Syracuse University

MATH 731:
Rings and Modules

Professor: Dr. Dan Zacharia
Notes By: Caleb McWhorter

Fall 2014

Last Updated: October 6, 2018

Contents

1 Introduction

1.1 Course Description

MAT 731 Rings and Modules: Submodules, factor modules, chain conditions, Hilbert basis theorem, division rings, Schur's lemma, Jacobson density theorem, semi-simple modules, socles, Jacobson radical, semi primitive rings, Artin-Wedderburn theorem, integral extensions, completions, localization.

1.2 Disclaimer

These notes were taken in Fall 2014 in a course taught by Professor Dan Zacharia. In some places, notation/material has been changed or added. Any errors in this text should be attributed to the typist – Caleb McWhorter – and not the instructor or any referenced text.

1.3 Assumptions

Unless otherwise stated, all rings are assumed to be noncommutative. All rings are assumed to have unity. For ring homomorphisms $\varphi : R \to S$, it is assumed that $\varphi(1_R) = 1_S$.

2 Elementary Category Theory

2.1 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 2.1.

(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 $f \cdot a \stackrel{\text{def}}{=} f(a)$, 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 $\overline{s} \in S^n$, write $\overline{s}$ as a row vector and compute $\overline{s}r$ via normal matrix multiplication. Writing $\overline{s} \in S^n$ as a column vector, compute $r\overline{s}$ via normal matrix multiplication.

◁

Example 2.2. Let S be a ring and let $R = M_n(S)$. Let

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

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

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

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 2.3. 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 2.4. 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 2.1. *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 2.2 (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 2.3 (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 2.4 (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 2.5 (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.*

2.2 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 2.5.

(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 ι_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 ${}_{\mathbb{Z}}\mathbf{Mod} = \mathbf{Ab}$.

◁

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 2.6.

(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 2.7.

(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* $T_A : \mathcal{C} \to \textbf{Sets}$, 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.**.

◁

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 $\mathcal{A}$:

$$\begin{array}{ccc} SA & \xrightarrow{\tau_A} & TA \\ {\scriptstyle Sf}\downarrow & & \downarrow{\scriptstyle Tf} \\ SA' & \xrightarrow[\tau_{A'}]{} & TA' \end{array}$$

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

Theorem 2.6 (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 $\gamma : \tau \mapsto \tau_A(1_A)$.

2.3 Products and Coproducts

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

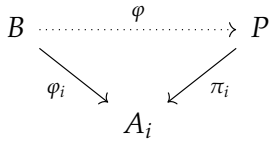
Definition (Product)**.** Let $\mathcal{C}$ be a category and $\{A_i \mid i \in \mathcal{I}\}$ be a family of objects of $\mathcal{C}$. A product for the family $\{A_i \mid i \in \mathcal{I}\}$ is an object P of $\mathcal{C}$ together with a family of morphisms

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

such that for any object B and any family of morphisms

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

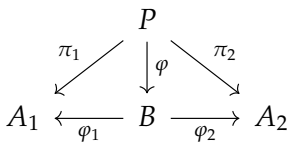
there is a unique morphism $\varphi : B \to P$ such that $\pi_i \circ \varphi = \varphi_i$ for all $i \in \mathcal{I}$. That is, there is a Universal Mapping Property.



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

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

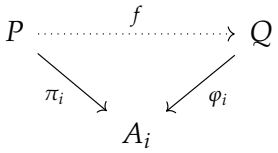
It is usually most helpful to describe products in terms of their commutative diagrams. A product for $\{A_1, A_2\}$ is a diagram of objects and morphisms $A_1 \xleftarrow{\pi_1} P \xrightarrow{\pi_2} A_2$ such that for any other diagram of the form $A_1 \xleftarrow{\varphi_1} B \xrightarrow{\varphi_2}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

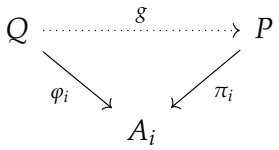


It is important to note that a product need not exist in a given category. However, this will not be a problem for the categories with which we will be working—abelian groups and sets. For example in the category of sets, the Cartesian product $\prod_{i\in\mathcal{I}} A_i$ is a product of the family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

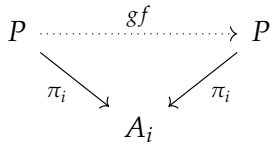
Theorem 2.7. *If $(P, \{\pi_i\})$ and $(Q, \{\varphi_i\})$ are both products of the family $\{A_i \mid i \in \mathcal{I}\}$ objects of a category $\mathcal{C}$, then P and Q are equivalent.*

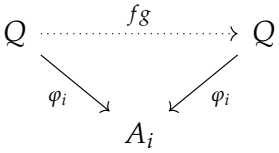
Proof. Since P, Q are both products, they each have their family of morphisms to the A_i's. We obtain the following commutative diagrams:





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





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 $\amalg_{i\in\mathcal{I}} A_i$.

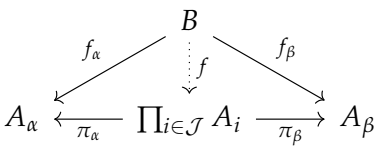
Notice again these do *not* assure existence, just uniqueness.

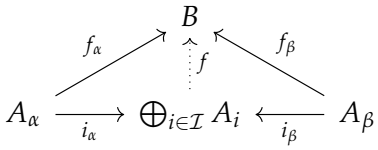
Theorem 2.8. *If $(S, \{\tau_i\})$ and $(S', \{\lambda_i\})$ are both coproducts for the family $\{A_i \mid i\mathcal{I}\}$ of objects of a category $\mathcal{C}$, then S and S' are equivalent.*

Proof. Simply use the dual of the argument of Theorem 2.7. □

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).





3 Exact Sequences

3.1 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 3.1.

(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 3.1. *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, $B/\operatorname{im} f \cong C$. □

3.2 The Short 5 Lemma

Lemma 3.1 (The Short 5 Lemma)**.** *Let* R *be a ring and let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow[f']{} & B' & \xrightarrow[g']{} & C' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of R*-modules and* R*-module homomorphisms such that each row is a short exact sequence, then*

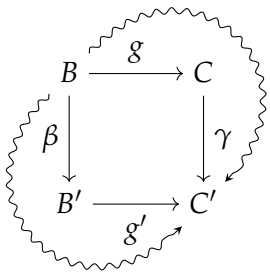
(i) If α, γ are monomorphisms then β is a monomorphism.

(ii) If α, γ are epimorphisms then β is an epimorphism.

(iii) If α, γ are isomorphisms then β 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'.

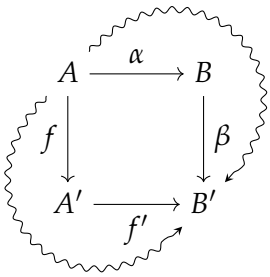
(i) Let $b \in B$ such that $\beta(b) = 0$, we want $b = 0$ (so we are going to show that the kernel is trivial).



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 γ 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:

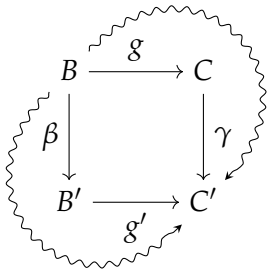


Using our initial assumption that $\beta(b) = 0$, we have

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

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



We know that $g'(b') \in C$. As γ 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 α 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 β is an epimorphism. □

3.3 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:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & {\scriptstyle f^{-1}}\uparrow\downarrow{\scriptstyle f} & & {\scriptstyle g^{-1}}\uparrow\downarrow{\scriptstyle g} & & {\scriptstyle h^{-1}}\uparrow\downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

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,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{s} & B & \xrightarrow{t} & C & \longrightarrow & 0 \\ & & {\scriptstyle f^{-1}}\uparrow\downarrow{\scriptstyle f} & & {\scriptstyle g^{-1}}\uparrow\downarrow{\scriptstyle g} & & {\scriptstyle h^{-1}}\uparrow\downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \xrightarrow{s'} & B' & \xrightarrow{t'} & C & \longrightarrow & 0 \end{array}$$

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 3.1. *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:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_N} & & \downarrow{\scriptstyle (f',g)} & & \downarrow{\scriptstyle 1_P} & & \\ 0 & \longrightarrow & N & \xrightarrow{i_1} & N \oplus P & \xrightarrow{\pi_2} & P & \longrightarrow & 0 \end{array}$$

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 3.1.

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{i_1} & N \oplus P & \xrightarrow{\pi_2} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_N} & & \downarrow{\scriptstyle f+g'} & & \downarrow{\scriptstyle 1_N} & & \\ 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

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 3.1. □

Definition (Split Exact Sequence)**.** A short exact sequence satisfying any of the equivalent conditions of Theorem 3.1 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 3.1 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 3.2. 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 3.1, 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. ◁

3.4 Idempotents and Indecomposables

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

Example 3.3.

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

(ii) Let

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

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 $(hg)^2 = (hg)(hg) = h(gh)g = h1g = hg$.

◁

Let M be an R-module and let $\mathrm{End}_R(M) = \{f : M \to M \mid f \text{ homomorphism}\}$. Then $\mathrm{End}_R(M)$ is a ring. We define $(f+g)(m) \stackrel{\text{def}}{=} f(m) + g(m)$ and $gf \stackrel{\text{def}}{=} g \circ f$. 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

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

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, $\mathrm{End}_R(M)$ always has nontrivial idempotents whenever M is decomposable. By contrapositive, if $\mathrm{End}_R(M)$ has no nontrivial idempotents, then M is indecomposable.

We summarize the preceding remark in the following proposition:

Proposition 3.2. *If* $\mathrm{End}_R(M)$ *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 3.4. Suppose we have a short exact sequence

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

By Theorem 3.1, $M \cong A \oplus C$. 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, $e_A e_C = e_C e_A = 0$ so that e_A and e_C are orthogonal idempotents. ◁

Lemma 3.2. *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. □

3.5 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. $g : M \to A$:

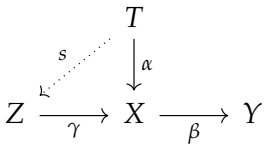
$$M \xrightarrow{g} A \xrightarrow{f} B$$

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 β 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 $\beta\alpha = 0$

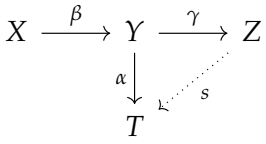


Then there exists a unique $s : T \to Z$ such that $\alpha = \gamma s$.

Let $\beta : X \to Y$ be a homomorphism. A cokernel of β 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 $s : Z \to T$.



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 3.3. *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

$$\begin{array}{ccccccccc} & & & & M & & & & \\ & & & \overset{s}{\swarrow} & \downarrow{\scriptstyle h} & & & & \\ 0 & \longrightarrow & A & \xrightarrow[f]{} & B & \xrightarrow[g]{} & C & \longrightarrow & 0 \end{array}$$

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 $\operatorname{Hom}_R(M, B)$. □

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 3.5. 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 π_* cannot be surjective. ◁

Example 3.6. 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 $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = 0$. Also, observe that $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, 2\mathbb{Z}) = 0$ so the above series is equivalent to

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

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

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 $\mathrm{Hom}_R(M, -)$ (this is said Hom_R M "blank") gives us abelian groups $\mathrm{Hom}_R(M, A)$, $\mathrm{Hom}_R(M, B)$, and $\mathrm{Hom}_R(M, C)$. In categorical terms, $\mathrm{Hom}_R(M, -)$ 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, $\mathrm{Hom}_R(M, -)$ is a left exact functor. The functor $\mathrm{Hom}_R(-, M)$ is similarly left exact but requires the original sequence to be exact on the right.

Proposition 3.4. *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

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

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

Proof. L.T.R.. □

Remark. As with Proposition 3.3, 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 3.4 says that $\mathrm{Hom}_R(-, M)$ is a (left exact) contravariant functor from R-modules to abelian groups. Putting Proposition 3.3 and Proposition 3.4 together, we obtain the following theorem:

Theorem 3.2. Hom *is a left exact functor from R-modules to abelian groups.*

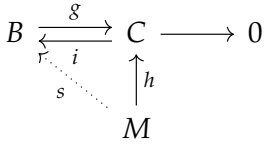
Note that while Proposition 3.3 and Proposition 3.4 do not generally yield exact sequence (only left exact), they do yield exact sequences when applied to split exact sequences.

Proposition 3.5. *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 3.3, 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 $h \in \mathrm{Hom}_R(M, C)$.



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 3.3

Proposition 3.6. *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.*

4 Free Modules, Projective Modules, and Injective Modules

4.1 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 4.1. *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 μ_b as

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

Denoting μ_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 4.2. *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 $s \in R$, $sv = \sum sr_b b$. 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 4.3. *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 $R = \mathrm{End}_k(V)$, 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.

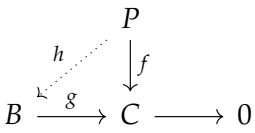
Theorem 4.1. *Every left R-module M is the quotient of a free left R-module F. Moreover, M is finitely generated if and only if F can be chosen to be finitely generated.*

Proof. Choose a generating set X of M. Let F be a free module on basis $\{b_x : x \in X\}$ (this makes use of Proposition 4.1). By Proposition 4.2, 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. □

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 4.1.

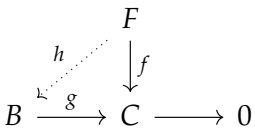
4.2 Projective Modules

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 $gh = f$.



Lemma 4.1. *Every free module is projective.*

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



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. □

In fact in some sense, projective modules are 'close' to being free modules in that they have a dual basis, see Lemma 4.2. There are also many equivalent definitions for a projective module, each useful in various situations.

Proposition 4.4. *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 $1_P : P \to P$.

$$\begin{array}{ccccc} & & & & P \\ & & \overset{h}{\swarrow} & & \downarrow 1 \\ X & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

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

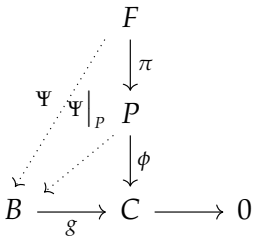
$$0 \longrightarrow \ker g \xrightarrow{\iota} F \xrightarrow{g} P \longrightarrow 0.$$

By assumption, there exists a map $h : P \to F$ such that $gh = 1_P$. But then by Theorem 3.1, P is a direct summand of F.

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

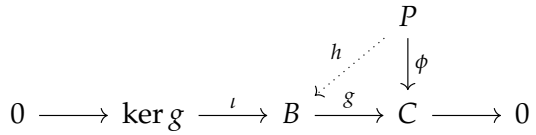
$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence. By Proposition 3.3, 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



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 4.2, 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



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. □

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 4.2 (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 4.5.

(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

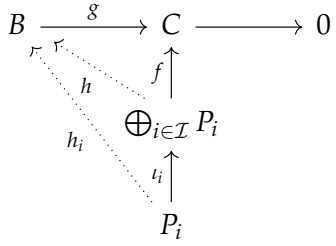
$$\bigoplus_{i\in\mathcal{I}} F_i = \bigoplus_{i\in\mathcal{I}} (P_i \oplus Q_i) = \bigoplus_{i\in\mathcal{I}} P_i \oplus \bigoplus_{i\in\mathcal{I}} Q_i.$$

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 4.6. *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:



where ι_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 4.1. 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 4.2. 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 4.7. *Suppose that the following diagram is commutative with exact rows*

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & & & \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

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

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

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \vdots{\scriptstyle h} & & \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

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

$$\begin{array}{ccc} b & \xrightarrow{g} & x = g(b) \\ \downarrow{\scriptstyle \beta} & & \\ \beta(b) & \longrightarrow & g'\beta(b) \end{array}$$

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

$$\begin{array}{ccc} b_1 & & \\ & \searrow & \\ b & \xrightarrow{g} & x = g(b) \\ \downarrow{\scriptstyle \beta} & & \\ \beta(b) & \longrightarrow & g'\beta(b) \end{array}$$

We need check that $g'(\beta(b)) = g'(\beta(b;))$. Note that $g(b_1 - b) = 0$ so that $b_1 - b = f(a)$ for some $a \in A$. Then $\beta(b_1 - b) = \beta(f(a)) = f'(\alpha(a))$. Moreover, $g'(\beta(b_1 - b)) = g'(f'(\alpha(a))) = 0$, because of exactness. So we know that $g'(\beta(b_1)) = g'(\beta(b))$ so that the map is well defined. By construction, it commutes the diagram.

However, there is an easier way of demonstrating this.

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \vdots{\scriptstyle h} & & \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

Note we have $B \xrightarrow{g} C$ and look at the cokernel of f. We have $g'\beta f = g'f'\alpha = 0$. Then simply use the Universal Property of the Cokernel.

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ & & \downarrow{\scriptstyle g'\beta} & \swarrow{\scriptstyle \exists! h} & \\ & & C' & & \end{array}$$

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,

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

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'.

$$\begin{array}{ccccccc} & & & & A & & \\ & & & \swarrow{\scriptstyle f'h} & \downarrow{\scriptstyle \beta f} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

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 $f'h = \beta f$. □

4.3 Injective Modules

Let $f : A \to B$ be a homomorphism and let M be another R-module. We have an induced map of abelian groups

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

given by $f^M_*(\beta) = \beta f$.

Proposition 4.8. *Let* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *be a short exact sequence. Then the sequence*

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

is exact.

Proof: Exercise

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

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B \\ & & \downarrow{\scriptstyle h} & \swarrow{\scriptstyle \exists p} & \\ & & M & & \end{array}$$

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

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B \\ & & \downarrow{\scriptstyle h} & \swarrow{\scriptstyle g} & \\ & & I & & \end{array}$$

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 4.9. *${}_RI$ 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.*

4.4 Baer's Criterion

Theorem 4.2 (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*

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{incl} & R \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle s} & \\ & & E & & \end{array}$$

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

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \longrightarrow & B \\ & & \downarrow{\scriptstyle f} & & \\ & & E & & \end{array}$$

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

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \hookrightarrow & B \\ & & \downarrow{\scriptstyle f} & & \\ & & E & & \end{array}$$

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

$$\begin{array}{ccccc} A & \hookrightarrow & A' & \hookrightarrow & B \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle f'} & & & \\ E & & & & \end{array}$$

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

$$\begin{array}{ccccccccc} A & & \subseteq & & A' & & \subseteq & & A'' & & \subseteq & & B \\ \downarrow{\scriptstyle f} & & & \swarrow{\scriptstyle f'} & & & & \swarrow{\scriptstyle f''} & & & & & \\ E & & & & & & & & & & & & \end{array}$$

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.

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \hookrightarrow & A^* & \hookrightarrow & B \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle f^*} & & & \\ & & E & & & & \end{array}$$

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

$$\begin{array}{ccccccc} 0 & \hookrightarrow & A & \hookrightarrow & A^* & \hookrightarrow & A^* + \langle b \rangle = \overline{A} \\ & & & & \downarrow{\scriptstyle f^*} & & \\ & & & & E & & \end{array}$$

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

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \hookrightarrow & R \\ & & \downarrow{\scriptstyle j} & \swarrow{\scriptstyle \exists \bar{j}} & \\ & & E & & \end{array}$$

where $j(r) \stackrel{\text{def}}{=} f^*(rb)$. 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) □

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.

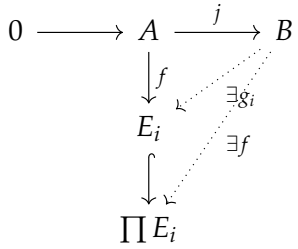
Proposition 4.10. *Let $\{E_i\}_{i \in \mathcal{I}}$ be a family of R-modules. Then each E_i is injective if and only if $\prod_{i \in \mathcal{I}} E_i$ is injective.*

Proof: Let each E_i be injective.

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{j} & B \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \exists g} & \\ & & \prod E_i & \swarrow{\scriptstyle g_i} & \\ & & \downarrow{\scriptstyle \pi_i} & & \\ & & E_i & & \end{array}$$

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.



Let $k_i(x) = (0, 0, \cdots, x, 0, 0, \cdots, 0)$, where the x occurs in the ith 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 $\pi_i\big((x_i)_{i\in\mathcal{I}}\big) \stackrel{\text{def}}{=} x_i$ and $\pi_i k_i = 1_{E_i}$. Let $g_i = \pi_i f$. Then one easily checks $\pi_i f j = \underbrace{\pi_i k_i}_{\text{id}} f_i = f_i$. □

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.

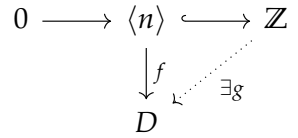
4.5 Divisible Modules and Snake Lemma

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 4.3. ${}_{\mathbb{Z}}\mathbb{Q}$ 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 4.11. *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



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

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle n \rangle & \hookrightarrow & \mathbb{Z} \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \exists g} & \\ & & D & & \end{array}$$

Let $f(an) \overset{\text{def}}{=} ay$. 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 $\mathbb{Z}$. □

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

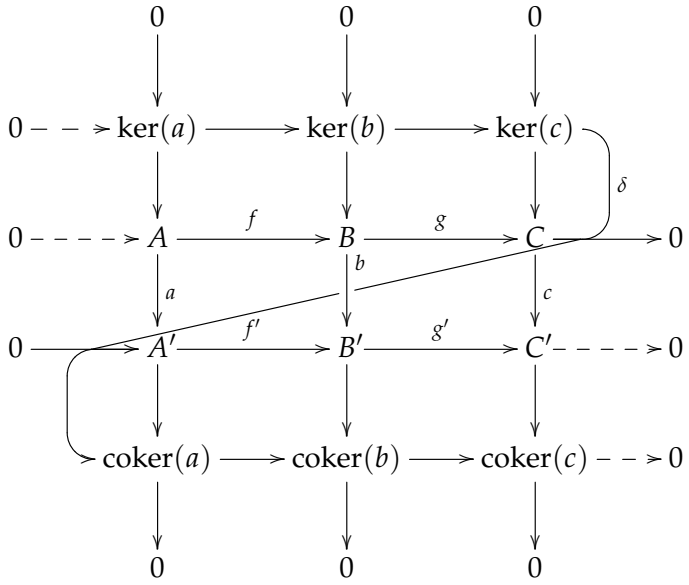
then there exists an exact sequence

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

Consider

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \cdots\cdots\rightarrow & \ker f & \cdots\cdots\rightarrow & \ker g & \cdots\cdots\rightarrow & \ker h & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \operatorname{coker} f & \cdots\cdots\rightarrow & \operatorname{coker} g & \cdots\cdots\rightarrow & \operatorname{coker} h & \cdots\cdots\rightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

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



Theorem 4.3. *Let ${}_{\mathbb{Z}}D$ be a divisible $\mathbb{Z}$-module and R be a ring. Then* $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ *is an injective R-module.*

5 Tensor Products and Flat Modules

5.1 Tensor Product

Definition (Biadditve R-function)**.** Let R be a ring. Let A_R and ${}_RB$ be right and left R-modules, respectively. Let G be a $\mathbb{Z}$-module. Then a biadditive R-function is a function $A \times B \to G$ with

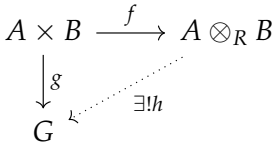
1.

$$f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$$
$$f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$$

2. $f(ar, b) = f(a, rb)$

for all $a, a_1, a_2 \in A$ and $b, b_1, b_2 \in B$. If R is commutative, then the function f is just a bilinear function.

