z}/d_1\mathbb{Z}) \oplus \dots \oplus (\mathbb{Z}/d_\ell\mathbb{Z})$$

   where $d_i \neq 0$ for all i. In tutorial we will prove that

   $$\mathrm{Ext}^n_R\left(\bigoplus V_i\right), W \cong \prod \mathrm{Ext}^n_R(V_i, W)$$

   But we have only finite number of items (since finitely generated), so

   $$\mathrm{Ext}^n_{\mathbb{Z}}(A, B) \cong \left(\bigoplus_{i=1}^{m} \mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}, B)\right) \oplus \left(\bigoplus_{i=1}^{\ell} \mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/d_i\mathbb{Z}, B)\right)$$

So when $n = 0$ we have

$$\mathrm{Ext}^0_{\mathbb{Z}}(A, B) \cong \left(\bigoplus_{i=1}^{m} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, B)\right) \oplus \left(\bigoplus_{i=1}^{\ell} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/d_i\mathbb{Z}, B)\right) \cong B^m \oplus \bigoplus_{i=1}^{\ell} {}_{d_i}B$$

where ${}_{d_i}B := \{b \in B : d_i b = 0\}$.

When $n = 1$ we have

$$\mathrm{Ext}^1_{\mathbb{Z}}(A, B) \cong 0 \oplus \bigoplus_{i=1}^{\ell} \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/d_i\mathbb{Z}, B) = \bigoplus B/d_iB$$

When $n \geq 2$ we have

$$\mathrm{Ext}^n_{\mathbb{Z}}(A, B) \cong 0 \oplus \bigoplus_{i=1}^{\ell} \mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/d_i\mathbb{Z}, B) = 0$$

Definition 3.2.24 (Injective resolution)**.** An injective resolution of an R-module W is an exact sequence

$$0 \to W \to Q_0 \to Q_1 \to \dots$$

such that each Q_i is injective R-module. We denote the injective resolution of W as $Q_\bullet \hookrightarrow W$.

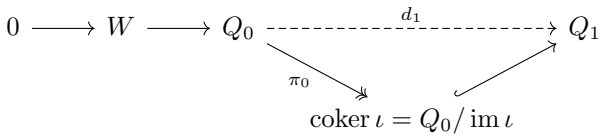
Proposition 3.2.25. *Every R-module has an injective resolution.*

Proof. The whole proof is similar to the proof of existence of projective resolution, except that we will be taking the cokernel.

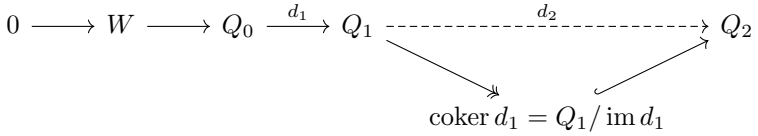
Recall that previously in the subsection of injective modules, we know that every R-module is a submodule of some injective R-module. Thus, suppose given W is an R-module, let Q_0 be an injective R-module such that $W \subseteq Q_0$. We have

$$0 \to W \xrightarrow{\iota} Q_0$$

Next we need to construct Q_1 from the existing information. Consider $\operatorname{coker} \iota$, i.e. $Q_0/\operatorname{im} \iota$, we have that $\pi_0 : Q_0 \twoheadrightarrow \operatorname{coker} \iota$ is the canonical surjection. Note $\operatorname{coker} \iota$ is also an R-module, thus it is contained in some injective R-module, say Q_1. Therefore, we can simply take the composition map of Q_0 to $\operatorname{coker} \iota$ and $\operatorname{coker} \iota$ to Q_1, giving us:



Note that since the map from $\operatorname{coker} \iota$ to Q_1 is injective, thus $\ker d_1 = \ker \pi_0$, and it is clear that $\ker \pi_0 = \operatorname{im} \iota$. This shows that $\ker d_1 = \operatorname{im} \iota$, implying that we have exactness. Repeat the above procedure again we obtain:



and the exactness can be verfied similarly. Inductively we can construct an exact sequence of injective modules, thus completing the proof. □

Definition 3.2.26 (Alternative definition of Ext)**.** Take an injective resolution $W \hookrightarrow Q_\bullet$ of W and take $\operatorname{Hom}_R(V, -)$. which we get

$$0 \xrightarrow{d_0^*} \operatorname{Hom}_R(V, Q_0) \xrightarrow{d_0^*} \operatorname{Hom}_R(V, Q_0) \xrightarrow{d_0^*} \operatorname{Hom}_R(V, Q_0) \to \dots$$

The n-th cohomology group of this complex is defined as

$$\operatorname{Ext}_R^n(V, W) := \frac{\ker d_{n+1}^*}{\operatorname{im} d_n^*}$$

Remark 3.2.27. Despite we are unable to prove that, but we have the following fact: the Ext group constructed from injective resolution is independent of the choice of the starting injective resolution. Also, the Ext group constructed from injective resolution is isomorphic to if it is constructed from a projective resolution.

Example 3.2.28. We verify that the $\operatorname{Ext}_R^0(V, W)$ constructed from projective resolution and injective resolution is isomorphic. Starting from 0-th Ext group constructed from an injective resolution:

$$\begin{aligned}
\operatorname{Ext}_R^0(V, W) &= \ker d_1^* \\
&= \{f : V \to Q_0 : d_1 \circ f = 0\} \\
&= \{f : V \to Q_0 : \operatorname{im} f \subseteq \ker d_1\} \\
&= \{f : V \to Q_0 : \operatorname{im} f \subseteq \operatorname{im} \iota, \iota : W \hookrightarrow Q_0\} \\
&= \{f : V \to \iota(W)\} \\
&\cong \operatorname{Hom}_R(V, W)
\end{aligned}$$

We have shown that the 0-th Ext group constructed from projective resolution is also isomorphic to $\operatorname{Hom}_R(V, W)$, this shows the 0-th Ext group is independet of the method of construction.

Remark 3.2.29 (Enough projective and enough injective)**.** In fact, all the mentioned theory can be generalized to any category.

A category $\mathcal{C}$ has enough projective if for any object X in $\mathcal{C}$ there is a projective object P such that $P \to X$ is an epimorphism. Since the definition of projective module is nothing except of lifting of maps, we need not 'module-like' object to define a projective object in the category $\mathcal{C}$, assuming that we can 'lift' the map.

Similarly, the category has enough injective if for any object X in $\mathcal{C}$ there is an injective object I such that $X \to I$ is a monomorphism. Construction of injective object shares the same philosophy, as it just requires construction of maps.

In the category R-mod, it is nice in the sense that it has both enough projective and enough injective. However, there might be some category where it is only enough projective, or vice versa. In this case, we might be restricted to construct the Ext group only from the projective resolution, or vice versa. The above says that they are equivalent.

Example 3.2.30.

1. Let A and B be abelian groups. We compute $\mathrm{Ext}^n_{\mathbb{Z}}(A, B)$ (again) using the injective resolution of B. Let Q_0 be an injective $\mathbb{Z}$-module such that $B \subseteq Q_0$. So

$$0 \to B \to Q_0 \to Q_0/B \to 0$$

   Recall that the quotient of injective module is injective, so Q_0/B is injective, and the above is an injective resolution of B. Taking hom we have

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A, Q_0) \to \mathrm{Hom}_{\mathbb{Z}}(A, Q_0/B) \to 0 \to 0 \to \dots$$

   We see that $\mathrm{Ext}^n_{\mathbb{Z}}(A, B) = 0$ for all $n \geq 2$, even without the assumption that A is finitely generated.

2. Let A be a torsion abelian group, i.e. any $a \in A$ there exists some $n \neq 0$ such that $n \cdot a = 0$. We compute $\mathrm{Ext}^0_{\mathbb{Z}}(A, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z})$, which is 0, since for any group homomorphism $\varphi : A \to \mathbb{Z}$ and any $a \in A$, let $n \neq 0$ such that $n \cdot a = 0$, and so

$$0 = \varphi(0) = \varphi(na) = n\varphi(a)$$

   implying that $\varphi(a) = 0$. Since a is arbitrary, so φ is the zero map, indicating that $\mathrm{Ext}^0_{\mathbb{Z}}(A, \mathbb{Z})$ is trivial. Next, we consider $\mathrm{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z})$. Take

$$0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Q} \xrightarrow{\pi} \mathbb{Q}/\mathbb{Z} \to 0$$

   where π is the canonical surjection, and ι is the inclusion map. The above is an injective resolution of $\mathbb{Z}$. Taking hom, we have

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}) \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) \to 0 \to 0 \to \dots$$

   We claim that $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}) = 0$. To see this, take $\varphi : A \to \mathbb{Q}$ be a group homomorphism and let $a \in A$ and $n \neq 0$ such that $n \cdot a = 0$. Note

$$0 = \varphi(0) = \varphi(na) = n\varphi(a)$$

   Similarly, since a is arbitrary, we have that φ is trivial, so $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}) = 0$. Lastly, simply take the first cohomology group and we obtained

$$\mathrm{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$$

   where $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ is called the Pontryagin dual group of A.

Remark 3.2.31. The reason why Ext group has its name is because of the following theorem:

Theorem 3.2.32. $\mathrm{Ext}^n_R(V, W)$ *is the equivalence classes of* n*-fold extensions of exact sequences that takes the following form*

$$0 \to W \to V_{n-1} \to \cdots \to V_0 \to V \to 0$$

When $n = 1$, we are considering the equivalence classes of the exact sequences of the form $0 \to W \to V_0 \to V \to 0$, which is just SES.

As an example, take $R = \mathbb{Z}$ and $V = W = \mathbb{Z}/p\mathbb{Z}$. Based on the previous computed example we have that

$$\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \cong \frac{\mathbb{Z}/p\mathbb{Z}}{p \cdot (\mathbb{Z}/p\mathbb{Z})} = \mathbb{Z}/p\mathbb{Z}$$

That is to mean that there are p equivalent classes of SES in the form of

$$0 \to \mathbb{Z}/p\mathbb{Z} \to - \to \mathbb{Z}/p\mathbb{Z} \to 0$$

In particular, they are either equivalent to

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{\iota} (\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z} \to 0$$

or, for any $j = 1, 2, \ldots, p-1$, that

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\cdot j} \mathbb{Z}/p\mathbb{Z} \to 0$$

where the formal one splits and the latter one doesn't.

3.3 Tor group

Definition 3.3.1 (Tor group)**.** Let D be a right R-module, B be a left R-module and $P_\bullet \twoheadrightarrow B$ be a projective resolution of B:

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} B \to 0 \to \ldots$$

We then construct the complex by taking tensor product over R:

$$\ldots \xrightarrow{1 \otimes d_3} D \otimes_R P_2 \xrightarrow{1 \otimes d_2} D \otimes_R P_1 \xrightarrow{1 \otimes d_1} D \otimes_R P_0 \to 0$$

which is indeed a complex since $(1 \otimes d_n) \circ (1 \otimes d_{n+1}) = 1 \otimes (d_n \circ d_{n+1}) = 0$, but it is not exact. In fact $D \otimes_R -$ is a right exact functor. The n-th Tor group is defined to be the n-th homology group of this complex, i.e.

$$\mathrm{Tor}^R_n(D, B) := \frac{\ker(1 \otimes d_n)}{\mathrm{im}\,(1 \otimes d_{n+1})}$$

The functor $\mathrm{Tor}^R_n(D, -)$ is the left covariant derived functor of the right covariant functor $D \otimes_R -$.

Proposition 3.3.2. $\mathrm{Tor}^R_0(D, B) \cong D \otimes_R B$.

Proof. By definition, we have that

$$\mathrm{Tor}^R_0(D, B) = \ker(1 \otimes d_0) / \mathrm{im}(1 \otimes d_1)$$

A direct observation says that $\ker(1 \otimes d_0)$ is $D \otimes P_0$.

