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

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 contents this note is only for my own use, and the note are not originally produced by me, except for the presentation of the written proofs. I do not take responsible for any grammatical and mathematical errors in the note. The note might or might not be complete, and, once completing the course, I will not update the note due to 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. $\square$

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 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

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

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-algebra and $\varphi : A \to B$ be a ring homomorphism. We then say φ is an algebra homomorphism from A to B if $\varphi(1_A) = 1_B$ and $\varphi(r \cdot a) = r \star \varphi(a)$. 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

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

   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:

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

This completes the proof. □

Remark 1.2.11. Let R, S be rings. An (R, S)-bimodule ${}_R M_S = ({}_R M, M_S)$ where $(rm)s = r(ms)$. Suppose we have ${}_R M_S$ and ${}_R N$. 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. By definition there exists a non-negative integer d such that $V = RA$ with $|A| = d$. Then we say that A is the minimal generating set of V.

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 $_RR$ is equivalent to a principal left ideal of R. Moreover, if R is a PID, then we have the following chain of equivalence:

$$\text{submodules of } {}_RR \equiv \text{cyclic submodules} \equiv \text{ideals} \equiv \text{principal ideals}$$

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 $_RR = R1$ 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 $j \in \{1, \ldots, m\}$ 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 $i = 1, \ldots, j-1,\ j+1, \ldots, m$. This implies that

$$\pi(\mathbf{0}, x_j, \mathbf{0}) = \pi(x_1, \ldots, x_{j-1},\ x_{j+1}, \ldots, x_m) \implies \pi(x_1, \ldots, x_{j-1}, -x_j,\ x_{j+1}, \ldots, x_m) = 0$$

So $(x_1, \ldots, x_{j-1}, -x_j,\ x_{j+1}, \ldots, x_m) \in \ker \pi$. By assumption π is isomorphism, so it is injective and has trivial kernel, indicating that $(x_1, \ldots, x_{j-1}, -x_j,\ x_{j+1}, \ldots, x_m) = (0, \ldots, 0)$ and thus $x_j = 0$, which is a contradiction.

[$2 \implies 3$]. 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 there is a unique representation.

[$3 \implies 1$]. Define $\pi : N_1 \times \cdots \times N_m \to N_1 + \cdots + N_m$ such that $(x_1, \ldots, x_m) \mapsto x_1 + \cdots + x_m$. It is easy to verify that π is a R-module homomorphism and is surjective. For injectivity, suppose that

$$\pi(x_1, \ldots, x_m) = \pi(y_1, \ldots, y_m)$$

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 $i = 1, 2, \ldots, m$. $\square$

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 a (internal) direct sum and we denote it by

$$\bigoplus_{i=1}^{m} N_i$$

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:

$$\begin{tikzcd}
A \arrow[r, hook, "\iota"] \arrow[dr, "\varphi"'] & F \arrow[d, dashed, "\exists!\Phi"] \\
& M
\end{tikzcd}$$

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. $\square$

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:

$$\begin{tikzcd} A \arrow[r, hook, "\iota"] \arrow[dr, "\varphi"'] & \iota(A) \arrow[d, "\varphi'"] \\ & M \end{tikzcd}$$

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

$$\begin{tikzcd} \iota(A) \arrow[r, hook, "j"] \arrow[dr, "\varphi'"'] & F \arrow[d, dashed, "\exists! g"] \\ & M \end{tikzcd}$$

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

$$\begin{tikzcd} A \arrow[r, hook, "\iota"] \arrow[dr, "\varphi"'] & \iota(A) \arrow[r, "j"] \arrow[d, "\varphi'"] & F \arrow[dl, dashed, "g"] \\ & M & \end{tikzcd}$$

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. $\square$

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

$$\begin{tikzcd}
A \arrow[r, hook, "\iota"] \arrow[dr, "j"'] & F_1 \arrow[d, dashed, "\exists!\Phi"] \\
& F_2
\end{tikzcd}$$

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

$$\begin{tikzcd}
A \arrow[r, hook, "j"] \arrow[dr, "\iota"'] & F_2 \arrow[d, dashed, "\exists!\Psi"] \\
& F_1
\end{tikzcd}$$

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. $\square$

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:*

$$\begin{tikzcd} M \times N \arrow[r, hook, "\iota"] \arrow[dr, "\beta"'] & M \otimes_R N \arrow[d, dashed, "\exists!\Phi"] \\ & L \end{tikzcd}$$

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 $\zeta \circ j = \beta$:

$$\begin{tikzcd} M \times N \arrow[r, hook, "j"] \arrow[dr, "\beta"'] & F(M \times N) \arrow[d, dashed, "\exists!\zeta"] \\ & L \end{tikzcd}$$

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 $\Phi(m \otimes n) := \zeta(m, n)$.

$$\begin{tikzcd} M \times N \arrow[r, hook, "\iota"] \arrow[dr, "\beta"'] & F(M \times N)/H \arrow[d, dashed, "\exists!\Phi"] \\ & L \end{tikzcd}$$

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

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

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 $\Psi = \Phi$. $\square$

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 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 $M := \operatorname{Hom}_S(Y_S, Z_S)$ is an abelian group where $(\alpha + \beta)(y) := \alpha(y) + \beta(y)$. Then 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 be omitted 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. $\square$

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.