Definition (Tensor Product)**.** A tensor product over R of A_R and ${}_RB$ is an abelian group $A \otimes_R B$ together with a biadditive function $A \times B \xrightarrow{f} A \otimes_R B$ satisfying the following universal property: for all $g : A \times B \to G$, a biadditive homomorphism of abelian groups, there is a unique homomorphism $h : A \otimes_R B \to G$ commuting the following diagram



Theorem 5.1. *Given A_R,$_R B$, their tensor product exists and is unique up to isomorphism.*

Proof: First, we prove the existence of such an object. Let F be the free abelian group with basis $A \times B$. So the elements of F are finite linear combinations of ordered pairs in $A \times B$ together with integer coefficients. Let S be the subgroup of F generated by elements of the form

(i) $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$

(ii) $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$

(iii) $(ar, b) - (a, rb)$

Define $A \otimes_R B \overset{\text{def}}{=} F/S$. Furthermore, define $a \otimes b$ to be the coset of (a, b), i.e. $(a, b) + S$. Observe that for all $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$, and $r \in R$, we have

(i) $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$

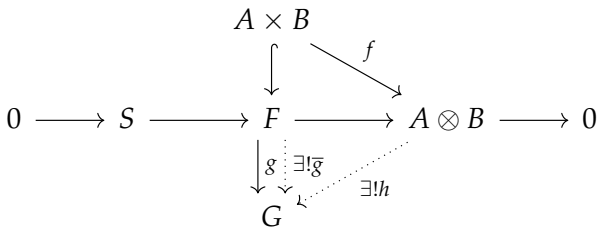
(ii) $a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$

(iii) $ar \otimes b = a \otimes rb$

We have a map $A \times B \xrightarrow{f} A \otimes_R B$. It is simple to show that f is biadditive. We also have an exact sequence of $\mathbb{Z}$-modules:

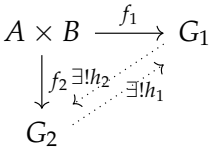
$$0 \longrightarrow S \xhookrightarrow{\text{incl}} F \xrightarrow{\overline{f}} A \otimes_R B \longrightarrow 0$$

We need show that the universal property of tensor products is satisfied.



Now g is a biadditive map and G is an abelian group. Now F is free on $A \times B$ so that there exists a unique map $g : F \to G$ such that $\overline{g}|_{A \times B} = g$. Now as g is biadditive, we have $S \subseteq \ker \overline{g}$. Using the universal property of the cokernel, there exists a unique map $h : A \otimes B \to G$ with $h\overline{f} = \overline{g}$. Now comparing this with $A \times B \hookrightarrow F$, we get $hf = g$.

Now we demonstrate uniqueness of the tensor product. Assume that G_1, G_2 are tensor products of A, B. Then



Now there exists a unique map h_1 since G_1 is a tensor product with $h_1 f_1 = f_2$. But as G_2 is a tensor product, there exists a unique map h_2 with $h_2 f_2 = f_1$. But then $(h_2 h_1) f_1 = f_1$. Note that the map $1_{G_1} f_1 = f_1$ works and must be unique. But then $h_2 h_1 = 1_{G_1}$. Similarly, $h_1 h_2 = 1_{G_2}$ so that we must have $G_1 \cong G_2$. □

Remark. The elements of $A \otimes_R B$ are of the form $\sum_{i \in \mathcal{I}} a_i \otimes b_i$, where $a_i \in A$ and $b_i \in B$. These elements are usually *not* of the form $a \otimes b$.

Remark. Assume R is a commutative ring. Let A, B be two R-modules. Form the tensor product $A \otimes_R B$ with F and S as given before. Then $A \otimes_R B$ is an R-module.

$$r\left(\sum_{i \in \mathcal{I}} a_i \otimes b_i\right) = \sum_{i \in \mathcal{I}} ra_i \otimes b_i = \sum_{i \in \mathcal{I}} a_i \otimes rb_i$$

Later, we will prove the following:

Theorem 5.2. *Let R be a commutative ring. Let A be a free module with basis $\{e_i\}_{i\in\mathcal{I}}$ and B a free module with basis $\{f_j\}_{j\in\mathcal{J}}$. Then $A \otimes_R B$ is a free R-module with basis $\{e_i \otimes f_j\}_{i\in\mathcal{I},j\in\mathcal{J}}$.*

Corollary 5.1. *Let F be a field and V a vector space with basis $\{e_i\}_{i\in\mathcal{I}}$ and W a vector space with basis $\{f_j\}_{j\in\mathcal{J}}$, then $V \otimes_F W$ is a vector space with basis $\{e_i \otimes f_j\}_{i\in\mathcal{I},j\in\mathcal{J}}$. If we have* $\dim V = n < \infty$, $\dim W = m < \infty$, *then* $\dim V \otimes_F W = nm$.

Example 5.1. Let F be a field. Let V be a 2-dimensional vector space with basis $\{v_1, v_2\}$. We look at $V \otimes_F V$. We know $\dim V \otimes_F V = 4$ and a basis for this vector space is $\{v_1 \otimes v_1, v_1 \otimes v_2, v_2 \otimes v_1, v_2 \otimes v_2\}$. We look at $v_1 \otimes v_1 + v_2 \otimes v_2 \in V \otimes_F V$. We claim we cannot write $v_1 \otimes v_1 + v_2 \otimes v_2$ as $u \otimes w$ for some $u \in V$, $w \in V$.

Assume to the contrary that this is possible. Let $u = a_1v_1 + a_2v_2$ and $w = b_1v_1 + b_2v_2$. Then

$$\begin{aligned} v_1 \otimes v_1 + v_2 \otimes v_2 &= (a_1v_1 + a_2v_2) \otimes (b_1v_1 + b_2v_2) \\ &= a_1b_1v_1 \otimes v_1 + a_2b_2v_2 \otimes v_2 + a_1b_2v_1 \otimes v_2 + a_2b_1v_2 \otimes v_1 \end{aligned}$$

But then using the chosen basis for the tensor product, we must have

$$\begin{aligned} a_1b_1 &= 1 \\ a_2b_2 &= 1 \\ a_1b_2 &= 0 \\ a_2b_1 &= 0 \end{aligned}$$

So $a_i \neq 0 \neq b_j$ for all i, j. This method works for any dimension, not just dimension 2. Only obtains *only* $u \otimes v$'s alone in dimension 1.

Example 5.2. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ for $n > 1$. The tensor product $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is generated (not equal to but generated by) elements of the form $q \otimes \overline{a}$, where $q \in \mathbb{Q}$ and $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. We claim that $q \otimes \overline{a} = 0$ for all $q \in \mathbb{Q}$ and $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Let $1 = \alpha/\beta$, then

$$q \otimes_{\mathbb{Z}} \overline{a} = \frac{\alpha}{n} \otimes_{\mathbb{Z}} \overline{a} = \frac{n\alpha}{n\beta} \otimes_{\mathbb{Z}} \overline{a} = \frac{\alpha}{n\beta} \otimes_{\mathbb{Z}} n\overline{a} = \frac{\alpha}{n\beta} \otimes_{\mathbb{Z}} 0 = 0$$

However, one can't always "move things over". Take $A \otimes_R B$. Suppose $a \otimes_R b$ and $b = 0$ for some $r \in R$ and $a = a'r$, where a' is not necessarily in A. Then one *cannot* write

$$a \otimes_R b \neq a' \otimes_R rb = 0$$

One is reminded of ideals, for $a = a'r$ with $a' \notin A$.

Proposition 5.1. *Let M be an R-module. Then $R \otimes_R M \cong M$.*

Proof: We know $R \otimes_R M$ is a left R-module via

$$r\left(\sum_{i\in\mathcal{I}} r_i \otimes m_i\right) = \sum_{i\in\mathcal{I}} rr_i \otimes m_i$$

Let $\sum r_i \otimes m_i \in R \otimes_R M$. As $r_i = 1 \cdot r_i$ and $r_i \otimes m_i = 1 \otimes r_i m_i$, we have

$$\sum 1 \otimes r_i m_i = 1 \otimes \sum r_i m_i$$

But $\sum r_i m_i \in M$ as M is an R-module. Define $g(r, m) \stackrel{\text{def}}{=} rm$. Now g is biadditive (as an M module). We have $f(r, m) = r \otimes m$.

$$\begin{array}{ccc} R \times M & \xrightarrow{\quad g \quad} & M \\ \Big\downarrow{\scriptstyle f} & \overset{\exists! h}{\nearrow} & \\ R \otimes_R M & & \end{array}$$

Then there exists a unique $h : R \otimes_R M \to M$ such that the above diagram commutes. We have $h(r \otimes m) = rm$. Now h is a left homomorphism of modules as $sh(r \otimes m) = s(rm) = (sr)m = h(sr \otimes m)$. We need an inverse homomorphism $\overline{h}$. Let $\overline{h} : M \to R \otimes_R M$ be $\overline{h}(m) = 1 \otimes m$. Then

$$\begin{aligned} \overline{h}(rm) &= 1 \otimes rm \\ &= r \otimes m \\ &= r(1 \otimes m) \\ &= r\overline{h}(m) \end{aligned}$$

so that $\overline{h}$ is a homomorphism. Observe also that $h\overline{h} = \overline{h}h = 1$. □

Proposition 5.2. *If M_R is an R-module, then there exists an isomorphism of right R-modules, $M \otimes_R R \xrightarrow{\sim} M$.*

Proposition 5.3. *If R is a commutative ring and A, B are R-modules then there is an isomorphism of R-modules $A \otimes_R B \xrightarrow{\sim} B \otimes_R A$.*

Proposition 5.4. *Let I be a two-sided ideal of R ($I \lhd R$). Let ${}_R M$ be a left R-module, then $R/I \otimes M$ is a left R-module. In fact, it is a left R/I-module via*

$$R : r(\overline{s} \otimes m) \stackrel{def}{=} r\overline{s} \otimes m$$

$$R/I : \overline{r}(\overline{s} \otimes m) \stackrel{def}{=} \overline{rs} \otimes m$$

Theorem 5.3. *If $I \lhd R$ and ${}_RM$, then there exists an isomorphism of R-modules (in fact of R/i-modules) from $R/I \otimes_R M \xrightarrow{\sim} M/IM$, where*

$$IM = \{\sum \alpha_i m_i \mid \alpha_i \in I, m_i \in M\}$$

Proof: An element in $R/I \otimes_R M$ is of the form $\sum \overline{r_i} \otimes_R m_i$, where $\overline{r_i} \in R/I$. But

$$\begin{aligned}\sum \overline{r_i} \otimes_R m_i &= \sum (\overline{1} \cdot r_i) \otimes_R m_i \\ &= \sum \overline{1} \otimes_R r_i m_i \\ &= 1 \otimes m\end{aligned}$$

for some $m \in M$. Now let $R/I \otimes_R M \xrightarrow{h} M/IM$ be given by $h(\overline{1} \otimes_R m) \stackrel{\text{def}}{=} m + IM$. We will denote $m + IM$ as $\overline{m}$. It is clear that h is a homomorphism of left modules. (Why?) Let $\overline{h} : M/IM \to R/I \otimes_R M$ be given by $\overline{h}(m + IM) = \overline{1} \otimes_R m$. It is clear that $\overline{h}$ is a homomorphism. (Why?) Then $h\overline{h} = \overline{h}h = 1$. □

Example 5.3. $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$. We can take $R = \mathbb{Z}$, $I = m\mathbb{Z}$, and $M = \mathbb{Z}/n\mathbb{Z}$.

5.2 Tensor Products of Homomorphisms

Suppose we have $A_R \xrightarrow{f} B_R$, ${}_RA' \xrightarrow{f'}{}_R B'$ be homomorphisms. We claim that there exists an induced homomorphism of abelian groups

$$A \otimes_R A' \xrightarrow{f \otimes f'} B \otimes_R B'$$

such that $(f \otimes f')(a \otimes a') = f(a) \otimes f'(a')$. We can say that

$$\begin{array}{ccc} A \times A' & \xrightarrow{g} & B \otimes B' \\ \downarrow f & \nearrow h & \\ A \otimes A' & & \end{array}$$

where $g(a, a') = f(a) \otimes f'(a')$ is a biadditive function. Then the Universal Property of the Kernel says that there exists a unique homomorphism $h : A \otimes A' \longrightarrow B \otimes B'$ with the "right" property.

Example 5.4. If M_R is a right R-module and we have a homomorphism of left R-modules ${}_RA \xrightarrow{f}{}_R B$, then we have a homomorphism of abelian groups

$$M \otimes_R A \xrightarrow{1_M \otimes f} M \otimes_R B$$

given by $m \otimes a \xrightarrow{m} \otimes f(a)$.

Now suppose that we have a short exact sequence

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

Given a right R-module M_R, we can ask about the sequence

$$0 \longrightarrow M \otimes A \xrightarrow{1_M \otimes f} M \otimes B \xrightarrow{1_M \otimes g} M \otimes C \longrightarrow 0$$

This sequence is not *usually* exact.

Theorem 5.4. *If* $0 \longrightarrow_R A \xrightarrow{f}_R B \xrightarrow{g}_R C \longrightarrow 0$ *is exact and* M_R *is a right* R*-module, then the sequence* $M \otimes A \xrightarrow{1_M \otimes f} M \otimes B \xrightarrow{1_M \otimes g} M \otimes C \longrightarrow 0$ *of abelian groups is exact. Furthermore, if the sequence* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *is split exact, then* $0 \longrightarrow M \otimes A \xrightarrow{1_M \otimes f} M \otimes B \xrightarrow{1_M \otimes g} M \otimes C \longrightarrow 0$ *is split exact.*

Proof: Let $x \in M \otimes_R C$. Now as g is onto

$$\begin{aligned} x &= \sum m_i \otimes c_i \\ &= \sum m_i \otimes g(b_i) \\ &= \sum 1_M(m_i) \otimes g(b_i) \\ &= \sum (1_M \otimes g)(m_i \otimes b_i) \\ &= (1_M \otimes g) \sum m_i \otimes b_i \end{aligned}$$

so that $1_M \otimes g$ is onto. Now

$$\begin{aligned} (1_M \otimes g)(1_M \otimes f)(m \otimes a) &= (1_M \otimes g)(m \otimes f(a)) \\ &= m \otimes \underbrace{g(f(a))}_{=0} = 0 \end{aligned}$$

as $gf = 0$. Therefore, $\mathrm{im}(1_M \otimes f) \subseteq \ker(1_M \otimes g)$. To prove that $\ker(1_M \otimes g) \subseteq \mathrm{im}(1_M \otimes f)$ is much harder and will not be treated here (see page 210 Hungerford *Algebra* or Dummit & Foote). □

Let R be a ring. Let ${}_RM$ be a left R-module. Then $\mathrm{Hom}_R(R, M)$ is a left R-module via $(rf)(s) \stackrel{\mathrm{def}}{=} f(sr)$, where $r, s \in R$ and $f \in \mathrm{Hom}_R(R, M)$. We claim that rf is in $\mathrm{Hom}_R(R, M)$.

Proposition 5.5. *There is an isomorphism of left* R*-modules* $\mathrm{Hom}_R(R, M) \xrightarrow{\psi} M$.

Proof (Sketch): We have $\psi : f \mapsto f(1)$ a homomorphism. Then let $M \xrightarrow{\varphi} \mathrm{Hom}_R(R, M)$ be given by $\varphi(m) \stackrel{\mathrm{def}}{=} f_M$, where $f_M(r) = rm$. Now f_M is a homomorphism so that φ is a homomorphism. Furthermore, φ and ψ are inverses of each other. □

5.3 Functorial

Theorem 5.5. *Let R be a ring. There is a functorial isomorphism $R \otimes M \xrightarrow{\varphi_M} M$ for every left module M.*

Functorial means for all modules ${}_RM \xrightarrow{g}{}_R N$, the following diagram commutes

$$\begin{array}{ccc} R \otimes_R M & \xrightarrow{\varphi_M} & M \\ \downarrow{\scriptstyle 1_R \otimes g} & & \downarrow{\scriptstyle g} \\ R \otimes_R N & \xrightarrow{\varphi_N} & N \end{array}$$

where φ_M, φ_N are isomorphisms. (Show this) We also have functorial isomorphisms $M \otimes_R R \longrightarrow M$.

Now let A_R and ${}_RB$ be R-modules with $A'_R, {}_RB'$ submodules. Let $a \in A'$ and $b \in B'$. Then $a \otimes b \in A' \otimes_R B'$ and $a \otimes b \in A \otimes_R B$. But it can be the case that $a \otimes b = 0$ in $A \otimes_R B$ but be nonzero in $A' \otimes_R B'$ so that $A' \otimes_R B'$ is *not* a subgroup of $A \otimes_R B$.

Example 5.5. Let $R = \mathbb{Z}$, $A = \mathbb{Z}$, $B = \mathbb{Z}/3\mathbb{Z}$, $A' = 3\mathbb{Z}$, and $B' = \mathbb{Z}/3\mathbb{Z}$. Let $0 \neq b \in B$, say $b = \overline{1}$. We look at $3 \otimes \overline{1}$. We have $3 \otimes \overline{1} \in A' \otimes B'$ nonzero but inside $A \otimes B$, $A \otimes_R B = \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$.

$$3 \otimes_Z \overline{1} = 1 \otimes_{\mathbb{Z}} \overline{3} = 1 \otimes 0 = 0$$

Example 5.6. We look at $0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow 0$, where $f(m) = 3m$. Let $M = \mathbb{Z}/3\mathbb{Z}$. Then $f \otimes 1_M$ is not injective. We have $f \otimes 1_M : \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$.

$$(f \otimes 1_M)(a \otimes b) = f(a) \otimes b = 3a \otimes_{\mathbb{Z}} b = a \otimes_{\mathbb{Z}} 3b = a \otimes 0 = 0$$

so $f \otimes 1_M$ is the zero map. This shows that the tensor product of injective maps need not be injective.

Theorem 5.6 (Adjoint Isomorphism Theorem)**.** *Let R, S be rings. Let $A_R, {}_RB_S, C_S$. Then there is an isomorphism of abelian groups*

$$\mathrm{Hom}_S(A \otimes_R B, C) \xrightarrow{\sim} \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$$

which is functorial in A, B, and C.

We explain what functorality in A, B, and C means. To be functorial in C, we have if g is homomorphism $C_S \xrightarrow{g} C'_S$, then we have

$$\begin{array}{ccc} \mathrm{Hom}_S(A \otimes B, C) & \xrightarrow{\varphi_{A,B,C}} & \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \\ \downarrow{\scriptstyle 1_R \otimes g} & & \downarrow{\scriptstyle g} \\ \mathrm{Hom}_S(A \otimes B, C') & \xrightarrow{\varphi_{A,B,C'}} & \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C')) \end{array}$$

where the map on the left is $\mathrm{Hom}(A \otimes B, g)$ and the map on the right is $\mathrm{Hom}(A, \mathrm{Hom}(B, g))$.

Functorality in A means given a homomorphism $A \xrightarrow{g} A'$, then $A \otimes B \xrightarrow{g \otimes 1_B} A' \otimes B \longrightarrow C$.

$$\begin{array}{ccc} \mathrm{Hom}(A' \otimes B, C) & \xrightarrow{\varphi_{A',B,C}} & \mathrm{Hom}(A', \mathrm{Hom}(B, C)) \\ \downarrow{\scriptstyle 1_R \otimes g} & & \downarrow{\scriptstyle g} \\ \mathrm{Hom}(A \otimes B, C) & \xrightarrow{\varphi_{A,B,C}} & \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \end{array}$$

where the map on the left is $\mathrm{Hom}(g \otimes 1_B, C)$ and the map on the right is $\mathrm{Hom}(g, \mathrm{Hom}_S(B, C))$ and $\varphi_{A',B,C}$, $\varphi_{A,B,C}$ are isomorphisms.

Now we show that it means to be functorial in B. (Exercise)

Theorem 5.7 (Adjoint Isomorphism Theorem)**.** *Let R, S be rings. Let $A_R, {}_R B_S, C_S$. Then there is an isomorphism of abelian groups*

$$\mathrm{Hom}_S(A \otimes_R B, C) \xrightarrow{\sim} \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$$

which is functorial in A, B, and C.