Next, note that we have the following exact sequence:

$$P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} B \to 0$$

which induces an exact sequence

$$D \otimes_R P_1 \xrightarrow{1 \otimes d_1} D \otimes_R P_0 \xrightarrow{1 \otimes \varepsilon} D \otimes_R B \to 0$$

Thus $\mathrm{im}(1 \otimes d_1) = \ker(1 \otimes \varepsilon)$. Altogether, we see that

$$\frac{D \otimes P_0}{\mathrm{im}(1 \otimes d_1)} = \frac{D \otimes P_0}{\ker(1 \otimes \varepsilon)}$$

By 1st Isomorphism Theorem, the RHS is isomorphic to $\mathrm{im}(1 \otimes \varepsilon)$, which is $D \otimes_R B$. This completes the proof. □

Example 3.3.3. We compute $\mathrm{Tor}_n^{\mathbb{Z}}(D, \mathbb{Z}/m\mathbb{Z})$. Let $B = \mathbb{Z}/m\mathbb{Z}$. Consider the projective resolution of B:

$$0 \to \mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z} \xrightarrow{\text{mod } m} \mathbb{Z}/m\mathbb{Z} \to 0$$

Note if $m = 0$ we have

$$0 \to \mathbb{Z} \xrightarrow{\cdot 1} \mathbb{Z} \to 0$$

In case of $m \neq 0$, remove the term $\mathbb{Z}/m\mathbb{Z}$, and take tensor product. Also, in case of $m = 0$, simply take tensor product,

$$\cdots \to 0 \to D \otimes_{\mathbb{Z}} \mathbb{Z} \xrightarrow{(\cdot m)_*} D \otimes_{\mathbb{Z}} \mathbb{Z} \to 0$$

which is equivalent to that

$$\cdots \to 0 \to D \xrightarrow{\cdot m} D \to 0$$

Thus we have $\mathrm{Tor}_0^{\mathbb{Z}}(0, \mathbb{Z}/m\mathbb{Z}) = D \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong D/mD$ where the last equality is a tutorial question. Also

$$\mathrm{Tor}_1^{\mathbb{Z}}(D, \mathbb{Z}/m\mathbb{Z}) = \ker(\cdot m)/0 = {}_mD = \{d \in D : md = 0\}$$

Proposition 3.3.4.

1. $\mathrm{Tor}_n^R(D, B)$ *is independent of the choice of the projective resolution of* B.
2. *For any* $f : B \to B'$, *we have an induced map of group homomorphism* $f_* : \mathrm{Tor}_n^R(D, B) \to \mathrm{Tor}_n^R(D, B')$.

Proof. The first statement is left as an tutorial question.

For the second statement, let $P_\bullet \twoheadrightarrow B$ and $P'_\bullet \twoheadrightarrow B'$ be projective resolutions of B and B' respectively. Then, by Comparison Theorem, we have

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_3 & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \longrightarrow & B & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} & & \\
\cdots & \longrightarrow & P'_3 & \xrightarrow{d'_3} & P'_2 & \xrightarrow{d'_2} & P'_1 & \xrightarrow{d'_1} & P'_0 & \longrightarrow & B' & \longrightarrow & 0
\end{array}$$

Taking tensor with F we have

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & D \otimes_R P_2 & \xrightarrow{d_2} & D \otimes_R P_1 & \xrightarrow{d_1} & D \otimes_R P_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle 1\otimes f_2} & & \downarrow{\scriptstyle 1\otimes f_1} & & \downarrow{\scriptstyle 1\otimes f_0} & & \\
\cdots & \longrightarrow & D \otimes_R P'_2 & \xrightarrow{d'_2} & D \otimes_R P'_1 & \xrightarrow{d'_1} & D \otimes_R P'_0 & \longrightarrow & 0
\end{array}$$

We shall denote the first and second row of complexes as $X^\bullet$ and $Y^\bullet$ respectively. We examine commutativity in the above diagram, where note

$$\begin{aligned}
(1 \otimes d_n) \circ (1 \otimes d_{n+1}) &= 1 \otimes (f_n \circ d_{n+1}) \\
&= 1 \otimes (d_n \circ f_{n+1}) \\
&= (1 \otimes d_n) \circ (1 \otimes f_{n+1})
\end{aligned}$$

Thus we indeed have commutativity. Therefore, this induces maps on the homology group

$$\mathcal{F}_* : H_n(X^\bullet) \to H_n(Y^\bullet)$$

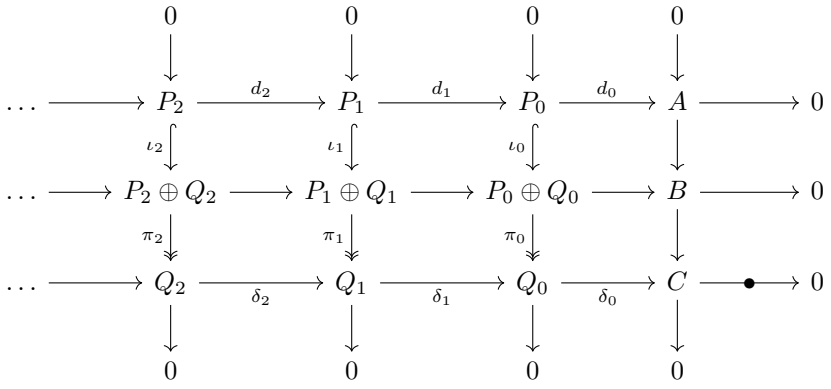
where $H_n(X^\bullet)$ is $\mathrm{Tor}_n^R(D, B)$ and $H_n(Y^\bullet)$ is $\mathrm{Tor}_n^R(D, B')$. This completes the proof. □

Theorem 3.3.5. *Let* $0 \to A \to B \to C \to 0$ *be a SES of left* R*-module and* D *be a right* R*-module. Then we have a LES (of abelian groups) given by*

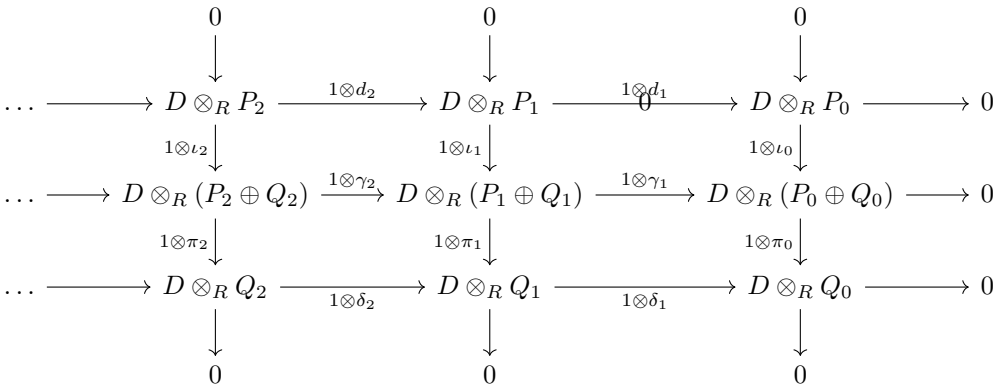
$$\cdots \to \mathrm{Tor}_2^R(D, C) \to \mathrm{Tor}_1^R(D, A) \to \mathrm{Tor}_1^R(D, B) \to \mathrm{Tor}_1^R(D, C)$$

$$\to D \otimes_R A \to D \otimes_R B \to D \otimes_R C \to 0$$

Proof. Let $P_\bullet \twoheadrightarrow A$ and $Q_\bullet \twoheadrightarrow C$ be projective resolutions of A and C respectively. By Horseshoe Lemma we have



Taking $D \otimes_R -$ we have



We shall denote the second, third, fourth row of complexes, which are non-zero, as $X_\bullet, Y_\bullet$, and $Z_\bullet$, and we claim that the column are SES of complexes.

To see this, we compute a map $1 \otimes \zeta_0 : D \otimes_R (P_0 \oplus Q_0) \to D \otimes_R P_0$, which is simply the projection to $D \otimes_R P_0$. Note

$$(1 \otimes \zeta_0) \circ (1 \otimes \iota_0) = 1 \otimes (\zeta_0 \circ \iota 0) = 1 \otimes \mathrm{id}_{P_0} = \mathrm{id}_{D \otimes_R P_0}$$

This implies that $1 \otimes \iota_0$ must be an injective map. In general $1 \otimes \iota_\bullet$ is injective. On the other hand, it is clear that $1 \otimes \pi_\bullet$ is surjective. Thus, we have that the columns of the commutative diagram is SES, i.e.

$$0 \to X_\bullet \to Y_\bullet \to Z_\bullet \to 0$$

This induces a LES

$$\cdots \to H_1(X_\bullet) \to H_1(Y_\bullet) \to H_1(Z_\bullet) \to H_0(X_\bullet) \to H_0(Y_\bullet) \to H_0(Z_\bullet) \to 0$$

where these homology groups are the Tor groups. This completes the proof. □

Proposition 3.3.6 (Characterization of flat modules)**.** *Let D be a right R-module. TFAE:*

1. *D is flat.*
2. *$\mathrm{Tor}_1^R(D, B) = 0$ for all left R-module B.*
3. *$\mathrm{Tor}_n^R(D, B) = 0$ for all left R-module B and $n \geq 1$.*

Proof.

[3. $\implies$ 2.] Trivial.

[2. $\implies$ 1.] Suppose given SES $0 \to A \to B \to B \to C \to 0$. By the previous theorem, we have a LES

$$\cdots \to \mathrm{Tor}_1^R(D, C) = 0 \to D \otimes_R A \to D \otimes_R B \to D \otimes_R C \to 0$$

This reduces to an SES

$$0 \to D \otimes_R A \to D \otimes_R B \to D \otimes_R C \to 0$$

Thus D is flat by definition.

[1. $\implies$ 3.] Let $P_\bullet \twoheadrightarrow B$ be a projective resolution of B. Since D is flat, from the LES

$$\cdots \to P_2 \to P_1 \to P_0 \to B \to 0 \to \dots$$

it induces another LES

$$\cdots \to D \otimes_R P_2 \to D \otimes_R P_1 \to D \otimes_R P_0 \to 0$$

where the term $D \otimes_R B$ is removed. Since this is a LES, thus all the homology group, i.e. the Tor groups, are trivial. This concludes the proof. □

Remark 3.3.7. Recall when R is commutative a left R-module is equivalent to a right R-module. In this case, $\operatorname{Tor}_n^R(A,B) \cong \operatorname{Tor}_n^R(B,A)$. To prove this it requires the use of double complex, which is not covered here, thus the proof is omitted.

However, we can check that the statement is true when $n = 0$. This is indeed true since

$$\operatorname{Tor}_0^R(A,B) \cong A \otimes_R B \cong B \otimes_R A \cong \operatorname{Tor}_0^R(B,A)$$

Here the tensor product is commutative due to commutativity of R.

Example 3.3.8. It is easy to show that $\operatorname{Tor}_n^R(A, \bigoplus B_i) \cong \bigoplus \operatorname{Tor}_n^R(A, B_i)$ (this is a tutorial question). We will use this to compute $\operatorname{Tor}_n^{\mathbb{Z}}(A,B)$ where B is a finitely generated Z-module. Note

$$B \cong Z^m \oplus (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_\ell\mathbb{Z})$$

And thus

$$\operatorname{Tor}_n^{\mathbb{Z}}(A,B) \cong \bigoplus_{i=1}^{m} \operatorname{Tor}_n^{\mathbb{Z}}(A,\mathbb{Z}) \oplus \bigoplus_{i=1}^{\ell} \operatorname{Tor}_n^{\mathbb{Z}}(A, \mathbb{Z}/d_i\mathbb{Z})$$

Note

$$\operatorname{Tor}_n^{Z}(A, \mathbb{Z}/d_i\mathbb{Z}) = \begin{cases} A/d_iA & , n = 0 \\ {}_{d_i}A & , n = 1 \\ 0 & , n \geq 2 \end{cases}$$

On the other hand,

$$\operatorname{Tor}_0^{\mathbb{Z}}(A,\mathbb{Z}) = A \quad \text{and} \quad \operatorname{Tor}_n^{\mathbb{Z}}(A,\mathbb{Z}) = 0 \ \forall n \geq 1$$

Therefore, in this case, $\operatorname{Tor}_n^{\mathbb{Z}}(A,B)$ is fully known.

3.4 Group Cohomology

Recall that $\mathbb{Z}G$ is the set of functions f from G to $\mathbb{Z}$ with finite support. Alternatively, we can think of $\mathbb{Z}G$ as

$$\left\{ \sum \lambda_g \cdot g : \lambda_g \in \mathbb{Z} \text{ where } \lambda_g \text{ are almost all zero} \right\}$$

For more details (including its operation), refer to Example 1.2.5. Note also that $\mathbb{Z}G$ is commutative if and only if G is abelian.

Definition 3.4.1 (G-module)**.** Let G be a group (not necessarily abelian) and A be an abelian group. We say A is a G-module if there is a group homomorphism $\varphi : G \to \operatorname{Aut}(A)$, i.e. G acts on A, i.e. A is a $\mathbb{Z}G$-module where $\mathbb{Z}G$ is the group algebra over $\mathbb{Z}$.