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:*

$$\begin{tikzcd} N \arrow[r, "j"] \arrow[dr, "\gamma"'] & S \otimes_R N \arrow[d, dashed, "\Phi"] \\ & L \end{tikzcd}$$

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 $\Phi\circ\iota = \beta$.

$$\begin{tikzcd} S\times N \arrow[r, "\iota"] \arrow[dr, "\beta"'] & S\otimes_R N \arrow[d, dashed, "\Phi"] \\ & L \end{tikzcd}$$

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 $\Phi\circ j = \beta$:

$$\begin{tikzcd} N \arrow[r, "j"] \arrow[dr, "\beta"'] & S\otimes_R N \arrow[d, dashed, "\Phi"] \\ & L \end{tikzcd}$$

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 $N/K\subseteq N/\ker\beta\subseteq N/\ker j$. 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 $\varphi : R \to R$ where $r \mapsto r$ 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

$$\begin{tikzcd}
n \arrow[rrr, bend left, mapsto] & \in N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & R \otimes_R N \arrow[d, dashed, "\Phi"] & \ni 1 \otimes n \\
& & N &
\end{tikzcd}$$

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

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:

$$\begin{tikzcd}
n \arrow[rrr, bend left, mapsto] \arrow[ddrr, mapsto] & \in \mathbb{Z} \arrow[r, "\iota"] \arrow[dr, "\beta"'] & \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} \arrow[d, dashed, "\Phi"] & \ni 1 \otimes n \\
& & \mathbb{Q} & \\
& & \frac{n}{1} \arrow[u, phantom, "\cup" rotate=90] &
\end{tikzcd}$$

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:

$$\begin{tikzcd}
(m,n) \arrow[r, phantom, "\in"] \arrow[rrr, bend left] & M \times N \arrow[r, "\iota"] \arrow[dr, "\beta"'] & M \otimes_R N \arrow[d, dashed, "\Phi"] \arrow[r, phantom, "\ni"] & m \otimes n \\
& & L &
\end{tikzcd}$$

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:

$$\begin{tikzcd}
(m,n) \arrow[rrrr, mapsto, bend left] \arrow[ddrr, mapsto] & \in M \times N \arrow[r, "\iota"] \arrow[dr, "\gamma"'] & M \otimes_R N \arrow[d, dashed, "\exists!\Phi"] & \ni & m \otimes n \\
& & M' \otimes_R N' \arrow[d, phantom, "\rotatebox[origin=c]{-90}{$\ni$}"] & & \\
& & \alpha(m) \otimes \beta(n) & &
\end{tikzcd}$$

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 readability. Similarly we have the following commutative diagram:

$$\begin{tikzcd}
(m,n) \arrow[rrrr, mapsto, bend left] \arrow[ddrr, mapsto] & \in M \times N \arrow[r, "\iota"] \arrow[dr, "\gamma"'] & M \otimes_R N \arrow[d, dashed, "\exists!\Phi"] & \ni & m \otimes n \\
& & M'' \otimes_R N'' \arrow[d, phantom, "\rotatebox[origin=c]{-90}{$\ni$}"] & & \\
& & (\lambda\alpha)(m) \otimes (\mu\beta)(n) & &
\end{tikzcd}$$

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 ${}_S L$. 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 $\Phi\left((m \otimes_R n) \otimes_S \ell\right) = m \otimes_R (n \otimes_S \ell)$. 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:

$$
\begin{tikzcd}
(m,n) \arrow[r, phantom, "\in"] \arrow[rrrr, mapsto, bend left] \arrow[ddrrr, mapsto] & M \times N \arrow[rr, "\iota"] \arrow[drr, "\beta"'] & & M \otimes_R N \arrow[d, dashed, "\exists!\Phi_\ell"] \arrow[r, phantom, "\ni"] & m \otimes n \arrow[ddl, mapsto, bend left] \\
 & & & M \otimes_R (N \otimes_S L) \arrow[d, phantom, "\cup"] & \\
 & & & m \otimes (n \otimes \ell) &
\end{tikzcd}
$$

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

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

And thus we obtain the following commutative diagram:

$$
\begin{tikzcd}
(m \otimes n, \ell) \arrow[r, phantom, "\in"] \arrow[rrrr, mapsto, bend left] \arrow[ddrrr, mapsto] & (M \otimes_R N) \times L \arrow[rr, "\iota'"] \arrow[drr, "\Phi"'] & & (M \otimes_R N) \otimes_S L \arrow[d, dashed, "\exists!\Psi"] \arrow[r, phantom, "\ni"] & (m \otimes n) \otimes \ell \arrow[ddl, mapsto, bend left] \\
 & & & M \otimes_R (N \otimes_S L) \arrow[d, phantom, "\cup"] & \\
 & & & \Phi_\ell(m \otimes n) &
\end{tikzcd}
$$

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:

$$\begin{tikzcd}
(m\otimes n,\ell) \arrow[rrrrr, mapsto, bend left] \arrow[dddrrr, mapsto] & \in & (M\otimes_R N)\times L \arrow[r] \arrow[dr, "\tilde{\Psi}\circ\Psi"'] & (M\otimes_R N)\otimes_S L \arrow[d, dashed, "\mathrm{id}"] & \ni & (m\otimes n)\otimes\ell \arrow[dddll, mapsto, bend left] \\
 & & & M\otimes_R (N\otimes_S L) & & \\
 & & & \rotatebox{90}{$\in$} & & \\
 & & & (m\otimes n)\otimes\ell & &
\end{tikzcd}$$

