Syracuse University

# MATH 731: Rings and Modules

Professor: Dr. Dan Zacharia
Notes By: Caleb McWhorter

Fall 2014

Last Updated: June 20, 2019

## Contents

# 1 Elementary Category Theory

## 1.1 $R$-modules

**Definition** ($R$-module)**.** Let $R$ be a ring. A left $R$-module is an additive abelian group, $M$, together with a function $\cdot : R \times M \to M$ (the image of $(r, m)$ being denoted $r \cdot m$, or simply $rm$ when no confusion will likely arise) such that for all $r, s \in R$ and $m, n \in M$, the following axioms hold:

- $r(m+n) = rm + rn$
- $(r+s)\,m = rm + sm$
- $r(sm) = (rs)\,m$

If $1_R \in R$ then we also demand the following axiom and call $M$ a unitary $R$-module.

- $1_R\, m = m$

A right $R$-module is defined mutatis mutandis. If $M$ is both a left and right module, $M$ is called a $R$-bimodule.

**Remark.** We will often denote a left $R$-module $M$ as ${}_RM$, a right $R$-module as $M_R$, and a $R$-bimodule as ${}_RM_R$. For a $R$-bimodule, we do not require $rm = mr$ for all $m \in M$ and $r \in R$. Furthermore, if $R$ is a division ring (or field), then a unitary $R$-module is called a vector space.

**Example 1.1.**

(i) For any additive abelian group $A$, we can make $A$ into a $R$-module by defining $r \cdot a = 0$ for all $r \in R$ and $a \in A$.

(ii) If $A$ is an abelian group and $R := \operatorname{End} A$ is the endomorphism ring of $A$, then $A$ is a unitary $R$-module via the action $f \cdot a \overset{\text{def}}{=} f(a)$, i.e. via evaluation.

(iii) Let $S$ be a ring and $R = M_n(S)$. If $I \subset S$ is a two-sided ideal, e.g. $S = \mathbb{Z}$ and $I = 2\mathbb{Z}$, then
$$M(I) = \{M \in R \mid \text{ All entries of } M \text{ are in } I\}$$
is a two-sided ideal of $R$; that is, $M(I)$ is a $R$-bimodule. Furthermore, $S^n$ can be made into a $R$-bimodule: if $\bar{s} \in S^n$, write $\bar{s}$ as a row vector and compute $\bar{s}r$ via normal matrix multiplication. Writing $\bar{s} \in S^n$ as a column vector, compute $r\bar{s}$ via normal matrix multiplication.

$\triangleleft$

**Example 1.2.** Let $S$ be a ring and let $R = M_n(S)$. Let

$$P_i = \{M \in R \mid M \text{ is 0 everywhere except perhaps in the } i\text{th row.}\}$$

If $P_i$ is a right ideal of $R$, then $P_i$ is a right $R$-module. Why?

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ \vdots & 0 & \cdots & 0 & \vdots \\ \sim & \sim & \cdots & \sim & \sim \\ \vdots & 0 & \cdots & 0 & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} \sim & \sim & \sim & \sim & \sim \\ \sim & \sim & \sim & \sim & \sim \\ \sim & \sim & \sim & \sim & \sim \\ \sim & \sim & \sim & \sim & \sim \\ \sim & \sim & \sim & \sim & \sim \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ \vdots & 0 & \cdots & 0 & \vdots \\ \sim & \sim & \cdots & \sim & \sim \\ \vdots & 0 & \cdots & 0 & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

Of course, letting

$$Q_i = \{M \in R \mid M \text{ is 0 everywhere except perhaps in the } i\text{th column.}\}$$

If $Q_i$ is a left ideal of $R$, then $Q_i$ is a right $R$-module by the same argument as above mutatis mutandis. ◁

**Example 1.3.** Let $I$ be a left ideal of $R$. Then $I$ is a $R/I$-module via the action $r(x+I) := rx + I$ for all $r \in R$ and $x \in R$. However, $R/I$ need not be a ring unless $I \lhd R$; that is, if $I$ is a two-sided ideal of $R$. ◁

**Definition** (Ring Homomorphism)**.** Let $M, N$ be modules over a ring $R$. A function $f : M \to N$ is a $R$-module homomorphism provided for all $x, y \in M$ and $r \in R$

- $f(x+y) = f(x) + f(y)$
- $f(rx) = rf(x)$

**Definition** (Submodule)**.** Let $R$ be a ring, $M$ a $R$-module, and $N$ a nonempty subset of $M$. Then $N$ is a submodule of $M$ provided that $N$ is also a $R$-module, i.e. $N$ is an additive subgroup of $M$ and $rn \in N$ for all $n \in N$. Of course, that means $rx - y \in N$ for all $x, y \in N$ because $1_R \in R$.

**Example 1.4.** If $R$ is a ring and $f : M \to N$ is an $R$-module homomorphism, then $\ker f$ is a submodule of $M$ and $\operatorname{im} f$ is a submodule of $N$. If $P$ is a submodule of $N$, then $f^{-1}(N)$ is a submodule of $M$. ◁

**Remark.** Submodules are to modules as normal subgroups are to groups and ideals are to rings. Unlike groups and rings, we can always form the quotient module as the underlying structure of a module is an abelian group.

**Theorem 1.1.** *Let $N$ be a submodule of $M$ over a ring $R$. Then the quotient group $M/N$ is a $R$-submodule with the action of $R$ on $M/N$ given by $r(m+N) = rm + B$ for all $r \in R, m \in M$. The projection map $\pi : M \to M/N$ given by $m \mapsto m + N$ is a $R$-module homomorphism. Moreover, the map is an epimorphism.*

The Isomorphism Theorem for Rings carry over to modules mutatis mutandis:

**Theorem 1.2** (First Isomorphism Theorem). *If $\phi : M \to N$ is a R-map, then there is an R-isomorphism $\phi : M/\ker\phi \to N$ given by $m + \ker\phi \mapsto \phi(m)$.*

**Theorem 1.3** (Second Isomorphism Theorem). *If $A, B$ are submodules of a R-module M, then there is a R-isomorphism $A/(A \cap B) \to (A + B)/B$.*

**Theorem 1.4** (Third Isomorphism Theorem). *If $A \subseteq B \subseteq M$ is a tower of submodules of a R-module M, then there is an isomorphism*

$$(M/A)/(B/A) \longrightarrow M/B$$

**Theorem 1.5** (Fourth Isomorphism Theorem/Correspondence Theorem). *If N is a submodule of a R-module M, then there is a bijection of submodules of M containing N and submodules of $M/N$.*

## 1.2 Categories and Functors

**Definition** (Category). A category $\mathcal{C}$ consists of three things: a class obj $\mathcal{C}$ of objects, a set of morphisms $\mathrm{Hom}(A, B)$ for every ordered pair $(A, B)$ of objects of $\mathcal{C}$, and composition $\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$ denoted by $(f, g) \mapsto gf$ for every ordered triple $(A, B, C)$ of objects of $\mathcal{C}$. These are subject to the following axions:

(i) the Hom sets are pairwise disjoint; that is, for each $f \in \mathrm{Hom}(A, B)$ have a unique domain and a unique target.

(ii) for each object $A$ in obj $\mathcal{C}$, there is an identity morphism $1_A \in \mathrm{Hom}(A, A)$ such that $f1_A = f$ and $1_B f = f$ for all $f : A \to B$.

(iii) composition is associative: given morphisms $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, then $h(gf) = (hg)f$.

**Example 1.5.**

(i) **Sets.** The objects in this category are sets (not proper classes), morphisms are functions, and composition is the usual composition of functions.

(ii) **Groups**. The objects in this category are groups, morphisms are homomorphisms, and composition is the usual composition of functions.

(iii) **Top.** The objects in this category are topological spaces, morphisms are continuous functions, and composition is the usual composition of functions.

(iv) Any partially ordered set (poset) $P$ can be regarded as a category: the objects are elements of $P$, the Hom sets are either empty or have only one element

$$\mathrm{Hom}(x,y) = \begin{cases} \emptyset, & \text{if } x \not\preceq y \\ \{\iota_y^x\}, & \text{if } x \preceq y \end{cases}$$

where $\iota_y^x$ is the unique element in the Hom set when $x \preceq y$, and composition is given by $\iota_z^y \iota_y^x = \iota_z^x$.

(v) **Ab.** The objets are abelian groups, morphisms are homomorphisms, and composition is the usual function composition.

(vi) **Rings.** The objects are rings, morphisms are ring homomorphisms (we assume that rings have unity and for a morphism $\phi : R \to S$, $\phi(1_R) = 1_S$).

(vii) $_R$**Mod.** The objects are left $R$-modules, morphisms are $R$-homomorphisms, and composition is the usual function composition. Note that if $R = \mathbb{Z}$, then $_\mathbb{Z}$**Mod** $=$ **Ab**.

◁

**Definition** (Subcategory)**.** A category $\mathcal{S}$ is a subcategory of a category $\mathcal{C}$ if

(i) obj $\mathcal{S} \subseteq$ obj $\mathcal{C}$

(ii) $\mathrm{Hom}_\mathcal{S}(A,B) \subseteq \mathrm{Hom}_\mathcal{C}(A,B)$ for all $A, B \in$ obj $\mathcal{S}$

(iii) if $f \in \mathrm{Hom}_\mathcal{S}(A,B), g \in \mathrm{Hom}_\mathcal{S}(B,C)$, then $gf \in \mathrm{Hom}_\mathcal{S}(A,C)$ is equal to the composite $gf \in \mathrm{Hom}_\mathcal{C}(A,C)$

(iv) if $A \in$ obj $\mathcal{S}$, then $1_A \in \mathrm{Hom}_\mathcal{S}(A,A)$ is the same as $1_A \in \mathrm{Hom}_\mathcal{C}(A,A)$.

A subcategory $\mathcal{S}$ of $\mathcal{C}$ is a full subcategory if for all $A, B \in$ obj $\mathcal{S}$, $\mathrm{Hom}_\mathcal{S}(A,B) = \mathrm{Hom}_\mathcal{C}(A,A)$.

**Example 1.6.**

(i) **Ab.** is a subcategory of **Groups**. In fact, **Ab.** is a full subcategory of **Groups**.

(ii) **Haus.**, the category of Hausdorff topological spaces, is a subcategory of **Top.**.

(iii) If $\mathcal{C}$ is any category and $\mathcal{S} \subseteq \mathcal{C}$, then the full subcategory generated by $\mathcal{S}$, denoted by $\mathcal{S}$, is the subcategory with obj $(\mathcal{S}) = \mathcal{S}$ and with $\mathrm{Hom}_\mathcal{S}(A,B) = \mathrm{Hom}_\mathcal{C}(A,B)$ for all $A, B \in$ obj $(\mathcal{S})$.