Proof: We need a map $\varphi : \mathrm{Hom}_S(A \otimes_R B, C) \longrightarrow \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$. Let $f : A \otimes_R B \longrightarrow C$. We have $\varphi(f) : A \longrightarrow \mathrm{Hom}_S(B, C)$ and $\varphi(f)(a) : B \longrightarrow C$. Now let $\varphi(f)(a)(b) \overset{\text{def}}{=} f(a \otimes b)$. We need to show that $\varphi(f)(a)$ is a S-homorphism, $\varphi(f)$ is a R-homomorphism, and φ is a homomorphism of abelian groups. We need an inverse $\psi : \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \longrightarrow \mathrm{Hom}_S(A \otimes_R B, C)$. Let $g : A \longrightarrow \mathrm{Hom}_S(B, C)$ be a R-module homomorphism. Then ψ_g is a unique homomorphism $A \otimes_R B \longrightarrow C$ such that $\psi_g(a \otimes b) = g(a)(b)$. To demonstrate this, we apply the Universal Property of Tensor Products

$$\begin{array}{ccc} & A \times B & \\ \swarrow & & \searrow \\ A \otimes B & \xrightarrow{\exists! \psi_g} & C \end{array}$$

It remains to show that ψ_g is a homomorphism of abelian groups and show that ψ, φ are inverses of each other. (Exercise) □

If ${}_R M$, then there exists a left projective R-module P with $P \longrightarrow M \longrightarrow 0$. If ${}_R M$, then there exists an injective R-module E and a monomorphism $M \longrightarrow E$. Furthermore, recall that over $\mathbb{Z}$, a module is injective if and only if it is divisible. So $\mathbb{Q}$ is an injective $\mathbb{Z}$-module. Then we obtain the following result:

Proposition 5.6. *Every $\mathbb{Z}$-module can be embedded in an injective module.*

Proof: Let ${}_{\mathbb{Z}}M = \bigoplus \mathbb{Z}/L$. Observe $\bigoplus \mathbb{Z}$ is free. As every quotient of a free module is free, ${}_{\mathbb{Z}}M$ is free. Now $\mathbb{Z} \subsetneq \mathbb{Q}$ is a submodule so $\bigoplus \mathbb{Z} \subsetneq \bigoplus \mathbb{Q}$. So we have $\bigoplus \mathbb{Q}/L$. This is a quotient of a divisible module so that it is divisible so that it is injective. □

Proposition 5.7. *Let R be any ring and let ${}_{\mathbb{Z}}D$ be a divisible group. Then the R module $E = \mathrm{Hom}_{\mathbb{Z}}({}_{\mathbb{Z}}R_R, {}_{\mathbb{Z}}D)$ is a left injective R-module, where E is a left R-module via $(rf)(s) = f(sr)$.*

Proof: Let $f : A \to E$. We need to show f can be extended to B.

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B \\ & & \downarrow{\scriptstyle f} & \swarrow & \\ & & E & & \end{array}$$

That is, we have to prove that $\mathrm{Hom}_R(B, E) \xrightarrow{\mathrm{Hom}_R(i,E)} \mathrm{Hom}_R(A, E) \longrightarrow 0$ or showing $\mathrm{Hom}_R(B, \mathrm{Hom}_{\mathbb{Z}}(R, D)) \longrightarrow \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(R, D)) \longrightarrow 0$. To show this, one need only follow the diagram arrows and get isomorphism compositions with onto maps to get the middle map onto and then perform the same to the top row. (Exercise)

$$\begin{array}{ccccc} \mathrm{Hom}_R(B, \mathrm{Hom}_{\mathbb{Z}}(R, D)) & \longrightarrow & \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(R, D)) & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \\ \mathrm{Hom}_{\mathbb{Z}}(R \otimes_R B, D) & \longrightarrow & \mathrm{Hom}_R(R \otimes_R A, D) & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \\ \mathrm{Hom}_{\mathbb{Z}}(B, D) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(A, D) & \longrightarrow & 0 \end{array}$$

Example 5.7. If $M \xrightarrow{h} N$ is an isomorphism, then $\mathrm{Hom}(M, X) \xrightarrow{\sim} \mathrm{Hom}(N, X)$. (Exercise)

Example 5.8. If $M \cong N$ and A is another R-module, then

$$\mathrm{Hom}(M, A) \cong \mathrm{Hom}(N, A)$$

and

$$\mathrm{Hom}(A, M) \cong \mathrm{Hom}(A, N)$$

It is also useful to take note of the following theorem,

Theorem 5.8. *Let $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ be a sequence of R-modules. Then the following are equivalent:*

(i) $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ *is exact.*

(ii) $g \circ f = 0$ *and for all* $h : M \to X$ *with* $hf = 0$*, there exists a unique* $h' : M_3 \to X$ *with* $h'g = h$ *(*g *is the cokernel of* f *so this gives us exactness).*

(iii) For all R-modules X*, we have an induced exact sequence of abelian groups*

$$0 \longrightarrow \mathrm{Hom}(M_3, X) \overset{\mathrm{Hom}(g,X)}{\longrightarrow} \mathrm{Hom}(M_2, X) \overset{\mathrm{Hom}(f,X)}{\longrightarrow} \mathrm{Hom}(M_1, X)$$

5.4 Flat Modules

Theorem 5.9. *(i) Let $\{A_i\}_{i\in\mathcal{I}}$ be a family of right R-modules and let B be a left R-module. Then there exists an isomorphism of abelian groups*

$$\bigoplus_{i\in\mathcal{I}} A_i \otimes_R B \xrightarrow{\sim} \bigoplus_{i\in\mathcal{I}} \left(A_i \otimes_R B \right)$$

(ii) Let A be a right R-module and let $\{B_i\}_{i\in\mathcal{I}}$ be a family of left R-modules. Then there exists an isomorphism of abelian groups

$$A \otimes_R \left(\bigoplus_{i\in\mathcal{I}} B_i \right) \xrightarrow{\sim} \bigoplus_{i\in\mathcal{I}} (A \otimes_R B_i)$$

Moreover if R is commutative, these are R-module isomorphisms.

Assume that we have ${}_S A_{R,R} B$ then $A \otimes_R B$ is also a left S-module via $s(a \otimes b) \stackrel{\text{def}}{=} sa \otimes b$. If $A_{R,R} B_S \to A \otimes_R B$ is a right S-module. Recall that if $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is a short exact sequence of left R-modules then for all M_R, we have the exact sequence

$$M \otimes A \xrightarrow{\mathrm{id}_M \otimes f} M \otimes B \xrightarrow{\mathrm{id}_M \otimes g} M \otimes C \longrightarrow 0$$

Example 5.9. If $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ splits then $1_M \otimes f$ is also injective.

Definition (Flat Module)**.** A right R-module M is called flat if for every short exact sequence of left modules

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

the induced sequence

$$0 \longrightarrow M \otimes A \xrightarrow{1_M \otimes f} M \otimes B \xrightarrow{1_M \otimes g} M \otimes C \longrightarrow 0$$

is exact. That is, tonsuring with flat modules preserves exactness.

Example 5.10. R_R is flat. To see this let $A \xrightarrow{f} B$ be a monomorphism. Then

$$\begin{array}{ccc} R \otimes_R A & \xrightarrow{1_R \otimes f} & R \otimes_R B \\ \downarrow{\scriptstyle \varphi_A} & & \downarrow{\scriptstyle \varphi_B} \\ A & \xrightarrow{\quad f \quad} & B \end{array}$$

where the left map is given by $r \otimes a \mapsto ra$ and the right map is given by $r \otimes b \mapsto rb$. Going around the left and bottom of the diagram is a homomorphism and going around the other away is a monomorphism so that $1_R \otimes f$ is a monomorphism.

Proposition 5.8. *Let $\{M_i\}_{i\in\mathcal{I}}$ be a family of right R-modules, then $\bigoplus_{i\in\mathcal{I}} M_i$ is flat if and only if M_i is flat for $i \in \mathcal{I}$.*

Proof (Sketch): The forward direction is an exercise. For the reverse direction, assume that each M_i is flat. We look at $0 \longrightarrow_R A \xrightarrow{f}_R B$. But then $M_i \otimes_R A \xrightarrow{1_M \otimes f} M_i \otimes_R B$ is a monomorphism for all $i \in \mathcal{I}$. Then we use the fact that $X_i \xrightarrow{h_i} Y_i$ is a monomorphism for all i if and only if $\bigoplus X_i \xrightarrow{\oplus h_i} \bigoplus Y_i$ is a monomorphism: $h((x_i)) \to (h_i(x_i))_i$.

$$\begin{array}{ccc} \bigoplus X_i & \longrightarrow & \bigoplus Y_i \\ {\scriptstyle k_i^X}\uparrow & & \uparrow{\scriptstyle k_i^Y} \\ X_i & \xrightarrow{h_i} & Y_i \\ \uparrow & & \uparrow \\ 0 & & 0 \end{array}$$

□

Corollary 5.2. *$M = L \bigoplus K$ is flat if and only if L and K are flat.*

Corollary 5.3. *(i) Every free module is flat.*

(ii) Every projective module if flat.

Proof:

(i) We know that a module is free if and only if it is isomorphic to a direct sum of copies of R.

(ii) We know that if P is projective then there exists a free module F such that $F = P \oplus Q$ for some Q. Then P is flat using the previous part.

□

It is important to note

$$\text{Free Modules} \longrightarrow \text{Projective Modules} \longrightarrow \text{Flat Modules}$$

We also have the following:

Theorem 5.10. *If R is a PID and P is projective then P is free.*

Theorem 5.11. *If R is Noetherian and M is finitely generated then M is flat if and only if M is projective.*

Example 5.11. $_{\mathbb{Z}}\mathbb{Q}$ is flat but not projective.

5.5 Rings & Modules of Fractions

Here let R be a commutative ring. A subset S of R is multiplicative if $1_R \in S$, $0 \notin S$, and S is closed under multiplication.

Example 5.12. If R is an integral domain, then $S = R - \{0\}$ is multiplicative.

Example 5.13. If $P \trianglelefteq R$ is a prime ideal of R, then $R \setminus P$ is multiplicative.

Now let $S \subset R$ be multiplicative. We look at $R \times S$ and introduce a equivalence relation to this set. Let $(a, s) \sim (b, t)$ if and only if there is a $u \in S$ with $u(at - bs) = 0$. Let $R_S = R \times S/\sim$. We can make R_S into a commutative ring with unity. Let a/s be equivalent to the class (a, s). We can now define an addition and multiplication to the set R_S:

$$+ : \frac{a}{s} + \frac{b}{t} \stackrel{\text{def}}{=} \frac{at + bs}{st}$$
$$\cdot : \frac{a}{s} \cdot \frac{b}{t} \stackrel{\text{def}}{=} \frac{ab}{st}$$

One need show that these defined operations are well defined, associative, distributive, and that the addition is commutative. We let 0 denote $0/s$ and 1 by $1/1$. We have a ring homomorphism $R \to R_S$ given by $\varphi(r) = r/1$. We call R_S the ring of fractions of S.

We can perform the same construction for modules. Let M be an R-module. Introduce $M \times S$ with the equivalence relation $(m, s) \sim (m', s')$ if and only if there is a $t \in S$ such that $t(s'm - sm') = 0$. Let m/s denote the equivalence class (m, s). We obtain an abelian group M_S, $M_S = M \times S/\sim$, with operations

$$+ : \frac{m}{s} + \frac{m'}{s'} \stackrel{\text{def}}{=} \frac{s'm + sm'}{ss'}$$
$$\cdot : \frac{r}{t} \cdot \frac{m}{s} \stackrel{\text{def}}{=} \frac{rm}{ts}$$

Observe that if $S \subset R$ is multiplicative nd ${}_RM \xrightarrow{f}_R N$ is a homomorphism, we can let $f_S : M_S \to N_S$ be given by $f_S(m/s) \stackrel{\text{def}}{=} \frac{f(m)}{s}$. It is easy to see that f_S is a homomorphism of R_S-modules.

Proposition 5.9. *Let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact sequence of R-modules and let $S \subset R$ be multiplicative. Then the sequence*

$$0 \longrightarrow A_S \xrightarrow{f_S} B_S \xrightarrow{g_S} C_S \longrightarrow 0$$

is a short exact sequence of R_S-modules.

Proof: To see that f_S is a monomorphism, let $f_S(a/s) = 0$. Then $f(a)/s = 0 = 0/1$. There exists a $t \in S$ with $t(f(a) - 0) = 0$ so $tf(a) = 0$. Now as f is a homomorphism so $f(ta) = 0$. Now f is injective so $ta = 0$.

$$\frac{a}{s} = \frac{ta}{ts} = \frac{0}{ts} = 0$$

so that f_S is injective. To see that g_S is onto, let $c/s \in C_S$, where $c \in C$ and $s \in S$. Now $c = g(b)$ for some $b \in B$.

$$\frac{c}{s} = \frac{g(b)}{s} = g_S(b/s)$$

so that g_S is onto. To see exactness at B_S,

$$g_S f_S(a/s) = g_S(f(a)/s) = g(f(a))/s = 0/s = 0$$

Now let $b/s \in \ker g_S$ so that $g_S(0) = g_S(b/s) = g(b)/s$. So there exists a $t \in S$ with $tg(b) = 0$. Then we have $g(bt) = 0$ so that $bt = f(a)$ for some a. But then $b/s = bt/st = f(a)/st = f_S(a/st)$. Therefore, $\ker g_S \subseteq \operatorname{im} f_S$. But by above we also have $\operatorname{im} f_S \subseteq \ker g_S$. □

It is important to note that taking fractions preserves exact sequences, as the above shows.

Theorem 5.12. *Let R be commutative. Let $S \subset R$ be multiplicative. Then there exists a natural (functorial) isomorphism of R_S-modules, $R_S \otimes_R M \xrightarrow{\varphi_M} M_S$.*

Proof: Exercise

A consequence of this theorem is that if $S \subset R$ is multiplicatively closed, then R_S is a flat R-module.

6 Noetherian and Artinian Rings/Modules

6.1 Noetherian Rings and Modules

Definition (Noetherian Ring)**.** A ring R is said to be left noetherian if it satisfies the ascending chain condition on left ideals. That is, for all chains

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

of left ideals, there is an $n_0 \in \mathbb{N}$ such that $I_{n_0} = I_N$ for all $n \geq n_0$, i.e. that that the chain stabilizes (at I_{n_0}).

Example 6.1. If R is a principal ideal domain, then R is noetherian.

Example 6.2. Let $R = \mathbb{Q}[x_i]_{i\in\mathbb{N}}$, the polynomial ring in infinitely many indeterminates. Then the ideal $I = \langle\{x_i\}\rangle$ cannot be finitely generated so that R is not noetherian.

Example 6.3. Let F ba field. Look at $R = F[X, Y] = \langle X^2, XY, Y^2\rangle$. Now R is a vector space over F with basis $\{1, \overline{X}, \overline{Y}\}$. All ideals of R are vector spaces so the only possible dimensions are 1, 2, and 3. So there can be no infinite ascending chain of spaces so R must be noetherian.

Theorem 6.1. *The following are equivalent for a ring R:*

(i) R is left noetherian.

(ii) Every nonempty set of left ideals has a maximal element with respect to inclusion.

(iii) Every left ideal of R modules is finitely generated.

Proof: $1 \to 2$: Let $S \neq \emptyset$ be a set of (left) ideals. Choose $I_1 \in S$. If I_1 is maximal, we are done. If not, choose $I_2 \in S$ such that $I_2 \supsetneq I_1$. Continue this process. If this sequence of chosen left ideals does not terminate, we have found a chain of ascending left ideals which does not stabilize, contradicting the fact that R is noetherian. Therefore, there is a maximal element, say I_{n_0} for some $n_0 \in \mathbb{N}$.

$2 \to 3$: Let S be the set of all finitely generated ideals of R contained within I. Let I be a nonzero left ideal of R. It is clear that S is nonempty as $0 \neq a \in I$ so that $\langle a\rangle \subset I$ so that $a \in S$. By assumption, S has a maximal element J. We claim that $J = I$. If not, let $x \in I \setminus S$. Say that $J = \langle i_1, i_2, \cdots, i_e\rangle$. But then $J \subset \langle i_1, \cdots, i_e, x\rangle \subset I$, contrary to the fact that J was maximal.

$3 \to 1$: Assume

$$I_1 \subseteq I_2 \subseteq \cdots$$

is a chain of ideals. Without loss of generality, assume that the inclusions are proper. Let

$$I = \bigcup_{i \in \mathcal{I}} I_i$$

It is clear that I is a left ideal. We wish to show that $I \neq R$. If $I = R$, then $1 \in I_n$ for some n. But then $I_n = R$, contrary to the fact that I_n is a proper ideal. Therefore, $I \neq R$. If we are in the finitely generated case, then say $I = \langle x_1, x_2, \cdots, x_n \rangle$, with $x_i \in I_i$. Choosing M large enough so that $x_1, x_2, cdots, x_m \in I_M$, then $I = I_M$ and the chain stabilizes. □

Definition (Noetherian Module)**.** Let R be a ring. An R-module M is said to be (left) noetherian if it satisfies the ascending chain condition on left modules.

Theorem 6.2. *The following are equivalent for a left module M:*

(i) M is left noetherian.

(ii) Every nonempty set of submodules of M has a maximal element under inclusion.

(iii) Every submodule of M is finitely generated.

Theorem 6.3. *If R is noetherian and I is a two sided ideal of R then R/I is also noetherian.*

Proof: This follows from the Correspondence Theorem. We know the ideals of R/I are in 1-1 correspondence to ideals of R containing I. □

Lemma 6.1. *Let*

$$0 \longrightarrow L \hookrightarrow M \longrightarrow N \longrightarrow 0$$

be a short exact sequence. If L, N are finitely generated then M is finitely generated.

Proof: Let $L = \langle x_1, x_2, \cdots, x_n \rangle$ and $N = \langle y_1 + L, y_2 + L, \cdots, y_m + L \rangle$. We claim that $M = \langle x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m \rangle$. Let $z \in M$. Then $z + L = r_1(y_1 + L) + \cdots + r_m(y_m + L)$, where $r_i \in R$. Then $z - \sum r_i y_i \in L$ so that $z = \sum r_i y_i + \sum s_j x_j$. □

Theorem 6.4. *Let R be a ring and let*

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

be a short exact sequence. Then B is noetherian if and only if A, C are noetherian.

Proof: Without loss of generality, assume that $A \longrightarrow B$ is an inclusion. (Why?)

Let B be noetherian and $A \leq B$. Every submodule of A is also a submodule of B so it is finitely generated. That C is noetherian follows from the Correspondence Theorem as every submodule of C corresponds to a submodule of B containing A.

To show the reverse direction, we wish to show that every submodule of B is finitely generated. Let X be a submodule of B. We want to show that X is finitely generated. Now $X \cap A$ is a submodule of A. As A is noetherian, $X \cap A$ is finitely generated.

$$0 \longrightarrow X \cap A \hookrightarrow X \longrightarrow X/X \cap A \longrightarrow 0$$

But we have $X/X \cap A \cong A + X/A \subseteq B/A = C$ and C is finitely generated. So $X/X \cap A$ is finitely generated and $X \cap A$ is finitely generated so that by the preceding lemma, X is finitely generated. □

Proposition 6.1. *A direct sum of two noetherian modules is noetherian.*

Proof: Let A, B be noetherian. Then we have the exact sequence

$$0 \longrightarrow A \xrightarrow{k_A} A \oplus B \xrightarrow{k_B} \longrightarrow 0$$

As A, B are noetherian, $A \oplus B$ is noetherian. A finite sum of noetherian modules is then noetherian by induction. □

We can extend this to an if and only if statement.

Proposition 6.2. *Let R be a noetherian ring. Let M be a finitely generated R-module. Then M is noetherian.*

Proof: Let M be finitely generated. Then there exists a finitely generated free module F mapping onto M. But this finitely generated free modules has

$$F \cong R^n = R \oplus \cdots \oplus R$$

But F is noetherian as $R^n = R \oplus \cdots \oplus R$ is noetherian being the finite sum of noetherian rings. So M is a quotient of noetherian modules. But then M is noetherian. □

6.2 Artinian Rings and Modules

Definition (Artinian Module)**.** Let M be an R-module. Then M is called left artinian if it satisfies the descending chain condition on submodules.

Example 6.4. Every field is an artinian ring (in fact, all division rings satisfy the artinian condition).

Example 6.5. $F[X,Y]/\langle X^2, XY, Y^2\rangle$ as seen before to be noetherian, must also necessarily be artinian.

Example 6.6. $\mathbb{Z}$ is not artinian as we have $\langle 2\rangle \supsetneq \langle 4\rangle \supsetneq \langle 16\rangle \supsetneq \cdots$.

Theorem 6.5. *Suppose R is a ring and let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of R-modules. Then B is artinian if and only if A, C are artinian.

Proof: The forward direction follows from the corresponding proof (no pun intended) for noetherian modules mutatis mutandis.