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. $\square$

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 $M_R, M'_R, {}_RN, {}_RN'$ 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:

$$\begin{tikzcd}
((m,m'),n) \arrow[dddrrr, mapsto] & \in & (M\oplus M')\times N \arrow[r] \arrow[dr, "\beta"'] & (M\oplus M')\otimes_R N & \ni & (m,m')\otimes n \\
 & & & (M\otimes_R N)\oplus(M'\otimes_R N) & & \\
 & & & \rotatebox{90}{$\in$} & & \\
 & & & (m\otimes n, m'\otimes n) & &
\end{tikzcd}$$

Diagram 2:

$$\begin{tikzcd}
(m,n) \arrow[dddrrr, mapsto] & \in & M\times N \arrow[r] \arrow[dr, "\gamma"'] & M\otimes_R N \\
 & & & (M\oplus M')\otimes_R N \\
 & & & \rotatebox{90}{$\in$} \\
 & & & (m,0)\otimes n
\end{tikzcd}$$

Diagram 3:

$$\begin{tikzcd}
(m',n) \arrow[dddrrr, mapsto] & \in & M'\times N \arrow[r] \arrow[dr, "\delta"'] & M'\otimes_R N \\
 & & & (M\oplus M')\otimes_R N \\
 & & & \rotatebox{90}{$\in$} \\
 & & & (0,m')\otimes n
\end{tikzcd}$$

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:

$$
\begin{tikzcd}
((m,m'),n) \arrow[r, phantom, "\in"] \arrow[rrr, mapsto, bend left] \arrow[ddrr, mapsto] & (M \oplus M') \times N \arrow[r] \arrow[dr, "\beta"'] & (M \oplus M') \otimes_R N \arrow[r, phantom, "\ni"] \arrow[d, dashed, "\exists! \Phi"] & (m,m') \otimes n \arrow[ddl, mapsto, bend left] \\
 & & (M \otimes_R N) \oplus (M' \otimes_R N) \arrow[d, phantom, "\rotatebox[origin=c]{90}{$\in$}"] & \\
 & & (m \otimes n, m' \otimes n) &
\end{tikzcd}
$$

Diagram 2:

$$
\begin{tikzcd}
(m,n) \arrow[r, phantom, "\in"] \arrow[rrr, mapsto, bend left] \arrow[ddrr, mapsto] & M \times N \arrow[r] \arrow[dr, "\gamma"'] & M \otimes_R N \arrow[r, phantom, "\ni"] \arrow[d, dashed, "\exists! \varphi"] & m \otimes n \arrow[ddl, mapsto, bend left] \\
 & & (M \oplus M') \otimes_R N \arrow[d, phantom, "\rotatebox[origin=c]{90}{$\in$}"] & \\
 & & (m,0) \otimes n &
\end{tikzcd}
$$

Diagram 3:

$$
\begin{tikzcd}
(m',n) \arrow[r, phantom, "\in"] \arrow[rrr, mapsto, bend left] \arrow[ddrr, mapsto] & M' \times N \arrow[r] \arrow[dr, "\beta"'] & M' \otimes_R N \arrow[r, phantom, "\ni"] \arrow[d, dashed, "\exists! \varphi'"] & m' \otimes n \arrow[ddl, mapsto, bend left] \\
 & & (M \oplus M') \otimes_R N \arrow[d, phantom, "\rotatebox[origin=c]{90}{$\in$}"] & \\
 & & (0,m') \otimes n &
\end{tikzcd}
$$

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. Note

$$R^m = \bigoplus_{i=1}^{m} R$$

and so

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

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
$$\dots \xrightarrow{d_{-2}} X_{-1} \xrightarrow{d_{=1}} X_0 \xrightarrow{d_0} X_1 \xrightarrow{d_1} \dots$$
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, first suppose that the sequence is exact. Then $\ker\alpha = \operatorname{im} 0 = \{0\}$, and thus α is injective. For the converse statement, suppose that α is injective, then $\ker\alpha = 0$. On the other hand, the map from 0 to X is a zero map. Together we have $\ker\alpha = 0 = \operatorname{im} 0$, so the sequence is exact.

For the second statement, first suppose that the sequence is exact. Then $\operatorname{im}\beta = \ker 0$. However, the zero map $0 : Z \to 0$ sends everything to 0, so the kernel is Z. Together we have $\operatorname{im}\beta = Z$, thus β is surjective. For the converse statement, suppose that β is surjective. Then $\operatorname{im}\beta = Z$. On the other hand, the map from Z to 0 is a zero map, so $\ker 0 = Z$. Together we have $\operatorname{im}\beta = Z = \ker 0$, so 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:
$$\begin{tikzcd}
s \arrow[rrrr, bend left, mapsto] \arrow[dddrrr, mapsto] & \in & S \arrow[r] \arrow[dr] & F(S) \arrow[d, dashed, two heads] & \bullet \arrow[dddl, bend left, mapsto] \\
 & & & M & \\
 & & & \cup & \\
 & & & s &
\end{tikzcd}$$