◁

**Definition** (Functor)**.** If $\mathcal{C}$ and $\mathcal{D}$ are categories, a functor $T : \mathcal{C} \to \mathcal{D}$ is a function such that

(i) if $A \in \text{obj}\,\mathcal{C}$, then $T(A) \in \text{obj}\,\mathcal{D}$

(ii) if $f : A \to A'$ in $\mathcal{C}$, then $T(f) : T(A) \to T(A')$ in $\mathcal{D}$

(iii) if $A \xrightarrow{f} A' \xrightarrow{g} A''$ in $\mathcal{C}$, then $T(A) \xrightarrow{T(f)} T(A') \xrightarrow{T(g)} T(A'')$ in $\mathcal{D}$ and $T(gf) = T(g)T(f)$.

(iv) $T(1_A) = 1_{T(A)}$ for every $A \in \text{obj}\,\mathcal{C}$

**Remark.** A functor as defined above is a covariant functor as given $f : A \to A'$, $T(f) : T(A) \to T(A')$. If a functor is such that given $f : A \to A'$, $T(f) : T(A') \to T(A)$, then $T$ is called a *contravariant functor*.

**Example 1.7.**

(i) If $\mathcal{C}$ is a category, then the *identity functor* $1_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ is given by $1_{\mathcal{C}}(A) = A$ for all objects $A \in \text{obj}\,(\mathcal{C})$ and $1_{\mathcal{C}}(f) = f$ for all morphisms $f$ in the category $\mathcal{C}$.

(ii) If $\mathcal{C}$ is a category and $A \in \text{obj}\,(\mathcal{C})$, then the *Hom functor* $T_A : \mathcal{C} \to$ **Sets**, denoted $\text{Hom}(A, -)$, is defined by

$$T_A(B) = \text{Hom}(A, B) \text{ for all } B \in \text{obj}\,(\mathcal{C})$$

and if $f : B \to B'$, where $B' \in \text{obj}\,(\mathcal{C})$, then $T_A(f) : \text{Hom}(A, B) \to \text{Hom}(A, B')$ is given by

$$T_A(f) : h \mapsto fh.$$

We call $T_A(f) = \text{Hom}(A, f)$ the induced map, and denote it by $f_*$. Thus, $f_* : h \mapsto fh$. By the definition of a category, $\text{Hom}(A, B)$ is a set. Check that composition 'makes sense', is associative, and if $1_B : B \to B$ is the identity, then $(1_B)_* = 1_{\text{Hom}(A,B)}$.

(iii) Define the *forgetful functor* $U$ : **Groups** $\to$ **Sets** as follows: $U(G)$ is the underlying set of a group $G$ and $U(f)$ is a homomorphism $f$ regarded simply as a function. That is, the forgetful functor 'forgets' part of the group structure. One can define similar functors for **Rings.** and **Top.**.

$\triangleleft$

**Definition** (Natural Transformation)**.** Let $S, T : \mathcal{A} \to \mathcal{B}$ be (covariant) functors. A natural transformation $\tau : S \to T$ is a one-parameter family of morphisms in $\mathcal{B}$,

$$\tau = (\tau_A : SA \to TA)_{A \in \text{obj}\,\mathcal{A}}$$

making the following diagram commute for all $f : A \to A'$ in $\mathcal{A}$:

$$\begin{tikzcd} SA \arrow[r, "\tau_A"] \arrow[d, "Sf"'] & TA \arrow[d, "Tf"] \\ SA' \arrow[r, "\tau_{A'}"'] & TA' \end{tikzcd}$$

Just as functors are maps between categories, natural transformations are maps between functors.

**Theorem 1.6** (Yoneda Lemma)**.** *Let $\mathcal{C}$ be a category, $A \in obj(\mathcal{C})$, and $G : \mathcal{C} \to$ **Sets** be a covariant functor. Then there is a bijection*

$$\gamma : Nat(\mathrm{Hom}_{\mathcal{C}}(A, -), G) \longrightarrow G(A)$$

*given by $\gamma : \tau \mapsto \tau_A(1_A)$.*

## 1.3 Products and Coproducts

Let $\mathcal{I}$ denote *any* indexed set.

**Definition** (Product)**.** Let $\mathcal{C}$ be a category and $\{A_i \mid i \in \mathcal{I}\}$ be a family of objects of $\mathcal{C}$. A product for the family $\{A_i \mid i \in \mathcal{I}\}$ is an object $P$ of $\mathcal{C}$ together with a family of morphisms

$$\{\pi_i : P \to A_i \mid i \in \mathcal{I}\}$$

such that for any object $B$ and any family of morphisms

$$\{\varphi_i : B \to A_i \mid i \in \mathcal{I}\},$$

there is a unique morphism $\varphi : B \to P$ such that $\pi_i \circ \varphi = \varphi_i$ for all $i \in \mathcal{I}$. That is, there is a Universal Mapping Property.

$$\begin{tikzcd} B \arrow[rr, dotted, "\varphi"] \arrow[dr, "\varphi_i"'] & & P \arrow[dl, "\pi_i"] \\ & A_i & \end{tikzcd}$$

$$\begin{aligned} \varphi(B) &= \prod_{i \in \mathcal{I}} \varphi_i(B) \\ b &\mapsto \prod_{i \in \mathcal{I}} \varphi_i(b) \end{aligned}$$

A product $P$ of $\{A_i \mid i \in \mathcal{I}\}$ is usually denoted $\prod_{i \in \mathcal{I}} A_i$.

It is usually most helpful to describe products in terms of their commutative diagrams. A product for $\{A_1, A_2\}$ is a diagram of objects and morphisms $A_1 \xleftarrow{\pi_1} P \xrightarrow{\pi_2} A_2$ such that for any other diagram of the form $A_1 \xleftarrow{\varphi_1} B \xrightarrow{\varphi_2} A_2$, there is a unique morphism $\varphi : B \to P$ such that the following diagram commutes:

$$\begin{tikzcd} & P \arrow[dl, "\pi_1"'] \arrow[d, "\varphi"] \arrow[dr, "\pi_2"] & \\ A_1 & B \arrow[l, "\varphi_1"] \arrow[r, "\varphi_2"'] & A_2 \end{tikzcd}$$

It is important to note that a product need not exist in a given category. However, this will not be a problem for the categories with which we will be working—abelian groups and sets. For example in the category of sets, the Cartesian product $\prod_{i \in \mathcal{I}} A_i$ is a product of the family $\{A_i \mid i \in \mathcal{I}\}$.

**Theorem 1.7.** *If $(P, \{\pi_i\})$ and $(Q, \{\varphi_i\})$ are both products of the family $\{A_i \mid i \in \mathcal{I}\}$ objects of a category $\mathcal{C}$, then $P$ and $Q$ are equivalent.*

*Proof.* Since $P$, $Q$ are both products, they each have their family of morphisms to the $A_i$'s. We obtain the following commutative diagrams:

$$\begin{tikzcd} P \arrow[rr, dotted, "f"] \arrow[dr, "\pi_i"'] & & Q \arrow[dl, "\varphi_i"] \\ & A_i & \end{tikzcd} \qquad \begin{tikzcd} Q \arrow[rr, dotted, "g"] \arrow[dr, "\varphi_i"'] & & P \arrow[dl, "\pi_i"] \\ & A_i & \end{tikzcd}$$

Then $g \circ f : P \to P$, i.e

$$\begin{tikzcd} P \arrow[rr, dotted, "gf"] \arrow[dr, "\pi_i"'] & & P \arrow[dl, "\pi_i"] \\ & A_i & \end{tikzcd} \qquad \begin{tikzcd} Q \arrow[rr, dotted, "fg"] \arrow[dr, "\varphi_i"'] & & Q \arrow[dl, "\varphi_i"] \\ & A_i & \end{tikzcd}$$

But by definition, such a morphism is unique. We have the map $P \xrightarrow{1_P} P$. By uniqueness, we know that $gf = 1_P$. Similarly, we know that $fg = 1_Q$. But then $f, g$ are isomorphisms. □

We also obtain the dual definition and theorem by reversing arrows in the definition and theorem above, respectively.

**Definition** (Coproduct)**.** A coproduct (or sum) for the family $\{A_i \mid i \in \mathcal{I}\}$ of objects in a category $\mathcal{C}$ is an object $S$ of $\mathcal{C}$ together with a family of morphisms $\{\tau_i : A_i \to S \mid i \in \mathcal{I}\}$ such that for any object $S$ and any family of morphisms $\{\tau_i : A_i \to S \mid i \in \mathcal{I}\}$ there is a unique morphism $\varphi : S \to B$ such that

$$\varphi \circ \tau_i = \varphi_i$$

A coproduct $S$ of $\{A_i \mid i \in \mathcal{I}\}$ is denoted $\bigoplus_{i \in \mathcal{I}} A_i$, $\sum_{i \in \mathcal{I}} A_i$, or sometimes $\amalg_{i \in \mathcal{I}} A_i$.

Notice again these do *not* assure existence, just uniqueness.

**Theorem 1.8.** *If $(S, \{\tau_i\})$ and $(S', \{\lambda_i\})$ are both coproducts for the family $\{A_i \mid i\mathcal{I}\}$ of objects of a category $\mathcal{C}$, then $S$ and $S'$ are equivalent.*

*Proof.* Simply use the dual of the argument of Theorem 1.7. □

**Remark.** Given a finite collection of objects in a category, $\mathcal{A} = \{A_i\}_{i=1}^{n}$, the product and coproduct of $\mathcal{A}$ are isomorphic. The reader should prove this in the case of $R$-modules. [For the general case, the category need have a zero object, which we shall not discuss here.]

**Remark.** There are many ways to diagrammatically summarize the universal properties of products and coproducts. In addition to the diagrams given above, the ones below are also common (the product on the left and the coproduct on the right).

$$\begin{tikzcd}
 & B \arrow[dl, "f_\alpha"'] \arrow[d, dotted, "f"] \arrow[dr, "f_\beta"] & \\
A_\alpha & \prod_{i\in\mathcal{J}} A_i \arrow[l, "\pi_\alpha"] \arrow[r, "\pi_\beta"'] & A_\beta
\end{tikzcd}
\qquad
\begin{tikzcd}
 & B & \\
A_\alpha \arrow[ur, "f_\alpha"] \arrow[r, "i_\alpha"'] & \bigoplus_{i\in\mathcal{I}} A_i \arrow[u, dotted, "f"'] & A_\beta \arrow[ul, "f_\beta"'] \arrow[l, "i_\beta"]
\end{tikzcd}$$

## 2 Exact Sequences

### 2.1 Exactness

**Definition** (Exactness)**.** A pair of module homomorphisms $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ is said to be exact at $B$ provided $\operatorname{im} f = \ker g$. We represent 'visually' as

$$A \xrightarrow{f} B \xrightarrow{g} C.$$

For longer sequences,

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_n} A_n$$

is exact provided $\operatorname{im} f_i = \ker f_{i+1}$ for $1 \leq i \leq n-1$. For infinite sequences, we say the sequence is exact if and only if $\operatorname{im} f_i = \ker f_{i+1}$ for all $i$.

**Remark.** Generally, $A \xrightarrow{f} B \xrightarrow{g} C$ does not mean that we have exactness at $B$ but merely $gf = 0$.