Now let $B_1 \supseteq B_2 \supseteq \cdots$ be a descending chain of submodules of B. Consider

$$A \cap B_1 \supseteq A \cap B_2 \supseteq \cdots$$

a descending chain of submodules of A. As A is artinian, this chain must stabilize at some n. We now look at $A + B_1 \supseteq A + B_2 \supseteq \cdots$, a descending chain of submodules of B containing A. Now look at

$$A + B_1/A \supseteq A + B_2 \supseteq \cdots$$

a descending chain of submodules of C. Now as C is artinian, this chain stabilizes. So there is a m such that the chain stabilizes at m. Then $A + B_m$ must stabilize by the Correspondence Theorem. Now we have

$$\begin{aligned} B_k \supseteq B_{k+1} \supseteq B_{k+2} \supseteq \cdots \\ A + B_k = A + B_{k+1} = \cdots \\ A \cap B_k = A \cap B_{k+1} = \cdots \end{aligned}$$

We claim that $B_k = B_{k+1} = \cdots$. It is sufficient to show $B_k \subseteq B_{k+1}$. Let $x \in B_k$ and $a \in A$. We know $a + x \in A + B_k$. Suppose $a + x = a' + y$ for some $a' \in A$ and $y \in B_{k+1} \subseteq B_k$. We know $a - a' \in A$ and $-x + y \in B_k$. Therefore,

$$-x + y \in A \cap B_k = A \cap B_{k+1}$$

so that $-x + y \in B_{k+1}$. We know $y \in B_{k+1}$ so that $x \in B_{k+1}$. But then $B_k \subseteq B_{k+1}$. □

Corollary 6.1. *A finite direct sum of modules is artinian if and only if each of the modules is artinian.*

Corollary 6.2. *Let R be an artinian ring and let M be a family of finitely generated R-modules. Then M is artinian.*

6.3 Hilbert's Basis Theorem

Theorem 6.6. *Let R be a noetherian commutative ring. Then $R[x]$ is noetherian. Consequently by induction, $R[x_1, x_2, \cdots, x_n]$ is noetherian.*

Proof: Let $I \trianglelefteq R[x]$. We want to show that I is finitely generated. Let

$$L = \{\text{all leading coefficients of polynomials in } I\}$$

We know that $0 \in L$ so that L is nonempty. We wish to show that L is an ideal of R. Let $a, b \in L$. There then exists $f = ax^m + \cdots \in I$ and $g = bx^n + \cdots \in I$. Without loss of generality, assume that $m > n$. As $f \in I$ and I is an ideal, $x^{m-n}g = ax^m + \cdots \in I$. We know $a + b$ is the leading coefficient of $f + x^{m-n}g$ so $a + b \in L$. But then $L \trianglelefteq R$. As R is noetherian, it must be that L is finitely generated. Then there exist $a_1, \cdots, a_n \in R$ with $L = \langle a_1, \cdots, a_n \rangle$.

Moreover, there exist polynomials $f_i \in I$ with $f_i = a_i x^{e_i} + \cdots$. The "guess" would be that $\langle f_1, \cdots, f_n \rangle = I$ but this would be incorrect. There are many f_i with a_i as a leading coefficient so this generating set is "probably not enough". Let $N = \max\{e_1, \cdots, e_n\}$. For each $0 \leq d \leq N - 1$, let

$$L_D = \{\text{all leading coefficients of polynomials in } I \text{ of degree } d\} \cup \{0\}$$

We claim that L_D is an ideal of R for each D. As R is noetherian, we know that L_D is finitely generated for all D. Then $L_D = \langle b_{d_0}, \cdots, b_{d_n d} \}$. We write $f_{d,i} =$ some polynomial in I of degree d with leading coefficient $b_{d,i}$. We claim that

$$I = \langle f_1, \cdots, f_n, \{f_{d,i}\}_{0 \leq d \leq N-1, 0 \leq i \leq n_d} \}$$

Let I' be the set on the right. It is clear that $I' \subseteq I$. We wish to show then that $I \subseteq I'$. Assume that $I \not\subseteq I'$. Choose a counterexample f of smallest degree such that $f \in I$ but $f \notin I'$. Let $\deg f = d$ so $f = ax^d + \cdots$. We claim $0 \leq d \leq N - 1$. Assume then that $d \geq N$. Let $a \in L$. As L is finitely generated, $a = r_1 a_1 + \cdots + r_n a_n$. We look at

$$g = \underbrace{r_1 x^{d-e_1} f_1}_{\deg e} + \cdots + \underbrace{r_n x^{d-e_n} f_n}_{\deg d}$$

The leading coefficient of g is a and $\deg g = d$. Now we know that $f - g \in I$ and $f - g \in I'$. Otherwise, $f \in I'$. But $f - g$ has degree less than d. But this contradicts the minimality of the degree of the counterexample, f. Now $d < N$. It follows that the leading coefficient of f, a, must be in L_D so we have $a = r_1 f_{d,1} + \cdots + r_{n_d} f_{d,n_d} \in I'$. Furthermore, the degree of g is d - the degree of f and both f and g have the same leading coefficient. Now as $f - g \in I$ but not in I', we have a contradiction of the minimality of the degree of f. $\square$

7 Semisimple Rings & Modules

7.1 Simple Rings & Modules

Definition (Simple Ring/Module)**.** Let R be a ring then an R-module $S \neq 0$ is simple if there are no nontrivial proper submodules. Note that simple is also at times called irreducible.

A module M is called semisimple (or completely irreducible) if each of its submodules is a direct sum of submodules. That is for all $L \leq M$, there is $X \leq M$ such that $M = L \oplus X$.

Example 7.1.1. Let K be a field. Then ${}_KK$ is simple. Let M be a vector space over K. Let $\mathcal{L} \leq M$ be a subspace of M. Every vector space has a basis and every vector subspace has a basis which can be extended to a basis of the whole space. Pick a basis B of $\mathcal{L}$ and extend this to a basis $\overline{B}$ of M. Then $\overline{B} = B \sqcup B'$ for some B'. Let $X = \langle B' \rangle$, then $M = \mathcal{L} \oplus X$. ▷

Example 7.1.2. Every simple module is semisimple. ▷

Example 7.1.3. Every division ring D is a simple ring and a simple D-module. ▷

Example 7.1.4. If S is simple, let $0 \neq x \in S$. Then $S = \langle x \rangle = Rx$. Therefore, every simple module is cyclic. Cyclic modules need not be simple. Take the cyclic $\mathbb{Z}$-module Z_6. ▷

Example 7.1.5. Let ${}_RS$ be simple. Then $S = Rx$ for some $0 \neq x \in S$. Let $R \xrightarrow{f} Rx$ given by $r \mapsto rx$ be a homomorphism of left modules. If f is onto, as Rx is a submodule, $R/\ker f \xrightarrow{\sim} Rx = S$. We also know $\ker f$ is a maximal ideal by the Correspondence Theorem.

▷

It is useful at this point to recall Schur's Lemma.

Lemma 7.1 (Schur's Lemma)**.** *Let S be a simple module. Then $End_R(S)$ is a division ring.*

However, the converse need not be true.

Lemma 7.2 (Modular Law)**.** *Let $A, B, C \leq M$ be R-submodules of the R-module M with $B \leq A$. Then*

(i)

$$A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C) = B \oplus (A \cap C)$$

(ii) If $A \oplus C = B \oplus C$ then $A = B$ and $A \cap C = A \cap B$.

Proposition 7.1. *Submodules and homomorphic images of semisimple modules are semisimple.*

Proof: Let M be semisimple. Let $\mathcal{L} \leq M$. Let $X \leq \mathcal{L}$. We need show that X is a direct summand of $\mathcal{L}$. We know that as $X \leq M$ and M is semisimple, $M = X \oplus K$ for some $K \leq M$. We need make $\mathcal{L}$ appear in this decomposition. Consider $\mathcal{L} \cap M = \mathcal{L}$. By the Modular Law,

$$\mathcal{L} = \mathcal{L} \cap M = (\mathcal{L} \cap X) \oplus (\mathcal{L}K)$$

But $\mathcal{L} \cap X = X$ and $X \cap K = \emptyset$. Therefore, $(\mathcal{L} \cap X) \cap (\mathcal{L} \cap K) = \emptyset$. Therefore, $L = X \oplus (\mathcal{L} \cap K)$.

Now we show that the quotient of a semisimple module is semisimple. That is, we want to show that M/L is semisimple. As M is semisimple, $M = \mathcal{L} \oplus K'$ for some $K' \leq M$. But then we have $M/L = L \oplus K'/L \cong K' \leq M$. As K' is semisimple, being a submodule of a semisimple module, it must be that M/L is semisimple.

Lemma 7.3. *Let M be a module and $\{S_i\}_{i \in \mathcal{I}}$ be a family of distinct simple submodules of M that generates M; that is, $M = \sum_{i \in \mathcal{I}} S_i$. Then if $\mathcal{L} \leq M$ then there exists a $J \subseteq I$ such that $M = \mathcal{L} \oplus \bigoplus_{j \in J} S_j$. In particular, M is semisimple.*

Proof: Note first that $\sum_{j \in J} S_j = \oplus_{j \in J} S_j$ for all subsets $J \subseteq I$. We want to show that the sum on the left is direct. That is, (after a possible relabeling) $(S_1 + S_2 + \cdots + S_t) \cap S_{t+1} = 0$. Suppose that this is not the case. Then we have for some t, $S_{t+1} = S_1 + S_2 + \cdots + S_t$, where $\langle x \rangle = S_{t+1}$. Write $x = s_1 + \cdots + s_t$. Without loss of generality, assume that $s_1 \neq 0$. Now $S_1 = \langle s_1 \rangle$, $S_2 = \langle s_2 \rangle$, $\cdots$, $S_l = \langle s_l \rangle$. Then we have $S_{t+1} = S_1 + S_2 + \cdots + S_t$ with the right side being simple if and only if $l = 1$. But then $S_{t+1} = S_1$, contradicting the fact that the family of simple submodules was distinct. Now let S denote all subsets of K_i of $\mathcal{I}$ with the property that their sum

$$L + \bigoplus_{k \in K} S_k$$

is an internal direct sum. We know that $S \neq \emptyset$ as $\emptyset \in S$. We now apply Zorn's Lemma. (Why?) Say S has maximal element J with respect to inclusion. Then

$$L + \bigoplus_{j \in J} S_j = L + \bigoplus_{j \in J} S_j \stackrel{\text{def}}{=} L'$$

We want to show that $L' = M$. Suppose that this is not the case. Assume $L' < M$. As the S_i generate M, there must be some $S_i \leq M$ not contained in L. So $S_i \cap L = 0$ as $L \leq M$ and S_i is simple. Now let $J_0 \stackrel{\text{def}}{=} J \cup \{i\}$, where i is the index of S_i where $S_i \cap L = 0$. Then $L + \bigoplus_{j \in J_0} S_j$ is direct. However, this contradicts the maximality of J. □

Lemma 7.4. *If M is a semisimple module, then M contains a simple submodule.*

Proof: Let $0 \neq x \in M$. Let S be all submodules of M not containing x. We know that S is nonempty as $0 \in S$. Order S by inclusion. We use Zorn's Lemma. (Why?) So S has a

maximal element N. Now $N \leq M$ so that $M = N \oplus S$ (because M is semisimple) for some $S \leq M$. We claim that S is simple.

Assume that S is not simple. Therefore, S contains a nonzero submodule T. But S is semisimple being a submodule of a semisimple module. Then $S = T \oplus V$ for some submodule V. But then we have $M = N \oplus T \oplus V$. We claim that either $x \notin N \oplus T$ or $x \notin N \oplus V$. Assume to the contrary that $x = a + v = b + t$ for some $a, b \in N$, $v \in V$, and $t \in T$. So $a - b = t - v \in N \cap (T \oplus V)$. However, $T \oplus V = S$ and $N \cap S = 0$ so that $a = b$ and $t = v$. As $T \cap V = 0$, we have $t = v = 0$. This implies $a = b$ so that $x = a = b \in N$, contradicting the definition of N. So $x \notin N \oplus T$ or $x \notin N \oplus V$. However, this contradicts the maximality of N so that S is a simple module of M. □

Theorem 7.1. *The following are equivalent for an R-module M:*

(i) M is a direct sum of simple submodules.

(ii) M is a direct sum of simple of simple submodules.

(iii) M is semisimple.

Proof: 1 → 2: This follows directly from the preceding lemma.

2 → 3: This follows from the final part of the preceding lemma.

3 → 1: Let L be the sum of all simple submodules of M. We want to show that $L = M$. Assume to the contrary that $L < M$. Then there is a $x \in M$ with $x \notin L$. Let S denote the set of all submodules K of M containing L not containing x. We know that S is nonempty as $L \in S$. Order S by inclusion and apply Zorn's Lemma. Therefore, S has a maximal element K_0. So $x \notin K_0$ and $L \subseteq K_0 \subseteq M$. However, as M is semisimple, we know that $M = K_0 \oplus U$ for some $U \leq M$. Now U cannot be simple for otherwise it would be contained in L and hence K_0 (this would be a contradiction as $K_0 \cap U = 0$).

Let A be a proper nonzero submodule of U. We have $U = A \oplus B$ for some nonzero submodule B. Then $M = K_0 \oplus A \oplus B$. We claim that $x \notin K_0 \oplus A$ or $x \notin K_0 \oplus B$. We use the idea of the previous lemma. Write $x = k_1 + a = k_2 + b$ for some $k_1, k_2 \in K_0$, $a \in A$, and $b \in B$. Then $k_1 - k - 2 = b - a \in K_0 \cap (A \oplus B) = 0$. Therefore, $k_1 = k_2$ and $a = b = 0$. Then $x \in K_0$, a contradiction. Then either $x \in K_0 \oplus A$ or $x \notin K_0 \oplus B$. But in either case, this contradicts the maximality of K_0. Therefore, $L = M$ and we are done. □

7.2 Composition Series

Definition (Series)**.** Let M be an R-module. A chain of submodules of M

$$0 = M_0 \leq M_1 \leq M_2 \leq \cdots \leq M_n = M$$

is called a series for M. The length of the above series is n. The modules $M_1/M_0, M_2/M_1, \cdots, M_n/M_{n-1}$ are called the factors for the series. Two series of a module M are equivalent if they have the same length and factors (corresponding) are isomorphic in the same order.

Definition (Refinement)**.** A series $0 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_p = M$ is a refinement of $0 = M_0 \leq M_1 \leq M_2 \leq \cdots \leq M_n = M$ if for all $1 \leq i \leq n$, there is a j so that $M_i = N_j$.

We have an important Lemma whose proof will come later.

Theorem 7.2 (Schreier-Zasenhaus Lemma)**.** *Any two series of a module have equivalent refinements.*

Definition (Composition Series)**.** Let M be an R-module. A composition series (if it exists) of M is a series of the form

$$0 = M_0 < M_1 < M_2 < \cdots < M_n = M$$

where M_{i+1}/M_i is simple.

Remark. We know that if $0 = M_0 \leq M_1 \leq M_2 \leq \cdots \leq M_n = M$ is a composition series then for all i, $M_i < M_{i+1}$ is a maximal submodule. Therefore, if we refine a composition series we can only insert modules already present so that we obtain $\{0\}$ composition factors (because of the repeated submodules). But then any two composition series should be equivalent.

Theorem 7.3 (Jordan-Hölder Theorem)**.** *Any two composition series of a module are equivalent. Furthermore, if a module M has a composition series and $0 = N_0 < N_1 < N_2 < \cdots < N_t = M$ is a series for M with nonzero factors, then this series can be refined into a composition series.*

Definition. Assume that M has a composition series

$$0 = M_0 < M_1 < M_2 < \cdots < M_n = M$$

Then n is called the length of M, denoted $l(M)$. The composition factors of M are $\{M_1/M_0, \cdots, M_n/M_{n-1}\}$.

Remark. Nonisomorphic modules need not have unique composition factors!

Theorem 7.4 (Schreier-Zasenhaus Lemma)**.** *Any two series of a module have equivalent refinements.*

Proof: Let M be a module and

$$0 = M_0 \leq M_1 \leq M_2 \leq \cdots \leq M_n = M$$
$$0 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_m = M$$

be two series for the module M. Refine the first series by inserting $M_{ij} = M_i + (M_{i+1} \cap N_j)$ for $i = 0, 1, 2, \cdots, n$ and $j = 0, 1, \cdots, m$. Observe that for all i, $M_i = M_{i,0}$ as $M_i + (M_{i+1} \cap N_0) = M_i + (M_{i+1} \cap 0) = M_i$. Observe further that $M_{i,m} = M_{n+1}$ as $N_m = M$. Then we have

$$M_i = M_{i,0} \leq M_{i,1} \leq M_{i,2} \leq \cdots \leq M_{i,m} = M_{n+1}$$

Then $\{M_{i,j}\}$ order appropriately with M on "top" is a refinement of the first series.

$$M_{0,0} \leq M_{0,1} \leq \cdots \leq M_{0,m} \leq M_{1,0} \leq \cdots \leq M_{1,m} \leq \cdots \leq M_{n,m} = M$$

Observe that $M_{i+1,0} = M_{i,m}$. The composition factors of $\{M_{i,j}\}$ are of the form $M_{i,j+1}/M_{i,j}$ for $i = 0, 1, \cdots, n-1$ and $j = 0, 1, \cdots, m-1$. We use the Second Isomorphism Theorem and the Modular Law along with the fact that $M_{i,j} = M_i + (M_{i+1} \cap N_{j+1})$ and

$$M_{i,j} + (M_{i+1} \cap N_{j+1}) = M_i + (M_{i+1} \cap N_j) + (M_{i+1} \cap N_{j+1})$$

Now let $A = M_{i,j}$ and $B = M_{i+1} \cap N_{j+1}$. Then

$$\begin{aligned} M_{i,j+1}/M_{i,j} &= \frac{M_i + (M_{i+1} \cap N_{j+1})}{M_{i,j}} \\ &= (A + B)/A \end{aligned}$$

By the Second Isomorphism Theorem,

$$\begin{aligned} M_{i,j+1}/M_{i,j} &= \frac{M_i + (M_{i+1} \cap N_{j+1})}{M_{i,j}} \\ &= (A + B)/A \\ &\cong B/(A \cap B) \\ &= \frac{M_{i+1} \cap N_{j+1}}{M_{i,j} \cap (M_{i+1} \cap N_{j+1})} \\ &= \frac{M_{i+1} \cap N_{j+1}}{(M_{i+1} \cap N_{j+1}) \cap M_{i,j}} \\ &= \frac{M_{i+1} \cap N_{j+1}}{(M_{i+1} \cap N_{j+1}) \cap (M_i + (M_{i+1} \cap N_J))} \end{aligned}$$

Then by the Modular Law,

$$\begin{aligned} &= \frac{M_{i+1} \cap N_{j+1}}{(M_{i+1} \cap N_{j+1}) \cap (M_i + (M_{i+1} \cap N_J))} \\ &= \frac{M_{i+1} \cap N_{j+1}}{M_{i+1} \cap N_{j+1} \cap M_i + M_{i+1} \cap N_j} \\ &= \frac{M_{i+1} \cap N_{j+1}}{M_i \cap N_{j+1} + M_{i+1} \cap N_j} \end{aligned}$$

Notice that this is symmetric in M, N. This tells us how to deal with the second series, $\{N_{i,j}\}_{\substack{i=0,1,\cdots,n \\ j=0,1,\cdots,m}}$. Now

$$N_{i,j} = N_j + (M_i \cap N_{j+1})$$

And it all works the same as before mutatis mutandis. Finally, the refinement with $\{N_{i,j}\}$ is equivalent with the refinement for the series involving $\{M_{i,j}\}$. □

Now any two composition series of a module are equivalent so any two have the same length and same <u>set</u> of composition factors.

Example 7.1. Suppose $M = S + T = S \oplus T$, where $S \neq T$ are simple submodules.

$$0 \subset S \subset M \text{ with composition factors } \{S, T \cong M/S\}$$
$$0 \subset T \subset M \text{ with composition factors } \{T, S\}$$

Example 7.2. An example of a module with no simple submodule (hence no composition series) is ${}_{\mathbb{Z}}\mathbb{Z}$ as it has no simple submodule. The only simple $\mathbb{Z}$-modules are isomorphic to $\mathbb{Z}/p\mathbb{Z}$, where p is some prime. But we have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}) = 0$ as $\mathbb{Z}/p\mathbb{Z}$ is torsion and $\mathbb{Z}$ is free. Of course, one can show that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$ for $n \neq 1$ (one only need look where 1 goes).

Definition (Length)**.** We have $l(M)$ denoting the length of the composition series for a module M (if such a series exists). If M has no composition series we say that the length of M is infinite and write $l(M) = \infty$.

Theorem 7.5. *If $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is a short exact sequence, then $l(M) = l(L) + l(N)$. Stated differently, let M be an R-module. Let $L \leq M$. Then M has a composition series if and only if L and M/L have composition series. When this happens $l(M) = l(L) + l(M/L)$. This implies that if $M = \bigoplus_{i=1}^{n} S_i$, where S_i is a simple submodule, then M has a composition series of length n so that $l(M) = n$.*

Proof: The infinite cases are easy. Assume $0 \neq L \leq M$. Assume that M has a composition series. Consider a series for M

$$0 < L < M$$

If this is a composition series, we are done. (Why?) If not, we can refine it to a composition series. Insert submodules between 0 and L and L and M. The composition series obtained

$$0 = M_0 < M_1 < \cdots < M_k = L < \cdots < M_n = M$$

Where we say that without loss of generality $M_k = L$. But $0 = M_0 < M_1 < \cdots < M_k = L$ is a composition series for L. Therefore, $l(L) = k$. Now we have

$$M_k = L < M_{k+1} < \cdots < M_n = M$$

and

$$0 = L/L = M_k/L < M_{k+1}/L < \cdots < M_n/L = M/L = N$$

is a composition series for M/L. Therefore, $l(M/L) = n - k$. But then together $L, M/L = N$ are composition series for M so that $l(M) = l(L) + l(M/L) = l(L) + l(N)$.

The reverse direction is an exercise (use the correspondence theorem).

Now if $M = S_1 + S_2 + \cdots + S_n = S_1 \oplus S_2 \oplus \cdots \oplus S_n$, then

$$0 = M_0 < S_1 < S_1 + S_2 < \cdots < S_1 + S_2 + \cdots + S_n = M$$

is a composition series of length n for M.

Remark. Artinian rings always have simple submodules.

Theorem 7.6. *Let M be an R-module. Then M ha a composition series if and only if M is both artinian and noetherian.*

Proof: We proceed by induction on $l(M)$. If M is simple, we are done as every simple module is both artinian and noetherian. So the case where $l(M) = 1$ is trivial. No assume that statement is true for any integer up to $n - 1$. Let $n = l(M) > 1$. Let $S = M_1$ be a simple submodule of M.

$$0 = M_0 < M_1 = S < M$$

so that we have a short exact sequence

$$0 \longrightarrow S \longrightarrow M \longrightarrow M/S \longrightarrow 0$$

But $l(M/S) = n - 1$. By the induction hypothesis, $S, M/S$ are both noetherian and artinian. But then the ends of the short exact sequence are artinian/noetherian so that M is artinian/noetherian.