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:

$$\begin{tikzcd} 0 \arrow[r] & X \arrow[r] \arrow[d, "\gamma_1"'] & Y \arrow[r] \arrow[d, "\gamma_2"'] & Z \arrow[r] \arrow[d, "\gamma_3"'] & 0 \\ 0 \arrow[r] & X' \arrow[r] & Y' \arrow[r] & Z' \arrow[r] & 0 \end{tikzcd}$$

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:

$$\begin{tikzcd} 0 \arrow[r] & X \arrow[r] \arrow[d, "\mathrm{id}"'] & Y \arrow[r] \arrow[d, "g"'] & Z \arrow[r] \arrow[d, "\mathrm{id}"'] & 0 \\ 0 \arrow[r] & X \arrow[r] & Y' \arrow[r] & Z \arrow[r] & 0 \end{tikzcd}$$

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:

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

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:*

$$\begin{tikzcd} M_1 \arrow[r, "g_1"] \arrow[d, "f_1"] & M_2 \arrow[r, "g_2"] \arrow[d, "f_2"] & M_3 \arrow[r, "g_3"] \arrow[d, "f_3"] & M_4 \arrow[r, "g_4"] \arrow[d, "f_4"] & M_5 \arrow[d, "f_5"] \\ N_1 \arrow[r, "h_1"] & N_2 \arrow[r, "h_2"] & N_3 \arrow[r, "h_3"] & N_4 \arrow[r, "h_4"] & N_5 \end{tikzcd}$$

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. $\square$

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. $\Longrightarrow$ 2. $\Longrightarrow$ 3. $\Longrightarrow$ 4. $\Longrightarrow$ 1..

[1. $\Longrightarrow$ 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 the map from 0 to X is a zero map, so $\ker\alpha = \operatorname{im} 0$ is trivial, meaning that 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:

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

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:

$$\begin{tikzcd}
0 \arrow[r, "0"] \arrow[d, leftrightarrow, "\mathrm{id}"] & X \arrow[r, "\alpha"'] \arrow[d, leftrightarrow, "\mathrm{id}"] & Y \arrow[r, "\beta"'] \arrow[l, bend right, "\delta"'] \arrow[d, "\varphi"] & Z \arrow[r, "0"] \arrow[d, leftrightarrow, "\mathrm{id}"] & 0 \arrow[d, leftrightarrow, "\mathrm{id}"] \\
0 \arrow[r, "0"] & X \arrow[r, "\iota"] & X \oplus Z \arrow[r, "\pi"] & Z \arrow[r, "0"] & 0
\end{tikzcd}$$

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:

$$\begin{tikzcd}
 & & y \arrow[rr, mapsto] & & \beta(y) \arrow[dddddd, leftrightarrow, bend left=40] & \\
 & & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} & \\
0 \arrow[r, "0"] & X \arrow[r, "\alpha"'] & Y \arrow[rr, "\beta"'] & & Z \arrow[r, "0"] & 0 \\
0 \arrow[u, leftrightarrow, "\mathrm{id}"'] \arrow[d, leftrightarrow] & X \arrow[u, leftrightarrow, "\mathrm{id}"'] \arrow[d, leftrightarrow] & & & Z \arrow[u, leftrightarrow, "\mathrm{id}"'] \arrow[d, leftrightarrow] & 0 \arrow[u, leftrightarrow, "\mathrm{id}"'] \arrow[d, leftrightarrow] \\
0 \arrow[r, "0"] & X \arrow[r, "\iota"] & X \oplus Z \arrow[rr, "\pi"] & & Z \arrow[r, "0"] & 0 \\
 & & \rotatebox{-90}{$\in$} & & \rotatebox{-90}{$\in$} & \\
 & & (0, \beta(y)) \arrow[rr, mapsto] & & \beta(y) &
\end{tikzcd}$$

with $Y \xrightarrow{\varphi} X \oplus Z$ the middle vertical map.

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. $\square$

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

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

implies that we have the SES

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

Proof. Suppose β is injective. Let $f \in \operatorname{Hom}_R(V, X)$ such that $\beta \circ f = 0$ for every $v \in V$. Then for any $v \in V$ we have

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

since β is injective. This shows that f is a zero map, so β_* is injective. $\square$

Remark 2.1.14. In general β_* is not surjective even if β 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

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

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

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_R(R,X) \arrow[r, "\alpha_*"] \arrow[d, leftrightarrow] & \mathrm{Hom}_R(R,Y) \arrow[r, "\beta_*"] \arrow[d, leftrightarrow] & \mathrm{Hom}_R(R,Z) \arrow[r] \arrow[d, leftrightarrow] & 0 \\
0 \arrow[r] & X \arrow[r, "\alpha"'] & Y \arrow[r, "\beta"'] & Z \arrow[r] & 0
\end{tikzcd}$$

where the linking between both sequences is the isomorphism defined above. We claim that the diagram is commutative. We only prove the commutativity between $\mathrm{Hom}_R(R, X) - \mathrm{Hom}_R(R, Y) - Y - X$, i.e. the first square. Let $f \in \mathrm{Hom}_R(R, X)$. 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 $f_x \in \mathrm{Hom}_R(R, X)$ 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 $f_y \in \mathrm{Hom}_R(R, Y)$ such that $f_y(1) = y$. Note that