**Example 2.1.**

(i) A sequence $0 \longrightarrow A \xrightarrow{f} B$ is exact if and only if $f$ is injective.

(ii) A sequence $B \xrightarrow{g} C \longrightarrow 0$ is exact if and only if $g$ is surjective.

(iii) A sequence $0 \longrightarrow A \xrightarrow{h} B \longrightarrow 0$ is exact if and only if $h$ is an isomorphism.

(iv) A sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is exact if and only if $f$ is injective, $g$ is surjective, and $\operatorname{im} f = \ker g$.

(v) Let $A$ be a submodule of $B$, then the sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} B/A \longrightarrow 0$ is exact.

(vi) If $A \subseteq B \subseteq C$ is a tower of submodules, then there is an exact sequence $0 \longrightarrow B/A \longrightarrow C/B \longrightarrow C/A \longrightarrow 0$.

◁

**Definition** (Short Exact Sequence)**.** An exact sequence of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is called a short exact sequence. This is also referred to as an extension of $A$ by $C$. [Note that other authors would define this to be an extension of $C$ by $A$, and others call the module $B$ the extension.]

**Proposition 2.1.** *If* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *is a short exact sequence, then* $A \cong \operatorname{im} f$ *and* $B/\operatorname{im} f \cong C$.

*Proof.* Clearly, $f$ is injective. Changing the target space gives an isomorphism $A \to \operatorname{im} f$. The First Isomorphism Theorem gives $B/\ker g \cong \operatorname{im} g$. By exactness, $\ker g = \operatorname{im} f$ and $\operatorname{im} g = C$. Therefore, $B/\operatorname{im} f \cong C$. □

## 2.2 The Short 5 Lemma

**Lemma 2.1** (The Short 5 Lemma)**.** *Let $R$ be a ring and let*

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

*be a commutative diagram of $R$-modules and $R$-module homomorphisms such that each row is a short exact sequence, then* *(i) If $\alpha, \gamma$ are monomorphisms then $\beta$ is a monomorphism.*

*(ii) If $\alpha, \gamma$ are epimorphisms then $\beta$ is an epimorphism.*

*(iii) If $\alpha, \gamma$ are isomorphisms then $\beta$ is an isomorphism.*

*Proof.* Notice that (iii) follows from the first two propositions, so it suffices to prove (i) and (ii). Our proof is by 'diagram chase'.

(i) Let $b \in B$ such that $\beta(b) = 0$, we want $b = 0$ (so we are going to show that the kernel is trivial).

$$\begin{tikzcd}
B \arrow[r, "g"] \arrow[d, "\beta"'] \arrow[dr, squiggly, bend left=80] \arrow[dr, squiggly, bend right=80] & C \arrow[d, "\gamma"] \\
B' \arrow[r, "g'"'] & C'
\end{tikzcd}$$

We look at $\gamma(g(b))$ and using the fact that the diagram commutes to find

$$\gamma(g(b)) = g'(\beta(b)) = g'(0) = 0.$$

But $\gamma$ is a monomorphism so that $g(b) = 0$. Therefore as the rows are exact, $g \in \ker g = \operatorname{im} f$. Then we have $b = f(a)$ for some $a \in A$. We can then use our other commuting diagram:

$$\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d, "f"'] \arrow[dr, squiggly, bend left=80] \arrow[dr, squiggly, bend right=80] & B \arrow[d, "\beta"] \\
A' \arrow[r, "f'"'] & B'
\end{tikzcd}$$

Using our initial assumption that $\beta(b) = 0$, we have

$$f'(\alpha(a)) = \beta(f(a)) = \beta(b) = 0.$$

Then $f'$ is injective so that it must be $\alpha(a) = 0$. We have $\alpha$ injective by assumption so that it must be that $a = 0$. Finally, we know that $b = f(a) = f(0) = 0$ so that $\beta$ must be a monomorphism.

(ii) Let $b' \in B'$. We want to show that there is a $b \in B$ such that $\beta(b) = b'$. We know that $g$, $g'$, and $\alpha$ are surjective. We proceed by going about the following diagram clockwise, "adjusting our target" so that we hit our goal "the long way" [about the diagram].

$$\begin{tikzcd}
B \arrow[r, "g"] \arrow[d, "\beta"'] \arrow[dr, squiggly, bend left=70] \arrow[dr, squiggly, bend right=70] & C \arrow[d, "\gamma"] \\
B' \arrow[r, "g'"'] & C'
\end{tikzcd}$$

We know that $g'(b') \in C$. As $\gamma$ is an epimorphism, there is some $c \in C$ such that $g'(b') = \gamma(c)$. But $g$ is an epimorphism so that $c = g(b)$ for some $b \in B$. Now we use the commutativity of the diagram to find

$$g'(\beta(b)) = \gamma(g(b)) = \gamma(c) = g'(b'),$$

which is only helpful in that we now know $g'(\beta(b)) - g'(b') = 0$; that is, that $g'\big(\beta(b) - b'\big) = 0$. What we is for $\beta(b) - b' = 0$. However, this is not necessarily so. But we do know that $\beta(b) - b' \in \ker g' = \operatorname{im} f$. So say $f'(a') = \beta(b) - b'$ for some $a' \in A'$. The $\beta(b) - b'$ is like an 'error'. Using the fact that $\alpha$ is an epimorphism, $a' = \alpha(a)$ for some $a \in A$. Now consider $b - f(a) \in B$ (this is our adjusting the 'error'). We have $\beta\big(b - f(a)\big) = \beta(b) - \beta(f(a))$.

Now using the commutativity of the diagram, we have

$$\beta(f(a)) = f'(\alpha(a)) = f'(a') = \beta(b) - b',$$

where the last equality follows from the last fact mentioned in the preceding paragraph. But then

$$f'(a') = \beta(b) - b' = \beta(b) - (\beta(b) - b') = b'.$$

Now as $f(a) \in B$, there exists a $b_0 \in B$ such that $b_0 = f(a)$ so that $\beta(b_0) = b'$. But then $\beta$ is an epimorphism. $\square$

## 2.3 Isomorphisms of Short Exact Sequences

Suppose we have two exact sequences $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ and $0 \longrightarrow A' \longrightarrow B' \longrightarrow C' \longrightarrow 0$ with isomorphisms $f : A \to A'$, $g : B \to B'$, and $h : C \to C'$. We can represent this diagrammatically below:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, shift left, "f"] & B \arrow[r] \arrow[d, shift left, "g"] & C \arrow[r] \arrow[d, shift left, "h"] & 0 \\
0 \arrow[r] & A' \arrow[r] \arrow[u, shift left, "f^{-1}"] & B' \arrow[r] \arrow[u, shift left, "g^{-1}"] & C' \arrow[r] \arrow[u, shift left, "h^{-1}"] & 0
\end{tikzcd}$$

An isomorphism between these two exact sequences will be maps $f, g, h$ such that $f, g, h$ are isomorphisms *and* they make the diagram commute. [The commutativity is key!] We need the diagram to commute with $f, g, h$ and $f^{-1}, g^{-1}, h^{-1}$. However, follows from the commutativity of the diagram with $f, g, h$: consider the following diagram of short exact sequences that commutes with isomorphisms $f$, $g$, $h$,

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "s"] \arrow[d, shift left, "f"] & B \arrow[r, "t"] \arrow[d, shift left, "g"] & C \arrow[r] \arrow[d, shift left, "h"] & 0 \\
0 \arrow[r] & A' \arrow[r, "s'"] \arrow[u, shift left, "f^{-1}"] & B' \arrow[r, "t'"] \arrow[u, shift left, "g^{-1}"] & C \arrow[r] \arrow[u, shift left, "h^{-1}"] & 0
\end{tikzcd}$$

We want to check if $sf^{-1}(a') = g^{-1}s'(a')$ for all $a' \in A'$. We have $f^{-1}(a') = a \in A$ for some $a$. That is, $f(a) = a'$. Then we have $s'(a') = s'f(a)$. The commutativity of the diagram in $f, g$ gives $s'f(a) = gs(a)$. Then

$$\begin{aligned}
s'f(a) &= s'(a') \\
gs(a) &= s'(a') \\
g^{-1}gs(a) &= g^{-1}s'(a') \\
s(a) &= g^{-1}s'(a') \\
sf^{-1}(a') &= g^{-1}s'(a'),
\end{aligned}$$

as desired. We need now check commutativity of the right square. That is, we want to show that $tg^{-1}(b') = h^{-1}t'(b')$ for all $b' \in B'$. We have $g^{-1}(b') = b \in B$ for some $b \in B$ so that $g(b) = b'$. The commutativity of the diagram in $g, h$ gives $t'g(b) = ht(b)$. Then

$$\begin{aligned}
t'(b') &= t'g(b) \\
t'(b') &= ht(b) \\
h^{-1}t'(b') &= h^{-1}ht(b) \\
h^{-1}t'(b') &= t(b) \\
h^{-1}t'(b') &= tg^{-1}(b'),
\end{aligned}$$

as desired. One can easily verify that isomorphisms of short exact sequences form an equivalence relation.

**Theorem 2.1.** *Let $R$ be a ring and*

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

*a short exact sequence of $R$-module homomorphisms. Then the following conditions are still equivalent:*

*(i) There is an $R$-module homomorphism $f' : M \to N$ with $f' \circ f = 1_N$.*

*(ii) There is an $R$-module homomorphism $g' : P \to M$ with $g \circ g' = 1_P$.*

*(iii) The given sequence is isomorphic with the identity maps on $N$ and $P$ to the direct sum exact sequence*

$$0 \longrightarrow N \xrightarrow{i_1} N \oplus P \xrightarrow{\pi_2} P \longrightarrow 0,$$

*and up to isomorphism there is only one such sequence. In particular, $M \cong N \oplus P$.*

*Proof.* It is clear that (iii) implies (i) and (ii): for (iii) implies (i), take $f'$ to be the projection of $M \cong N \oplus P$ onto $N$, while for (iii) implies (ii), take $g'$ to be the inclusion of $P$ into $M \cong N \oplus P$. It now remains to show (i) and (ii) imply (iii).

Now assume there is an $R$-module homomorphism $f' : M \to N$ with $f' \circ f = 1_N$. Consider the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "f"] \arrow[d, "1_N"] & M \arrow[r, "g"] \arrow[d, "(f'{,}g)"] & P \arrow[r] \arrow[d, "1_P"] & 0 \\
0 \arrow[r] & N \arrow[r, "i_1"] & N \oplus P \arrow[r, "\pi_2"] & P \arrow[r] & 0
\end{tikzcd}$$

One routinely verifies that the diagram is commutative with exact rows. As the left and right vertical maps are isomorphisms, so too must the middle map be an isomorphism by Lemma 2.1.