Example 3.4.2.

1. (Trivial G-module). $\mathbb{Z}$ is a G-module with the trivial G-action, i.e. $g \cdot n = n$ for every $g \in G$ and $n \in \mathbb{Z}$. One shall note, however, that this does not mean $\alpha \cdot n = n$ for every $\alpha \in \mathbb{Z}G$, for example

$$(1+g) \cdot n = 1 \cdot n + g \cdot n = n + n = 2n$$

2. Let A be a G-module. The fixed point submodule of A by G is defined to be

$$A^G = \{a \in A : ga = a \forall g \in G\} \leq A$$

This is a submodule of A where G acts trivially.

3. Let V be a vector space over field F. Then V is $\mathrm{GL}(V)$-module, where recall $\mathrm{GL}(V)$ is just the group fo linear transformation from V to V. Furthermore, $V^{\mathrm{GL}(V)} = \left\{\vec{0}\right\}$.

4. Let K be a Galois extension of F (for example $\mathbb{Q}$). Then K is a G-module where $G = \mathrm{Gal}(K/F)$. Also $K^G = F$ by the Galois correspondence.

Lemma 3.4.3. *Let A be a G-module. Then $A^G \cong \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ as groups.*

Proof. Define $\varphi : A^G \to \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ by $\varphi(a) = \alpha_a$ where $\alpha_a : n \mapsto n \cdot a$ for any $a \in A^G$.

We first check well-definedness. We check that $\alpha_a \in \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$. Since element of $\mathbb{Z}G$ can be expressed as formal sum of G, thus it suffices to check that $\alpha_a(g \cdot n) = g \cdot \alpha_a(n)$

$$\alpha_a(g \cdot n) = \alpha_a(n) = na = n(g \cdot a) = g \cdot (na) = g \cdot \alpha_a(n)$$

Next, we check that φ is a group homomorphism. To show $\varphi(a + b) = \varphi(a) + \varphi(b)$, we just have to note that

$$\alpha_{a+b}(n) = n(a + b) = na + nb = \alpha_a(n) + \alpha_b(n) = (\alpha_a + \alpha_b)(n)$$

We now show that φ is a group isomorphism by defining its inverse map. Consider $\phi : \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \to A^G$ where $\alpha \mapsto \alpha(1)$. It is easy to check that the composition of ϕ and φ gives identity map, and is thus omitted here. □

Proposition 3.4.4. *Let $F_n := \bigotimes_{i=1}^{n+1} \mathbb{Z}G$ where tensor product is over $\mathbb{Z}$. Then*

$$\cdots \to F_n \xrightarrow{d_n} F_{n-1} \xrightarrow{d_{n-1}} \ldots F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

is a free resolution of $\mathbb{Z}$ as $\mathbb{Z}G$-module where

1. *F_n is $\mathbb{Z}G$-module defined by $g \cdot (g_0 \otimes g_1 \otimes \cdots \otimes g_n) := (gg_0) \otimes g_1 \otimes \ldots g_n$.*

2. *F_n is a free $\mathbb{Z}G$-module of rank $|G|^n$, i.e. $F_n \cong \bigoplus_{i=1}^{|G|^n} \mathbb{Z}G$ with a free basis*

$$\{1 \otimes g_1 \ldots \otimes g_n : g_1, \ldots, d_n \in G\}$$

3. *$\varepsilon =: d_0 : F_0 \to \mathbb{Z}$ is defined by $d_0(g_0) = 1$. For $d_1 : F_1 \to F_0$ where $d_1(g_0 \otimes g_1) = g_0(g_1 - 1)$. For $n \geq 2$, we define*

$$\begin{aligned} d_n(g_0 \otimes g_1 \otimes \ldots \otimes g_n) =& (g_0 g_1 \otimes g_2 \otimes \ldots \otimes g_n) \\ &+ \sum_{i=1}^{n-1} (-1)^i (g_0 \otimes g_1 \otimes \ldots \otimes g_{i-1} \otimes g_i g_{i+1} \otimes \dot{\otimes} g_n) \\ &+ (-1)^n (g_0 \otimes g_1 \otimes \ldots \otimes g_{n-1}) \end{aligned}$$

Proof. The proof is tedious and lengthy, thus it is left as a tutorial question. □

Definition 3.4.5 (Bar resolution / Standard Resolution)**.** The free resolution constructed in the previous proposition is called the bar resolution of $\mathbb{Z}$.

Remark 3.4.6. Historically, instead of writting $(g_0 \otimes g_1 \otimes \ldots \otimes g_n)$, it was written as

$$(g_0 \mid g_1 \mid \cdots \mid g_n)$$

and this is why it is called bar resolution. We shall adapt this style of writting as well.

Definition 3.4.7 (Group cohomology)**.** Let A be a G-module. The n-th group cohomology of G with coefficient set A is defined to be

$$\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$$

where $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$ is the n-th cohomology group of the complex obatined from taking hom on the bar resolution of $\mathbb{Z}$:

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(F_0, A) \xrightarrow{d_1^*} \mathrm{Hom}_{\mathbb{Z}G}(F_1, A) \xrightarrow{d_2^*} \mathrm{Hom}_{\mathbb{Z}G}(F_2, A) \xrightarrow{d_3^*} \dots$$

Remark 3.4.8. Given group G, recall the invariant subgroup A^G of a G-module A is defined to be

$$A^G := \{a \in A : ga = a \ \forall g \in G\}$$

In fact, we can view it as a factor $-^G : \mathrm{Ab} \to G\text{-mod}$. It is a left exact functor. Then, group cohomology is then the right-derived functor of the invariant subgroup functor $-^G$. Roughly speaking, group cohomology measures the failure of being fixed by G. For example, if a G-module A is invariant under G, then it should have trivial group cohomology.

Example 3.4.9. We compute the cohomology $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$ of the finite cyclic group $G = C_n = \langle\sigma\rangle$. By definition

$$\mathbb{Z}G = \left\{\sum_{i=0}^{n-1} n_i\sigma^i : n_i \in \mathbb{Z}\right\}$$

Consider $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$. We have a free resolution of $\mathbb{Z}$ given by

$$\dots \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}G \xrightarrow{\cdot N} \mathbb{Z}G \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

where

$$\varepsilon(g) = 1 \quad \text{and} \quad \varepsilon\left(\sum n_i\sigma^i\right) = \sum_{i=0}^{n-1} n_i$$

Since G is abelian, so $\mathbb{Z}G$ is commutative, thus we have

$$(\sigma - 1)N = N(\sigma - 1) = (1 + \sigma + \cdots + \sigma^{n-1})(\sigma - 1) = \sigma^n - 1 = 0$$

Thus $\mathrm{im}(\cdot(\sigma - 1)) \subseteq \ker(\cdot N)$, and $\mathrm{im}(\cdot N) \subseteq \ker(\cdot(\sigma - 1))$.

Next, to show that $\ker(\cdot(\sigma - 1)) \subseteq \mathrm{im}(\cdot N)$, let $\sum n_i\sigma^i \in \ker(\cdot(\sigma - 1))$. By definition

$$0 = (\sigma - 1)(\sum n_i\sigma^i) = \sum_{j=0}^{n-1}(n_{j-1} - n_j)\sigma^j$$

This means that all coefficients are zero, so $n_{j-1} = n_j$ for all j, and thus we have $\sum n_i\sigma^i = \lambda N$ for some $\lambda \in \mathbb{Z}$.

Also, we have to show that $\ker(\cdot N) \subseteq \mathrm{im}(\cdot(\sigma - 1))$. First note that for every $g \in G$, we have

$$\varepsilon((\sigma - 1) \cdot g) = \varepsilon(\sigma g - g) = 1 - 1 = 0$$

suggesting that $\mathrm{im}(\cdot(\sigma - 1)) \subseteq \ker\varepsilon$. Let $\sum n_i\sigma^i \in \ker\varepsilon$, i.e. $\sum n_i = 0$. So

$$\ker\varepsilon = \mathrm{span}_{\mathbb{Z}}\left\{1 - \sigma, \sigma - \sigma^2, \dots, \sigma^{n-2} - \sigma^{n-1}\right\}$$

so $\ker\varepsilon \subseteq \mathrm{im}(\cdot(\sigma - 1))$.

In short, this shows that the above complex is indeed a free resolution.

Next, we compute the Ext group. Taking hom and ignore the first term we have

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \xrightarrow{(\cdot(\sigma-1))_*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \xrightarrow{(\cdot N)_*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \xrightarrow{(\cdot(\sigma-1))_*}$$

This is equivalent to

$$0 \to A \xrightarrow{\cdot(\sigma-1)} A \xrightarrow{\cdot N} A \xrightarrow{\cdot(\sigma-1)} \dots$$

We can now compute the Ext group: when n is 0

$$\mathrm{Ext}^0_{\mathbb{Z}G}(\mathbb{Z}, A) \cong A^{\mathbb{Z}G} = A^G$$

When $n \neq 0$ is even:

$$\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A) = \frac{\ker(\cdot(\sigma - 1))}{\mathrm{im}(\cdot N)} = \frac{{}^{\sigma-1}A}{NA} = \frac{A^G}{NA}$$

and when n is odd we have

$$\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A) = \frac{\ker(\cdot N)}{\mathrm{im}(\cdot(\sigma - 1))} = \frac{{}^{N}A}{(\sigma - 1)A}$$

Definition 3.4.10 (n-cochain of G with coefficient in A)**.** Let A be a G-module. Define $C^0(G, A) := A$, and for all $n \geq 1$ define

$$C^n(G, A) := \{\text{maps from } G^n \text{ to } A\}$$

where maps refer to general maps. These are called the n-cochain of G with coefficient in A.

Proposition 3.4.11. *Let A be a G-module. For $n \geq 1$, the n-cohcain $C^n(G, A)$ is an abelian group defined by the group operation*

$$(\alpha + \beta)(g_1, \ldots, g_n) = \alpha(g_1, \ldots, g_n) + \beta(g_1, \ldots, g_n)$$

where $\alpha, \beta \in C^n(G, A)$. In particular, $C^n(G, A)$ is an abelian group for all n.

Furthermore, we have isomorphism

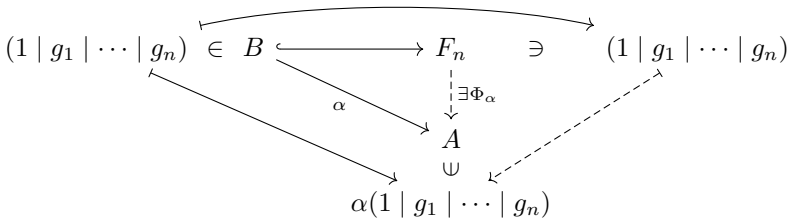
$$\begin{array}{ccccc} & (g_1, \ldots, g_n) \mapsto \beta(1|g_1|\ldots|g_n) & \longleftarrow \Psi \longmapsto & \beta & \\ & \cap & & \cap & \\ \Phi : & C^n(G, A) & \longleftrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(F_n, A) & : \Psi \\ & \cup & & \cup & \\ & \alpha & \longmapsto \Phi \longrightarrow & \Phi_\alpha : 1|g_1|\ldots|g_n \mapsto \alpha(g_1, \ldots, g_n) & \end{array}$$

Proof. The proof of $C^n(G, A)$ being abelian group is clear, thus omitted.

For the second part of the statement, we start by first showing that Φ is well-defined. Let $\alpha \in C^n(G, A)$, so $\alpha : G^n \to A$ is a map. Note F_n has a $\mathbb{Z}G$-basis

$$B := \{1 \mid g_1 \mid \cdots \mid g_n : g_1, \ldots, g_n \in G\}$$

This implies that F_n is a free module. By the universal property of free module, we have the following commutative diagram:



so we now obtain Φ_α that maps from the $\mathbb{Z}G$-basis B of G^n to A. We can extend the map Φ_α linearly such that the Φ_α maps from G^n, since B is a basis. It is ensured by the universal property that Φ_α is indeed an $\mathbb{Z}G$-module homomorphism. This shows that Φ is indeed well-defined.