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

But $\beta_*(f_y) \in \mathrm{Hom}_R(R, Z)$, and there is an isomorphism between $\mathrm{Hom}_R(R, Z)$ 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 $g_x \in \mathrm{Hom}_R(R, X)$ 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. $\mathrm{Hom}_R(X, Y \oplus Z) \cong \mathrm{Hom}_R(X, Y) \oplus \mathrm{Hom}_R(X, Z)$
2. $\mathrm{Hom}_R(X \oplus Y, Z) \cong \mathrm{Hom}_R(X, Z) \oplus \mathrm{Hom}_R(Y, Z)$

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. $\square$

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

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

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.*
$$\begin{tikzcd} & P \arrow[dl, dashed, "\exists g"'] \arrow[d, "f"] & \\ Y \arrow[r, "\beta"'] & Z \arrow[r] & 0 \end{tikzcd}$$

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:
$$\begin{tikzcd} & & & P \arrow[dl, dashed, "\exists g"'] \arrow[d, leftrightarrow, "\mathrm{id}_P"] & \\ 0 \arrow[r] & X \arrow[r, "\iota"] & Y \arrow[r, "\pi"] & P \arrow[r] & 0 \end{tikzcd}$$
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 α_* is injective, 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:
$$\begin{tikzcd} s \arrow[r, mapsto] \arrow[d, phantom, sloped, "\in"] & s \arrow[d, phantom, sloped, "\in"] \\ S \arrow[r, hook] & F(S) \arrow[d, two heads, "\pi"] \\ & P \arrow[u, bend right=60, "\iota"'] \arrow[d, "f"] \\ Y \arrow[r, "\beta"'] & Z \end{tikzcd}$$

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 inded well-defined since β is surjective. Thus we now have the following diagram:

$$\begin{tikzcd}
 & & s \arrow[r, mapsto] \arrow[dddd, bend right, start anchor=west, to=5-1] & s \arrow[ddddrr, bend left] & & \\
 & & \rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} & & \\
 & & S \arrow[r, hook] \arrow[dd, "\varphi"'] & F(S) \arrow[d, "\pi"] \arrow[ddl, dashed, "\exists g"] & & \\
 & & & P \arrow[d, "f"] \arrow[u, bend right, "\iota"'] & & \\
m_s \arrow[rrrrr, bend right] & \in & Y \arrow[r, "\beta"'] & Z & \ni & (f \circ \pi)(s) = \beta(m_s)
\end{tikzcd}$$

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:

$$\begin{tikzcd}
s \arrow[r, mapsto] & s \\
\rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} \\
S \arrow[r, hook] \arrow[dr, "f\circ\pi = \beta\circ g"'] & F(S) \arrow[d, shift right, "f\circ\pi"'] \arrow[d, shift left, "\beta\circ g"] \\
 & Z
\end{tikzcd}$$

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. □

Remark 2.2.2. As shown and stated previously in Proposition 2.1.13, if $\beta : X \to Y$ is exact, then $\beta_* : \mathrm{Hom}_R(V, X) \to \mathrm{Hom}_R(V, Y)$ is exact 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 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

$$\begin{tikzcd} X \arrow[r, "\alpha"] \arrow[dr, "\beta\circ\alpha"'] & Y \arrow[d, "\beta"] \\ & Z \end{tikzcd}$$

then we have the commutative diagram:

$$\begin{tikzcd} \mathcal{F}(X) \arrow[r, "\mathcal{F}(\alpha)"] \arrow[dr, "\mathcal{F}(\beta\circ\alpha)=\mathcal{F}(\beta)\circ\mathcal{F}(\alpha)"'] & \mathcal{F}(Y) \arrow[d, "\mathcal{F}(\beta)"] \\ & \mathcal{F}(Z) \end{tikzcd}$$

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

$$\begin{tikzcd} X \arrow[r, "\alpha"] \arrow[dr, "\beta\circ\alpha"'] & Y \arrow[d, "\beta"] \\ & Z \end{tikzcd}$$

  then we have the commutative diagram:

$$\begin{tikzcd} \mathcal{F}(X) & \mathcal{F}(Y) \arrow[l, "\mathcal{F}(\alpha)"'] \\ & \mathcal{F}(Z) \arrow[u, "\mathcal{F}(\beta)"'] \arrow[ul, "\mathcal{F}(\beta\circ\alpha)=\mathcal{F}(\alpha)\circ\mathcal{F}(\beta)"] \end{tikzcd}$$

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, in general, 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. 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.

6. 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:

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

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

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

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. In other words, for all $y \in Y$ we have $f(\beta(y)) = 0$. By assumption β is surjective, thus let 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.

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 $f(z) = g(y)$ 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-modole homomorphism by assumption. Next, for the action, 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 part of the statement.

For the second statement, the forward direction is a immediate result of 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

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

In other words, take $V = \text{coker } \beta$. 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 we have $\alpha^* \circ \beta^*$ is zero map. So

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

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

Lastly, we show that $\ker\beta \subseteq \operatorname{im}\alpha$. Let $V = \text{coker } \alpha = Y/\operatorname{im}\alpha$. 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 $g \in Z \to V$ 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-homomorphism $\varphi : Z \to Y$ and R-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

$$\begin{tikzcd}
 & Q \\
Y \arrow[ur, dashed, "\exists f"] & Z \arrow[l, hook', "\varphi"] \arrow[u, "g"']
\end{tikzcd}$$

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

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

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 $\gamma |_{Y'} = f$. 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

$$r\left(Q/Q'\right) = rQ/Q' = Q/Q'$$

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

Example 2.3.4.