Now assume there is an $R$-module homomorphism $g' : P \to M$ with $g \circ g' = 1_P$. Consider the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "i_1"] \arrow[d, "1_N"] & N \oplus P \arrow[r, "\pi_2"] \arrow[d, "f+g'"] & P \arrow[r] \arrow[d, "1_N"] & 0 \\
0 \arrow[r] & N \arrow[r, "f"] & M \arrow[r, "g"] & P \arrow[r] & 0
\end{tikzcd}$$

where $(f + g')(n, p) = f(n) + g'(p)$. One routinely verifies that the diagram is commutative with exact rows. As the left and right vertical maps are isomorphisms, so too must the middle map be an isomorphism by Lemma 2.1. $\square$

**Definition** (Split Exact Sequence)**.** A short exact sequence satisfying any of the equivalent conditions of Theorem 2.1 is said to be split or a split exact sequence. The maps $h$, $k$ are sometimes called splittings.

**Remark.** If we change $R$-modules with groups and $R$-maps with group homomorphisms, the statements of Theorem 2.1 are no longer equivalent. Specifically, conditions (i) and (ii) are no longer equivalent. For a short exact sequence $1 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow 1$, (i) corresponds to $G$ being $H \times K$ while (ii) corresponds to $G$ being $H \rtimes K$. The underlying reason is the general non-abelianness of groups. However for a short exact sequence of abelian groups, (i) and (ii) are again equivalent (this is the special case of $R = \mathbb{Z}$, as abelian groups are $\mathbb{Z}$-modules).

**Example 2.2.** Let $R = k$ be a field. Every short exact sequence of $R$-modules, i.e. of vector spaces over $k$,

$$0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow 0$$

is split exact: if $\{b_i\}_{i\in\mathcal{I}}$ is a basis of $W$, one can choose inverse images $c_i \in g^{-1}(b_i)$ by the surjectivity of $g$. Then there is a (unique) linear map $g' : W \to V$ with $g'(b_i) = c_i$. Hence, $gg' = 1_W$. Therefore by Theorem 2.1, the sequence is split exact. One can prove this similarly by choosing a basis for $U$, identify $U$ with its image in $V$ via the injection $f$, and then extend this to a basis for $V$. $\triangleleft$

## 2.4 Idempotents and Indecomposables

**Definition** (Idempotent)**.** Let $R$ be a ring with unity. Then $e \in R$ is an idempotent if $e^2 = e$.

**Example 2.3.**

(i) In any ring, 0 is an idempotent. If $R$ is any ring with identity, then 1 is an idempotent.

(ii) Let

$$R = \left\{ \begin{pmatrix} a & 0 & 0 \\ b & d & 0 \\ c & e & f \end{pmatrix} \mid a, b, c, d, e, f \in \mathbb{R} \right\}$$

Then the following elements are idempotents:

$$e_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(iii) If $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is a split short exact sequence, there is a map $h : C \to B$ such that $gh = 1_C$. Then $hg \in \operatorname{End} B$ is an idempotent as $(hg)^2 = (hg)(hg) = h(gh)g = h1g = hg$.

$\triangleleft$

Let $M$ be an $R$-module and let $\text{End}_R(M) = \{f : M \to M \mid f \text{ homomorphism}\}$. Then $\text{End}_R(M)$ is a ring. We define $(f+g)(m) \overset{\text{def}}{=} f(m) + g(m)$ and $gf \overset{\text{def}}{=} g \circ f$. One should verify that these are homomorphisms and also verify the distributive property.

**Definition** (Indecomposable)**.** A module $M$ is indecomposable if whenever $M = A \oplus B$, where $A, B \leq M$, then either $A$ or $B$ is zero. That is, $M$ cannot be written nontrivially as a direct sum of $M$-submodules. If $M$ is not indecomposable, then we say that $M$ is decomposable.

**Remark.** Let $M = A \oplus C$ be a nonzero decomposable module, where $A$, $C$ are proper submodules of $M$.

$$A \underset{\pi_A}{\overset{i_A}{\rightleftarrows}} M = A \oplus C \underset{i_C}{\overset{\pi_C}{\rightleftarrows}} C$$

where $i_A, i_C$ are the canonical injections. We think of $i_A = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\pi_A = \begin{pmatrix} 1 & 0 \end{pmatrix}$. We have $\pi_A i_A = 1_A$ and $\pi_C i_C = 1_C$. Now define

$$e_A \overset{\text{def}}{=} i_A \pi_A : M \to M$$
$$e_C \overset{\text{def}}{=} i_C \pi_c : M \to M$$

Observe that

$$e_A^2 = (i_A \pi_A)(i_A \pi_A) = i_A(\pi_A i_A)\pi_a = i_A 1_A \pi_A = i_A \pi_A = e_A$$

so that $e_A$ is an idempotent. Similarly, $e_C$ is an idempotent. Furthermore, one can verify that $e_A \neq 1_H \neq e_C$ so that $e_A, e_C$ are nontrivial idempotents. Therefore, we always have nontrivial idempotents whenever $M$ is decomposable. That is, $\text{End}_R(M)$ always has nontrivial idempotents whenever $M$ is decomposable. By contrapositive, if $\text{End}_R(M)$ has no nontrivial idempotents, then $M$ is indecomposable.

We summarize the preceding remark in the following proposition:

**Proposition 2.2.** *If* $\text{End}_R(M)$ *has no nontrivial idempotents, then* $M$ *is indecomposable.*

**Definition** (Orthogonal Idempotents)**.** Two idempotents $e_1, e_2$ in any ring $R$ are orthogonal if $e_1 e_2 = e_2 e_1 = 0$.

**Example 2.4.** Suppose we have a short exact sequence

$$0 \longrightarrow A \xrightarrow{f} M \xrightarrow{g} C \longrightarrow 0$$

By Theorem 2.1, $M \cong A \oplus C$. We can then consider $A$ and $C$ as submodules of $M$. This gives us the following:

$$A \underset{\pi_A}{\overset{i_A}{\rightleftarrows}} M = A \oplus C \underset{i_C}{\overset{\pi_C}{\rightleftarrows}} C$$

But then $e_A + e_C = i_A\pi_A + i_C\pi_C = 1_M$. Furthermore, $e_Ae_C = e_Ce_A = 0$ so that $e_A$ and $e_C$ are orthogonal idempotents. ◁

**Lemma 2.2.** *Let $M$ be an $R$-module and let $e : M \to M$ be an idempotent map, i.e. $e^2 = e$, then*

$$M = \ker e \oplus \operatorname{im} e$$

*Proof.* First, we show that $\operatorname{im}(1-e) = \ker e$. If $x \in \ker e$, then $x = x - e(x) = (1-e)(x) \in \operatorname{im}(1-e)$, showing $\ker e \subseteq \operatorname{im}(1-e)$. Now let $x \in \operatorname{im}(1-e)$ so that $x = (1-e)(y)$ for some $y \in M$.

$$e(x) = e(1-e)(y) = (e-e^2)(y) = (e-e)(y) = 0(y) = 0.$$

But then $x \in \ker e$, showing $\operatorname{im}(1-e) \subseteq \ker e$. Therefore, $\operatorname{im}(1-e) = \ker e$.

By the work above, it suffices to prove $M = \operatorname{im}(1-e) \oplus \operatorname{im} e$. Let $x \in M$. Then

$$x = (1-e)(x) + e(x) \in \operatorname{im}(1-e) + \operatorname{im}(e)$$

To show that the sum is direct, we need only show that $\operatorname{im}(1-e) \cap \operatorname{im}(e) = 0$. We know that $\operatorname{im}(1-e) = \ker e$. Now let $x \in \ker e \cap \operatorname{im} e$. Then $x = e(y)$ for some $y \in M$ and because $x \in \ker e$, we have

$$0 = e(x) = e(e(y)) = e^2(y) = e(y) = x$$

so that the intersection is trivial. □

## 2.5 The Functor $\operatorname{Hom}_R(M, -)$

Now we look a bit more at exact sequences. Let $A$, $B$ be $R$-modules. Usually, $\operatorname{Hom}_R(A, B)$ is an abelian group only. Given another module $M$ and a homomorphism $f : A \to B$, we have an induced homomorphism of abelian groups

$$f_* = \operatorname{Hom}_R(M, A) \longrightarrow \operatorname{Hom}_R(M, B)$$

given by $f_*(g) \overset{\text{def}}{=} fg$, where $g \in \operatorname{Hom}_R(M, A)$, i.e. $g : M \to A$:

$$M \xrightarrow{g} A \xrightarrow{f} B$$

One need show that this is a homomorphism of abelian groups. But first, we introduce the universal property of the kernel and cokernel.

**Definition** (Universal Property of the Kernel/Cokernel)**.** Let $\beta : X \to Y$ be a homomorphism. A kernel of $\beta$ is a homomorphism $\gamma : Z \to X$ such that

(i) If we have $Z \xrightarrow{\gamma} X \xrightarrow{\beta} Y$, then $\beta\gamma = 0$.

(ii) For all homomorphisms $T \xrightarrow{\alpha} X$ with $\beta\alpha = 0$

$$\begin{tikzcd} & T \arrow[dl, dotted, "s"'] \arrow[d, "\alpha"] & \\ Z \arrow[r, "\gamma"'] & X \arrow[r, "\beta"'] & Y \end{tikzcd}$$

Then there exists a unique $s : T \to Z$ such that $\alpha = \gamma s$.

Let $\beta : X \to Y$ be a homomorphism. A cokernel of $\beta$ is a morphism $Y \xrightarrow{\gamma} Z$ such that

(i) $\gamma\beta = 0$

(ii) If there is a homomorphism $Y \xrightarrow{\alpha} T$, then there exists a unique homomorphism $s : Z \to T$.

$$\begin{tikzcd} X \arrow[r, "\beta"] & Y \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & Z \arrow[dl, dotted, "s"] \\ & T & \end{tikzcd}$$

Again, note that this merely defines what it takes to be a kernel or cokernel. We have not proved that such objects exist. Indeed for a general category, there will not be a kernel and cokernel. However, these objects will exist in our most important category—$R$-modules.

**Proposition 2.3.** *Let $R$ be a ring. Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

*be a short exact sequence. Let $M$ be an $R$-module. Then we have an induced exact sequence*

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{f_*} Hom_R(M, B) \xrightarrow{g_*} \mathrm{Hom}_R(M, C)$$

*Proof.* We first show that $f_*$ is a monomorphism. Suppose $h : M \to A$ is such that $f_*(h) = 0$, i.e. $fh = 0$. Since $f$ is injective, this implies that $h = 0$. But then $\ker f_* = 0$ so that $f_*$ is injective.