Next we show that Φ is a group homomorphism. Let $\alpha, \alpha' \in C^n(G, A)$. Then

$$\begin{aligned} (\Phi(\alpha + \alpha'))(g_1, \ldots, g_n) &= \Phi_{\alpha+\alpha'}(g_1, \ldots, g_n) \\ &= (\alpha + \alpha')(1 \mid g_1 \mid \cdots \mid g_n) \\ &= \alpha(1 \mid g_1 \mid \cdots \mid g_n) + \alpha'(1 \mid g_1 \mid \cdots \mid g_n) \\ &= \Phi_\alpha(g_1, \ldots, g_n) + \Phi_{\alpha'}(g_1, \ldots, g_n) \\ &= (\Phi_\alpha + \Phi_{\alpha'})(g_1, \ldots, g_n) \\ &= (\Phi(\alpha) + \Phi(\alpha'))(g_1, \ldots, g_n) \end{aligned}$$

This shows that $\Phi(\alpha+\alpha')=\Phi(\alpha)+\Phi(\alpha')$.

On the other hand, there is no ambiguity in the well-definedness of Ψ. We prove that Ψ is indeed a group homomorphism: Let $\beta,\beta'\in\mathrm{Hom}_{\mathbb{Z}G}(F_n,A)$, then

$$\begin{aligned}(\Psi(\beta+\beta'))(g_1,\dots,g_n)&=(\beta+\beta')(1\mid g_1\mid\cdots\mid g_n)\\&=\beta(1\mid g_1\mid\cdots\mid g_n)+\beta'(1\mid g_1\mid\cdots\mid g_n)\\&=(\Psi(\beta))(g_1,\dots,g_n)+(\Psi(\beta'))(g_1,\dots,g_n)\\&=(\Psi(\beta)+\Psi(\beta'))(g_1,\dots,g_n)\end{aligned}$$

This shows that $\Psi(\beta+\beta')=\Psi(\beta)+\Psi(\beta')$.

Lastly, we show that Φ and Ψ is isomorphism pair. Firstly note $(\Psi\circ\Phi)(\alpha)=\Psi(\Phi(\alpha))=\Psi\circ\Phi_\alpha$, so

$$((\Psi\circ\Phi)(\alpha))(g_1,\dots,g_n)=(\Psi\circ\Phi_\alpha)(g_1,\dots,g_n)=\Phi_\alpha(1\mid g_1\mid\cdots\mid g_n)=\alpha(g_1,\dots,g_n)$$

So $(\Psi\circ\Phi)(\alpha)=\alpha$. Conversely, see that

$$((\Phi\circ\Psi)(\beta))(1\mid g_1\mid\cdots\mid g_n)=(\Psi(\beta))(g_1,\dots,g_n)=\beta(1\mid g_1\mid\cdots\mid g_n)$$

This shows that $(\Phi\circ\Psi)(\beta)=\beta$. In summary, this shows that Ψ and Φ are indeed invserses of each other, so the proof is completed. □

Proposition 3.4.12. *Under the isomorphism* $\mathrm{Hom}_{\mathbb{Z}G}(F_n,A)\cong C^n(G,A)$*, the differential maps* $d^*_{n+1}:\mathrm{Hom}_{\mathbb{Z}G}(F_n,A)\to\mathrm{Hom}_{\mathbb{Z}G}(F_{n+1},A)$ *translate to, for* $n\geq 1$*, that*

$$\delta_{n+1}:C^n(G,A)\to C^{n+1}(G,A),\ \ f\mapsto\delta_{n+1}(f)$$

where $f\mapsto\delta_{n+1}(f)$

$$\begin{aligned}&\delta_{n+1}(f)(x_1,\dots,x_{n+1})\\&=x_1f(x_2,\dots,x_{n+1})+\sum_{i=1}^{n}(-1)^nf(x_1,\dots,,x_{i-1},x_ix_{i+1},\dots,x_{n+1})+(-1)^{n+1}f(x_1,\dots,x_n)\end{aligned}$$

and when $n=0$*, the map* $\delta_1:C^0(G,A)\to C^1(G,A)$ *is defined to be* $a\mapsto(g\mapsto ga-a)$.

Proof. Firstly, we examine the case for $n=0$.

$$\begin{array}{ccccccc}(\Phi_a:1\mapsto a) & \in & \mathrm{Hom}_{\mathbb{Z}G}(F_0,Z) & \xrightarrow{d_1^*} & \mathrm{Hom}_{\mathbb{Z}G}(F_1,A) & \ni & \Phi_a\circ d_1\\ \uparrow & & \Phi\uparrow & & \downarrow\Psi & & \downarrow\\ a & \in & A=C^0(G,A) & \xrightarrow[\delta_1]{} & C^1(G,A) & \ni & \Psi(\Phi_a\circ d_1)(g)\end{array}$$

We want that the above diagram is commutative, i.e. we want to show that $\Psi(\Phi_a\circ d_1)(g)=\delta_1(a)$. Simply note

$$\begin{aligned}\Psi(\Phi_a\circ d_1)(g)&=(\Phi_a\circ d_1)(1\mid g)\\&=\Phi_a(d_1(1\mid g))\\&=\Phi_a(g-1)\\&=(g-1)\cdot\Phi_a(1)\\&=(g-1)a\\&=ga-a\\&=\delta_1(g)\end{aligned}$$

This shows that the statement holds for $n=0$. For $n\geq 1$, we have

$$\begin{array}{ccccccc}\Phi_\beta & \in & \mathrm{Hom}_{\mathbb{Z}G}(F_n,Z) & \xrightarrow{d_{n+1}^*} & \mathrm{Hom}_{\mathbb{Z}G}(F_{n+1},A) & \ni & \Phi_\beta\circ d_{n+1}\\ \uparrow & & \Phi\uparrow & & \downarrow\Psi & & \downarrow\\ \beta & \in & C^n(G,A) & \xrightarrow[\delta_{n+1}]{} & C^{n+1}(G,A) & \ni & \Psi(\Phi_\beta\circ d_{n+1})\end{array}$$

□ what?

Remark 3.4.13. Altogether, the previous few proposition implies that we have isomorphism of complex

$$\Phi : \mathrm{Hom}_{\mathbb{Z}G}(F_\bullet, A) \to C^\bullet(G, A)$$

By previous result, we see that $H^n(G, A) := H^n(C^\bullet(G, A)) \cong \mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A)$ where

$$H^n(C^\bullet(G, A)) = \frac{\ker \delta_{n+1}}{\mathrm{im}\, \delta_n}$$

Here, we call $\ker \delta_{n+1}$ as the n-cocycles, and $\mathrm{im}\, \delta_n$ the n-coboundaries.

Example 3.4.14.

1. Note the 0-th group cohomology

$$H^0(G, A) = \ker \delta_1 = \{a \in A : \delta_1(a) = 0\} = \{a \in A : \forall g \in G,\ ga - a = 0\} = A^G$$

   is just the submodule of $\mathbb{Z}G$ fixed by G.

2. When $G = \{1\}$ is the trivial group, from previous example we see that $H^0(G, A) = A$. For $n \geq 1$, note $H^n(G, A) = H^n(C^n(G, A)) = 0$, since $C^n(G, A)$ is the maps from $G^n = \{1\}^n$ to A, where there is only one possible ma.

Theorem 3.4.15 (LES in group cohomology)**.** *Let $0 \to A \to B \to C \to 0$ be a SES of G-module. Then we have a LES*

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \dots$$

Proof. The proof is immediate follows from LES in Ext groups, since by definition group cohomology is just a special type of Ext group. □

Corollary 3.4.16. *Suppose that $H^n(G, B) = 0$ for all $n \geq 1$, then we have exact sequence*

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to 0$$

and isomorphism

$$H^{n+1}(G, A) \cong H^n(G, C)$$

Proof. Simply apply the assumption on the LES in group cohomology. The isomorphism comes from the exactness. □

3.5 Induced Module

Definition 3.5.1 (Induced module)**.** Let H be a subgroup of G, then $\mathbb{Z}H$ is a subalgebra (subring) of $\mathbb{Z}G$. Let A be an H-module. We define the induced G-module by

$$M_H^G(A) := \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A) = \{\varphi : \mathbb{Z}G \to A : h\varphi(g) = \varphi(hg) \forall h \in H, \forall g \in G\}$$

where we consider $\mathbb{Z}G$ as the bimodule ${}_{\mathbb{Z}H}\mathbb{Z}G_{\mathbb{Z}G}$.

Remark 3.5.2. In the case where G is finite, then

$$M_H^G(A) \cong \mathbb{Z}G \otimes_{\mathbb{Z}H} A$$

Proposition 3.5.3 (Transitivity of induced module)**.** *Let $K \leq H \leq G$ and A is a K-module. Then*

$$M_K^G(A) \cong M_H^G(M_K^H(A))$$

Proof. By definition we have

$$M_H^G(M_K^H(A)) = \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, \mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}H, A))$$

Recall that Tensor-hom adjunction says that if we have R-module $X_R,\ {}_RY_S,\ Z_S$, then

$$\mathrm{Hom}_S(X \otimes_R Y, Z) \cong \mathrm{Hom}_R(X, \mathrm{Hom}_S(Y, Z))$$

Note also that if we have an left $\mathbb{Z}G$-module V, we can define

$$v * g = g^{-1} \cdot v$$

to make V into a right $\mathbb{Z}G$-module.

With all the previous setup, we apply the conversion of left module to right module, if necessary, and apply tensor-hom adjunction to obtain

$$\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, \mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}H, A)) \cong \mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}G \otimes_{\mathbb{Z}H} \mathbb{Z}H, A)$$

Note $\mathbb{Z}G \otimes_{\mathbb{Z}H} \mathbb{Z}H \cong \mathbb{Z}G$, thus we have

$$\mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}G \otimes_{\mathbb{Z}H} \mathbb{Z}H, A) \cong \mathrm{Hom}_{\mathbb{Z}K}(\mathbb{Z}G, A) = M_K^G(A)$$

This completes the proof. □

Proposition 3.5.4. *Suppose that G is a finite group and $0 \to A \to B \to C \to 0$ be a SES of H-module, where $H \leq G$. Then we have a SES of G-module*

$$0 \to M_H^G(A) \to M_H^G(B) \to M_H^G(C) \to 0$$

Proof. Note we can write

$$G = \bigcup_{i=1}^{m} g_i H$$

for some m, thus we have

$$\mathbb{Z}G = \bigoplus_{i=1}^{m} g_i \mathbb{Z}H$$

as abelian groups. But note $g_i\mathbb{Z}H$ is isomorphic with the regular right $\mathbb{Z}H$-module $\mathbb{Z}H$, so $g_i\mathbb{Z}H$ has a free $\mathbb{Z}H$-basis $\{g_i h \mid h \in H\}$.

So $\mathbb{Z}G$ is a right free $\mathbb{Z}H$-module. Moreover, recall that free implies projective implies flat, so an SES $0 \to A \to B \to C \to 0$ induces

$$0 \to \mathbb{Z}G \otimes_{\mathbb{Z}H} A \to \mathbb{Z}G \otimes_{\mathbb{Z}H} B \to \mathbb{Z}G \otimes_{\mathbb{Z}H} C \to 0$$

Note that each non-zero entries in the above SES is isomorphic to $M_H^G(A)$, $M_H^G(B)$, and $M_H^G(C)$ respectively. Thus we have an equivalent SES

$$0 \to M_H^G(A) \to M_H^G(B) \to M_H^G(C) \to 0$$

This concludes the proof. □

Proposition 3.5.5. *Let $H \leq G$ and A be a G-module. Then we have an injective G-module homomorphism*

$$\varphi : A \to M_H^G(A) = \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)$$

where $a \mapsto \varphi(a)(x) = xa$ for all $x \in G$, $a \in A$.

Proof. We first check well-definedness, i.e. $\varphi(a) \in M_H^G(A)$. For every $x \in G$ and $h \in H$, we have

$$\varphi(a)(hx) = (hx)a = h(xa) = h(\varphi(a)(x))$$

This shows that $\varphi(a)$ is indeed contained in $M_H^G(A)$. Secondly, we check that φ is an G-module homomorphis: for every $g \in G$, $x \in G$, we have

$$\varphi(g \cdot a)(x) = x(ga) = (xg)(a) = \varphi(a)(xg) = (g \cdot \varphi(a))(x)$$

This shows that $\varphi(g \cdot a) = g \cdot \varphi(a)$.