1. Q is injective $\mathbb{Z}$-module because $\mathbb{Q}$ is divisible. However $\mathbb{Z}$ is not injective $\mathbb{Z}$-module because $2\mathbb{Z} \neq \mathbb{Z}$. But $\mathbb{Z}$ is a free module, so $\mathbb{Q}/\mathbb{Z}$ is injective module. Recall we have seen that $\mathbb{Q}/\mathbb{Z}$ is not projective.
2. Let F be a field. Then any F-module is injective.
3. Over any ring R, any injective R-module is divisible.

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 Q-module. Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module. For any $n \in \mathbb{Z}$ is non-zero, 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 injective $\mathbb{Z}$-module.

Next, observe that $\ker\pi \subseteq F(A) \cong \bigoplus_{a\in A}\mathbb{Z}$ and we can embeed $\bigoplus_{a\in A}\mathbb{Z}$ 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 $Q/\ker\pi$, an injective $\mathbb{Z}$-module. ☐

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 $\operatorname{Hom}_Z(R, M) \subseteq \operatorname{Hom}_Z(R, Q)$ due to the following arguments:

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

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

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

And we will 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 struction to R.

Next, to show that $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module, let X and Y be any R-modules, and 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:

$$\begin{tikzcd} X \arrow[r, hook, "\alpha"] \arrow[d, "g"'] & Y \arrow[dl, dashed] \\ \mathrm{Hom}_{\mathbb{Z}}(R, Q) & \end{tikzcd}$$

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.

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

$$\begin{tikzcd} X \arrow[r, hook, "\alpha"] \arrow[d, "g'"'] & Y \arrow[dl, dashed, "\exists f'"] \\ Q & \end{tikzcd}$$

In particular $f' \circ \alpha = g'$. Define $f : Y \to \mathrm{Hom}_Z(R, Q)$ by $y \mapsto f_y$ such that f_y is defined by $f_y : r \mapsto f'(ry)$. 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:

$$\begin{tikzcd} X \arrow[r, hook, "\alpha"] \arrow[d, "g"'] & Y \arrow[dl, dashed, "\exists f"] \\ \mathrm{Hom}_{\mathbb{Z}}(R, Q) & \end{tikzcd}$$

Therefore $\mathrm{Hom}_Z(R, Q)$ is an injective R-module. This completes the proof. $\square$

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. *If I is isomorphic with a submodule of Y, then the following SES splits:*

$$0 \to I \to Y \to Y/I \to 0$$

And hence $I \mid Y$.

Proof. Tutorial questions. $\square$

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.

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

$$\begin{tikzcd} X \arrow[r, "\alpha"] \arrow[dr, "\beta\circ\alpha"'] & Y \arrow[d, "\beta"] \\ & Z \end{tikzcd}$$

  Then we have that

$$\begin{tikzcd} \mathcal{F}(X) \arrow[r, "\mathcal{F}(\alpha)"] \arrow[dr, "\mathcal{F}(\beta\circ\alpha)"'] & \mathcal{F}(Y) \arrow[d, "\mathcal{F}(\beta)"] \\ & \mathcal{F}(Z) \end{tikzcd}$$

  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 $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ 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 $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ 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 $\beta\circ\alpha = 0$. Thsu $(1\otimes\beta)(1\otimes\alpha) = 1\otimes(\beta\circ\alpha) = 1 \otimes 0 = 0$. 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:

$$\begin{tikzcd}
R \otimes_R X \arrow[r, "1\otimes\alpha"] \arrow[d, leftrightarrow] & R \otimes_R Y \arrow[r, "1\otimes\beta"] \arrow[d, leftrightarrow] & R \otimes_R Z \arrow[r] \arrow[d, leftrightarrow] & 0 \\
X \arrow[r, "\alpha"] & Y \arrow[r, "\beta"] & Z \arrow[r] & 0
\end{tikzcd}$$

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. $\square$

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. *Projection (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 $0 \to X \xrightarrow{\alpha} Y$ is exact, then $0 \to D \otimes_R X \xrightarrow{1\otimes\alpha} D \otimes_R Y$ 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 $(\bigoplus R) \otimes_R X \cong \bigoplus(R \otimes RX)$. We have also seen previously that $R \otimes_R X \cong X$. Altogether we obtain the following commutative diagram:

$$\begin{tikzcd}
 & & F \otimes_R X \arrow[r, "1\otimes\alpha"] \arrow[d, leftrightarrow] & F \otimes_R Y \arrow[d, leftrightarrow] & & \\
\sum(\mathbb{1}_a \otimes x_a) \arrow[rrrrr, mapsto, bend left] & \in & (\bigoplus R) \otimes_R X \arrow[r] \arrow[d, leftrightarrow] & (\bigoplus R) \otimes_R Y \arrow[d, leftrightarrow] & \ni & \sum(\mathbb{1}_a \otimes \alpha(x_a)) \arrow[d, mapsto] \\
\sum(1 \otimes x_a) \arrow[u, mapsto] & \in & \bigoplus(R \otimes_R X) \arrow[r] \arrow[d, leftrightarrow] & \bigoplus(R \otimes_R Y) \arrow[d, leftrightarrow] & \ni & \sum(1 \otimes \alpha(x_a)) \arrow[d, mapsto] \\
\sum x_a \arrow[u, mapsto] & \in & \bigoplus_{a\in A} X \arrow[r, "\varphi"] & \bigoplus_{a\in A} Y & \ni & \sum \alpha(x_a)
\end{tikzcd}$$