Now we wish to show exactness at $\mathrm{Hom}_R(M, B)$; that is, we want to show $\mathrm{im}\, f_* = \ker g_*$. Let $h \in \mathrm{Hom}_R(M, A)$. Then

$$g_* f_*(h) = g_*(fh) = g(fh) = (gf)h$$

Our original sequence was exact so that $gf = 0$. Then $g_* f_*(h) = (gf)h = 0(h) = 0$, showing $\operatorname{im} f_* \subseteq \ker g_*$. To show $\ker g_* \subseteq \operatorname{im} f_*$, we use the universal property of the kernel. Let $h \in \ker g_* : \operatorname{Hom}_R(M, B) \to \operatorname{Hom}_R(M, C)$. Then we have a composition of maps $M \xrightarrow{h} B \xrightarrow{g} C$ with $gh = 0$. We want to show $h \in \operatorname{im} f_*$. Observe we have the diagram

$$\begin{tikzcd}
 & & M \arrow[dl, dotted, "s"'] \arrow[d, "h"] & & \\
0 \arrow[r] & A \arrow[r, "f"'] & B \arrow[r, "g"'] & C \arrow[r] & 0
\end{tikzcd}$$

Now $gf = 0$ and $A \cong \operatorname{im} f = \ker g$. By the universal property of the kernel, there exists a unique map $s : M \to A$ making the diagram commute. But then by the commutativity of the diagram,

$$h = fs = f_*(s),$$

so that $\ker g_* \subseteq \operatorname{im} f_*$. But then $\operatorname{im} f_* = \ker g_*$ so that the sequence is exact at $\operatorname{Hom}_R(M, B)$. $\square$

**Remark.** Note in the result above, we did not make use of the fact that $g$ is surjective, i.e. we need only start with an exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$.

One might ask if the induced map $g_*$ is onto. Generally, the map $g_* : \operatorname{Hom}_R(M, B) \to \operatorname{Hom}_R(M, C)$ is not onto.

**Example 2.5.** Let $R = \mathbb{Z}$. Consider the exact sequence of $R$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i} \mathbb{Q} \xrightarrow{\pi} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Note that the coset $\frac{1}{2} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ has order two and that there are no nonzero elements in $\mathbb{Q}$ with finite order. Apply the map $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$ to obtain the exact sequence

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{i_*} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}) \xrightarrow{\pi_*} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0.$$

Now $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \neq 0$ since it contains the nonzero map $[1] \mapsto \frac{1}{2} + \mathbb{Z}$. However, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}) = 0$ by the remarks above. But then $\pi_*$ cannot be surjective. $\triangleleft$

**Example 2.6.** Let $R = \mathbb{Z}$.

$$0 \longrightarrow 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Let $M = \mathbb{Z}/2\mathbb{Z}$. Then

$$0 \longrightarrow \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z}, 2\mathbb{Z}) \xrightarrow{f^*} \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{g^*} \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

Observe that $\mathbb{Z}/2\mathbb{Z}$ is a torsion submodule of the free module $\mathbb{Z}$ so that $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = 0$. Also, observe that $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, 2\mathbb{Z}) = 0$ so the above series is equivalent to

$$0 \longrightarrow 0 \longrightarrow 0 \xrightarrow{g^*} \text{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

and $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \neq 0$ so that $g^*$ is not onto. $\triangleleft$

Let us put this in broader terms: we begin with a sequence of $R$-modules $M$, $A$, $B$, and $C$ with maps between them. Applying the map $\text{Hom}_R(M, -)$ (this is said $\text{Hom}_R$ $M$ "blank") gives us abelian groups $\text{Hom}_R(M, A)$, $\text{Hom}_R(M, B)$, and $\text{Hom}_R(M, C)$. In categorical terms, $\text{Hom}_R(M, -)$ is a (covariant) functor from $R$-modules to abelian groups. While the original sequence is exact, the newly obtained sequence is only exact "on the left". In categorical terms, $\text{Hom}_R(M, -)$ is a left exact functor. The functor $\text{Hom}_R(-, M)$ is similarly left exact but requires the original sequence to be exact on the right.

**Proposition 2.4.** *Let $R$ be a ring. Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

*be a short exact sequence. Let $M$ be an $R$-module. Then we have an induced exact sequence*

$$0 \longrightarrow \text{Hom}_R(C, M) \xrightarrow{g^*} \text{Hom}_R(B, M) \xrightarrow{i^*} \text{Hom}_R(A, M),$$

*where $g^* : \text{Hom}_R(C, M) \to \text{Hom}_R(B, M)$ is given by $g^*(f) = fg$, where $f : C \to M$. and $i^*$ is defined mutatis mutandis.*

*Proof.* L.T.R.. $\square$

**Remark.** As with Proposition 2.3, we do not need the original sequence to be exact on the left, only on the right. That is, we need only begin with an exact sequence $A \longrightarrow B \longrightarrow C \longrightarrow 0$.

Note that Proposition 2.4 says that $\text{Hom}_R(-, M)$ is a (left exact) contravariant functor from $R$-modules to abelian groups. Putting Proposition 2.3 and Proposition 2.4 together, we obtain the following theorem:

**Theorem 2.2.** Hom *is a left exact functor from $R$-modules to abelian groups.*

Note that while Proposition 2.3 and Proposition 2.4 do not generally yield exact sequence (only left exact), they do yield exact sequences when applied to split exact sequences.

**Proposition 2.5.** *Let* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *be a split exact sequence. Let* $M$ *be an* $R$*-module. Then the sequence*

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{f_*} \mathrm{Hom}_R(M, B) \xrightarrow{g_*} \mathrm{Hom}_R(M, C) \longrightarrow 0$$

*is exact.*

*Proof.* From Proposition 2.3, we need only show that the sequence is exact at $\mathrm{Hom}_R(M, C)$; that is, we need show that $g^*_M$ is onto. Let $h \in \mathrm{Hom}_R(M, C)$.

$$\begin{tikzcd} B \arrow[r, shift left, "g"] & C \arrow[l, shift left, "i"] \arrow[r] & 0 \\ & M \arrow[u, "h"] \arrow[ul, dotted, "s"] & \end{tikzcd}$$

We want $h = g_*(s)$ for some function $s : M \to B$. Using the fact that the original sequence is split exact, let $i$ be such that $gi = 1_C$. Define $s = ih : M \to B$ and observe

$$g_*(s) = g_*(ih) = g(ih) = (gi)h = 1_C h = h,$$

which is exactly what we had hoped to show. □

Note that in a special case, we even have a partial converse to Proposition 2.3

**Proposition 2.6.** *Let* $f : A \to B$ *and* $g : B \to C$ *be R-maps. If for every R-module* $M$*,*

$$0 \longrightarrow \mathrm{Hom}_R(C, M) \xrightarrow{g^*} \mathrm{Hom}_R(B, M) \xrightarrow{f^*} \mathrm{Hom}_R(A, M)$$

*is an exact sequence of abelian groups, then*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

*is an exact sequence of R-modules.*

## 3 Free Modules, Projective Modules, and Injective Modules

### 3.1 Free Modules

The 'simplest' type of modules are free modules.

**Definition** (Free Module)**.** A left $R$-module $F$ is a free left $R$-module if $F$ is isomorphic to a direct sum of copies of $R$; that is, there is a (possibly infinite) index set $\mathcal{B}$ such that $F = \bigoplus_{i \in \mathcal{B}} R_i$, where $R_i = \langle b_i \rangle \cong R$ for all $i \in \mathcal{B}$. We call $\mathcal{B}$ a basis for $F$.

The term 'free' refers to the fact that the basis elements have no $R$-linear relations, i.e. there are no collections $\{b_s\}$, $\{r_s\}$ such that $\sum_j r_j b_j = 0$. A free $\mathbb{Z}$-module is called a free abelian group. Every ring $R$, when considered as a left module over itself, is a free $R$-module. Despite having a rigid structure, free modules have a rich theory—think of Linear Algebra. In fact in the case where $R = k$ is a field, this is precisely Linear Algebra. These modules are also very ubiquitous, as the following proposition shows.

**Proposition 3.1.** *Let $R$ be a ring. Given any set $B$, there exists a free $R$-module $F$ with basis $B$.*

*Proof.* The set of functions $R^B = \{\phi : B \to R\}$ is a left $R$-module, where for all $b \in B$ and $r \in R$, define $\phi + \psi : B \to R$ via $b \mapsto \phi(b) + \psi(b)$ and $r\phi : B \to R$ via $r \cdot \phi(b)$. Define the function $\mu_b$ as

$$\mu_b(a) = \begin{cases} 1, & \text{if } a = b \\ 0, & \text{if } a \neq b \end{cases}$$

Denoting $\mu_b$ by $b$, $R^B$ is the direct product $\prod_{b \in B} \langle b \rangle$. Now $R \cong \langle b \rangle$ via the map $r \mapsto r\mu_b$. Then the submodule $F$ of $R^B$, generated by $B$, is a direct sum of copies of $R$. But then $F$ is a free left $R$-module with basis $B$. □

Free modules also have strong properties on their maps as well. In Linear Algebra, one has the notion of extending maps by linearity. One has a similar result for free modules.

**Proposition 3.2.** *Let $R$ be a ring and let $F$ be a free left $R$-module on a basis $B$. If $M$ is a left $R$-module and $f : B \to M$ is a function, there exists a unique $R$-map $\tilde{f} : F \to M$ with $\tilde{f}\mu = f$, where $\mu : B \to F$ is the inclusion map; that is, $\tilde{f}(b) = f(b)$ for all $b \in B$, i.e. $\tilde{f}$ extends $f$.*

*Proof.* Every $v \in F$ has a unique expression of the form $v = \sum_{b \in B} r_b b$, where $r_b \in R$ and $r_b = 0$ for almost all $b$. Therefore, there is a well defined function $\tilde{f} : F \to M$ given by $v \mapsto \sum_{b \in B} r_b f(b)$. It is routine to verify that $\tilde{f}$ extends $f$. Then if $s \in R$, $sv = \sum s r_b b$. If $v' = \sum r'_b b$, then $v + v' = \sum (r_b + r'_b) x$. But then $\tilde{f}$ is an $R$-map. Since, $F = \langle B \rangle$, $\tilde{f}$ is the unique map extending $f$. [One can easily verify that two $R$-maps agreeing on a generating set are equal.] □

Free modules share further parallels to Linear Algebra, as the reader can easily verify.

**Proposition 3.3.** *Let $R$ be a nonzero commutative ring.*

*(i) Any two bases of a free $R$-module $F$ have the same cardinality.*

*(ii) Free $R$-modules $F$ and $F'$ are isomorphic if and only if there are bases having the same cardinality.*

*(iii) If $n$ and $m$ are integers, then $R^n \cong R^m$ if and only if $n = m$.*

If a ring $R$ has the property that $R^n \cong R^m$, where $n$ and $m$ are integers, that $n = m$ is said to have IBN (invariant basis number). If $R$ has IBN, the number of elements in a basis of a free $R$-module $F$ is called the rank of $F$, denoted rank $F$. By the work above, if $R$ has IBN and $F$ is a finitely generated free left $R$-module, then every two bases of $F$ have the same number of elements. All nonzero commutative rings $R$ have IBN. The proof of this generalizes to show that any noncommutative ring $R$ with a two-sided ideal $I$ for which $R/I$ is a division ring, e.g. every local ring, has IBN. Furthermore, every division ring and noetherian ring has IBN. For an example where $R$ does not have IBN, take $R = \operatorname{End}_k(V)$, where $k$ is a field and $V$ is an infinite dimensional vector space over $k$. [For this, consider maps $\phi : V \to V \oplus V$ and $V \oplus V \to V$.] Finally, every module arises from a free module in some way.