Now assume that M is artinian and noetherian. As M is artinian, there exists a simple submodule of M, say M_1. We look at M/M_1. This is a homomorphic image of a artinian module so that M/M_1 is artinian. Hence, M/M_1 has a simple submodule, say M_2. By the Correspondence Theorem, we have $M_2 \supset M_1$. We continue this process to obtain

$$0 = M_0 < M_1 < M_2 \cdots$$

But as M is noetherian, this process must terminate sot that there is an n such that the chain stabilizes.

$$0 = M_0 < M_1 < M_2 < \cdots < M_{n-1} < M_n = M$$

But then M has a composition series. □

7.3 Wedderburn Rings

Definition (Wedderburn Ring)**.** A ring R is a left Wedderburn ring if it is left artinian and has no nonzero nilpotent left ideals. That is, if I is a left ideal of R and $I^m = 0$, then $I = 0$.

We say also that a left ideal of R is a minimal left ideal in R if and only if it is a simple left ideal when viewed as a module over R.

Lemma 7.5. *Let ${}_RI$ be a left ideal of R, then*

(i) $I = Re$, where e is an idempotent of R, if and only if I is a direct summand of R as a left module.

(ii) If I is a minimal left ideal of R then either $I^2 = 0$ or $I = Re$.

Proof:

(i) If $I = Re$ and $e = e^2$, then $R = Re \oplus R(1-e)$. Assume then that $R = I \oplus J$. Then $1 = e + f$, where $e \in I$ and $f \in J$. Let $x \in I$. Then $x = x \cdot 1 = 1 \cdot x$. We have $x \in I$ and $x = xe + xf$, where $xe \in I$ and $xf \in J$. So as $I \cap J = 0$, $xf = 0$ so that $x = xe \in Re$. But $1 \in Re$ so that $x = e$ and as above we must have $e = x = xe = ee = e^2$.

(ii) Let ${}_RI$ be a minimal left ideal. Assume that $I^2 \neq 0$. Then there is $0 \neq a \in I$ such that $Ia =\neq 0$. But $Ia \subset I$ is a nonzero left ideal. As I is minimal, it must be that $Ia \supset I$ so that $Ia = I$. But $a \in Ia$ so there is $e \in I$ so that $a = ea$. Now $0 \neq Re \subset I$. As I is minimal, $I \subset Re$ so that $I = Re$. We are done except for that we demand $e^2 = e$. Assume that $e \neq e^2$.

$$\begin{aligned} a &= ea \\ ea &= e^2a \\ a &= e^2a \\ a - e^2a &= 0 \end{aligned}$$

Consider $(e - e^2)a = 0$. Let $J = \{r \in I \mid ra = 0\}$. We know $0 \neq e - e^2 \in J$. Now J is a left ideal contained in I so that $J \subset I$. But $I \subset J$ so that by minimality, $I = J$. But $Ia \neq 0$ so J cannot be I so that $Ja \neq 0$, contrary to the definition of J. Therefore, $e^2 = e$.

□

7.4 Semisimple Rings

Definition (Semisimple Ring)**.** A ring R satisfying any of the equivalent conditions of Theorem 7.7 is called a left semisimple ring.

Theorem 7.7. *The following are equivalent for a ring R:*

(i) *Every left R-module is projective.*

(ii) *Every left R-module is injective.*

(iii) *${}_RR$ is semisimple.*

(iv) *R is a left Wedderburn ring.*

Proof: $(i \to iv)$:

$(i \to ii)$: Let A be an R-module. Then there exists an injective module E with the property that $0 \longrightarrow A \xrightarrow{f} E$ so that

$$0 \longrightarrow A \xrightarrow{f} E \longrightarrow B \longrightarrow 0$$

where $B = \operatorname{coker} f$. But B is projective so the sequence splits so that $E \cong A \oplus B$. But A is a summand of an injective module so that A is injecitve.

$(ii \to i)$: Every module is a quotient of a projective module. We look at the kernel of the sequence and realize that the sequence splits. So we have that the module is isomorphic to a sum of projective modules and hence is projective.

$(i, ii \to iii)$: Let M be an R-module. Let $L \leq M$. We know that L is injective so there exists $K \leq M$ with $M = K \oplus L$. But then M is semisimple.

$(iii \to iv)$: Trivial

$(iv \to i)$: We know that ${}_RR$ is semisimple. So R is a direct sum of simple submodules. So every free module is isomorphic to a direct sum of copies of R so that it is isomorphic to a direct sum of simple submodules. All modules are quotients of free modules. All free modules are semisimple. So the quotient of semisimple modules are semisimple. Let M be a module then

$$0 \longrightarrow A \hookrightarrow F \longrightarrow M \longrightarrow 0$$

Where F is free so that it is semisimple. We know $F = A \oplus M'$, where $M' \cong M$. But this shows that M is projective.

$(iv \to v)$: Suppose ${}_RR$ is semisimple. So $R = \sum_{i \in \mathcal{I}} S_i = \bigoplus_{i \in \mathcal{I}} S_i$; that is, R is a direct sum of simple submodules. We want to show that this sum is finite. We know $1 \in R$ so that $1 \in \sum_{i \in \mathcal{I}} S_i$. Without loss of generality, say $1 = s_1 + \cdots + s_n \in S_1 + \cdots + S_n$. But then $r = r \cdot 1 = r(s_1 + \cdots + s_n)$ so that $R = S_1 \oplus \cdots \oplus S_n$, a direct sum of finitely many simple submodules. Each of these simple submodules have length 1. So R has length n. To see this,

$$0 \longrightarrow S_1 \longrightarrow S_1 \oplus S_2 \oplus \cdots \oplus S_n \longrightarrow S_2 \oplus \cdots \oplus S_n \longrightarrow 0$$

We know $l(S_1) = 1$ and by induction $l(S_2 \oplus \cdots \oplus S_n) = n - 1$ so that $l(S_1 \oplus \cdots \oplus S_n) = n$. As R has finite length, R is both noetherian and artinian when viewed as a left R-module. Let ${}_RI$ be an ideal of R. Now ${}_RR$ is semisimple by assumption so that we can write $R = I \oplus J$ for some J. We also have $I = Re$ with $e = e^2$ by Lemma 7.5. Furthermore, $e^n \neq 0$ for any n. But then I cannot be nilpotent. Therefore, R is left Wedderburn.

$(v \rightarrow i, ii, iii)$: By Lemma 7.5, every minimal left ideal I of R has the form $I = Re$, where e is an idempotent. But these ideals are projective so that every minimal left ideal is projective. It is enough to show that every left ideal is projective. (Why?) To do this, it is enough to show that every left ideal is a direct sum of minimal left ideals.

Assume that this is not the case. Let

$$S = \{\text{all left ideals not the sum of minimal left ideals}\}$$

Assume $S \neq \emptyset$. As R is artinian, there is a minimal element in S, say L. We look at the left ideals of L. Say there exists ${}_RI \subsetneq L$ with I a minimal left ideal. Now I is not nilpotent by assumption. So $I = Re$ forcing $R = I \oplus J$ for some left ideal J. By the Modular Law,

$$L = (L \cap I) \oplus (L \cap J) = I \oplus (L \cap J)$$

Now $L \cap I = I$ as $I \subset L$. We know that $I \oplus (L \cap J) \neq 0$ as $L \cap J \subset L$. But this is a sum of minimal left ideals. This shows that L is the sum of minimal left ideals, a contradiction. But then every left ideal of R is projective. □

Corollary 7.1. *Let R be a left semisimple ring. Let ${}_RM$ be a finitely generated module. Then M has a composition series of finite length. In particular, M is noetherian and artinian.*

Proof (Sketch): Now as R is semisimple so that R is left artinian. But then M is finitely generated artinian. So there exists

$$\underbrace{R \oplus \cdots \oplus R}_{n \text{ times}} \xrightarrow{\pi} M \longrightarrow 0$$

But $l(R)$ is finite so that $l(R^n) < \infty$. But then M is a quotient module with finite length so that $l(M) < \infty$. But then M is noetherian and artinian. □

7.5 Nilpotent Ideals

Definition (Nil)**.** Let R be a ring. A left ideal I of R is called nil if every element of I is nilpotent.

By definition, if ${}_RI$ is nilpotent then ${}_RI$ is nil. It should be noted that if ${}_RI$ is a nilpotent ideal, then IR is a right ideal. If $I^n = 0$, then $(IR)^n = 0$ so IR is a two-sided nilpotent ideal (hence also a nil ideal). But then every left/right nilpotent ideal is contained in a two-sided nilpotent ideal. Furthermore, if $x \in R$ is nilpotent then $1 - x$ is invertible as $(1-x)(1+x+\cdots+x^{n-1}) = 1$ from the fact that $x^n = 0$.

Proposition 7.2. *Let $I \trianglelefteq R$ be a two sided nil ideal of R. Then*

(i) If J/I is a left nil ideal of R/I then J is a nil left ideal of R.

(ii) If $I, J \trianglelefteq R$ are nil then $I + J$ is nil and any arbitrary sum of two sided nil ideals is nil.

Proof:

(i) Let $x \in J$. We want to show that x is nilpotent. We look at $x + I \in J/I$. We know that $x + I$ is nilpotent so that $(x+I)^n = x^n + J = 0 = I$. But then $x^n \in I$. As I is nil, $I^m = 0$ so that $(x^n)^m = x^{nm} = 0$.

(ii) We look at $I + J/I$ is a nil ideal of R/I. (Why?) Then by the previous part, $I + J$ is nil. By induction, a finite sum of nil ideals is nil. Let $\{I_k\}$ be a family of nil ideals $I_k \lhd R$. Let $x \in \sum_k I_k$, where x is a finite sum. Without loss of generality, assume that $x \in I_1 + \cdots + I_n$. But then x is nilpotent.

Conjecture (Köthes Conjecture)**.** If I, J are left nil ideals in a ring R, then $I + J$ is nil.

Despite it's unusual simplicity, Könthes Conjecture has gone unsolved for 85 years.

Definition (Nilradical)**.** Let R be a ring. Then the nilradical of R, denoted $\mathrm{Nil}(R)$ is a sum of all two sided nil ideals of R.

Note that $\mathrm{Nil}(R/\mathrm{Nil}(R)) = 0$ (Exercise: Use the Correspondence Theorem) This shows that $R/\mathrm{Nil}(R)$ has no nonzero two sided nil ideals.

Theorem 7.8. *Let R be a left artinian ring. Let N be* $\mathrm{Nil}(R)$*. Then R/N is a left Wedderburn ring and N is the unique largest nilpotent 2-sided ideal of R.*

Theorem 7.9 (Variation on Nakayama's Lemma)**.** *Let R be a ring. Let I be a nilpotent left ideal of R. Let M be a left R-module and let $L \leq M$. Assume that $M = L + IM$ then $M = L$. In particular, if $M = IM$ then $M = 0$.*

Proof: We show this by induction on I. Let $M = L + I^iM$. Now

$$M = L + IM = L + I(L + IM) = L + IL + I^2M = L + I^2(L + IM) = \cdots$$

If $I^i = 0$ for some i, that is if I is nilpotent, then $L = M$. If $L = 0$, then $M = IM$. □

Theorem 7.10. *Let ${}_RS$ be a simple R-module. Let I be a nilpotent left ideal. Then $IS = 0$.*

Proof: We know that $IS \leq S$. But S is simple. Then either $IS = S$ but by the previous theorem, $S = 0$. But this is not possible as S is simple or $IS = 0$. □

Notice that we then know that if R is a left artinian ring and $N = \text{Nil}(R)$, we know that N is nilpotent. So for all simple modules S, $NS = 0$. Furthermore, as a semisimple ring is a sum of simple submodules we have

$$N(S_1 \oplus S_2 \oplus \cdots\cdots S_n) = 0$$

as N annihilates all the S_i. It is our goal to show that if R is a left Wedderburn ring, then R is left semisimple. We have already shown that every left ideal of R is a sum of minimal left ideals so that it is a sum of simple submodules and ${}_RR$ is semisimple.

Theorem 7.11. *Let R be a left artinian ring. Let N be the nilradical of R. Then R/N is left Wedderburn and N is the unique nilpotent two-sided ideal of R.*

Proof: As R is left artinian, we know that R/N is left artinian. We also know that $\text{Nil}(R/N) = 0$. So R/N has no nonzero two-sided nil ideals. We want to show that R/N has no nilpotent left ideals. If $A \neq 0$ was such then $A \cdot R/N$ is a two-sided nilpotent ideal of R/N. But then $A \cdot R/N$ is a nonzero two-sided nil ideal, a contradiction. So R/N is left Wedderburn.

It remains to show that N is the unique two-sided ideal of R. We look at $N \supseteq N^2 \supseteq \cdots$. As R is left artinian, this chain must stabilize. Then $N^k = N^{k+n}$ for some $n \in \mathbb{N}$. Let $I = \{r \in R \mid N^k r = 0\}$. As $0 \in I$, I is nonempty. Since $N \lhd R$, I is a left ideal. It is enough to prove that $I = R$. Then $N^k \cdot 1 = N^k = 0$.

Assume that $I \neq R$. Then $I \subsetneq R$. Let S be the set of all left ideals of R properly containing I. As R is artinian, S has a minimal element, say J. Then $I \subsetneq J$. Let $a \in J \setminus I$. Then $\langle a, I\rangle \supset I$. But by the minimality of J, we have $I + Ra = J$. Then

$$\begin{aligned} 1 + NJ &= I + N(I + Ra) \\ &= I + NI + Na \\ &= I + Na \end{aligned}$$

But $I \subset I + NJ \subset J$. Assume $NJ \not\subseteq I$ so we have $I \subsetneq I + NJ$. By minimality, $I + Na = I + NJ = J$. But then $a = i + xa$ for some $i \in I$ and $x \in N$. Then $(1 - x)a = i$. As x is nilpotent, we know that $1 - x$ is invertible. Now let $y \in R$ such that $y = (1 - x)^{-1}$. Then $a = yi \in I$. But this is a contradiction as $a \in J \setminus I$. Then $NJ \subset I$. Finally, we have

$$N^{k+1}J \subset N^k I = 0$$

so $N^k J = 0$. But this is the defining property of I so that $J = I$, a contradiction. Therefore, it must be that $I = R$. □

Theorem 7.12. *Let R be a left artinian ring. Then up to isomorphism there are finitely many simple left R-modules, $S_1, \cdots, S_n$, and every simple R-module can be written up to isomorphism uniquely as a direct sum of simple modules.*

Proof: We have seen that if ${}_RS$ is simple then $NS = 0$, where N is the nilradical (though this is true for all left nilpotent ideals). So every simple R-module S can be viewed as a simple R/N-module. Then $(r + M)s = rs$. (Exercise)

Conversely, if S is a simple R/N-module then S is also a simple R-module by restriction of scalars

$$r \cdot s = (r + N)s$$

so there is a one-to-one correspondence between the simple left R-modules and simple left R/N-modules. We want to show that there are finitely many nonisomorphic simple R/N-modules. As R/N is left Wedderburn, we know that R/N is a direct sum of simple submodules. We want this to be a finite sum. But R/N is also left artinian so it is a finite sum as there would otherwise be an infinite descending chain of submodules. Now say $R/N = S_1 \oplus \cdots \oplus S_n$, where the S_i are simple modules.

We need show that these are all the simple submodules. We know that the simple modules are isomorphic to R/J, where J is a maximal ideal. So $R \longrightarrow T \longrightarrow 0$, where T is simple. But then $R/N/A \xrightarrow{\sim} T$.

$$0 \longrightarrow A \longrightarrow R/N \longrightarrow T \longrightarrow 0$$

where R/N is semisimple. But then this sequence splits so that $T = R/A$. But then T is one of the S_i. To see uniqueness, Note that M is semisimple and finitely generated so that M is a finite direct sum of simple modules. (Why?) Assume that $M = S_1 \oplus \cdots \oplus S_n = T_1 \oplus \cdots \oplus T_n$, where the S_i, T_j are simple. Assume that $s \geq n$. We prove this by induction on s. If $s = 1$, we are done. If $s > 1$, then $S_1 \subseteq T_1 \oplus \cdots \oplus T_s$. Pick a generator for S_1 in one of the T_j, then there is a j with $S_1 = T_j$. (Why?) Without loss of generality, assume that $S_1 = T_1$. We have

$$\begin{array}{ccccccc} 0 & \longrightarrow & S_1 & & S_1 \oplus \cdots \oplus S_n & \longrightarrow & S_2 \oplus \cdots \oplus S_n \longrightarrow 0 \\ & & \downarrow \sim & & \downarrow \sim & & \vdots\ \exists! \\ 0 & \longrightarrow & T_1 & & T_1 \oplus \cdots \oplus T_n & \longrightarrow & T_2 \oplus \cdots \oplus T_s \longrightarrow 0 \end{array}$$

then using the Isomorphism Theorem along with the fact that $S_1 \cong T_1$. Therefore, $n = s$. $\square$

Theorem 7.13 (Hopkins-Levitsky Theorem)**.** *Let R be a left artinian ring then every finitely generated R-module has finite lengths (so that it has a composition series). As a module has finite length if and only if R is artinian and noetherian.*

Proof: Let M be finitely generated. Let $N = \text{Nil}(R)$. We know that N is nilpotent. Let k be such that $N^k = 0$ and $N^{k-1} \neq 0$. As M is finitely generated over R, we know that ${}_RM$ is artinian. So every submodule of M is artinian.

$$M \geq NM \geq N^2M \geq \cdots \geq N^kM = 0$$

Note that $N^iM = N^{i+1}M = N(N^iM)$ so $N^iM = 0$ as N is nilpotent. So the above inclusions are proper. We look at $N^iM/N^{i+1}M$. We know that this is artinian, being the quotient of artinian modules over R/N. As N annihilates each of them, we know that this is also left Wedderburn. Each of the $N^iM/N^{i+1}M$ is a direct sum of simple submodules and are artinian so that they are a finite direct sum. Then $N^iM/N^{i+1}M$ must have finite length. Induction will show that N must therefore have finite length.

Suppose $N^{k-1}M = N^{k-1}M/N^kM$ has finite length. Then

$$0 \longrightarrow \underbrace{N^{k-1}M}_{\text{finite length}} \longrightarrow N^{k-2}M \longrightarrow \underbrace{N^{k-2}M/N^{k-1}M}_{\text{finite length}} \longrightarrow 0$$

So the module must have finite length. We “keep moving to the left" so that we know all the N^iM have finite length. This must be true especially for $i = 0$, so that M has finite length. But then M is both artinian and noetherian as a left R-module. Specializing to $M_R = R$, we know that R is noetherian. □

We know that a left artinian *ring* is a left noetherian *ring*. In general, an artinian module need not be noetherian modules.

8 Classification of Injective Modules

8.1 Motivation and Review

We know that if M is a module then there exists a projective module P with $P \longrightarrow M \longrightarrow 0$ and an injective module E with $0 \longrightarrow M \longrightarrow E$. We want the "smallest" projective module mapping onto M and the "smallest" injective module containing M. If R is artinian then we could define "the smallest" as the module with the smallest length. If M were finitely generated, we could look at all finitely generated projective modules P, $P \longrightarrow M \longrightarrow 0$ and choose P with smallest length. The same thing works for injective modules. We still have to define "smallest" for non-artinian modules.

We now recap a bit about injective modules.

Definition (Injective Module)**.** A module E is injective if for all diagrams

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B \\ & & \downarrow{\scriptstyle f} & \swarrow_{\exists g} & \\ & & E & & \end{array}$$

there is a g such that $gi = f$.

Also, recall Baer's Criterion.

Theorem 8.1 (Baer's Criterion)**.** *E is an injective R-module if and only if every module homomorphism from some ideal I of R to M can be extended to R.*

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{i} & R \\ & & \downarrow{\scriptstyle f} & \swarrow_{g} & \\ & & E & & \end{array}$$

Theorem 8.2. *Every module can be embedded into an injective module.*

8.2 Properties of Injective Modules

1. E is injective if and only if the sequence $0 \longrightarrow E \xrightarrow{\text{incl}} M$ splits if and only if $\text{Hom}_R(-, E)$ is exact.
2. Direct sums of injective modules are injective.
3. If $E_1, E_2, \ldots, E_n$ are injective then $\bigoplus_{i=1}^{n} E_i$ is injective.
4. If $\{E_i\}_{i \in \mathcal{A}}$ is a family of injective modules then $\prod_{i \in \mathcal{A}} E_i$ is injective.

Theorem 8.3. *R is left Noetherian if and only if every direct sum of injective modules is injective.*

Proof: Let $\{E_i\}_{i\in\mathcal{I}}$ be a family of injective modules. We use Baer's Criterion. Let I be a left ideal of R.

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\text{incl}} & R \\ & & \downarrow & & \\ & & \bigoplus_{i\in\mathcal{I}} E_i & & \end{array}$$

We know that if M is a module then there exists a projective module $P \longrightarrow M \longrightarrow 0$ and there exists an injective module $0 \longrightarrow M \longrightarrow E$. But we want the "smallest" projective module mapping onto M and the "smallest" injective module containing M. If R is artinian then we could define the "smallest" as the module with the smallest length having the particular property.

Suppose that M is finitely generated. We look at all finitely generated projective modules P, $P \longrightarrow M \longrightarrow 0$ and choose a P of smallest length. The same thing works for injective modules. It remains to create a definition for nonartinian modules. Before this, we briefly review injective modules.

Definition (Injective Module)**.** A module E is injective if there exists a g such that the following diagram commutes

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B \\ & & {\scriptstyle f}\downarrow & \swarrow_{g} & \\ & & E & & \end{array}$$

That is, $gi = f$.