where $\mathbb{1}_a$ denotes the direct sum indexed by A which is only 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:

$$\begin{tikzcd}
a \otimes x \arrow[rrrrr, mapsto, bend left] & \in & F \otimes_R X \arrow[r, "1\otimes\alpha"] \arrow[d, leftrightarrow] & F \otimes_R Y \arrow[dd, leftrightarrow] & \ni & a \otimes \alpha(x) \arrow[dd, mapsto] \\
(a+0) \otimes x \arrow[u, mapsto] & \in & (P \oplus P') \otimes_R X \arrow[d, leftrightarrow] & & & \\
(a \otimes x, 0) \arrow[u, mapsto] & \in & (P \otimes_R X) \oplus (P' \otimes_R X) \arrow[r] & (P \otimes_R Y) \oplus (P' \otimes_R Y) & \ni & (a \otimes \alpha(x), 0)
\end{tikzcd}$$

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. $\square$

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 $\mathbb{Q}/\mathbb{Z}$.

Definition 2.4.7 (Functor adjunction)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be categories. Let X and Z be an object of $\mathcal{C}$ and $\mathcal{D}$ respectively. 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 $\mathrm{Mor}_{\mathcal{D}}(\mathcal{L}(X), Z) \cong \mathrm{Mor}_{\mathcal{C}}(X, \mathcal{R}(Z))$.

Theorem 2.4.8 (Tensor-Hom Adjunction)**.** *Let X be a right R-module, Y be a (R, S)-bimodule, and Z be a right S-module. Then $(- \otimes_R Y,\ \mathrm{Hom}_S(Y, -))$ is a pair of adjunct functors. In other words, we have an isomorphism of abelian group:*

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

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

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

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 map on their respective domain, i.e. they are isomorphisms.

We first need to show that f is well-defined, which will be broken down into several item. First, we show that $f(\varphi)$ is really an R-module homomorphism 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. 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 respective ψ'.

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

$$g : \psi \mapsto \psi' : X \otimes_R Y \to Z$$

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. $\square$

Remark 2.4.9. 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 2.4.10. *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 a surjective R-module homomorphism:

$$\begin{tikzcd} & P \otimes_R P' \arrow[dl, dashed, "?"'] \arrow[d, "h"] \\ X \arrow[r, two heads, "\beta"'] & Y \end{tikzcd}$$

We want to construct a map from $P \otimes_R P' \to X$. First, note that β induces the following surjective map

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

where $\alpha \mapsto \beta \circ \alpha$. This further induces a surjective map

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

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

$$\begin{tikzcd} & f(\gamma) \arrow[r, mapsto] \arrow[d, phantom, "\cap"] & (\beta_*) \circ (f(\gamma)) \arrow[d, phantom, "\cap"] \arrow[dr, mapsto, bend left] & \\ & \mathrm{Hom}_R(P, \mathrm{Hom}_R(P', X)) \arrow[r, two heads, "(\beta_*)_*"] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(P', Y)) \arrow[d, "g"] & \\ \gamma \arrow[uur, mapsto, bend left] \arrow[rrr, mapsto, bend right] & \in \quad \mathrm{Hom}_R(P \otimes_R P', X) \arrow[u, "f"] & \mathrm{Hom}_R(P \otimes_R, P', Y) \quad \ni & h \end{tikzcd}$$

where f and g are as defined in Theorem 2.4.8. Here the element γ is explicit defined according to the following argument:

- 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 $\beta \circ \gamma = h$. 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. $\square$

3 Chain Complex

3.1 Chain Complex and Homology

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

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

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)**.** Homology and cohomology detects failure of exactness. In particular, the n-th homology (cohomology) is 0 if and only if the n-th position of the chain (cochain) 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 (cochain) complexes)**.** Let $(X^\bullet, d^\bullet)$ and $(Y^\bullet, \delta^\bullet)$ be two (cochain) 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:

$$\begin{tikzcd}
\dots \arrow[r, "d^{n-1}"] & X^{n-1} \arrow[r, "d^n"] \arrow[d, "\varphi_{n-1}"] & X^n \arrow[r, "d^{n+1}"] \arrow[d, "\varphi_n"] & \dots \\
\dots \arrow[r, "\delta^{n-1}"] & Y^{n-1} \arrow[r, "\delta^n"] & Y^n \arrow[r, "\delta^{n+1}"] & \dots
\end{tikzcd}$$

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 $\overline{x} \mapsto \overline{\varphi(x)}$.*

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:

$$\begin{tikzcd}
\dots \arrow[r] & X^n \arrow[r, "d^{n+1}"] \arrow[d, "\varphi_n"] & X^{n+1} \arrow[r] \arrow[d, "\varphi_{n+1}"] & \dots \\
\dots \arrow[r] & Y^n \arrow[r, "\delta^{n+1}"] & Y^{n+1} \arrow[r] & \dots
\end{tikzcd}$$

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 $\overline{\varphi_n(x)} \in H^{n+1}(X)$. This shows that 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 means that $x, x' \in \ker \operatorname{im} d_n$, and so $x - x' \in \ker d_{n+1}$. It then follows from the definition of complexes that we have $x - x' \in \operatorname{im} d_n$, 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. $\square$

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 from some previous remark that exactness of a complex is equivalent to that the cohomology is trivial. According to the first statement we have obtained the long exact sequence

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

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.