Lastly, we show that φ is injective. let $\varphi(a) = 0$, then for every $x \in G$ we have $\varphi(a)(x) = 0$. Take $x = 1$, note

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

But $\varphi(a)(1) = 0$, so $a = 0$. This shows that φ is injective. □

Theorem 3.5.6 (Shapiro's Lemma)**.** *Let $H \leq G$ and A be an H-module. For any $n \geq 0$, we have*

$$H^n(G, M_H^G(A)) \cong H^n(H, A)$$

Proof. Let $P_\bullet \twoheadrightarrow \mathbb{Z}$ be a projective resolution of $\mathbb{Z}$ as $\mathbb{Z}G$-module. Since P_n is a projective $\mathbb{Z}G$-module, then P_n is a direct summand of $\mathbb{Z}G$-module:

$$P_n | \bigoplus \mathbb{Z}G$$

By restriction to $\mathbb{Z}H$, we see that

$$_{\mathbb{Z}H}P_n | \bigoplus \ _{\mathbb{Z}H}\mathbb{Z}G$$

But since $_{\mathbb{Z}H}\mathbb{Z}G \cong \bigoplus \mathbb{Z}H$, so we have

$$_{\mathbb{Z}H}P_n | \bigoplus \mathbb{Z}H$$

This says that P_n is projective as $\mathbb{Z}H$-modules. In other words, we have a projective resolution $P_\bullet \twoheadrightarrow \mathbb{Z}$ as $\mathbb{Z}H$-modules, with all the differential maps are the same.

Take $\mathrm{Hom}_{\mathbb{Z}G}(-, M_H^G(A))$ for the projective resolution of $\mathbb{Z}$ as $\mathbb{Z}G$-module, and take $\mathrm{Hom}_{\mathbb{Z}H}(-, A)$ for the projective resolution of $\mathbb{Z}$ as $\mathbb{Z}H$-module. We also define the maps $\varphi_n : \mathrm{Hom}_{\mathbb{Z}G}(P_n, M_H^G(A)) \to \mathrm{Hom}_{\mathbb{Z}H}(P_0, A)$ by $f \mapsto \varphi_n(f)$ where $\varphi_n(f)$ is defined as the map $x \mapsto f(x)(1)$. We thus have the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_0, M_H^G(A)) & \xrightarrow{d_1^*} & \mathrm{Hom}_{\mathbb{Z}G}(P_1, M_H^G(A)) & \xrightarrow{d_2^*} & \mathrm{Hom}_{\mathbb{Z}G}(P_2, M_H^G(A)) & \xrightarrow{d_3^*} & \dots \\
 & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \\
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_0, A) & \xrightarrow{d_1^*} & \mathrm{Hom}_{\mathbb{Z}H}(P_1, A) & \xrightarrow{d_2^*} & \mathrm{Hom}_{\mathbb{Z}H}(P_2, A) & \xrightarrow{d_3^*} & \dots
\end{array}$$

Our goal is to show that $\varphi_\bullet$ is a chain complex isomorphism. In particular, we have to show the above diagram commutes, and that each φ_n is an isomorphism.

Firstly, to show commutativity, we show that $d_n^* \circ \varphi_{n-1} = \varphi_n d_n$. In particular, we see that the following occurs:

$$\begin{array}{ccccccc}
 & & f & \longmapsto & f \circ d_n & & \\
\dots & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_{n-1}, M_H^G(A)) & \xrightarrow{d_n^*} & \mathrm{Hom}_{\mathbb{Z}G}(P_n, M_H^G(A)) & \longrightarrow & \dots \\
 & & \downarrow{\scriptstyle \varphi_{n-1}} & & \downarrow{\scriptstyle \varphi_n} & & \\
\dots & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_{n-1}, A) & \xrightarrow{d_n^*} & \mathrm{Hom}_{\mathbb{Z}H}(P_n, A) & \longrightarrow & \dots \\
 & & g : x \mapsto f(x)(1) & \longmapsto & (g \circ d_n) = \varphi_n(f \circ d_n) & &
\end{array}$$

where the equality at the lower right corner is achieved as follow: Note $\varphi_n(f \circ d_n)$ is defined to be the map $x \mapsto (f \circ d_n)(x)(1)$. On the other hand we note $g \circ d_n$ sends x to $(g \circ d_n)(x) = g(d_n(x))$, where by the definition of g we see

$$g(d_n(x)) = f(d_n(x))(1) = (f \circ d_n)(x)(1)$$

In short, we have $g \circ d_n$ sends x to $(f \circ d_n)(x)(1)$, which has the same effect as $\varphi_n(f \circ d_n)$. This shows commutativity.

Next, to show that φ_n is an isomorphism, note that $\mathrm{Hom}_{\mathbb{Z}G}(V, M_H^G(A)) = \mathrm{Hom}_{\mathbb{Z}G}(V_{\mathbb{Z}G}, M_H^G(A)_{\mathbb{Z}G})$. By tensor-hom adjunction, we have the following isomorphism

$$\mathrm{Hom}_{\mathbb{Z}G}(V_{\mathbb{Z}G}, M_H^G(A)_{\mathbb{Z}G}) \cong \mathrm{Hom}_{\mathbb{Z}H}(V \otimes_{\mathbb{Z}G} \mathbb{Z}G, A_{\mathbb{Z}H})$$

where the isomorphism is given by $f \mapsto (v \otimes g \mapsto f(v)(g))$. Recall that $V \otimes_{\mathbb{Z}G} \mathbb{Z}G \cong V$, thus we have that

$$\mathrm{Hom}_{\mathbb{Z}H}(V \otimes_{\mathbb{Z}G} \mathbb{Z}G, A_{\mathbb{Z}H}) \cong \mathrm{Hom}_{\mathbb{Z}H}(V_{\mathbb{Z}H}, A_{\mathbb{Z}H})$$

where the isomorphism is given by

$$(v \otimes g \mapsto f(v)(g)) \mapsto (v \mapsto f(v)(1))$$

Lastly, we see $\mathrm{Hom}_{\mathbb{Z}H}({}_{\mathbb{Z}H}V,\ {}_{\mathbb{Z}H}A) = \mathrm{Hom}_{\mathbb{Z}H}(V_{\mathbb{Z}H}, A_{\mathbb{Z}H})$. In short, the above discussion can be summarized as follow:

$$\begin{array}{ccccc} & \mathrm{Hom}_{\mathbb{Z}G}(V, M_H^G(A)) & \ni & f \\ & & & \downarrow \\ = & \mathrm{Hom}_{\mathbb{Z}G}(V_{\mathbb{Z}G}, M_H^G(A)_{\mathbb{Z}G}) & & \\ & & & \downarrow \\ \cong & \mathrm{Hom}_{\mathbb{Z}H}(V \otimes_{\mathbb{Z}G} \mathbb{Z}G, A_{\mathbb{Z}H}) & \ni & v \otimes g \mapsto f(v)(g) \\ & & & \downarrow \\ \cong & \mathrm{Hom}_{\mathbb{Z}H}(V_{\mathbb{Z}H}, A_{\mathbb{Z}H}) & \ni & v \mapsto f(v)(1) \\ & & & \\ = & \mathrm{Hom}_{\mathbb{Z}H}({}_{\mathbb{Z}H}A,\ {}_{\mathbb{Z}H}A) & & \end{array}$$

This completes the proof. □

Corollary 3.5.7. *Let A be a G-module. Denote the trivial subgroup of G as 1. For all $n \geq 1$ we have*

$$H^n(G, M_1^G(A)) = 0$$

Proof. It follows from Shapiro's Lemma that $H^n(G, M_1^G(A)) \cong H^n(1, A) \cong 0$. □

Corollary 3.5.8 (Degree shifting)**.** *For any G-module A, we have*

$$H^{n+1}(G, A) \cong H^n(G, M_1^G(A)/A)$$

Proof. SInce we have an injective G-module homomorphism $A \hookrightarrow M_1^G(A)$, we get a SES

$$0 \to A \to M_1^G(A) \to M_1^G(A)/A \to 0$$

where we define it as $0 \to X \to Y \to Z \to 0$. This induces a LES

$$0 \to H^0(G, X) \to H^0(G, Y) \to H^0(G, Z)$$

$$\to H^1(G, X) \to H^1(G, Y) \to H^1(G, Z) \to H^2(G, X) \to H^2(G, Y) \to \dots$$

But note from previous corollary we see that $H^n(G, Y) = 0$, thus we have

$$\cdots \to 0 \to H^n(G, Z) \to H^{n+1}(G, X) \to 0 \to \dots$$

The result follows □

3.6 Inflation, Restriction, and Corestriction Homomorphisms

Definition 3.6.1 (Compatible)**.** Let A and A' be G and G'-module respectively. A group homomorphism $\alpha : G' \to G$ is compatible with a (abelian) group homomorphism $f : A \to A'$ if

$$g' \cdot f(a) = f(\alpha(g') \cdot a)$$

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

Remark 3.6.2. Compatibility simultaneously generalizes both module homomorphism and restriction. For example, if $\alpha = \mathrm{id}_G$ and $G' = G$, then

$$g \cdot f(a) = f(g \cdot a)$$

On the other hand, if $A' = A$, and take $f = \mathrm{id}_A$, then

$$g' * a = \alpha(g') \cdot a$$

where in most scenario we might be taking G' as a subgroup of G, and α as the inclusion map.

Proposition 3.6.3. *Suppose that $\alpha : G' \to G$ and $: A \to A'$ are compatible. Then, for all $n \geq 0$ we have a homomorphism*

$$\lambda_n : H^n(G, A) \to H^n(G', A'),\ [\varphi] \mapsto [f \circ \varphi \circ \alpha^n]$$

where $\alpha^n : (G')^n \to G^n$ such that $(h_1, \dots, h_n) \mapsto (\alpha(h_1), \dots, \alpha(h_n))$. Note that here $\varphi : G^n \to A$.

Proof. To show that we have a homomorphism from $H^\bullet(G,A)$ to $H^n(G',A')$, it suffices to show that there is a homomorphism from $C^\bullet(G,A)$ to $C^\bullet(G',A')$. Define

$$\Phi_0 : C^0(G,A) \to C^0(G',A'),\ a \mapsto f(a)$$

Also, define for each $n \geq 1$ that

$$\Phi_n : C^n(G,A) \to C^n(G',A'),\ \varphi \mapsto f \circ \varphi \circ \alpha^n$$

This gives a diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C^0(G,A) & \xrightarrow{\delta_1} & C^1(G,A) & \xrightarrow{\delta_2} & C^2(G,A) & \xrightarrow{\delta_3} & \cdots \\
 & & \downarrow{\scriptstyle \Phi_0} & & \downarrow{\scriptstyle \Phi_1} & & \downarrow{\scriptstyle \Phi_2} & & \\
0 & \longrightarrow & C^0(G',A') & \xrightarrow{\delta_1} & C^1(G',A') & \xrightarrow{\delta_2} & C^2(G',A') & \xrightarrow{\delta_3} & \cdots
\end{array}$$

where by abuse of notation we are denoting the differential maps of both complexes as $\delta_\bullet$. It remains to show that the diagram commutes, i.e. $\Phi\delta = \delta\Phi$, where indices are dropped.