Theorem 8.4 (Baer's Criterion)**.** *A module E is injective if and only if for all left ideals I and maps $f : I \to E$ we can extend f to R. That is, there is a map g such that the following diagram commutes.*

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{incl} & R \\ & & {\scriptstyle f}\downarrow & \swarrow_{g} & \\ & & E & & \end{array}$$

Theorem 8.5. *Every module can be embedded into an injective module.*

Properties of Injective Modules

(1) E is injective if and only if every sequence $0 \longrightarrow E \xrightarrow{\text{incl}} M$ splits if and only if $\text{Hom}(-, E)$ is exact.

(2) A direct sum of injective modules is injective.

(3) If $E_1, \ldots, E_n$ are injective then $\bigoplus_{i=1}^{n} E_i$ is injective.

(4) If $\{E_i\}_{i\in\mathcal{I}}$ is a family of injective modules then $\prod_{i\in\mathcal{I}} E_i$ is injective.

Theorem 8.6. *R is left noetherian if and only if every direct sum of injective modules is injective.*

Proof: Let $\{E_i\}_{i\in\mathcal{I}}$ be a family of injective modules. We use Baer's Criterion. Let I be a left ideal of R. Then we have

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\text{incl}} & R \\ & & {\scriptstyle f}\downarrow & \swarrow_{g} & \\ & & \bigoplus_{i\in\mathcal{I}} E_i & & \end{array}$$

But R being finitely generated implies that $I = \langle a_1, a_2, \cdots, a_n\rangle$ for some nonzero $a_i \in R$. So $f(a_i)$ has finite support in $\bigoplus_{i\in\mathcal{I}} E_i$; that is, only finitely many entries of $f(a_j)$ are nonzero. Since I is finitely generated, there are only finitely many of the a_i so that $f(I)$ has finite support in $\bigoplus_{i\in\mathcal{I}} E_i$. Therefore, finitely many of the E_i support $f(I)$. But then

$$\text{im } f = f(I) \subseteq \bigoplus_{i=1}^{n} E_i \hookrightarrow \bigoplus_{i\in\mathcal{I}} E_i$$

for some $n \in \mathbb{N}$. But then we have

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\text{incl}} & R \\ & & \downarrow & \swarrow_{\exists g} & \\ & & E_{i_1} \oplus \cdots \oplus E_{i_j} & & \\ & & \downarrow & & \\ & & \bigoplus_{i\in\mathcal{I}} E_i & & \end{array}$$

But then R is an injective module.

To show the other direction, we show that if R is not noetherian then we can construct a family of injective modules which is not injective which shall serve as our contradiction. So assume that R is not noetherian. Then there exists a proper ascending chain of (proper) left ideals

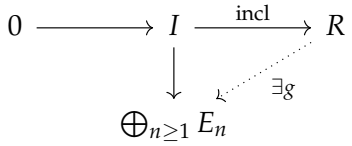
$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots$$

Let $I = \bigcup_{n\geq 1} I_n$. It is clear that I is a left ideal of R and that for all n, we have $I/I_n \neq 0$.

$$I \xrightarrow{\pi_n} I/I_n \hookrightarrow E_n$$

We embed I/I_n into an injective module E_n for all n and claim that $\bigoplus_{n\geq 1} E_n$ is not injective.

Let $\pi_n : I \to I/I_n$ be the canonical surjection for all n. Then for all $a \in I$, there is an $n \in \mathbb{N}$ such that $\pi_n(a) = 0$. We look at $I \to \prod_{n\geq 1} E_n$. We know that $f(a) = \left(\pi_n(a)\right)_{n\geq 1}$. If at some point an entry is 0, then as $I_n \subset I_{n+1}$, the rest of the entries are 0 so that $f(a)$ has finite support. But this shows that $\operatorname{im} f \subset \oplus_{n\geq 1} E_n$.



Assume that $\oplus_{n\geq 1} E_n$ is injective. So there is a $g : R \to \oplus_{n\geq 1} E_n$ extending f. We write $g(1) = (x_n)_n$ and this must have finite support. For $m \geq 1$, choose $a \notin I_m$ such that $\pi_m(a) \neq 0$; that is, choose $a \in I_{m+1} \setminus I_m$. So we have $f(a) = g(a)$ has mth coordinate $\pi_m(a)$. But

$$g(a) = g(a \cdot 1) = ag(1)$$

Now we choose m large enough so that the mth entry of $g(1)$ is 0 ($g(1)$ has finite support so this is possible). This is a contradiction.

8.3 Essential Extensions

Definition (Essential Extension)**.** Let R be a ring and $M \subset E$ be an inclusion (extension) of R-modules. Then we say that "the extension $M \subset E$ is essential" and write $M \overset{\text{ess}}{\subset} E$ if for all nonzero submodules L of E, $L \cap M \neq 0$.

Example 8.1. Let $R = \mathbb{Z}$ and look at $\mathbb{Z} \subset \mathbb{Q}/$. This is essential since if $0 \neq L \leq \mathbb{Q}$ and $a/b \in L$ then $b \cdot a/b \in L \subset \mathbb{Z}$.

Example 8.2. Let $M = S_1 \oplus S_2$ with S_1, S_2 simple, i.e. M is semisimple. Then $S_! \subset M$ is *not* essential as $S_1 \cap S_2 = 0$ - though we do not need simplicity for this.

Example 8.3. The socle of a module is always an essential submodule; that is, every module is an essential extension of the socle (if it exists).

Definition. Let M be a R-module. The socle of M is the (unique) largest semisimple module of M (if such a submodule exists). When it exists, it is denoted $\operatorname{soc} M$.

Example 8.4. $\operatorname{soc}_{\mathbb{Z}} \mathbb{Z} = 0$ as the only simple $\mathbb{Z}$-modules are of the form $\mathbb{Z}/p\mathbb{Z}$, where p is prime.

Proposition 8.1. *Assume M is artinian. Then* $\operatorname{soc} M \overset{ess}{\subset} M$.

Proof: Let $0 \neq L \leq M$. But $L \leq M$ is artinian being a submodule of an artinian module. So L has a simple submodule, $S \subseteq L \subseteq M$. So $S \subset \operatorname{soc} M$. But then $L \cap \operatorname{soc} M \neq 0$. □

Proposition 8.2. *Assume $K \overset{ess}{\subset} L \overset{ess}{\subset} M$, then $K \overset{ess}{\subset} M$ (that is, $\overset{ess}{\subset}$ is transitive).*

Proof: Let $0 \neq X \leq M$. Then observe

$$\begin{aligned} X \cap K &= X \cap (L \cap K) \\ &= (X \cap L) \cap K \end{aligned}$$

Observe that $K \cap L = K$ as $K \overset{\text{ess}}{\subset} L$ and $X \cap L$ is nonzero as $X \leq M$ and $L \overset{\text{ess}}{\subset} M$. But then $(X \cap L) \cap K \neq 0$. □

Proposition 8.3. *Let R be a ring. Let ${}_RE$ be a module. Then E is injective if and only if E has no proper essential extensions.*

Proof: Let E be injective and $E \subsetneq M$. As E is injective, $M = E \oplus N$ where $0 \neq N \leq M$ as E is proper. But then $N \cap E = 0$ so the extension is not essential.

Now assume that E has no proper essential extensions. Assume that E is not injective. There is an injective module L with $E \subset L$ no essential. So there is a nonzero submodule of L intersecting E only at 0. Let $S = \{0 \neq X \leq L \mid X \cap E\}$. This set is nonempty by assumption. We can apply Zorn's Lemma (Why?) so that S has a maximal element X_0. Consider the following:

$$E \cong E/(E \cap X_0) \cong (E + X_0)/X_0 \subseteq L/X_0$$

where $E/(E \cap X_0) \cong (E + X_0)/X_0$ follows from the First Isomorphism Theorem.

We claim that $(E + X_0)/X_0 \overset{\text{ess}}{\subset} L/X_0$. Let $0 \neq Y/X_0 \subseteq L/X_0$ so that $X_0 < Y \leq L$. By the maximality of X_0 in S, we have $Y \cap E \neq 0$. Then $Y \cap E \not\subseteq X_0$ since $X_0 \cap E = 0$ so that then we have $Y \cap (E + X_0) > X_0$. (Why?)

Now $E \cong (E + X_0)/X_0$ and E has no proper essential extensions so we must have

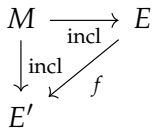
$$(E + X_0)/X_0 \cong L/X_0$$

so $E + X_0 \cong L$. But we also have $E \cap X_0 = 0$ so that $L = E \oplus X_0$ so E is injective as L is injective. But this is a contradiction. □

Our aim is to prove that for all modules M, there is an injective module E and extension $M \overset{\text{ess}}{\subset} E$. So M can be embedded by an essential extension. We also want to demonstrate some uniqueness to this extension. That is, if $M \overset{\text{ess}}{\subset} E_1$ and $M \overset{\text{ess}}{\subset} E_2$, where E_1, E_2 are injective, then $E_1 \cong E_2$. That is, the injective module E described has the property that there is no injective module $\overline{E}$ such that $M \overset{\text{ess}}{\subset} \overline{E} \overset{\text{ess}}{\subset} E$. This injective module E is called the injective envelope, or the injective hull, of the module M.

8.4 Injective Envelope/Injective Hull

Definition (Injective Envelope/Hull)**.** Given a module M, there exists an injective module E with $M \overset{\text{ess}}{\subset} E$ called the injective envelope (or injective hull of M. Furthermore, if E has the property that if E' is another injective module with



then f is an isomorphism.

Lemma 8.1. *Let $M \subset E$ be an extension of R-modules. Then $M \overset{ess}{\subset} E$ if and only if for all $0 \neq x \in E$, there is $r \in R$ such that $0 \neq rx \in M$.*

Proof: Let $0 \neq L = \langle x \rangle \leq E$. Since $x \neq 0$, we know that $L \cap M \neq 0$ so the result follows. The other direction is an exercise. □

Lemma 8.2. *Let M be a submodule of E. Let $\{E_i\}_{i \in A}$ be a chain of submodules of E such that $M \overset{ess}{\subset} E_i \subset E$. Then $M \overset{ess}{\subset} \bigcup_{i \in A} E_i$.*

Proof: Let $0 \neq x \in \cup_{i \in A} E_i$. Then there is an i_0 such that $x \in E_{i_0}$. But as $M \overset{\text{ess}}{\subset} E_{i_0}$, there is $0 \neq r \in R$ such that $0 \neq rx \in M$ so that by the previous lemma, $M \overset{\text{ess}}{\subset} \cup_{i \in A} E_i$. □

Lemma 8.3. *Consider the double extension*

$$M \overset{ess}{\subset} E_1 \subset E_2$$

where $M \overset{ess}{\subset} E_2$, then $E_1 \overset{ess}{\subset} E_2$.

Proof: We have $0 \neq L \leq E_2$, then $L \cap M \neq 0$. But $L \cap E_1 \neq 0$. (Why?) □

Lemma 8.4. *Assume $M \overset{ess}{\subset} E$ and let $f : E \to X$ be a homomorphism such that $f|_M$ is a monomorphism, then f is a monomorphism.*

Proof: We want to show that $\ker f = 0$. Assume that this is not the case. Then $0 \neq \ker f \leq E$. But then $\ker f \cap M \neq 0$. Take $0 \neq x \in \ker f \cap M$. But then $f|_M$ is not a monomorphism, a contradiction. □

Theorem 8.7. *Consider an extension $M \subset E$. The following are equivalent:*

1. *E is a maximal essential extension of M in the sense that no proper extension of E is an essential extension of M.*
2. *$M \overset{ess}{\subset} E$ and E is injective.*
3. *If E injective and there does not an exist injective module $\overline{E}$ such that $M \subset \overline{E} \subsetneq E$.*

Moreover, given a module M, an extension E as above exists.

Proof: $1 \to 2$: Let F be a proper extension of E. It is enough to show that $E \subset F$ is not essential by a previous Lemma/Theorem. Observe

$$M \overset{\text{ess}}{\subset} E \overset{\text{ess}}{\subsetneq} F$$

But by transitivity, $M \overset{\text{ess}}{\subset} F$. But this contradicts the assumed maximality of E.

$2 \to 3$: Assume there is $M \overset{\text{ess}}{\subset} \overline{E} \subsetneq E$, where $\overline{E}, E$ are injective. Then $E = \overline{E} \oplus L$ for some $0 \neq L \leq E$. But $L \cap M \subseteq L \cap \overline{E}$ but $L \cap E = 0$. This contradicts the fact that $M \overset{\text{ess}}{\subset} E$.

$3 \to 1$ (Existence): Look at all essential extensions of M that are contained in E. That is,

$$S = \{X \subseteq E \mid M \overset{\text{ess}}{\subset} X\}$$

We know $S \neq \emptyset$ as $M \in S$. Using Lemma 8.2, we can apply Zorn's Lemma. (Why?) Then there exists a minimal element of S, say X_0. We have $M \overset{\text{ess}}{\subset} X_0 \subset E$ with E injective. Assume there exists $Z > X_0$ such that $M \overset{\text{ess}}{\subset} Z$.

$$\begin{array}{ccccc} 0 & \longrightarrow & X_0 & \xrightarrow{\text{incl}} & Z \\ & & \downarrow{\scriptstyle \text{incl}} & \swarrow{\scriptstyle \exists f} & \\ & & E & & \end{array}$$

There exists a $f : Z \to E$ from the injectivity of E. Furthermore, $f|_{X_0}$ is a monomorphism as it is an inclusion. But using Lemma 8.4, we obtain $f(Z) \subset E$ and $f(X_0) \subset f(Z) \subset E$. However, the maximality of X_0 implies that $X_0 = f(Z) \cong Z$.

So X_0 has no proper essential extensions Z; otherwise, we would have $M \overset{\text{ess}}{\subset} X_0 \overset{\text{ess}}{\subset} Z$ so that $M \overset{\text{ess}}{\subset} Z$, contradicting the maximality of X_0. Then X_0 is injective. But E has no proper injective modules so that $X_0 = E$.

To show that such an extension always exists, we start with $\hat{E}$, an injective module containing M. We look at $M \subset \hat{E}$. We construct X_0 as above:

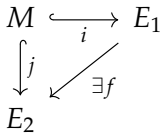
$$S = \{X \subseteq \hat{E} \mid M \overset{\text{ess}}{\subset} X\}$$

Then $E \subset S$ is the maximal element and E is injective. □

Definition. Let M be a R-module. An injective envelope (or hull) of M is an extension $M \overset{\text{ess}}{\subset} E$, where E is injective. We denote this extension $E(M)$ or $I(M)$.

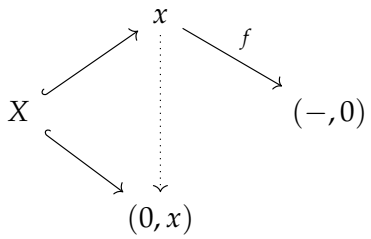
Theorem 8.8. *Any two injective envelopes of M are isomorphic.*

Proof: Suppose E_1, E_2 are two injective envelopes of an R-module M.



As E_2 is injective, there exists a function f such that $fi = j$. Now $f|_M$ is a monomorphism, we know by Lemma 8.4 that f is a monomorphism.

Now assume that f is not onto: im $f \subsetneq E_2$ and $f(E_1) \subsetneq E_2$. But using the injectivity of E_2, $f(E_1)$ splits so $E_2 = f(E_1) \oplus L$ for some nonzero L. Now $L \cap \neq 0$. Take $0 \neq x \in L \cap M$.



But $(-, 0) \neq (0, x)$. This is a contradiction so that f is onto. □

Example 8.5. We have $E(\mathbb{Z}) = Q$ as $\mathbb{Z} \overset{\text{ess}}{\subset} \mathbb{Q}$ and $\mathbb{Q}$ is divisible so it is injective.

Example 8.6. Let p be prime. Let $S = \{1, p, p^2, \cdots\}$ be a multiplicative subset of $\mathbb{Z}$. We look at $\mathbb{Z}_{(p)} = \{a/p^n \mid a \in \mathbb{Z}, n \geq 0\}$, the localization of $\mathbb{Z}$ at S. We have $\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Q}$ so $\mathbb{Z}_{(p)}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ so that

$$\begin{aligned} M &= \{a/p^n + \mathbb{Z} \mid a \in \mathbb{Z}, n \geq 0\} \\ &= \langle 1/p^n + \mathbb{Z} \mid n \geq 1 \rangle \end{aligned}$$

Proposition 8.4. *If M is divisible, then M is injective.*

Proof: Let $x \in M$. Consider $x = a/p^n + \mathbb{Z}$ for some n. Let $k \in \mathbb{Z}$, we want $y \in M$ such that $ky = x$.

Case 1 - $(k, p) = 1$: If $(k, p) = 1$, then $(k, p^n) = 1$ so there exists α, p such that $k\alpha + \beta p^n = 1$. But then

$$\begin{aligned} k\alpha + \beta p^n &= 1 \\ k(\alpha a) + (\beta a)p^n &= a \\ (k\alpha)a/p^n + \beta a &= a/p^n \end{aligned}$$

Let $y = (\alpha a)/p^n + \mathbb{Z}$ so that $ky = x$.

Case 2 - $k = p^m$: Let $x = a/p^n + \mathbb{Z}$ and let $y = a/p^{n+m} + \mathbb{Z}$. Then $ky = x$.

General Case: Let $k \in \mathbb{Z}$ and write $k = p^n k'$ with $p \nmid k'$. Let $x = a/p^n + \mathbb{Z}$. Then there exists a $y \in M$ such that $p^m y = x$ by Case 2. Then by Case 1, there exists a $z \in M$ such that $k'z = y$, then $kz = x$.

We have seen that the only submodules of M are $M_n = \langle 1/p^n + \mathbb{Z} \rangle$ and they form a chain of cyclic modules strictly contained in M but are non disjoint so that $M_n \overset{\text{ess}}{\subset} M$. But then we have $M = E(M_n)$. So we have a chain of cyclic submodules with the same injective envelope with each M_n noetherian but the injective envelope itself is not noetherian. □

8.5 Invariant Basis Number

Definition (Invariant Basis Number)**.** A ring R has an invariant basis number if given a free module F, any two bases of F have the same cardinality.

It is enough to look at finitely generated free modules. Recall that “free" means that it has a basis which is a linearly independent set that generates the module.

Theorem 8.9. *Let F be a R-module, then F is free if and only if $F \cong \bigoplus_{i \in \mathcal{I}} R_i$, where $R_i =_R R$.*

Proof: If F is free with basis $\{e_i\}_{i \in \mathcal{I}}$, then $F = \bigoplus_{i \in \mathcal{I}}$. Then we have an isomorphism $\bigoplus_{i \in \mathcal{I}} R \to F = \bigoplus_{i \in \mathcal{I}} Re_i$ given by $(r_i)_i \mapsto \sum r_i e_i$ where both $r_i \in R$ and $\sum r_i e_i$ have finite support.

The reverse direction is an exercise. □

Theorem 8.10. *Let F be a finitely generated free module, then every basis of F is finite.*

Proof: Let $x_1, x_2, \cdots, x_n$ be a set of generators for F. Choose a basis $B = \{e_i\}_{i \in \mathcal{I}}$ of F. All the x_i are linear combinations of elements from B. To express the $x_1, \cdots, x_n$ as such

linear combinations, we use only finitely many of the e_i's, say $\{e_i\}_{i\in\mathcal{I}_0}$, where $\mathcal{I}_0 \subset \mathcal{I}$ is finite.

Let $B_0 = \{e_i\}_{i\in\mathcal{I}_0}$. Now B_0 is clearly a basis, but $B_0 \subset B$. But B is a basis so that $B_0 = B$. □

Theorem 8.11. *Let F be a free module but not finitely generated. Any two bases of F have the same cardinality.*

Proof: Let B_1, B_2 be two bases of F. But by Theorem 8.10, both must be infinite. Let B_2' be the members of B_2 used in the linear combinations to express elements of B, as in the construction of Theorem 8.10. So as B_2' generates F, B_2' is a basis. However, $B_2' \subset B_2$ implies that $B_2' = B_2$. But then

$$|B_2| = |B_2'| \leq \aleph_0 \cdot |B_1| = |B_1|$$

where the inequality follows from the finite linear combinations used above and the final equality holds because B_1 is infinite. □

Theorem 8.12. *Every division ring has an invariant basis number.*

Proof: The proof is identical to the standard proof of this fact for fields. □

Theorem 8.13. *Every commutative ring has an invariant basis number.*

Proof: Assume that $R^n \cong R^m$ as R-modules. Let K be R/M, where M is a maximal idea, $M \lhd R$. So K is a field. We have the following isomorphism of R/M-modules - not R-modules

$$R/M \otimes_R R^n \cong R/M \otimes_R R^m$$

Then

$$R/M \otimes_R \underbrace{R \oplus R \oplus \times \oplus R)}_{n \text{ times}} \cong R/M \otimes_R \underbrace{(R \oplus R \oplus \times \oplus R)}_{m \text{ times}}$$

Then

$$\bigoplus^n \left(R/M \otimes_R R \right) \cong \bigoplus^m \left(R/M \otimes_R R \right)$$

is an isomorphism of K-modules. We have the following isomorphism of R/M-modules

$$R/M \otimes_R R \cong R/M = K$$

so that $K^n \cong K^m$ as $\oplus^n K \cong \oplus^m K$. But as K is a field, it has invariant basis number so that $n = m$. □

Theorem 8.14. *If R is a local ring (not necessarily commutative), then R has an invariant basis number.*

Proof: Let $M = J$, the Jacobson radical of R. Then $K = R/J$ is a division ring. The proof is then the same proof as the previous Theorem. □

Theorem 8.15. *Let R, S be rings, with S having an invariant basis number. Let $\varphi : R \to S$ be a ring homomorphism. Then R has invariant basis number.*

Proof: Note that if R is commutative then $S = R/M$ and φ is the canonical surjection, R local then $S = R/J$ and φ is the canonical surjection.