**Theorem 3.1.** *Every left $R$-module $M$ is the quotient of a free left $R$-module $F$. Moreover, $M$ is finitely generated if and only if $F$ can be chosen to be finitely generated.*

*Proof.* Choose a generating set $X$ of $M$. Let $F$ be a free module on basis $\{b_x \colon x \in X\}$ (this makes use of Proposition 3.1). By Proposition 3.2, there exists an $R$-map $g : F \to M$, where $g(b_x) = x$ for all $x \in X$. Clearly, $g$ is a surjection as $\operatorname{im} g$ is a submodule of $M$ containing $X$. But then $F/\ker g \cong M$. If $M$ is finitely generated, then there is a finite generating set $X$ and the free module $F$ constructed above is finitely generated. The converse is immediate since the image of a finitely generated module is finitely generated. $\square$

This theorem implies that there given any $R$-module, there is always a free module which surjectively maps onto it. We will often use this theorem without mention. One could always obtain this from Proposition 3.1.

## 3.2 Projective Modules

**Definition** (Projective Module)**.** An $R$-module ${}_RP$ is projective if for all homomorphisms $B \xrightarrow{g} C \longrightarrow 0$ and maps $f : P \to C$, there exists a lift of $f$ to $B$; that is, there exists a homomorphism $h : P \to B$ with $gh = f$.

$$\begin{tikzcd} & P \arrow[dl, dotted, "h"'] \arrow[d, "f"] & \\ B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

**Lemma 3.1.** *Every free module is projective.*

*Proof.* Assume that $F$ is free on a basis $\{t_\alpha\}_{\alpha \in \mathcal{I}}$.

$$\begin{tikzcd} & F \arrow[dl, dotted, "h"'] \arrow[d, "f"] & \\ B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

We examine the image of the basis under $f$: $\{f(t_\alpha)\}_{\alpha\in\mathcal{I}} \subseteq C$. As $g$ is onto, for all $\alpha \in \mathcal{I}$, we have $f(t_\alpha) = g(b_\alpha)$ for some $b_\alpha \in B$. Let $h : F \to B$ be the unique homomorphism with $h(t_\alpha) = b_\alpha$, extending by linearity. Therefore, we have

$$g\left(h\left(\sum_i r_i t_i\right)\right) = \sum_i g(h(r_i t_i)) = \sum_i r_i g(h(t_i)) = \sum_i r_i g(b_i) = \sum_i r_i f(t_i) = f\left(\sum_i r_i t_i\right).$$

But then $gh = f$ so that $F$ is projective. $\square$

In fact in some sense, projective modules are 'close' to being free modules in that they have a dual basis, see Lemma 3.2. There are also many equivalent definitions for a projective module, each useful in various situations.

**Proposition 3.4.** *The following are equivalent for a module $P$:*

*(i)* *$P$ is a projective module.*

*(ii)* *For all $X \xrightarrow{g} P$ with $g$ onto, the mapping splits. That is, there exists $h : P \to X$ with $gh = 1_P$.*

*(iii)* *$P$ is isomorphic to a direct summand of a free module.*

*(iv)* $\mathrm{Hom}(P, -)$ *is exact; that is, if*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

*is any exact sequence, then*

$$0 \longrightarrow \mathrm{Hom}(P, A) \xrightarrow{f_*} \mathrm{Hom}(P, B) \xrightarrow{g_*} \mathrm{Hom}(P, C) \longrightarrow 0$$

*is exact.*

*Proof.* $(i) \to (ii)$: Suppose $g : X \to P$ is onto. Consider the identity map $1_P : P \to P$.

$$\begin{tikzcd} & P \arrow[d, "1"] \arrow[dl, dotted, "h"'] & \\ X \arrow[r, "g"] & P \arrow[r] & 0 \end{tikzcd}$$

Since $P$ is projective, there exists a lift of $1_P$ to $X$, i.e. a map $h : P \to X$ such that $hg = 1_P$.

$(ii) \to (iii)$: Let $F$ be a free module mapping surjectively onto $P$ via a map $g : F \to P$. There is an exact sequence

$$0 \longrightarrow \ker g \xrightarrow{\iota} F \xrightarrow{g} P \longrightarrow 0.$$

By assumption, there exists a map $h : P \to F$ such that $gh = 1_P$. But then by Theorem 2.1, $P$ is a direct summand of $F$.

$(iii) \to (iv)$: Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence. By Proposition 2.3, we already know that $\mathrm{Hom}(P, -)$ is left exact. We need only prove exactness on the right, i.e. exactness at $\mathrm{Hom}(P, C)$. This is proving that $g^*$ is surjective. Let $\phi \in \mathrm{Hom}(P, C)$. By assumption, $P$ is a direct summand of $F$, say $F = A \oplus P$. We have a diagram

$$\begin{tikzcd}
 & F \arrow[d, "\pi"] \arrow[dl, dotted, "\Psi"'] \\
 & P \arrow[d, "\phi"] \arrow[dl, dotted, "\Psi|_P"'] \\
B \arrow[r, "g"'] & C \arrow[r] & 0
\end{tikzcd}$$

There is the canonical surjection from $F$ onto $P$, $\pi : F \to P$. Then $\phi\pi : F \to C$ is an $R$-map. By Proposition 3.2, there is a map $\Psi : F \to B$ such that $g\Psi = \phi\pi$. Now $\pi\big|_P = 1_P$. Then $g\Psi\big|_P = \phi\pi\big|_P = \phi 1_P = \phi$. Define $\tilde{\Psi} := \Psi\big|_P : P \to B$. Then $\tilde{\Psi} \in \mathrm{Hom}(B, C)$ with $g_*(\tilde{\Psi}) = g\tilde{\Psi} = g\Psi\big|_P = \phi \in \mathrm{Hom}(P, C)$ so that $g_*$ is surjective.

$(iv) \to (i)$: Suppose that $g : B \to C$ is a surjection and $\phi : P \to C$ is an $R$-map. We have an exact sequence and diagram

$$\begin{tikzcd}
 & & & P \arrow[d, "\phi"] \arrow[dl, dotted, "h"'] \\
0 \arrow[r] & \ker g \arrow[r, "\iota"] & B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$

Now there is an exact sequence

$$0 \longrightarrow \mathrm{Hom}(P, \ker g) \xrightarrow{\iota_*} \mathrm{Hom}(P, B) \xrightarrow{g_*} \mathrm{Hom}(P, C) \longrightarrow 0$$

Since $g_*$ is surjective, there exists a map $h \in \mathrm{Hom}(P, B)$, i.e. an $R$-map $h : P \to B$, such that $g_*(h) = \phi$. But $\phi = g_*(h) = gh$ so that $P$ is projective. $\square$

The reader should try to prove direct equivalences between all the equivalent conditions of the previous proposition as an exercise. Furthermore, these equivalences allow us to prove the Dual Basis Lemma.

**Lemma 3.2** (Dual Basis Lemma)**.** *An $R$-module $P$ is projective if and only if there exists a family of elements $\{a_i\}_{i\in\mathcal{I}} \subseteq P$ and linear functions $\{f_i\}_{i\in\mathcal{I}} \subseteq P^* = \mathrm{Hom}_R(P, R)$ such that for any $a \in P$, $f_i(a) = 0$ for almost all $i$ and $a = \sum_i a_i f_i(a)$.*

*Proof.* Suppose that $P$ is projective. Fix an epimorphism $g$ from a free module $F = \bigoplus Re_i$ onto $P$. But as $P$ is projective, $g$ has a splitting $h : P \to F$, which can be expressed as

$$h(a) = \sum_i f_i(a)e_i.$$

The $f_i$ are $R$-linear and $f_i(a) = 0$ for almost all $i$. Therefore, $f_i \in P^*$. But then

$$a = gh(a) = \sum f_i(a)a_i,$$

where $a_i := g(e_i) \in P$.

Now suppose that the $a_i, f_i$ exist as in the statement of the lemma. Define $F : \bigoplus Re_i$ and an epimorphism $g : F \to P$ given by $g(e_i) = a_i$ for all $i \in \mathcal{I}$. Define also a map $h : P \to F$ via $a \mapsto \sum f_i(a)e_i$. One routinely verifies that $h$ is an $R$-map. It is also routine to verify that $h$ is a splitting for $g$. But then $P$ is isomorphic to a direct summand of $F$. Therefore, $P$ is projective. □

**Remark.** The pairings $\{(a_i, f_i)\}_{i\in\mathcal{I}}$ are often referred to as "a pair of dual bases." Note that the $a_i$ are only a generating set for $P$ and are not necessarily a basis for $P$.

**Proposition 3.5.**

*(i) Every direct summand of a projective module is itself projective.*

*(ii) Every direct sum of projective modules is projective.*

*Proof.*

(i) A module is projective if and only it is a direct summand of a free module. But then any module that is a summand of a projective module is a summand of a free module, and hence is projective.

(ii) Let $\{P_I\}_{i\in\mathcal{I}}$ be a family of projective modules. For all $i \in \mathcal{I}$, there exists a free module $F_i$ such that $F_i = P_i \oplus Q_i$ for some $Q_i \subseteq F_i$. Now $\bigoplus_{i\in\mathcal{I}} F_i$ is free (a basis being the union of the bases for the $F_i$), and

$$\bigoplus_{i\in\mathcal{I}} F_i = \bigoplus_{i\in\mathcal{I}} (P_i \oplus Q_i) = \bigoplus_{i\in\mathcal{I}} P_i \oplus \bigoplus_{i\in\mathcal{I}} Q_i.$$

But then $\bigoplus_{i\in\mathcal{I}} P_i$ is a summand of a free module, hence free. □

In fact, the last statement in the above proposition is an if and only if.