Firstly, we have

$$\begin{aligned}
&(\Phi\delta)(\varphi)(h_1,\ldots,h_{n+1}) \\
&= (f \circ \delta(\varphi) \circ \alpha^{n+1})(h_1,\ldots,h_{n+1}) \\
&= (f \circ \delta(\varphi))(\alpha(h_1),\ldots,\alpha(h_{n+1})) \\
&= f(\alpha(h_1) \cdot \varphi(\alpha(h_1),\ldots,\alpha(h_{n+1}))) \\
&\quad + \sum_{i=1}^{n} (-1)^i \varphi(\alpha(h_1),\ldots,\alpha(h_{i-1},\alpha(h_i)\alpha(h_{i+1}),\ldots,\alpha(h_{n+1}))) \\
&\quad + (-1)^{n-1}\varphi(\alpha(h_1),\ldots,\alpha(h_n)) \\
&= h_1 \cdot (f \circ \varphi)(\alpha(h_2),\ldots,\alpha(h_{n+1})) \\
&\quad + \sum_{i=1}^{n} (-1)^i \varphi(\alpha(h_1),\ldots,\alpha(h_{i-1},\alpha(h_i)\alpha(h_{i+1}),\ldots,\alpha(h_{n+1}))) \\
&\quad + (-1)^{n-1}\varphi(\alpha(h_1),\ldots,\alpha(h_n))
\end{aligned}$$

On other other hand, we have

$$\begin{aligned}
&(\delta\Phi)(\varphi)(h_1,\ldots,h_{n+1}) \\
&= \delta(f \circ \varphi \circ \alpha^n)(h_1,\ldots,h_{n+1}) \\
&= h_1(f \circ \varphi \circ \alpha^n)(h_2,\ldots,h_{n+1}) \\
&\quad + \sum_{i=1}^{n} (-1)^i \varphi(\alpha(h_1),\ldots,\alpha(h_{i-1},\alpha(h_i)\alpha(h_{i+1}),\ldots,\alpha(h_{n+1}))) \\
&\quad + (-1)^{n-1}\varphi(\alpha(h_1),\ldots,\alpha(h_n))
\end{aligned}$$

where in the last equality we have applied the compatibility that $h(f(a)) = f(\alpha(h)a)$. Therefore, we see that we have commutativity in the above diagram, and thus Φ_n is indeed a chain homomorphism. □

Definition 3.6.4 (Natural transformation)**.** Let $\mathcal{F}$ and $\mathcal{F}'$ be covariant functors from category $\mathcal{C}$ to $\mathcal{D}$. A natural transformation η from $\mathcal{F}$ to $\mathcal{F}'$ is a collection $\{\eta_X : \mathcal{F}(X) \to \mathcal{F}'(X) \mid \forall X \in \mathrm{Obj}(\mathcal{C})\}$ of morphism in category $\mathcal{D}$ such that for any $\varphi \in \mathrm{Mor}_{\mathcal{C}}(X,Y)$ we have the following commutative diagram

$$\begin{array}{ccc}
\mathcal{F}(X) & \xrightarrow{\eta_X} & \mathcal{F}'(X) \\
{\scriptstyle \mathcal{F}(\varphi)}\downarrow & & \downarrow{\scriptstyle \mathcal{F}'(\varphi)} \\
\mathcal{F}(Y) & \xrightarrow{\eta_Y} & \mathcal{F}'(Y)
\end{array}$$

We denote a natural transformation from $\mathcal{F}$ to $\mathcal{F}'$ as $\eta : \mathcal{F} \implies \mathcal{F}'$.

Example 3.6.5. Let $\alpha : G' \to G$ be a group homomorphism. We have covariant functors

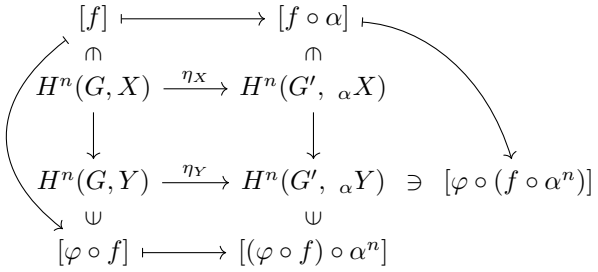
$$H^n(G, -) : \text{G-mod} \to \text{Ab}$$

$$H^n(G', {}_\alpha -) : \text{G-mod} \to \text{Ab}$$

We have the natural transformation

$$\eta_X : H^n(G, X) \to H^n(G', {}_\alpha X),\ [f] \mapsto [f \circ \alpha^n]$$

For each G-module homomorphism $\varphi : X \to Y$, we have the following diagram



Since composition is associative, so $[(\varphi \circ f) \circ \alpha^n] = [\varphi \circ (f \circ \alpha^n)]$, and thus the diagram is commutative. This shows that η is a natural transformation.

Definition 3.6.6 (Restriction homomorphism, Inflation homomorphism)**.**

1. Consider $H \leq G$ and $\iota : H \hookrightarrow G$ be the inclusion map. Let A be G-module, and $\mathrm{id}_A : A \to A$. Note the pair (ι, id_A) is compatible. The restriction homomorphism (of group cohomology) is defined to be
$$\mathrm{res} : H^n(G, A) \to H^n(H, A),\ [f] \mapsto [f \circ \iota^n]$$

2. Let $N \triangleleft G$ and A is a G-module. Define the fixed point module by N as
$$A^N = \{a \in A : n \cdot a = a\ \forall n \in N\}$$
Then N acts trivially on A^N. Also, for any $g \in G$, $a \in A^N$, $n \in N$, then
$$n(ga) = g(g^{-1}ng)a = ga$$
So $ga \in A^N$, and thus A^N is a G-module.

   Therefore A^N is a (G/N)-module. Consider the canonical surjection $\pi : G \twoheadrightarrow G/N$ and the inlcusion map $\varphi : A^N \to A$. Then the pair (π, φ) is compatible, i.e.
$$g * \varphi(a) = g * a = \varphi(g * a) = \varphi(\pi(g)a)$$
for all $g \in G$ and $a \in A^N$.

   The inflation homomorphism (of group cohomology) is defined to be
$$\inf : H^n(G/N, A^N) \to H^n(G, A),\ [f] \mapsto [\iota \circ f \circ \pi^n]$$

Proposition 3.6.7. *Let $H \leq G$ such that $[G : H] < \infty$. Let A be a G-module. Define $\psi : M_H^G(A) \to A$ by*

$$\psi(f) = \sum_{i=1}^{m} g_i \cdot f(g_i^{-1})$$

where $\{g_1, \ldots, g_n\} = G/H$. Then ψ is a surjective G-module homomorphism independent of the choice of coset representatives of G/H.

Proof. We first prove that ψ is independent of the choice of coset representatives. For each i, let $g_i' = g_i h_i$ where $h_i \in H$. If we consider the set of representative $\{g_1', \dots, g_n'\}$, then

$$\Psi(f) = \sum_{i=1}^{m} g_i' f(g_i'^{-1}) = \sum_{i=1}^{m} g_i h_i f(h_i^{-1} g_i^{-1}) = \sum_{i=1}^{m} g_i h_i h_i^{-1} f(g_i^{-1}) = \sum_{i=1}^{m} g_i f(g_i^{-1})$$

This shows that the defined map is independent of the choice of coset representatives.

The proof of ψ being a group homomorphism is left as an exercise. We show that the defined map is a G-module homomorphism. Note for each $g \in G$ and $j = 1, \dots, m$, we can write

$$g g_j = g_{j_i} h_j$$

since gg_j lives in some cosets of H. We see that

$$\psi(g \cdot f) = \sum_{i=1}^{m} g_i (g \cdot f)(g_i^{-1}) = \sum_{i=1}^{m} g_i (f(g_i^{-1} g))$$

Since the sum is running through 1 to m, thus it is equivalent to write

$$\begin{aligned}
\psi(g \cdot f) &= \sum_{i=1}^{m} g_{j_i} f(g_{j_i}^{-1} g) \\
&= \sum_{i=1}^{m} g_{j_i} f(h_j g_j^{-1}) \\
&= \sum_{i=1}^{m} g_{j_i} h_j f(g_j^{-1}) \\
&= \sum_{i=1}^{m} g g_j f(g_j^{-1}) \\
&= g \sum_{i=1}^{m} g_j f(g_j^{-1}) \\
&= g\psi(f)
\end{aligned}$$

This shows that ψ is a G-module homomorphism.

Lastly, for the surjectivity of ψ, for each $i = 1, \dots, m$ and $a \in A$, we define $f_{i,a} : \mathbb{Z}G \to A$ where

$$f_{i,a}(x) = \begin{cases} ha & , \ x = h g_i^{-1}, \ h \in H \\ 0 & , \ \text{otherwise} \end{cases}$$

Observe that the criterion $x = hg_i^{-1}$ can be rewritten as $x^{-1} = g_i h^{-1} \in g_i H$. We claim that $f_{i,a} \in M_H^G(A)$, i.e. we want to show that for $h \in H$ and $x \in G$ we have $f_{i,a}(hx) = h f_{i,a}(x)$. By definition, we have

$$f_{i,a}(hx) = \begin{cases} h'(a) & , \ hx = h' g_i^{-1}, h' \in H \\ 0 & , \ \text{otherwise} \end{cases}$$

and

$$h f_{i,a}(x) = \begin{cases} h(h"a) & , \ x = h" g_i^{-1}, h" \in H \\ 0 & , \ \text{otherwise} \end{cases}$$

To show that the above two maps are equivalent, note

$$x = h" g_i^{-1} \implies hx = hh" g_i^{-1} \implies h' g_i^{-1}$$

where the last implication is given by the condition of $f_{i,a}(hx)$. This shows that $h' = hh"$. Using this

equality we see that $hf_{i,a}(x)$ can be rewritten as

$$\begin{aligned} hf_{i,a}(x) &= \begin{cases} h'(a) & , \ x = h^{-1}h'g_i^{-1}, h^{-1}h' \in H \\ 0 & , \ \text{otherwise} \end{cases} \\ &= \begin{cases} h'(a) & , \ hx = h'g_i^{-1}, h' \in H \\ 0 & , \ \text{otherwise} \end{cases} \\ &= f_{i,a}(hx) \end{aligned}$$

Thus the claim that $f_{i,a} \in M_H^G(A)$ holds. The proof of surjectivity is now accessibile: for every $a \in A$, consider

$$\begin{aligned} \psi(f_{j,g_j^{-1}a}) &= \sum_{i=1}^{m} g_i f_{j,g_i^{-1}a}(g_i^{-1}) \\ &= g_j f_{j,g_j^{-1}a}(g_j^{-1}) \\ = g_j(g_j^{-1}a) &= a \end{aligned}$$

where the second last equality follows from observing that the sum is non-zero for when $i = j$, given by the definition of $f_{i,a}$ defined previously. This shows surjectivity of ψ, and thus the proof is completed. □

Definition 3.6.8 (Corestriction homomorphism)**.** Let $H \leq G$ such that $[G : H] < \infty$. Let A be a G-module. Define $\psi : M_H^G(A) \to A$ by

$$\psi(f) = \sum_{i=1}^{m} g_i f(g_i^{-1})$$

where $\{g_1, \ldots, g_n\} = G/H$. Previous proposition asserts that $\psi(f)$ is a G-module homomorphism. It induces a group homomorphism $\psi^* : H^n(G, M_H^G(A)) \to H^n(G, A)$ where

$$[f] \mapsto [\psi \circ f]$$

By Shapiro's lemma, we have

$$H^n(H, A) \cong H^n(G, M_H^G(A))$$

The corestriction homomorphism (on group cohomology) is the composition of these two maps

$$H^n(H, A) \xrightarrow{\cong} H^n(G, M_H^G(A)) \xrightarrow{\psi^*} H^n(G, A)$$

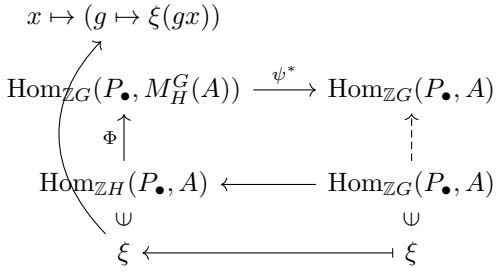
Remark 3.6.9. Corestrictionis analogous to transfer map in module theory for groups.

Proposition 3.6.10. *Let H be a subgroup of G where $[G : H] = m < \infty$. Let A be a G-moduke. Then*

$$\operatorname{cores} \circ \operatorname{res} : H^n(G, A) \to H^n(G, A), \ z \mapsto mz$$

for all $n \geq 0$.

Proof. Consider the following diagram:



where Φ is given in Shapiro's Lemma. The doted arrow is our desired map, where it is the composition of all the maps. Note for every $x \in P_\bullet$, we have

$$\begin{aligned}
(\psi^*\Phi(\xi))(x) &= (\psi \circ \Phi(\xi))(x) \\
&= \psi(\Phi(\xi)(x)) \\
&= \sum_{i=1}^{m} g_i \Phi(\xi)(x)(g_i^{-1}) \\
&= \sum_{i=1}^{m} g_i \xi(g_i^{\lfloor} - 1]x) \\
&= \sum_{i=1}^{m} g_i g_i^{-1} \xi(x) \\
&= \sum_{i=1}^{m} \xi(x) \\
&= m\xi(x) \\
&= (m\xi)(x)
\end{aligned}$$

So $(\psi^* \circ \Phi)(\xi) = m\xi$. This induces map on the n-th cohomology that

$$[\xi] \mapsto [m\xi] = m[\xi]$$

and the proof is completed. □

Corollary 3.6.11. *Suppose that G is a group with $|G| = m$. Then $m \cdot H^n(G, A) = 0$ for every G-module A and $n \geq 1$.*

Proof. In the previous proposition, take H to be the trivial subgroup. Then we have

$$\cdot m = \text{cores} \circ \text{res} : H^n(G, A) \to H^n(G, A)$$

But note we have the following commutative diagram

$$\begin{array}{ccc}
H^n(G,A) & \xrightarrow[\cdot m = \text{cores} \circ \text{res}]{} & H^n(G,A) \\
& {\scriptstyle \text{res}} \searrow \quad \nearrow {\scriptstyle \text{cores}} & \\
& H^n(\{1\}, A) = 0, \ \forall n \geq 1 &
\end{array}$$

where the computation of $H^n(\{1\}, A)$ is done previously. Since the map factors through 0, so we must have $\cdot m = 0$. This completes the proof. □

Corollary 3.6.12. *If $|G| < \infty$, then $H^n(G, A)$ is a torsion abelian group for all $n \geq 1$, for any given G-module A.*

Proof. From previous corollary, we see that for every $c \in H^n(G, A)$ we have $m \cdot c = 0$, where $m = |G|$. This is exactly the definition of torsion group. □

Definition 3.6.13 (Exponent of a group)**.** Given group G. The exponent of G is defined to be the smallest non-negative integer such that for all $g \in G$ we have $g^n = 1$.