We have $R^m \cong R^n$. Observe that S is a right R-module via

$$s \cdot r \stackrel{\text{def}}{=} s\varphi(r)$$

where $s\varphi(r)$ is multiplication in S. But then we have the following isomorphism of left S-modules

$$S \otimes_R R^m \cong S \otimes_R R^n$$

But then we have

$$S \otimes_R R^m \cong S^m \text{ and } S \otimes_R R^n \cong S^n$$

isomorphic as S-modules. Then using the fact that there is an isomorphism of S-modules $S \otimes_R R \cong S$ via $s \otimes_R 1 \mapsto s$. But S has invariant basis number so $m = n$. Therefore, R has invariant basis number. □

Lemma 8.5. *Let M be noetherian and $\varphi : M \to N$ onto. Then φ is an isomorphism. (This is part of Fitting's Lemma.)*

Proof: Exercise

Theorem 8.16. *Let R be a left noetherian ring, then R has invariant basis number.*

Proof: Let $\{e_1, \cdots, e_n\}$ and $\{f_1, \cdots, f_n\}$ two basis of a free module F. Assume that $m \geq n$. Now F is a finitely generated R-module, R left noetherian, so that F is a noetherian module. There exists a homomorphism $\varphi : F \to F$. It is enough to say where the basis goes as F is free.

$$\begin{aligned} \varphi(f_1) &= e_1 \\ \varphi(f_2) &= e_2 \\ &\vdots \\ \varphi(f_n) &= e_n \end{aligned}$$

so that $\varphi(f_i) = 0$ if $i > n$. But φ is clearly onto. But by Lemma 8.5, φ is an isomorphism. Therefore, $\ker \varphi = 0$ so that there are no f_i, where $i > n$, so that $m = n$. □

Corollary 8.1. *Every semisimple ring has invariant basis number.*

Corollary 8.2. *Every left artinian ring has invariant basis number.*

Back to injective modules

We have the following modification of Baer's Criterion:

Theorem 8.17. *Let E be an R-module. Then E is injective if and only if for all left ideals I of R such that $I \overset{ess}{\subset} R$, every homomorphism $I \to E$ can be extended to a homomorphism $R \to E$.*

Proof: This will come shortly. (See Theorem 8.21.) □

Example 8.7. $E({}_{\mathbb{Z}}\mathbb{Z}) = \mathbb{Q}$. We can generalize this example to the following: If R is an integral domain with field of fractions F, then $E(R) = F$. Note that we have $0 \lhd R$, a prime ideal. Then $E(R/(0))$ generates "more or less" all injective modules.

We have proved that if R is a ring and M a module, then there exists an injective hull (or envelope) of M. That is, there exists an injective module E and a monomorphism $M \xrightarrow{f} E$ and E "minimal" with this property - "minimal" in the sense that if there is another injective module E', then

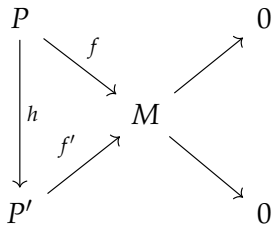
$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{f} & E \\ & & & \searrow^{g} & \downarrow{\scriptstyle f'} \\ & & & & E' \end{array}$$

with f' a monomorphism. This is another way of saying there exists a left minimal monomorphism from $M \xrightarrow{f} E$; that is, for all diagrams

$$\begin{array}{ccc} M & \xrightarrow{f} & E \\ \downarrow{\scriptstyle f'} & \swarrow_{h} & \\ E' & & \end{array}$$

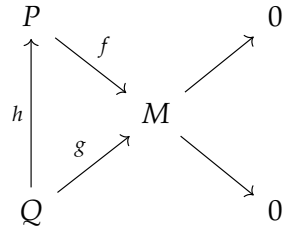
there is an isomorphism h making the diagram commute. (Exercise)

Remark. Let M be a module. A projective cover of M is a projective module D mapping onto M, $P \xrightarrow{f} M$ with f right "minimal"; that is,



then there is an isomorphism h making the diagram commute.

Proposition 8.5 (Projective Cover)**.** *Let P be projective: $P \xrightarrow{f} M \to)$ is a projective cover if for all $Q \xrightarrow{g} M \to 0$ with Q projective, then there exists an onto map $h : Q \to P$*



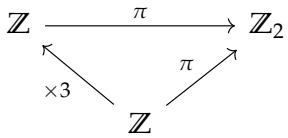
This projective cover (if it exists) is unique up to isomorphism.

Proof: Exercise.

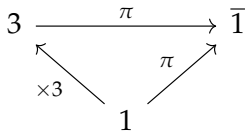
Example 8.8. There is no projective cover for $\mathbb{Z}/2\mathbb{Z}$ as a $\mathbb{Z}$-module. The only possible candidate is $\mathbb{Z}$ because it being projective makes it free.

$$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_2$$

But we have



Looking where 1 maps,



But the multiplication map is not an isomorphism.

Theorem 8.18. *The following are equivalent for a ring R:*

(1) Every module has a projective cover.

(2) Every flat module is projective.

So here we have flat = projective. There is also a notion of a flat cover.

Definition (Flat Cover)**.** A flat cover of M is a map $X \xrightarrow{f} M \to 0$, where X is flat and f is right minimal in the previously mentioned sense.

The existence of flat covers was only solved in the last 10 years.

Theorem 8.19. *If R is a ring, then R has a flat cover and this cover is unique up to isomorphism.*

Theorem 8.20. *Let R be a left artinian ring. Let M be a finitely generated, then M has a projective cover.*

"Proof": We always have $P \xrightarrow{f} M \to 0$, where f is an epimorphism and P is a finitely generated projective module. As R is artinian, it is noetherian so that P is both artinian and noetherian. Hence, P has finite length. Pick P projective having the smallest length mapping onto M. This will serve as a projective cover of M. □

Back to injective modules

Lemma 8.6. *Let R be a ring and M be an R-module. Let $K, L \leq M$ with $K \overset{ess}{\subset} M$, then $K \cap L \overset{ess}{\subset} L$.*

Proof: Let $0 \neq X \leq L$. Then

$$X \cap (K \cap L) = X \cap K$$

□

Lemma 8.7. *If $\{L_i\}_{i=1}^n$ is a collection of submodules of a module M with $L_i \overset{ess}{\subset} M$, then $\cap_{i=1}^n L_i$ is essential in M.*

Proof: It is enough to show the statement for the intersection of two modules, the general case follows by induction. Let $0 \neq X \leq M$. Then

$$\begin{aligned} X \cap (L_1 \cap L_2) &= (X \cap L_1) \cap L_2 \\ &= S' \cap L_2 \end{aligned}$$

where $S' = X \cap L_1$ is nonzero as $L_1 \overset{\text{ess}}{\subset} M$. But then $S' \leq M$ so that $S' \cap L_2 \neq 0$. □

Lemma 8.8. *Let $L_i \overset{ess}{\subset} M_i$ for some $i = 1, 2, \cdots, n$, then $\oplus_{i=1}^n L_i \overset{ess}{\subset} \oplus_{i=1}^n M_i$.*

Proof: It is enough to show this for the direct sum of two modules as the general case follows via induction. Let $0 \neq x \in M_1 \oplus M_2$. We show that $\langle x \rangle \cap (L_1 \oplus L_2) \neq 0$. This is equivalent to showing $L_1 \oplus L_2$ is essential in $M_1 \oplus M_2$. Let $x = m_1 + m_2$. As $x \neq 0$, one of the m_i must be nonzero. Without loss of generality, suppose that $m_1 \neq 0$. Now $L_1 \overset{\text{ess}}{\subset} M_1$ so that there exists $0 \neq r \in R$ with $0 \neq rm_1 \overset{\text{def}}{=} l_1 \in L_1$. Then

$$rx = rm_1 + rm_2 = l_1 + rm_2$$

If $rx =$ is the sum of a nonzero term with something else, as the sum in $M_1 \oplus M_2$ is direct, there is only one way to write 0 so that $rx \neq 0$.

Case 1: If $rm_2 = 0$, then we are done since $0 \neq rx \in L_1 \subset L_1 \oplus L_2$.

Case 2: As $L_2 \overset{\text{ess}}{\subset} M_2$, there exists $0 \neq s \in R$ with $0 \neq srm_2 \overset{\text{def}}{=} l_2$. Then

$$(sr)x = sl_1 + srm_2 = sl_1 + l_2$$

as $srx \neq 0$, by the uniqueness of the direct sum, we have $\langle x \rangle \cap (L_1 \oplus L_2) \neq 0$. □

Proposition 8.6. *Let $K, L \leq M$ with $L \overset{ess}{\subset} M$. Then*

(1) $E(L) = E(M)$

(2) If $L = L_1 \oplus L_2 \oplus \cdots \oplus L_m$, then $E(L) = E(L_1) \oplus E(L_2) \oplus \cdots \oplus E(L_n)$.

(3) There exists $X \leq M$ with $K \oplus X \overset{ess}{\subset} M$. In particular,

$$\begin{aligned} E(M) &= E(K \oplus X) \\ &= E(K) \oplus E(X) \end{aligned}$$

so that $E(K)$ is a direct summand of $E(M)$.

Proof: (1) If $L \overset{\text{ess}}{\subset} M \overset{\text{ess}}{\subset} E(M)$, then $L \overset{\text{ess}}{\subset} E(M)$ so that $E(M) = E(L)$.

(2) If $L_i \overset{\text{ess}}{\subset} E(L_i)$, then $L_1 \oplus \cdots \oplus L_n \overset{\text{ess}}{\subset} \underbrace{E(L_1) \oplus \cdots \oplus E(L_n)}_{\text{injective}}$. By the same argument as in (1),

$$E(L_1) \oplus \cdots \oplus E(L_n) = E(L)$$

(3) We look at $S = \{X \leq M \mid X \cap K = 0\}$. We know that $S \neq \emptyset$ as $0 \in S$. We apply Zorn's Lemma. (Why?) There is a minimal element X. We know that $X \cap K = 0$ and

$XL \leq M$. But then $K + X = K \oplus X \leq M$. We want to show that $K \oplus X$ is essential in M, to do so we use the maximality of X.

Exercise (The rest of (3) follows from (2) and (1)). □

Theorem 8.21 (Modification of Baer's Criterion)**.** *Let E be an R-module, then E is injective if and only if for every left ideal $I \overset{ess}{\subset} R$ and any homomorphism $f : I \to E$, f can be extended to R.*

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{incl} & R \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \exists g} & \\ & & E & & \end{array}$$

Proof: The forward direction is trivial. Now let I be a left ideal of R and $f : I \to E$, then by (3) of the previous proposition, there exists $J \leq R$ be a left ideal such that $I \oplus J \overset{\text{ess}}{\subset} R$.

$$\begin{array}{ccccc} I & \xrightarrow{\text{incl}_1} & I \oplus J & \xrightarrow{\text{ess,incl}_2} & R \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \overline{f}} & & \swarrow{\scriptstyle \exists g} & \\ E & & & & \end{array}$$

where $I \hookrightarrow I \oplus J$ is given by $a \mapsto \begin{pmatrix} a \\ 0 \end{pmatrix}$ and $\overline{f}$ is given by $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto f(a)$. Observe that $\overline{f} \circ \text{incl}_1 = f$ and $g \circ \text{incl}_2 = \overline{f}$. Therefore, f can be extended to R. □

Proposition 8.7. *Let R be an integral domain and F be the field of fractions of R, then $E(R) = F$.*

Proof: It is easy to see that $R \overset{\text{ess}}{\subset} F$. It remains to show that F is injective. We use Baer's Criterion. Let $I \lhd R$ and let $f : I \to F$.

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\text{incl}} & R \\ & & \downarrow{\scriptstyle f} & & \\ & & F & & \end{array}$$

Note that for all $0 \neq a, b \in I$, we have $f(ab) = af(b) = bf(a)$. But then $f(a)/a = f(b)/b \in F$. Let $u \in F$ be $f(a)/a$ for $0 \neq a \in I$. We want a map $g : R \to F$.

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\text{incl}} & R \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle g} & \\ & & F & & \end{array}$$

Let $g(r) \stackrel{\text{def}}{=} ru \in F$. This map is a homomorphism. (Exercise) If $r = a \in I$, then $g(a) = ua = f(a)$ by the above definition. So $g|_I = f$. □

8.6 Uniform Modules

Definition (Indecomposable)**.** A module M is indecomposable if one cannot write M as a direct sum of two nonzero proper submodules. That is, M cannot be written as $M = M_1 \oplus M_2$, where $M_1, M_2 \leq M$ and $M_1 \neq 0 \neq M_2$.

Earlier we say that R is noetherian if and only if every direct sum of injective modules is injective. We will prove that if R is noetherian then every injective module is a direct sum of indecomposable injective modules. So "knowing" the indecomposable modules means knowing all injective modules.

Definition (Uniform Dimension)**.** Let M be a module over R. Then the uniform dimension of M, denoted udim M, is the largest integer k such that there exists an inclusion $L_1 \oplus L_2 \oplus \cdots \oplus L_k \subseteq M$, where $0 \neq L_i \leq M$. If no such k exists, we say that the uniform dimension of M is infinite. By definition, udim $M = 0$ if and only if $M = 0/$

Example 8.9. Look at ${}_{\mathbb{R}}\mathbb{Q}$. If $\{e_i\}_{i\in\mathbb{R}}$ is a basis for $\mathbb{Q}$, then $\mathbb{Q} = \oplus \mathbb{R}e_i$ so that $\text{udim}_{\mathbb{R}} \mathbb{Q} = \infty$.

Example 8.10. Let S be a simple module. Then udim $S = 1$.

Example 8.11. Let M be an artinian module. Then soc $M \neq 0$. Submodules of artinian modules are artinian so there are finitely many submodules (as M has finite composition length). Then soc $M = S_1 \oplus \cdots \oplus S_k \leq M$. We claim that udim $M = k$. It is clear that udim $M \geq k$. We want to show that udim M cannot be greater than k. Assume that there exists $m > k$ and nonzero submodules $L_1, \cdots, L_m$ of M with $L_1 \oplus \cdots \oplus L_m \leq M$. As M is artinian, L_i is artinian for all i. So there is at least one simple submodule. So $L_1 \oplus \cdots \oplus L_m$ has at least m simple submodules - all distinct. This contradicts the fact that M is the sum of only k simple submodules. Therefore, udim $M = k$.

Definition (Uniform)**.** An R-module M is uniform if udim $M = 1$.

Remark. A uniform module is always indecomposable. However, the other direction is almost never true. (Think about making soc M "large".)

Uniform Modules

If M is a uniform module then by definition udim $M = 1$. We have seen that every uniform module is indecomposable. The converse is almost never true.

Example 8.12. Let k be a field. Let R be the ring $R = k[x, y]/(x, y)^2$. Then as a vector space,

$$R = k[x, y]/(x, y)^2 = k \oplus k\overline{x} \oplus k\overline{y}$$

So $\dim_k R = 3$. Therefore, R is a commutative artinian ring. Let $J = \langle \overline{x}, \overline{y} \rangle$. We have $J \lhd R$ and $R/J \cong K$. So R is a local artinian ring but not semisimple as the Jacobson radical, J, is nonzero. What is $\operatorname{soc} R$? As $\dim_k R = 3$, $\dim \operatorname{soc} R < 3$. In fact, one can show that

$$\operatorname{soc} R = R\overline{x} \oplus R\overline{y}$$

so that $\dim \operatorname{soc} R = 2$. Then R contains the sum of 2 simple modules so $\operatorname{udim} R > 1$ so R is not uniform. However, R viewed as a module over itself is indecomposable. (Exercise: Suppose R decomposes and look at how to write 1 as a sum of 2 idempotent and orthogonal then contradiction)

Lemma 8.9. *Let $M \neq 0$ be a module. The following are equivalent:*

1. *M is uniform.*

2. *For any nonzero submodules X, Y of M, $X \cap Y \neq 0$.*

3. *For any nonzero submodule $L \leq M$, we have $L \overset{ess}{\subset} M$.*

Proof: Exercise
$1 \to 2$: $X + Y \subset M$. $2 \to 3$: Take 2 submodules intersection nonzero.

Definition. Let R be a ring, then a proper left ideal I is (meet) irreducible if whenever $I = A \cap B$ for some left ideals A, B, then $A = I$ or $B = I$.

Lemma 8.10. *Let $I \lhd R$ be an ideal. Then I is meet irreducible if and only if the intersection of any two nonzero left ideals in R/I is nonzero if and only if R/I is uniform.*

Proof: Exercise (Use the Correspondence Theorem)

Lemma 8.11. *Let $E \neq 0$ be an injective R-module, where R is a commutative ring. The following are equivalent:*

1. *E is uniform.*

2. *E is the injective hull of some uniform module.*

3. *$E \cong E(R/I)$ is the injective envelope of $I \lhd R$ is a meet irreducible ideal.*

4. *E is isomorphic to the injective hull of each of its nonzero submodules.*

5. *E is indecomposable.*

Proof: $1 \to 5$: This is clear.

$5 \to 4$: Let $0 \neq L \leq E$, then $E(L)$ is isomorphic to a direct summand of E. Then $E = E(L) \oplus E'$ but E is indecomposable so that $E' = 0$.

$3 \to 2$: This follows from Lemma 8.10.

$2 \to 1$: Let $E = E(M)$, where M is a uniform module. But $M \overset{\text{ess}}{\subset} E$ so that $\operatorname{udim} M = \operatorname{udim} E = 1$.

$4 \to 3$: Find an ideal I such that R/I is uniform and is isomorphic to a submodule of E. Let $0 \neq x \in E$. Let $x = \langle x \rangle = Rx \leq E$. Let $0 \neq Y$ be a submodule of X: $Y \leq X \leq E$. But $Y \overset{\text{ess}}{\subset} X$ and $Y \overset{\text{ess}}{\subset} E$ so that $X \overset{\text{ess}}{\subset} E$. Let $R \xrightarrow{\varphi} X \to 0$ be given by $\varphi(r) = rx$. Let $I = \ker \varphi$, which is the left annihilator of X. We know $I \lhd R$ so that $R/I \cong X$ so that $E(R/I) \cong E(X) = E$. I is meet irreducible as R/I is isomorphic to a uniform module and a previous lemma. □

Remark. The previous lemma holds for arbitrary rings. The change is I is a left ideal of R is meet irreducible if and only if 0 is not the intersection of 2 nonzero left submodules of R/I, where in this case R/I is not necessarily a ring but is still a module.

Theorem 8.22. *Let R be a left noetherian ring. Let $E \neq 0$ be an injective module, then E is uniquely a direct sum of indecomposable injective modules.*

The following lemma demonstrates the uniqueness of the preceding Theorem.

Lemma 8.12. *Let $E = \oplus_{i \in \mathcal{I}} E_i$ be a direct sum of indecomposable modules over some left noetherian ring R. Assume $E \supset I_1 \oplus \cdots \oplus I_n$ for some uniform injective submodules $I_1, I_2, \cdots, I_n$. Then there exists distinct $i_1, i_2, \cdots, i_n \in I$ such that $E_{i_1} \cong I_1, E_{i_2} \cong I_2, \cdots, E_{i_n} \cong I_n$.*

Proof: We proceed by induction on n. Let $0 \neq x \in I_1$. Let $M = Rx \leq I_1$. M is also uniform so $x \in I_1 \subset E$. Now X has finite support in E so there exists $i_1, i_2, \cdots, i_k \in I$ with $M \subseteq E_{i_1} \oplus \cdots \oplus E_{i_k} \overset{\text{def}}{=} E' \leq E$. Let

$$0 \longrightarrow K_j \longrightarrow E \xrightarrow{\pi_j} E_{i_j} \longrightarrow 0$$

for $j = 1, 2, \cdots, k$, where $K_j = \ker \pi_j$ and π_j is the canonical projection. As $M \leq E'$, we know that $\cap_{j=1}^{k} M \cap K_j = 0$. (Exercise) But M is uniform and $M \cap K_j \leq M$ and is nonzero. But this cannot be so as M is uniform so by an earlier lemma, one of the intersections is 0. Without loss of generality, assume that $M \cap K_1 = 0$. Now $M \overset{\text{ess}}{\subset} I_1$ and $I_1 \cap M \cap K_1 = 0$ so that $(I_1 \cap K_1) \cap M = 0$. We know $I_1 \cap K_1$ and M is a submodule of I_1. But I_1 is uniform

so that the intersection is again zero. As $M \neq 0$, $I_1 \cap K_1 = 0$. Then $I_1 + K_1 = I_1 \oplus K_1$. Furthermore, $\pi_1(I_1) \cong I_1$ since $\pi_1|_{I_1}$ is a monomorphism. (Exercise) Now $\pi_1(I_1) \subseteq E_{j_1}$ so that $I_1 \overset{\sim}{\hookrightarrow} E_{j_1}$. But I_1 and E_{j_1} are uniform injective modules so that $E_{j_1} \cong I_1$.