**Proposition 3.6.** *Let $\{P_i\}_{i\in\mathcal{I}}$ be a family of modules. Then $\bigoplus_{i\in\mathcal{I}}$ is projective if and only if $P_i$ is projective.*

*Proof.* The reverse direction was shown in the previous proposition. We need only show the forward direction. Suppose that $\bigoplus_{i\in\mathcal{I}}$ is projective. Let $g : B \to C$ be a surjection and let $f : \bigoplus_{i\in\mathcal{I}} \to C$ be an $R$-map. Consider the following diagram:

$$\begin{tikzcd}
B \arrow[r, "g"] & C \arrow[r] & 0 \\
& \bigoplus_{i\in\mathcal{I}} P_i \arrow[u, "f"] \arrow[ul, dotted, "h"] & \\
& P_i \arrow[u, "\iota_i"] \arrow[uul, dotted, "h_i"] &
\end{tikzcd}$$

where $\iota_i$ is the canonical injection. Since $\bigoplus_{i\in\mathcal{I}}$ is projective, there exists a lift $h$ of $f$ to $B$. Define $h_i : P_i \to B$ via $h_i := h\iota_i$. Clearly, $h_i$ is an $R$-map. We have $f = hg$ so that $f\big|_{P_i} = h\big|_{P_i} g = h\iota_i g = h_i g$. But then $P_i$ is projective. □

**Remark.** If $R$ is a local principal ideal domain, then $R$ is free as an $R$-module.

**Example 3.1.** Not all projective modules are free. Let

$$R = \begin{pmatrix} \mathbb{Q} & 0 & 0 \\ \mathbb{Q} & \mathbb{Q} & 0 \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \end{pmatrix}$$

That is, let $R$ be the set of lower triangular matrices. We know $\dim_{\mathbb{Q}} R = 6$. So if $F$ is a finite dimensional free module, then $\dim F$ is a multiple of 6.

$$P = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \mathbb{Q} & 0 \\ 0 & \mathbb{Q} & 0 \end{pmatrix} \subseteq R$$

As $P$ is a submodule (in fact a left ideal of $R$), then as a left module $\dim_R P = 2$ so that $P$ is not free. ◁

**Example 3.2.** Let $R = \mathbb{Z}/6\mathbb{Z}$. Note that $R = \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Let $I = \mathbb{Z}/2\mathbb{Z}$ and $J = \mathbb{Z}/3\mathbb{Z}$. Now $R$ is free as an $R$-module. Since $I, J$ are direct summands of $R$, $I$ and $J$ are projective $\mathbb{Z}/6\mathbb{Z}$-modules. However, neither $I$ nor $J$ are free as a (finitely generated) free $\mathbb{Z}/6\mathbb{Z}$-module must be a direct sum of $n$-copies of $\mathbb{Z}/6\mathbb{Z}$, and so they must have $6^n$ elements. However, both $I$ and $J$ are too small for this to be the case. ◁

**Proposition 3.7.** *Suppose that the following diagram is commutative with exact rows*

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

*Then there exists a unique map $h : C \to C'$ making the diagram commute. Moreover, $h$ is an isomorphism if $\alpha$ and $\beta$ are isomorphisms.*

*Proof.* Assume we have the following commutative diagram with exact rows.

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

First, we show there exists a unique $h : C \to C'$ such that $hg = g'\beta$. Let $x \in C$. As $g$ is onto, there is a $b \in B$ such that $x = g(b)$.

$$\begin{tikzcd}
b \arrow[r, "g"] \arrow[d, "\beta"] & x = g(b) \\
\beta(b) \arrow[r] & g'\beta(b)
\end{tikzcd}$$

We try the map $h(x) \stackrel{\text{def}}{=} g'\beta(b)$. We need check that this map is well defined. Let $b_1 \in B$ such that $g(b_1) = g(b) = x$. We have

$$\begin{tikzcd}
b \arrow[r, "g"] \arrow[d, "\beta"] & x = g(b) & b_1 \arrow[l, "g"'] \arrow[d, "\beta"] \\
\beta(b) \arrow[r, "g'"] & g'\beta(b) & \beta(b_1) \arrow[l, "g'"']
\end{tikzcd}$$

We need check that $g'(\beta(b)) = g'(\beta(b_1))$. Note that as $x = g(b) = g(b_1)$, we have $g(b_1) - g(b) = g(b_1 - b) = 0$. But then using exactness at $B$, $b_1 - b \in \ker g = \operatorname{im} f$. Therefore, $b_1 - b = f(a)$ for some $a \in A$. Then by commutativity, $\beta(b_1 - b) = \beta(f(a)) = f'(\alpha(a))$. By exactness, we know that $g'f' = 0$ so that $g'(\beta(b_1 - b)) = g'(f'(\alpha(a))) = 0$. Then

$$0 = g'(\beta(b_1 - b)) = g'(\beta(b_1) - \beta(b)) = g'(\beta(b_1)) - g'(\beta(b)) = h(b_1) - h(b)$$

so that $h(b_1) = h(b)$, proving $h$ is well defined. By construction, if $b \in B$ and $c := g(b)$, then $(hg)(b) = h(g(b)) = h(c) = (g'\beta)(b)$ so that the diagram commutes.

However, there is an easier way of demonstrating the existence of the map.

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

Note we have a map $B \xrightarrow{g} C$. Consider the cokernel of $f$. Using exactness, we have $0 = g'f'\alpha = g'\beta f$.Using the Universal Property of the Cokernel,

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] \arrow[d, "g'\beta"'] & C \arrow[dl, dotted, "\exists! h"] \\ & C' & \end{tikzcd}$$

We have yet to show that $h$ is unique and a homomorphism. We show this by showing that for any commutative diagram with exact rows, as below,

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, dotted, "h"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[d, "\gamma"] \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \end{tikzcd}$$

there exists a unique $h : A \to A'$ with $f'h = \beta f$. The idea is the same as above but we use the Universal Property of the Kernel. We have $f' : A' \to B'$ is the kernel of $g'$.

$$\begin{tikzcd} & & A \arrow[dl, dotted, "h"] \arrow[d, "\beta f"] & \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \end{tikzcd}$$

We know also that $g'\beta f = 0$. But then the Universal Property of the Kernel says there exists a unique $h : A \to A'$ with $f'h = \beta f$. $\square$

### 3.3 Injective Modules

Let $f : A \to B$ be a homomorphism of $R$-modules and let $M$ be another $R$-module. If we have a map $\beta : B \to M$ then we can obtain a map $A \to M$ by (pre)composing the map from $\beta : B \to M$ with $f$; that is, we have an induced map of abelian groups

$$\mathrm{Hom}_R(B, M) \xrightarrow{\mathrm{Hom}_R(f,M) = f_M^*} \mathrm{Hom}_R(A, M)$$

given by $f_M^*(\beta) := \beta f$. Note that if the module $M$ is understood, we often drop the $M$. Similarly, if we have a map $f : M \to A$, then given a map $A \to B$, we obtain a map $M \to B$ via composition; that is, we have an induced map of abelian groups

$$\mathrm{Hom}_R(M, A) \xrightarrow{\mathrm{Hom}_R(M,f) = f_*^M} \mathrm{Hom}_R(M, B)$$

Again, we will often drop the $M$ if will be understood. These induced maps behave fairly well with regards to exact sequences, as the next proposition shows.

**Proposition 3.8.** *Suppose that*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$
$$0 \longrightarrow X \xrightarrow{r} Y \xrightarrow{s} Z$$

*are exact sequences of R-modules and M is an R-module. Then there are exact sequences of abelian groups*

$$0 \longrightarrow \operatorname{Hom}(C, M) \xrightarrow{g^*} \operatorname{Hom}(B, M) \xrightarrow{f^*} \operatorname{Hom}(A, M)$$
$$0 \longrightarrow \operatorname{Hom}(M, X) \xrightarrow{r_*} \operatorname{Hom}(M, Y) \xrightarrow{s_*} \operatorname{Hom}(M, Z)$$

*Proof.* We prove the existence of the first exact sequence and leave the second as a routine exercise which follow mutatis mutandis from the proof we shall give for the first. By Example 2.1, to prove exactness at $\operatorname{Hom}(C, M)$, it suffices to prove that $g^*$ is injective. Suppose that $\psi : C \to M$ is such that $g^*(\psi) = 0$, i.e. $0 = g^*(\psi) = \psi g$. We want to show that $\psi$ is the zero map. We know for all $b \in B$, $g^*(\psi)(b) = 0$, i.e. $\psi g(b) = 0$. But as $g$ is surjective, we know that $g(B) = C$ so that it must be that $\psi(C) = 0$. But then $\psi$ is the zero map. Therefore, $g^*$ is injective.

Now we prove exactness at $\operatorname{Hom}(B, M)$, i.e. we prove $\operatorname{im} g^* = \ker f^*$. Now if $\psi : C \to M$ is a map, then by exactness $f^* g^*(\psi) = f^*(\psi g) = (\psi g) f = \psi(gf) = \psi(0) = 0$. Therefore, $\operatorname{im} g^* \subseteq \ker f^*$.

Now suppose $\theta \in \ker f^*$, i.e. $\theta : B \to M$ is such that $0 = f^*(\theta) = \theta f$. Consider the $\operatorname{coker} f := N/\operatorname{im} f$. Because $\theta f = 0$, by the Universal Property of the Cokernel, there exists a unique map $h : \operatorname{coker} f \to M$ such that $\theta = h\pi$.

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "\theta"] \arrow[d, "\pi"'] & M \\ & \operatorname{coker} f \arrow[ur, dotted, "h"'] & \end{tikzcd}$$

where $\pi : B \to \operatorname{coker} f$ is the projection map $b \mapsto b + \operatorname{im} f$. But by exactness, $\operatorname{im} f = \ker g$ so that $\operatorname{coker} f = B/\operatorname{im} f = B/\ker g$. Furthermore as $g : B \to C$ is surjective, we know by the First Isomorphism Theorem that $B/\ker g \cong C$. But then via this isomorphism, we can view $h$ as $h : C \to M$, i.e. $h \in \operatorname{Hom}(C, M)$.

Over a field, HOm Exact
Note that $f_*^M$ is onto if for any $h : A \to M$, there is a $p : B \to M$ with $pf = h$.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[dl, dotted, "\exists p"] \\ & M & \end{tikzcd}$$

Furthermore, we know that if $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is a split exact sequence then for all $M$ the sequence

$$0 \longrightarrow \mathrm{Hom}_R(C, M) \longrightarrow \mathrm{Hom}_R(B, M) \longrightarrow \mathrm{Hom}_R(A, M) \longrightarrow 0$$

is exact.

**Definition** (Injective Module)**.** An $R$-module $I$ is injective if whenever we have

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[dl, dotted, "g"] \\ & I & \end{tikzcd}$$

$h$ can be "extended" to $B$. That is, there exists $g : B \to I$ with $gf = h$.

First note that ${}_RI$ is injective if and only if for all short exact sequences

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

the following sequence is exact

$$0 \longrightarrow \mathrm{Hom}(C, M) \xrightarrow{g_*^M} \mathrm{Hom}(B, M) \xrightarrow{f_*^M} \mathrm{Hom}(A, M) \longrightarrow 0$$

**Proposition 3.9.** *${}_RI$ is injective if and only if for all monomorphisms $0 \longrightarrow I \xrightarrow{f} X$ splits, i.e. there exists $p : X \to I$ with $pf = id_I$. So $I$ is isomorphic to a direct summand of $X$.*

### 3.4 Baer's Criterion

**Theorem 3.2** (Baer's Criterion)**.** *Let $R$ be a ring and $E$ a left $R$-module. Then ${}_RE$ is injective if and only if for all left ideals ${}_RI$ of $R$ and*

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, hook, "incl"] \arrow[d, "f"] & R \arrow[dl, dotted, "s"] \\ & E & \end{tikzcd}$$

*then $f$ can be extended to $R$, i.e. there exists a homomorphism $s : R \to E$ such that $s|_I = f$.*

Proof: The forward direction is trivial as when $E$ is injective the result is trivial. Now assume the converse. Let the following the homomorphisms of $R$-modules

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "f"] & B \\ & E & \end{tikzcd}$$

Without loss of generality, assume that $A \xrightarrow{\text{incl}} B$. (Why?) Then we have

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, hook] \arrow[d, "f"] & B \\ & E & \end{tikzcd}$$

Let $S = \{(A', f') \mid A \subseteq A' \subseteq B, f' : A' \to E \text{ and extends } f\}$.