Corollary 3.6.14. *Let G be a group where $|G| = m$. Let k be the exponent of a given G-module A. If $\gcd(m, k) = 1$, then $H^n(G, A) = 0$ for all $n \geq 1$. In particular, if $|A| < \infty$ and $\gcd(m, |A|) = 1$, then $H^n(G, A) = 0$ for all $n \geq 1$.*

Proof. Recall that $m \cdot [c] = 0$ for all $[c] \in H^n(G, A)$. Recall also that the order of $[c]$, denoted as $o([c])$, is a divsior of m, by Lagrange's Theorem. Note that the representative c is actually a map where $c : G^n \to A$. Thus we have that

$$(k \cdot c)(g) = k \cdot c(g) = 0$$

Since k is the order of A, and $c(g)$ is an element of A. This means that $k \cdot [c] = [k \cdot c] = 0$, so we must have $o([c]) \mid k$. However $\gcd(m, k) = 1$, so this forces $o([c]) = 1$, which is equivalent to that $[c] = 0$. Since $[c]$ is arbitrary, so $H^n(G, A) = 0$.

Next, if $|A| < \infty$, then $k \mid |A|$, since $|A| \cdot a = 0$ for all $a \in A$. Applying the first part of the statement, if $\gcd(m, |A|) = 1$, then $\gcd(m, k) = 1$, and the conclusion follows. □

Example 3.6.15. Suppose taking $A = \mathbb{F}_p$. If $p \nmid |G|$, then $H^n(G, A) = 0$. If $p \mid |G|$, then, taking for granted, we have

$$H^n(G, A) \cong \mathrm{Ext}^n_{\mathbb{F}_p G}(\mathbb{F}_p, \mathbb{F}_p)$$

where this is a consequence of Cartan-Eilenberg Mapping Theorem.

3.7 Intepretation of First and Second Group Cohomology

Definition 3.7.1 (Derivation)**.** Let A be a G-module. A map $D : G \to A$ is called a derivation (from G to A) if for all $x, y \in G$ we have $D(xy) = D(x) + xD(y)$.

Also, for any $a \in A$, the map $D_a : G \to A$ defined by $D_a(g) = g \cdot a - a$ is called an inner derivation.

We use the notation $\mathrm{Der}(G, A)$ to the denote the set of all derivations, and $\mathrm{Inn}(G, A)$ be the set of all inner derivations.

Theorem 3.7.2. *We have that $Z^1(G, A) = \mathrm{Der}(G, A)$ and $B^1(G, A) = \mathrm{Inn}(G, A)$. So*

$$H^1(G, A) = \frac{\mathrm{Der}(G, A)}{\mathrm{Inn}(G, A)}$$

which is the outer derivation.

Proof. Recall that $Z^1(G, A)$ is defined to be $\ker \delta_2$, where $\delta_2 : C^1(G, A) \to C^2(G, A)$ is the differential map. Let $f \in \ker \delta_2$, this is to saying that for all $g_0, g_1 \in G$ we have

$$\begin{aligned} & \delta_2(f)(g_0, g_1) = g_0 f(g_1) - f(g_0 g_1) + f(g_0) = 0 \\ \iff & f(g_0, g_1) = g_0 f(g_1) + f(g_0) \\ \iff & f \in \mathrm{Der}(G, A) \end{aligned}$$

Recall that $B^1(G, A)$ is defined to be $\mathrm{im}\, \delta_1$, where $\delta_1 : C^0(G, A) \to C^1(G, A)$ is the differential map. Note δ_1 is defined by sending a to

$$g \mapsto g \cdot a - a$$

where the image is clearly what D_a does. So $B^1(G, A) = \mathrm{Inn}(G, A)$. □

Corollary 3.7.3. *Let A be a trivial G-module. Then*

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

where $\mathrm{Hom}_{Ab}(G, A)$ is the set of abelian group homomorphism from G to A.

Proof. For any $a \in A$, we have $D_a(g) = g \cdot a - a = a - a = 0$ since A is a trivial G-module. This shows that $\mathrm{Inn}(G, A) = 0$.

If $f \in \mathrm{Der}(G, A)$, then

$$f(xy) = f(x) + xf(y) = f(x) + f(y)$$

since, again, $x \in G$ and $f(y) \in A$, and that A is a trivial G-module. This shows that f is a group homomorphism. So $\mathrm{Der}(G, A) = \mathrm{Hom}_{\mathrm{Ab}}(G, A)$. This completes the proof. □

Remark 3.7.4. Since A is a G-module, we have group homomorphism $\varphi : G \to \mathrm{Aut}\,(A) = \mathrm{Hom}_{\mathrm{Ab}}(A, A)$. We get the semi-direct product $E := A \rtimes_\varphi G$, where

$$(a, g) \cdot (a', g') = (a + g \cdot a', gg')$$

Remark 3.7.5. We establish some notations here before proceeding to the next section. Let Y be a normal subgroup of X. We define

$$_Y\operatorname{Aut}(X) = \{\sigma \in \operatorname{Aut}(X) : \sigma(y) = y \ \forall y \in Y,\ \sigma(x)Y = xY \ \forall x \in X\}$$

If Y is abelian, then we have a group homomorphism $Y \to {}_Y\operatorname{Aut}(X)$ defined by $z \mapsto \tau_z$ where $\tau_z : x \mapsto z^{-1}xz$. We are interested in the conjugation structure. Note since $z \in Y$ is an element of a normal subgroup, so we have $x^{-1}z^{-1}x \in Y$, and thus $x^{-1}z^{-1}xz \in Y$. Therefore

$$z^{-1}xz \in xY$$

Next, we observe that the kernel of the defined map τ is

$$\{z \in Y : \tau_z = \mathrm{id}_X\} = \{z \in Y : z \in Z(X)\} = Y \cap Z(X)$$

where $Z(X)$ is the center of X. We denote the kernel $Y \cap Z(X)$ as $Z_Y(X)$. It is clear that from 1st isomorphism theorem we obtained an injection

$$Y/Z_Y(X) \hookrightarrow {}_Y\operatorname{Aut}(X)$$

Proposition 3.7.6. *Let A be a G-module and $E = A \rtimes_\varphi G$. Then*

$$H^1(G, A) \cong \frac{{}_A\operatorname{Aut}(E)}{A/Z_A(E)}$$

where $Z_A(E) := A \cap Z(E)$, where $Z(E)$ is the center of E. The isomorphism is given by

$$[f] \mapsto [\sigma_f]$$

where $\sigma_f : (a, g) \mapsto (a + f(g), g)$.

Proof. Define $\Phi : Z^1(G, A) \to {}_A\operatorname{Aut}(E)$ where $f \mapsto \sigma_f$. If we show that Φ is an isomorphism, and Φ maps $B^1(G, A)$ to $(A/Z_A(E))$, the result follows.

We need to show that Φ is well-defined, i.e. $\sigma_f \in {}_A\operatorname{Aut}(E)$. First, we show that σ_f is a homomorphism:

$$\sigma_f((a, g)(a', g')) = \sigma_f(a + g \cdot a', gg') = (a + ga' + f(gg'), gg')$$

and

$$\sigma_f(a, g)\sigma_f(a', g') = (a + f(g), g)(a' + f(g'), g') = (a + f(g) + g \cdot (a' + f(g')), gg')$$

Both are equal, since $f(gg') = f(g) + gf(g')$ due to $Z^1(G, A) = \operatorname{Der}(G, A)$. We also show that σ_f respects identity. This shows σ_f is a homomorphism. Next, we need to show that σ_f is an automorphism. Note

$$f(1) = f(1 \cdot 1) = f(1) + 1 \cdot f(1) = f(1) + f(1)$$

So $f(1) = 0$, which implies that

$$\sigma_f(a, 1) = (a + f(1), 1) = (a, 1)$$

Given $(a, g) \in E$, we have

$$\sigma_f(a, g) = (a + f(g), g) \implies A\sigma_f(a, g) = A(a + f(g), g)$$

Note $(a + f(g), g) = (f(g), 1)(a, g)$, so $\sigma_f \in {}_A\operatorname{Aut}(E)$. This shows that Φ is well-defined.

Next, we show that Φ is a group homomorphism. See that

$$\Phi(f + f')(a, g) = (a + (f + f')(g), g) = (a + f(g) + f'(g), g)$$

and that

$$\Phi(f) \circ \Phi(f')(a, g) = \Phi(f)(a + f'(g), g) = (a + f'(g) + f(g), g)$$

This shows that $\Phi(f + f') = \Phi(f) + \Phi(f')$.

Next, we show that Φ is an isomorphism, where we will give its inverse map explicitly. Define $\Psi : \mathrm{Aut}\,(E) \to Z^1(G,A)$ where $\sigma \mapsto (g \mapsto a)$ if $\sigma(0,g) = (a,g)$. Again, we have to show that Ψ is well-defined, i.e. $\Psi(\sigma)$ is a derivation. If $\sigma(0,g) = (a,g)$ and $\sigma(0,g') = (a',g')$, then

$$\sigma(0,gg') = \sigma(0,g)\sigma(0,g') = (a,g)(a',g') = (a + g \cdot a', gg')$$

The above implies that

$$\Psi(a)(gg') = a + ga' = \Psi(a)(g) + g \cdot \Psi(a)(g')$$

This shows that Ψ is well-defined.

We omit the proof for $\Phi\Psi$ and $\Psi\Phi$ being identities, as it is more or less routine. Lastly, we want to show that $\Phi(B^1(G,A)) = A/Z_A(E)$. Recall that $B^1(G,A) = \mathrm{Inn}(G,A)$. Take $a \in A$, and consider $\Phi(D_a)$. Note that

$$\Phi(D_a)(a',g') = (a' + D_a(G'), g') = (a' + g' \cdot a - a, g')$$

Consider $\tau_a : E \to E$, notice that

$$\tau_a(a',g') = (-a,1) \cdot (a',g')(a,1) = (-a + a', g')(a,1) = (-a + a' + g' \cdot a, g')$$

We see that we obtain an equality. Thus $\Phi(D_a) = [\tau_a]$. This completes the proof. □

Definition 3.7.7 (Group extension)**.** Let A be a G-module. An extension of A by G is an SES of groups with the form

$$0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$$

Here 0 and 1 both denote the trivial group. Notation 0 is used to emphasize that A is always abelian, where 1 is used to emphasize that G need not be abelian. The extension is said to respect the action of G on A if there is a set section $\sigma : G \to E$ (i.e. $\pi\sigma = \mathrm{id}_G$) such that

$$\iota(g \cdot a) = \sigma(g)\iota(a)\sigma(g)^{-1}$$

Since ι is injective, by abuse of notation we will drop the symbol ι, where we identified an element of A as an element of E.

Definition 3.7.8 (Equivalence of two group extension)**.** Let $\mathcal{E}(G,A)$ be the set of all group extension of A by G with respect to the action of G. We define an equivalence relation on $\mathcal{E}(G,A)$ as follow: given two elements of $\mathcal{E}(G,A)$, we say that they are equivalent if there is a group isomorphism π from E to E'.

$$\begin{array}{ccccccccc}
 & & & & & \overset{\sigma}{\curvearrowleft} & & & \\
0 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\
 & & \uparrow\downarrow & & \downarrow\varphi & & \uparrow\downarrow & & \\
0 & \longrightarrow & A & \xrightarrow{\iota'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1
\end{array}$$

Remark 3.7.9. Note the equivalence relation has to be proved. First we need to show that it is well-defined, in the sense that we have to show that the second row really gives a group extension that respects the action of G. This is claer, since we have $\sigma' := \varphi \circ \sigma : G \to E'$, where we see that $\pi'\sigma' = \pi'\varphi\sigma = \pi\sigma = \mathrm{id}_G$. Moreover, we have

$$\begin{aligned}
\iota'(g \cdot a) &= \varphi(\iota(g \cdot a)) \\
&= \varphi(\sigma(g)\iota(a)\sigma(g)^{-1}) \\
&= \sigma'(g)\varphi\iota(a)\sigma'(g)^{-1} \\
&= \sigma'(g)\iota'(a)\sigma'(g)^{-1}
\end{aligned}$$

This shows well-defined. Secondly, we have to see that the defined relation is really equivalent, this is clear, and is left as an exercise.