Thus the proof is completed. $\square$

Definition 3.1.9 (Projective resolution)**.** Let V be an R-module. A projective resolution of V is an exact complex

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

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 3.1.10. Similarly we can define a free resolution, which is omitted here.

Proposition 3.1.11. *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

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

Let ε be d_0, and by our conrstruction 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. $\square$

With slight modification, a similar statement on free resolution can be proven:

Proposition 3.1.12. *Every R-module has a free resolution.*

Remark 3.1.13. If V is a projective R-module, then we have a projective resolution

$$\cdots \to 0 \to V \xrightarrow{\text{id}} V \to 0 \to 0 \ldots$$

Also, projective resolution is not unique, where the following

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

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

Definition 3.1.14 (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)

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

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

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

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

Proposition 3.1.15. *Let V and W be R-modules. Then*

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

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

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

By 1st isomorphism theorem on ε^* we get

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

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

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

This completes the proof. □

Example 3.1.16.

1. We compute $\operatorname{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$ for any abelian group D, where $m \geq 2$. From previous proposition we know
$$\operatorname{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$$
Let $\varphi \in \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$. By definition
$$m(\varphi(\overline{1})) = \varphi(\overline{m}) = 0$$
Thus we know
$$\operatorname{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \{d \in D : m \cdot d = 0\}$$
where we will denote it as ${}_mD$. To investigate the general case, we have to come up with the projective resolution:
$$\cdots \to 0 \to \mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \xrightarrow{\bmod m} \mathbb{Z}/m\mathbb{Z} \to 0$$
This is indeed a free resolution of $\mathbb{Z}/m\mathbb{Z}$ (one can verify the exactness easily). Thus taking hom we get
$$0 \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \xrightarrow{(\times m)^*} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \to 0 \to \dots$$
And it is clear that $\operatorname{Ext}^2_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) = 0$ for all $n \geq 2$. We compute the Ext^1 as follow: note $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \cong D$ with isomorphism given by $\varphi \mapsto \varphi(1)$. Thus:
$$\begin{tikzcd}
 & \varphi \arrow[rr, mapsto] \arrow[d, phantom, "\rotatebox{90}{$\in$}"] \arrow[ddd, bend right, mapsto] & & m\varphi \arrow[d, phantom, "\rotatebox{90}{$\in$}"] \arrow[ddd, bend left, mapsto] & & \\
0 \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \arrow[rr, "(\times m)^*"] \arrow[d] & & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \arrow[r] \arrow[d] & 0 \arrow[r] & \dots \\
0 \arrow[r] & D \arrow[rr] \arrow[d, phantom, "\rotatebox{90}{$\ni$}"] & & D \arrow[r] \arrow[d, phantom, "\rotatebox{90}{$\ni$}"] & 0 \arrow[r] & \dots \\
 & \varphi(1) \arrow[rr] & & m\varphi(1) = \varphi(m) & &
\end{tikzcd}$$
and $\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong D/mD$.

2.

explain on how to construct

Remark 3.1.17. 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 3.1.18 (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: 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 $f_n - g_n = \delta_{n+1}s_n + s_{n-1}d_n$.*

insert diagram

Proof. Idea: use projective to get a map, and do induction.

Part 2: Changing between straight square and slanted square, use projective module's property to get a lifting map, and perform induction.

proof

□

Definition 3.1.19 (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 $s_n : X^n \to Y^{n+1}$ 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 $' : Y^\bullet \to X^\bullet$ such that $f \circ f' \simeq \mathrm{id}_{Y^\bullet}$ and $f' \circ f \simeq \mathrm{id}_{X^\bullet}$.

Proposition 3.1.20.

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.

proof

□

Theorem 3.1.21. *The n-th cohomology group $\mathrm{Ext}^n_R(V, W)$ is independent, up to isomorphism, of the choice of the projective residue of V.*

Proof. □

proof

Theorem 3.1.22 (Snake Lemma)**.**

statement, proof is left as tutorial exercise

Proof. Left as tutorial exercise. □

Theorem 3.1.23 (Horseshoe Lemma)**.**

statement, proof is left as tutorial exercise

Proof. Left as tutorial exercise. □

Theorem 3.1.24. *Let $0 \to X \to Y \to Z \to 0$ be a SES of R-modules. Then we have a LES of abelian groups*
$$0 \to \mathrm{Hom}_R(Z, D) \to \mathrm{Hom}_R(Y, D) \to \mathrm{Hom}_R(X, D)$$
$$\to \mathrm{Ext}^1_R(Z, D) \to \mathrm{Ext}^1_R(Y, D) \to \mathrm{Ext}^1_R(X, D) \to \mathrm{Ext}^2_R(Z, D)$$

Proof. □

proof

Theorem 3.1.25. *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. □

proof