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, "f"] & A' \arrow[r, hook] \arrow[dl, "f'"] & B \\ E & & \end{tikzcd}$$

We know that $S \neq \emptyset$ as the pair $(A, f) \in S$. We put an ordering on $S$ given by $(A', f') \leq (A'', f'')$ if

$$\begin{tikzcd} A \arrow[d, "f"] & \subseteq & A' \arrow[dll, "f'"] & \subseteq & A'' \arrow[dllll, "f''"] & \subseteq & B \\ E & & & & & & \end{tikzcd}$$

This is an ordering. (Why?) We claim that $S$ has a maximal element. Pick a chain $\{(A_i, f_i)\}_i$ in $S$. We look at $\left(\bigcup A_i, \overline{f}\right)$, where $\overline{f} : \bigcup A_i \to E$ defined by $\overline{f}(a_i) = f_i(a_i)$. This is an upper bound for the chain. Then Zorn's Lemma says that there exists $(A^*, f^*)$ which is a maximal element of $S$.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, hook] \arrow[d, "f"] & A^* \arrow[r, hook] \arrow[dl, "f^*"] & B \\ & E & & \end{tikzcd}$$

We want to show that $A^* = B$. Suppose that this is not the case. Then there is a $b \in B \setminus A^*$. Then

$$\begin{tikzcd} 0 \arrow[r, hook] & A \arrow[r, hook] & A^* \arrow[r, hook] \arrow[d, "f^*"] & A^* + \langle b \rangle = \overline{A} \\ & & E & \end{tikzcd}$$

Let $I = \{r \in R \mid rb \in A^*\}$. We know that $0 \in I$ so that $I \neq \emptyset$. It is trivial to show that $I$ is a left ideal of $R$. Then

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, hook] \arrow[d, "j"] & R \arrow[dl, dotted, "\exists \bar{j}"] \\ & E & \end{tikzcd}$$

where $j(r) \overset{\text{def}}{=} f^*(rb)$. The map $j$ is a $R$-module homomorphism where $\bar{j}|_I = j$. We look at $\bar{j}(1) \in E$. We construct $\overline{f} : \overline{A} \to B$ so that $\overline{f}|_{A^*} = f^*$. Then we have $\overline{f}|_A = f$. So we have $(\overline{A}, \overline{f}) > (A^*, f^*)$ as $\overline{A} \supsetneq A^*$. This contradicts our ordering from above; that is, this contradicts the maximality of $(A^*, f^*)$.

Define $\overline{f}(a^* + rb) = f^*(a^*) + r\bar{j}(1)$. We claim that $\overline{f}$ is well defined and is a map of $R$-modules. We first show the map is well defined. Let $a_1^* + r_1 b = a_2^* + r_2 b$. Then we have $a_1^* - a_2^* = (r_2 - r_1)b$. Then $r_2 - r_1 \in I$.

$$f^*(a_1^* - a_2^*) = f^*((r_2 - r_1)b) = j(r_2 - r_1) = \bar{j}(r_2 - r_1) = \bar{j}(r_2) - \bar{j}(r_1)$$

But $f^*(a_1^*) - f^*(a_2^*) = f^*(a_1^* - a_2^*)$ so that $f^*(a_1^*) + \bar{j}(r_1) = f^*(a_2^*) + \bar{j}(r_2) = \overline{f}(a_2^* + r_2 b)$. But $\overline{f}(a_1^* + r_1 b) = f^*(a_1^*) + \bar{j}(r_1)$. Therefore, the map is well defined. It remains to show that $\overline{f}$ is a $R$-module homomorphism. (Exercise) $\square$

Now recall that if $\{P_i\}_{i \in \mathcal{I}}$ is a family of modules, then each $P_i$ is projective if and only if $\bigoplus_{i \in \mathcal{I}} P_i$ is projective. We have a similar result for injective modules.

**Proposition 3.10.** *Let $\{E_i\}_{i \in \mathcal{I}}$ be a family of $R$-modules. Then each $E_i$ is injective if and only if $\prod_{i \in \mathcal{I}} E_i$ is injective.*

Proof: Let each $E_i$ be injective.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "j"] \arrow[d, "f"] & B \arrow[dl, dotted, "\exists g"] \arrow[ddl, dotted, "g_i"] \\ & \prod E_i \arrow[d, "\pi_i"] & \\ & E_i & \end{tikzcd}$$

We need find a map $g : B \to \prod E_i$. As the $E_i$ are injective, there is a map $g_i : B \to E_i$. Let $g = \prod g_i$. That is, let $g(b) = \big(g_i(b)\big)_{i \in \mathcal{I}}$. This map works. (Why?)

Now assume $\prod E_i$ is injective.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "j"] \arrow[d, "f"] & B \arrow[dl, dotted, "\exists g_i"] \arrow[ddl, dotted, "\exists f"] \\ & E_i \arrow[d, hook] & \\ & \prod E_i & \end{tikzcd}$$

Let $k_i(x) = (0, 0, \cdots, x, 0, 0, \cdots, 0)$, where the $x$ occurs in the $i$th position. As the $\prod E_i$ is injective, there exists a module homomorphism $f : B \to \prod E_i$. Note that there is also $\pi_i : \prod E_i \to E_i$, where $\pi_i\big((x_i)_{i \in \mathcal{I}}\big) \overset{\text{def}}{=} x_i$ and $\pi_i k_i = 1_{E_i}$. Let $g_i = \pi_i f$. Then one easily checks $\pi_i f j = \underbrace{\pi_i k_i}_{\text{id}} f_i = f_i$. $\square$

It is important to take note of a few things:

1. A *finite* direct sum of injective modules is injective because a finite direct sum is equal to a finite direct product.
2. You can have infinitely many injective modules and have $\bigoplus E_i$ *not* injective.
3. You can have an infinite family of projective modules $\{P_i\}$ but $\prod P_i$ *not* projective.
4. Each summand of an injective module is injective.

### 3.5 Divisible Modules and Snake Lemma

**Definition** (Divisible Group)**.** An abelian group $D$ is divisible if for all $y \in D$ and $n \in \mathbb{Z} \setminus \{0\}$, there is $x \in D$ such that $y = nx$.

**Example 3.3.** ${}_{\mathbb{Z}}\mathbb{Q}$ is divisible since if $y = a/b$, where $a, b \in \mathbb{Z}$ and $b \neq 0$, we let $x = \frac{a}{bn}$ and $nx = y$.

**Proposition 3.11.** *An abelian group $D$ is divisible if and only if ${}_{\mathbb{Z}}D$ is injective.*

Proof: Assume that $D$ is divisible. Let $I \neq 0$ be a left ideal of $\mathbb{Z}$. So $I = \langle n \rangle$ for some $n$. Consider

$$\begin{tikzcd} 0 \arrow[r] & \langle n \rangle \arrow[r, hook] \arrow[d, "f"] & \mathbb{Z} \arrow[dl, dotted, "\exists g"] \\ & D & \end{tikzcd}$$

to show that $f$ can be extended, let $y = f(n)$. Let $x \in D$ such that $nx = y$. Let $g : \mathbb{Z} \to D$, where $g(m) = mx$ and so $g(1) = x$. Then $g(an) = anx = ay$ so that $g|_{\langle x \rangle} = f$.

Now let $D$ be an injective $\mathbb{Z}$-module. Let $y \in D$ and $0 \neq n \in \mathbb{Z}$. We look at

$$\begin{tikzcd} 0 \arrow[r] & \langle n \rangle \arrow[r, hook] \arrow[d, "f"] & \mathbb{Z} \arrow[dl, dotted, "\exists g"] \\ & D & \end{tikzcd}$$

Let $f(an) \stackrel{\text{def}}{=} ay$. So $f$ is a homomorphism of $R$-modules. By Baer's Criterion, there is a $g$ with $g|_{\langle nrange} = f$ since $D$ is injective. Let $x = g(1)$. Then $g(n) = n \cdot g(1) = nx$. But $g(n) = f(n) = y$ so that $D$ is divisible. This also shows ${}_{\mathbb{Z}}\mathbb{Q}$ is an injective module over $\mathbb{Z}$. $\square$

It is also important to note that a direct sums of divisible modules is divisible and a quotient of divisible modules is divisible. Our goal to show that for any ring $R$ and $M$ an $R$-module then there is an injective $R$-module $E$ and a monomorphism $M \longrightarrow E$.

Now assume we have the following diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "f"] & B \arrow[r] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0 \end{tikzcd}$$

then there exists an exact sequence

$$\underbrace{0 \longrightarrow \ker f \longrightarrow \ker g}_{\text{Unv. Property Kernel}} \longrightarrow \underbrace{\ker h}_{\text{Exactness}} \xrightarrow{\delta} \underbrace{\operatorname{coker} f \longrightarrow \operatorname{coker} g \longrightarrow \operatorname{coker} h \longrightarrow 0}_{\text{Unv. Property of Cokernel}}$$

Consider

$$\begin{tikzcd} & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\ 0 \arrow[r, dotted] & \ker f \arrow[r, dotted] \arrow[d] & \ker g \arrow[r, dotted] \arrow[d] & \ker h \arrow[d] & \\ 0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & A' \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & C' \arrow[r] \arrow[d] & 0 \\ & \operatorname{coker} f \arrow[r, dotted] \arrow[d] & \operatorname{coker} g \arrow[r, dotted] \arrow[d] & \operatorname{coker} h \arrow[r, dotted] \arrow[d] & 0 \\ & 0 & 0 & 0 & \end{tikzcd}$$

This important result is often referred to as the Snake Lemma. To see why, simply look at the following diagram:

$$
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r, dashed] & \ker(a) \arrow[r] \arrow[d] & \ker(b) \arrow[r] \arrow[d] & \ker(c) \arrow[d] \arrow[dddll, rounded corners, "\delta"] & \\
0 \arrow[r, dashed] & A \arrow[r, "f"] \arrow[d, "a"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] \arrow[d] & B' \arrow[r, "g'"] \arrow[d] & C' \arrow[r, dashed] \arrow[d] & 0 \\
 & \operatorname{coker}(a) \arrow[r] \arrow[d] & \operatorname{coker}(b) \arrow[r] \arrow[d] & \operatorname{coker}(c) \arrow[r, dashed] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}
$$

**Theorem 3.3.** *Let ${}_{\mathbb{Z}}D$ be a divisible $\mathbb{Z}$-module and $R$ be a ring. Then* $\operatorname{Hom}_{\mathbb{Z}}(R, D)$ *is an injective $R$-module.*