Definition 3.7.10. Given the following element in $\mathcal{E}(G,A)$:

$$\begin{array}{ccccccccc}
 & & & & & \overset{\sigma}{\curvearrowleft} & & & \\
0 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G & \longrightarrow & 1
\end{array}$$

We define the factor set $f_\sigma : G \times G \to A$ by

$$\iota(f_\sigma(x,y)) := \sigma(x)\sigma(y)(\sigma(xy))^{-1}$$

Lemma 3.7.11. *Every element in E can be written uniquely as $a\sigma(g)$ where $a \in A$ and $g \in G$. Furthermore, if $x = a\sigma(g)$, then $g = \pi(x)$.*

Proof. Let $e \in E$. Since σ is a section, so we have $\pi\sigma\pi(e) = \pi(e)$. So

$$\pi(\sigma\pi(e))\pi(e)^{-1} = \pi(\sigma\pi(e)e^{-1}) = 0 \implies \sigma\pi(e)e^{-1} \in \ker\pi = \operatorname{im}\iota$$

So there exists some element in A, say a^{-1}, such that

$$\sigma\pi(e)e^{-1} = a^{-1}$$

and recall that we have dropped the symbol ι. Rewriting it, we obtain

$$e = a(\sigma\pi(e)) = a\sigma(\pi(e))$$

Note $\pi(e)$ belongs in G, we denote it as $g := \pi(e)$. So, we have write an element e of E as $a\sigma(g)$. This shows that the expression is indeed valid.

Next, we show that this expression is unique. Suppose $a\sigma(g) = a'\sigma(g')$. Rewriting gives $\sigma(g)\sigma(g')^{-1} = a^{-1}a' \in A$. Note $\ker\pi = A$, so $\sigma(g)\sigma(g')^{-1} \in \ker\pi$, implying that

$$\pi(\sigma(g)\sigma(g')^{-1}) = 1 \implies \pi\sigma(gg'^{-1}) = 1$$

By definition $\pi\sigma$ is the identity map, so $gg'^{-1} = 1$, implying that $g = g'$, and so $a = a'$. This shows uniqueness.

Lastly, if $x = a\sigma(g)$, then $\pi(x) = \pi(a\sigma(g)) = \pi(a)\ \pi(\sigma(g)) = 1 \cdot g = g$, completing the proof. □

Remark 3.7.12. For any $x, y \in G$, we have $\sigma(x)\sigma(y)$ is an element fo E, so we can write them as $a\sigma(g)$ for some $a \in A$ and $g \in G$. Taking π both sides, we have

$$g = \pi(\sigma(x)\sigma(y)) = xy$$

Therefore we get

$$\sigma(x)\sigma(y) = a\sigma(xy)$$

Moving $\sigma(xy)$ to LHS, we see that it is exactly the form of factor set. This motivates the definition of factor sets.

Lemma 3.7.13. *Given $\mathcal{E} \in \mathcal{E}(G, A)$. We have $f_\sigma \in Z^2(G, A)$.*

Proof. Recall that $Z^2(G, A)$ is the kernel of $\sigma_3 : C^2(G, A) \to C^3(G, A)$ where δ_3 is the differential map. So $f \in Z^2(G, A)$ is equivalent to that $\delta(f) = 0$, i.e. for every $x, y, z \in G$, we have

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$$

To show $f_\sigma \in Z^2(G, A)$, we examine that f_σ satisfies the above identity. For the sake of convenience, we write our identity multiplicatively instead of additively. We start from noting by associativity we have

$$(\sigma(x)\sigma(y))\sigma(z) = \sigma(x)(\sigma(y)\sigma(z))$$

Firstly, LHS can be rewritten as

$$(\sigma(x)\sigma(y))\sigma(z) = (f_\sigma(x, y)\sigma(xy))\sigma(z) = f_\sigma(x, y)f_\sigma(xy, z)\sigma(xy)\sigma(z) = f_\sigma(x, y)f_\sigma(xy, z)\sigma(xyz)$$

On the other hand, from RHS we have

$$\sigma(x)(\sigma(y)\sigma(z)) = \sigma(x)(f_\sigma(y, z)\sigma(yz)) = \sigma(x)f_\sigma(y, z)\sigma(x)^{-1}\sigma(x)\sigma(yz) = x \cdot f_\sigma(y, z)f_\sigma(x, yz)\sigma(xyz)$$

Note $\sigma(xyz)$ can be cancelled. The result follows by moving every from RHS to LHS and reading it additively. This completes the proof. □

Lemma 3.7.14. *Suppose given $\mathcal{E} \in \mathcal{E}(G, A)$ where*

$$0 \longrightarrow A \xrightarrow{\iota} E \underset{\sigma'}{\overset{\sigma}{\rightleftarrows}} G \xrightarrow{\pi} 1$$

where both σ and σ' are sectors. Then

$$f_\sigma - f_{\sigma'} \in B^2(G, A)$$

i.e. $[f_\sigma] = [f_{\sigma'}]$ in $H^2(G, A)$.

Proof. Recall that $B^2(G, A) = \operatorname{im} \delta_2$ where $\delta_2 : C^1(G, A) \to C^2(G, A)$. Note $f \in B^2(G, A)$ is equivalent to saying that there exists $\gamma : G \to A$ such that $f = \delta_2 \gamma$, i.e. for every $x, y \in G$ we have

$$f(x, y) = x\gamma(y) - \gamma(xy) + \gamma(x)$$

Similar for previous, for the sake of convenience we shall write all our equations multiplicatively for the moment. We claim that $\sigma'(g) \in A\sigma(g)$. To see this, we start by noting that $\sigma'(g) \in E$, so we can write $\sigma'(g) = a\sigma(g')$ for some $a \in A$ and $g' \in G$. Taking π both sides we have

$$\pi\sigma'(g) = \pi(a\sigma(g')) \implies \pi\sigma'(g) = \pi(a)\pi\sigma(g') \implies g = g'$$

since both σ and σ' are sectors, and recall also that $a = \iota(a)$, so $\pi\iota(a) = 1$. So we have $\sigma'(g) = a\sigma(g) \in A\sigma(g)$, thus the claim is proven.

The proven claim allows us to conclude that $\sigma'(g) = \gamma(g)\sigma(g)$ for some $\gamma : G \to A$. We now claim that $f_\sigma - f_{\sigma'} = \delta_2\gamma$. We start from $\sigma'(x)\sigma'(y)$ and rewrite it in two ways. Firstly, we can write

$$\sigma'(x)\sigma'(y) = f_{\sigma'}(x, y)\sigma'(xy) = f_{\sigma'}(x, y)\gamma(xy)\sigma(xy)$$

This will be our RHS. On the other hand, we have

$$\begin{aligned}\sigma'(x)\sigma'(y) &= \gamma(x)\sigma(x)\gamma(y)\sigma(y) \\ &= \gamma(x)\sigma(x)\gamma(y)\sigma(x)^{-1}\sigma(x)\sigma(y) \\ &= \gamma(x)x \cdot \gamma(y)f_\sigma(x, y)\sigma(xy)\end{aligned}$$

and this will be our LHS. We see that $\sigma(xy)$ is common term of two sides, so we can cancel it. Lastly, reading the equation additively, we see that

$$\gamma(x) + x \cdot \gamma(y) + f_\sigma(x, y) = f_{\sigma'}(x, y) + \gamma(xy) \implies \gamma(x) + x \cdot \gamma(y) - \gamma(xy) = f_{\sigma'}(x, y) - f_\sigma(x, y)$$

This is to say that $f_{\sigma'} - f_\sigma = \delta_2\gamma$, which implies that $[f_\sigma] = [f_{\sigma'}]$ in $H^2(G, A)$. □

Remark 3.7.15. So, the above lemmas combine to say that we have a well-defined map

$$\mathcal{E}(G, A) \to H^2(G, A), \ \mathcal{E} \mapsto [f_\sigma]$$

where σ is the section of $\mathcal{E}$. Let $E = A \rtimes_\sigma G$ where $\varphi : G \to \operatorname{Aut}(A)$, then we obtain the following SES $\mathcal{E}$:

$$0 \longrightarrow A \xrightarrow{\iota} A \rtimes_\varphi G \underset{\sigma}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1$$

where

- $\iota : a \mapsto (a, 1)$
- $\pi : (a, g) \mapsto g$
- $\sigma : g \mapsto (0, g)$

It should be clear that $\mathcal{E} \in \mathcal{E}(G, A)$. Next, observe that for any $f_\sigma : G \times G \to A$ we have

$$\begin{aligned}\iota(f_\sigma(x, y)) &= \sigma(x)\sigma(y)(\sigma(xy))^{-1} \\ &= (0, x)(0, y)(0, xy)^{-1} \\ &= (0, 1)\end{aligned}$$

This says that f_σ is the zero in $Z^2(G, A)$, and thus $[f_\sigma]$ represents the zero element in $H^2(G, A)$.

Lemma 3.7.16. *If $\mathcal{E}$ and $\mathcal{E}'$ are equivalent where, say, the isomorphism is given by $\varphi : E \to E'$. Then*

$$[f_\sigma] = [f_{\sigma'}]$$

in $H^2(G, A)$. In other words, we have a well-defined map

$$\frac{\mathcal{E}(G, A)}{\sim} \to H^2(G, A)$$

Proof. It is clear that $\sigma' = \varphi\sigma$ is a section of π'. We start from definition of factor set that

$$\sigma(x)\sigma(y) = f_\sigma(x, y)\sigma(xy)$$

By taking φ both sides, we obtain

$$\varphi(\sigma(x)\sigma(y)) = \varphi(f_\sigma(x, y)\sigma(xy))$$

i.e. $\sigma'(x)\sigma'(y) = (\varphi f_\sigma)(x, y)\sigma'(xy)$. The LHS can be rewritten as

$$\varphi(\sigma(x)\sigma(y)) = f_{\sigma'}(x, y)\sigma'(xy) = \iota'(f_{\sigma'}(x, y)\sigma'(xy))$$

On the other hand, the RHS can be rewritten as

$$(\varphi f_\sigma)(x, y)\sigma'(xy) = \varphi\iota(f_\sigma(x, y)) = \iota' f_\sigma(x, y)$$

Together, we shown that

$$\iota' f_{\sigma'}(x, y) = \iota' f_{\sigma'}(x, y)$$

Thus $f_\sigma(x, y) = f_{\sigma'}(x, y)$. This shows that $[f_\sigma] = [f_{\sigma'}]$, thus completing the proof. □

Remark 3.7.17. In fact, we have an isomorphism

$$\frac{\mathcal{E}(G, A)}{\sim} \cong H^2(G, A)$$

The defined map is the previous lemma is actually an isomorphism. To show that it is really an isomorphism, here we give the inverse map of it, i.e. a map

$$\Phi : H^2(G, A) \to \frac{\mathcal{E}(G, A)}{\sim}$$

Given $z \in H^2(G, A)$, we can pick a normalized $f \in Z^2(G, A)$, i.e. $f(1, g) = 0 = f(g, 1)$ for all $g \in G$, such that $z = [f]$. We define $E_f = A \times G$ such that

$$(a, x)(b, y) := (a + x \cdot b + f(x, y), xy)$$

Here, the identity element is $(0, 1)$ and the inverse is $(a, x)^{-1} = (-x^{-1} \cdot a - f(x^{-1}, x), x^{-1})$. One can check the well-definedness on his own. Then, the image $\Phi(z)$ is defined to be the equivalence classes represented by the SES

$$0 \longrightarrow A \xrightarrow{\iota} E_f \underset{\sigma}{\overset{-\pi\to}{\curvearrowleft}} G \longrightarrow 1$$

One can also show that Φ is indeed the inverse of the map defined in the previous lemma.