The induction case is an exercise. $I_2 \oplus \cdots \oplus I_n \overset{\sim}{\hookrightarrow} M/I_1$ using the fact $M \subseteq E_{i_1} \oplus \cdots \oplus E_{i_k} \overset{\text{def}}{=} E' \leq E$.

$$M/I_1 \cong \bigoplus_{j \neq 1} E_j$$

it then follows from induction. □

As a consequence, we obtain

Theorem 8.23. *Let R be a left artinian ring. Let $S_1, \cdots, S_n$ be a complete set of simple R-modules. Then every injective module is uniquely (up to isomorphism) a direct sum of injective envelopes of these simple modules. Consequently, there are finitely many nonisomorphic indecomposable injective modules.*

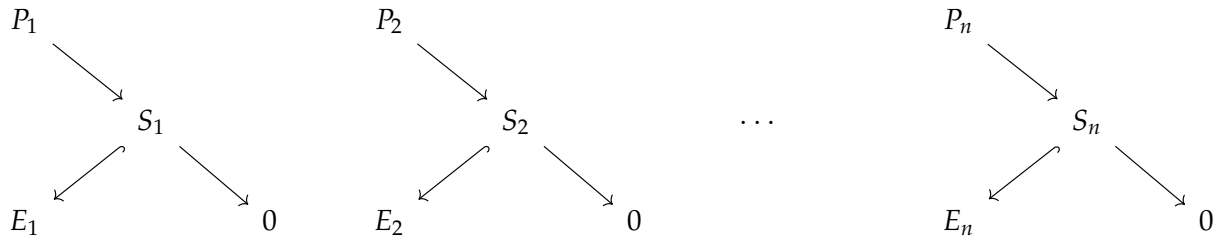
Proof: Let S be a simple module. We look at $E(S)$. We know that $E(S)$ is uniform as $S \overset{\text{ess}}{\subset} E(S)$. Therefore, each $E(S_i)$ is indecomposable and injective. Let E be an indecomposable injective module. Choose a nonzero finitely generated submodule of E. As this submodule is finitely generated over an artinian ring, this submodule is artinian. This artinian submodule must contain a simple submodule, say S. Now $S \subset$ summand $\subset E$, so that $S \subset E$ is simple. As E is uniform, S must be uniform as $X \oplus Y \subset E(S)$, $L \leq M$ so that udim $L \leq$ udim M with equality if $L \overset{\text{ess}}{\subset} M$. But as S is uniform, it must be so. But as S is uniform, udim $S = 1$. Therefore, $S \overset{\text{ess}}{\subset} E$ but $E = E(S)$ as E is injective. □

Remark. Let R be a left artinian ring. Each indecomposable projective module is of the form (up to isomorphism) Re, where e is a primitive idempotent of R. (Exercise) That is, e cannot be written as a direct sum of two idempotents, i.e. $e \neq e_1 + e_2$ with $e_i^2 = e_i$ and $e_1 e_2 = e_2 e_1 = 0$.

Remark. Indecomposable injective is equivalent to uniform.

Remark. The number of nonisomorphic indecomposable projective modules is the same as the number of nonisomorphic simple modules which is the same as the number of

nonisomorphic indecomposable injective modules.



Remark. If R is a finite dimensional k-algebra, k a field, then R is both left/right artinian so that it is both left and right noetherian.

$$\text{left } R \text{ modules} \xleftrightarrow{D} \text{right } R \text{ modules}$$

where D is a "duality map". We have $D({}_RM) = \mathrm{Hom}_k(M, k)$ a right R-module, consisting of linear functionals on M, and $D(M_R)$ a left R-module. But then M is finitely generated over R if and only if M is finite dimensional over k. The map D takes projective modules and sends them to injective modules and vice versa. The map D also takes indecomposable left modules and sends them to indecomposable right modules and vice versa.

$$M \longrightarrow D(M) \longrightarrow D(D(M)) \cong M$$

where the isomorphism follows as vector spaces *and* modules.

$$E \longrightarrow D(E) \longrightarrow D(D(E)) \cong E$$

where E is an indecomposable injective module, $D(E)$ is a finite dimensional indecomposable injective module, and $D(D(E))$ is finite dimensional.

The following is commentary of a homework problem referring to a commutative local artinian ring.

Example 8.13. Let $R = k[x]/\langle x^n \rangle$ or $k[x, y, z]/(x, y, z)^n$, where k is a field, are examples of a commutative local artinian ring.

Our goal is to describe all indecomposable injective modules over a commutative noetherian ring. This is Mattis' Theorem.

Theorem 8.24. *If R is noetherian, then every injective module is a direct sum of indecomposable injective modules. This decomposition is unique up to isomorphism.*

It remains to describe the indecomposable injective modules over a commutative noetherian ring. To do this, we introduce primes and primary ideals. We show that irreducible modules are primary and that primary ideals are irreducible. Then we show that every ideal is the finite intersection of irreducible ideals.

Theorem 8.25 (Mattis' Theorem)**.** *Let R be a commutative noetherian ring. Let* Spec R *be the set of prime ideals of R. Then there is a one-to-one correspondence between* Spec R *and the set of isomorphism classes of indecomposable injective R-modules given by*

$$P \text{ prime} \xrightarrow{\sim} E(R/P)$$

Remark. We claim that P prime implies that P is irreducible. If $P = A \cap B$, where A, B are ideals of R, then $P \supseteq AB$. However, P being prime implies that $P \supset A$ or $P \supset B$. But then $P = A$ or $P = B$ so P is irreducible. Therefore, we know that we have a map Spec R to the isomorphism classes of indecomposable injective R-modules. We that if R is an integral domain, $E(R)$, the injective envelope of R, is the field of fractions of R. Then P a prime ideal of R corresponds to $E(R/P)$.

It remains to show that this map is one-to-one and onto. Let R be a commutative ring. An ideal $R \lhd R$ is a minimal prime ideal if it is prime and if $P' \subseteq P$, then P' prime implies that $P' = P$.

Example 8.14. $\langle 0 \rangle \lhd \mathbb{Z}$ is minimal prime. In fact, this is true in every integral domain.

Remark. Assume P_1, P_2 are both minimal prime. If $P_1 \not\subseteq P_2$ and $P_2 \not\subseteq P_1$, we say that P_1, P_2 are incomparable.

Theorem 8.26. *Let P be a prime ideal in R, then P contains a minimal prime ideal.*

Proof: If P is minimal, we are done. If not, P contains properly some prime ideal. Let $S = \{Q \lhd R \mid Q < P, Q \text{ prime}\}$ and order S by inclusion. We want to find a minimal element. Pick a chain $\{Q_i\}_{i \in \mathcal{I}}$ in S. Look at $\cap_{i \in \mathcal{I}} Q_i$. We want to show that this is a prime ideal. Let $ab \in \cap Q_i$. So for all i, $ab \in Q_i$. Assume $a, b \notin \cap_{i \in \mathcal{I}} Q_i$. Then $a \notin Q_{i_0}$ but that $b \in Q_{i_0}$ for some $i_0 \in \mathcal{I}$. Assume $b \notin Q_{j_0}$ but $a \in Q_{j_0}$ for some $j_0 \in \mathcal{I}$. This is a chain, so say without loss of generality $Q_{i_0} \leq Q_{j_0}$. But $b \in Q_{i_0}$ so that $b \in Q_{j_0}$, a contradiction. So there exists a lower bound. Using Zorn's Lemma, S has a minimal element. □

Lemma 8.13. *Let $P_1, P_2, \cdots, P_n$ be incomparable prime ideals of R such that $P_1 P_2 \cdots P_n = 0$, then the set $\{P_1, P_2, \cdots, P_n\}$ is the set of all minimal prime ideals of R.*

Proof: We show first by contradiction that each P_i is a minimal prime. Assume there exists a prime ideal P such that $P_i \supsetneq P$ for some i. Then $P_i \supsetneq P \supset 0 = P_1 P_2 \cdots P_n$. But P is prime so that $P \supseteq P_j$ for some $j = 1, 2, \cdots, n$. Then

$$P_i \supsetneq P \supset P_j$$

if $i \neq j$, then P_i and P_j are comparable, a contradiction. If $i = j$, then $P_i = P$, a contradiction. Therefore, all the P_i are minimal prime ideals.

Now we want to show that this is all the minimal prime ideals of R. Assume that P is a minimal prime ideal of R.

$$P \supseteq 0 = P_1 P_2 \cdots P_n$$

so $P \supseteq P_j$ for some j. But P_j a minimal prime ideal forces $P = P_j$. □

8.7 Primary Ideals

Definition (Primary Ideal)**.** A proper ideal $Q \lhd R$ is called primary if whenever $ab \in Q$, then $a \in Q$ or $b^n \in Q$ for some $n \geq 1$.

Remark. It is immediate that P prime ideal that P is a primary ideal. However, the other direction need not be true.

Example 8.15. Let $R = \mathbb{Z}$ and $Q = \langle 4 \rangle$. Let $ab \in \langle 4 \rangle$. Then $ab = 4k$ for some integer k. Then $2 \mid ab$ so that $2 \mid a$ or $2 \mid b$. If $2 \mid a$ then $4 \mid a^2$ so that $a^2 \in Q$. If $2 \mid b$, then for the same reason, $b^2 \in Q$. So Q is a primary ideal. However, Q is not prime. Let $a = b = 2$.

Example 8.16. Let $R = \mathbb{Z}$, then $Q \lhd \mathbb{Z}$ is primary if and only if $Q = \langle p^n \rangle$ for some prime p and $n \geq 1$. To see this, assume to the contrary that $Q = \langle d \rangle$ with $p_1, q_1 \mid d$, for distinct primes p_1, q_1. Let $A = p^n q^m$, were $p \neq q$ are primes. Let $a = p^n$ and $b = q^m c$. Now no power of $a, b \in Q$ but $ab \in Q$. For the opposite direction, let $ab \in \langle p^n \rangle$. Then $p \mid a$ or $p \mid b$. If $p \mid a$, the $p^n \mid a^n$. If $p \mid b$, then $p^n \mid b^n$ so a^n or $b^n \in Q$.

Proposition 8.8. *Let R be a commutative noetherian ring. Then*

(i) Every ideal of R is a finite intersection of irreducible ideals.

(ii) Every ideal of R is a primary ideal

Therefore, every ideal of R is a finite intersection of primary ideals.

Proof: We prove the first part by contradiction. Assume there exist a counterexample. As R is noetherian, there exists a maximal counterexample, say I. Now I cannot be irreducible. If I were reducible, then it must be the finite intersection so that $I = A \cap B$, where $I \subsetneq A$ and $I \subsetneq B$ and A, B are not a counterexample to the statement of the proposition. But A, B are obtained through finite intersections so that I comes from a finite intersection, a contradiction.

Now let Q be a irreducible ideal. We want to show that Q is primary. Let $M \stackrel{\text{def}}{=} R/Q$. We know that M is uniform. Furthermore, M is finitely generated being a quotient of finitely generated modules. Let $a, b \in Q$. We look at $\text{Ann}_M(b)$:

$$\text{Ann}_M(b) = \{x \in M \mid bx = 0\}$$

We have

$$\mathrm{Ann}_M(b) \leq \mathrm{Ann}_M(b^2) \leq \cdots$$

is an ascending chain. Then as M is a noetherian (begin a finitely generated R-module where R is noetherian), this chain stabilizes at some power of b, say b^n. Then we have $\mathrm{Ann}_M(b^n) = \mathrm{Ann}_M(b^{2n})$. We claim that $b^n M \leq M$ (because R is commutative, this is indeed a submodule). We claim

$$b^n M \cap \mathrm{Ann}_M(b^n) = 0$$

To see this, let $v \in b^n M \cap \mathrm{Ann}_M(b^n)$. Then $b^n v = 0$ and $v = b^n x$ for some $x \in M$. But $b^{2n} x = 0$ so that $x \in \mathrm{Ann}_M(b^{2n}) = \mathrm{Ann}_M(b^n)$. So $b^n x = 0$ so that $b = 0$. Now $M \supseteq b^n M \oplus \mathrm{Ann}_M(b^n)$. But M is uniform so that $b^M = 0$ or $\mathrm{Ann}_M(b^n) = 0$.

If $b^n M = 0$, then $b^n R/Q = 0$ so that $b^n R \mod Q = 0$ which of course implies that $b^n \in Q$. On the other hand, if $\mathrm{Ann}_M(b^n) = 0$, we have $a + Q = Q$ so that $a \in Q$. (Why?) Now $\mathrm{Ann}_M(b^n) = \mathrm{Ann}_M(b) = 0$ is in M. □

Remark. A primary ideal need not imply that the ideal is irreducible.

Definition (Minimal Prime)**.** Let $I \lhd R$. A prime ideal $P \supseteq I$ is a minimal prime over I (or a covering of I) if there does not exist a prime ideal P_0 such that $P > P_0 \geq I$.

Remark. This type of ideal corresponds to the minimal prime ideals in R/i.

Lemma 8.14. *Let R be a commutative noetherian ring. Let $Q \lhd R$ be a primary ideal. Let $P = \sqrt{Q} = \{x \in R \mid x^n \in Q \text{ for some } n \in \mathbb{N}\}$, then P is a prime ideal containing Q and $P^m \subseteq Q \subseteq P$ for some $m \geq 1$. Furthermore, P is the unique minimal prime ideal over Q.*

Proof: If $I \lhd R$, then $\sqrt{I} = \{x \in R \mid x^n \in I \text{ for some } n \geq 1\}$. So we always have $I \leq \sqrt{I}$ (these are ideals in a commutative ring so $\sqrt{I} \lhd R$). We show $P = \sqrt{Q}$ is prime. Let $ab \in P$, then $(ab)^n \in Q$ for some n. Then $a^n b^n \in Q$. If $a^n \in Q$, then $a \in P$. If $b^m \in Q$, then $b^{nm} \in Q$ so that $b \in P$. Therefore, P is prime.

Now R is noetherian, so $P = \sqrt{Q}$ is finitely generated. Say $P = \langle x_1, x_2, \cdots, x_n \rangle$. So for all i, there is a n_i such that $x_i^{n_i} \in Q$. Let $m = \max\{m_i\}_{i=1}^n$. Then $x_i^{mn} \in Q$ so that $P^{mn} \subseteq Q$.

To see uniqueness, let $P^n \leq Q \leq P$, where P is prime and $P^n \leq Q \leq P' \leq P$, where P' is prime. Then $P' \geq P^n$ and as P' is prime, $P' \supseteq P$ so that $P' = P$. □

Definition (p-primary)**.** A primary ideal Q is called p-primary if $P = \sqrt{Q}$, where P is prime.

Lemma 8.15. *Let R be a commutative noetherian ring. Let P be a prime ideal of R. Then*

(i) A finite intersection of p-primary ideal is p-primary. (For this, one does not need noetherian.)

(ii) If Q is a p-primary ideal and $0 \neq x \leq R/Q$, then there is $0 \neq Y \leq X$ such that for all $y \in Y$, $\mathrm{Ann}_R(y) = P$.

Proof: To see the first part, let $Q = Q_1 \cap Q_2 \cdots Q_n$, where Q_i is p-primary. We want to show that Q is primary with $P = \sqrt{Q}$. Now $\sqrt{Q_i} = P$ for all i. Let $x \in P$. Then for all i, there is a n_i such that $x^{n_i} \in Q_i$. Let $k = \max\{n_i\}$. Then $x^k \in Q_i$ for all i so that $x \in Q$. But then $P \subseteq \sqrt{Q}$. Now let $x \in \sqrt{Q}$. Then $x^m \in Q$ for some $m \geq 1$. Now as $x \in \sqrt{Q_i}$ for all i which implies that $x \in P$. Therefore, $P = \sqrt{Q}$.

Now we want to show that Q is primary. Let $ab \in Q$. Assume that $b \notin \sqrt{Q}$; that is, $b^n \notin Q$ for all n. But $ab \in Q_i$ for all i. As $P = \sqrt{Q}$ and Q_i is primary for all i, the fact that $b^n \in Q_i$ for all n implies that $a \in Q_i$ for all i.

We now show the second part. Let $0 \neq X \leq R/Q$. Then $X = Z/Q$ for some submodule $Q < Z \leq R$ (this is via the Correspondence Theorem). By the previous lemma, we choose m minimal with the property that $ZP^m \leq Q$. Let $Y = (ZP^{m-1} + Q)/Q$. We know that $Y \neq 0$ as $ZP^{n-1} \not\subset Q$ so that $PY = 0$.

So for every $0 \neq y \in Y$, we have $Py = 0$ so that $P \in \mathrm{Ann}_R(y)$. We need to demonstrate equality. Let $0 \neq y \in \mathrm{Ann}_R(y)$. Say $y = a + Q$. We know $a \notin Q$ for otherwise $y = a + Q = 0$. Let $b \in \mathrm{Ann}_R(y)$. Then $0 = by = ab + Q$ so that $ab \in Q$. Now as $a \notin Q$ and Q being primary implies that $b^k \in Q$ for some k. Therefore, $b \in P$. So $\mathrm{Ann}_R(y) \subseteq P$. □

Theorem 8.27 (Mattis' Theorem)**.** *Let R be a commutative noetherian ring. Recall* Spec R *is the set of prime ideals of R. Let I be the set of isomorphism classes of indecomposable injective R-modules. Then there is a one-to-one correspondence between* Spec R *and I given by*

$$\begin{aligned} \mathrm{Spec}\, R &\xrightarrow{\varphi} I \\ P &\mapsto E(R/P) \end{aligned}$$

Proof: As P prime implies that P is irreducible, there is indeed a map. First, we show that φ is onto. Let $E \in I$ be an indecomposable injective module. Let $0 \neq x \in E$. Let $Q = \mathrm{Ann}_R(x)$. Then $R/Q \cong Rx \leq E$. But $E = E(Rx)$ as $Rx \leq E$ so that $E(Rx) \leq R$. But $E = E(Rx) \oplus E'$ so that $E = E(Rx)$ as E is indecomposable. But we also have $E(Rx) \cong E(R/Q)$. Then $E \cong E(R/Q)$ is indecomposable. So Q is irreducible. But Q is primary so Q is p-primary. That is, $P = \sqrt{Q}$. By the previous lemma, this shows that there exists a nonzero $y \in R/Q$ with $\mathrm{Ann}_R(y) = P$. Now $R/P \cong Ry \leq R/Q$ so that $E(R/P) \cong E(Ry) \leq E(R/Q)$. But $E(Ry) \cong E$ so that $E(R/P) \cong E$. Therefore, φ is surjective.

Now we show that φ is injective. Assume P, P' are prime ideals with $E \overset{\text{def}}{=} E(R/P) \cong E(R/P') \overset{\text{def}}{=} E'$. Using the previous lemma (How?), E contains a submodule Y with $\mathrm{Ann}_R(y) = P$ for all $0 \neq y \in Y \neq 0$. There is a submodule Y' of E' with $\mathrm{Ann}_R(y') - P'$ for all $0 \neq y' \in Y' \neq 0$. But E is uniform so that $Y \cap Y' \neq 0$. Then there exists $0 \neq z \in Y \cap Y'$.

But then $P = \text{Ann}_R(z) = P'$ so that $P = P'$. Therefore, φ is injective. □

Lemma 8.16. *Every finitely generated module contains a uniform submodule.*

Proof: Assume not. Let $V_0 = M$. We show by induction on n that M contains nonzero submodules X_n, Y_n with $Y_{n-1} \supseteq X_n \oplus Y_n$ (why?). Continue with $M \supseteq \oplus_{n=1}^{\infty} X_n$. But M is finitely generated so the generators are supported by finitely many X so that the sum cannot be infinite or otherwise we contradict the fact that M is noetherian. □

Theorem 8.28. *Let R be noetherian. Then every injective module is a direct sum of indecomposable injective modules. This decomposition is unique up to isomorphism and reshuffling.*

Proof: Let E be an injective module. For the purposes of this problem, we say that $F = \{E_i\}_{i \in \mathcal{I}}$ a family of indecomposable injective submodules of E is free if $\sum_i E_i = \bigoplus_i E_i$. That is, for all finite subsets $E_{i_1}, E_{i_2}, \cdots, E_{i_t}$ of F, we have $\left(\sum_{j \neq k} E_{i_j}\right) \cap E_{i_k} = 0$.

Let

$$S = \{F \mid F \text{ is a free family of indecomposable injective submodules of } E\}$$

Order S by inclusion. We claim that $S \neq \emptyset$. We show this below. Assuming $S \neq \emptyset$, Zorn's Lemma applied so that S has a maximal element under inclusion, say F_0. Let $M = \oplus_{E' \in F_0} E' \leq E$. So M splits in E: $E = M \oplus X$, where $0 \neq X$ is injective. But every injective module contains an indecomposable injective submodule. Then X contains E'', an indecomposable injective modulo. Then $F_0 \cup E'' \supset F_0$, a contradiction the maximality of F_0. Therefore, $X = 0$ so that $E = M$, as desired.

We now only need prove our assertion that $S \neq \emptyset$. We know that $0 \neq X \in E$. We look at $Rx < E$, which is finitely generated. By the previous Lemma, we know that Rx contains U, where U is uniform. So $E(U) < E$ but this is an injective envelope of a uniform indecomposable module so that $E(U)$ is indecomposable. [Rx is a noetherian module as it is finitely generated and R is noetherian.] □

9 Exercises

Problem 1: Recall that if $f : A \to B$ is a map of R-modules, then we defined ker f as a pair (K, i), where $i : K \to A$ satisfying the following conditions

(i) the composition $fi = 0$

(ii) whenever $g : L \to A$ is such that $fg = 0$, the map g factors through i, i.e. there exists a map $h : L \to K$ with $ih = g$

(a) Prove that the kernel is unique up to isomorphism; that is, if (K', i') is another kernel of f, then there exists an isomorphism $t : K \to K'$ such that $i't = i$.

(b) Let $\ker f$ be the 'usual' kernel of $f : A \to B$; that is, the set of all $x \in A$ with $f(x) = 0$. Prove that the pair $(\ker f, j)$, where j is the usual inclusion map, is a kernel of the map f.

(c) Prove that if the pair (K, i) is a kernel of the map $f : A \to B$, then i is one-to-one.

(d) Let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ be exact. Prove that the pair (A, f) is a kernel of the map g.

Problem 2: Let R be a ring and let e be an idempotent of R. Prove that $1 - e$ is also an idempotent of R and that e and $1 - e$ are orthogonal to each other. Then prove that $R = Re \oplus R(1 - e)$. Deduce that for each idempotent, e, of R, the module Re is projective.

Problem 3: Prove that $\mathbb{Z}/4\mathbb{Z}$ is *not* a projective $\mathbb{Z}$-module.

Problem 4: Prove that a direct sum of divisible modules is divisible, and that a quotient of a divisible module is divisible.

Problem 5: Let R be a ring. Prove that the following statements are equivalent:

(a) The sequence of R-modules $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ is exact.

(b) For every R-module X, the sequence of abelian groups

$$0 \longrightarrow \mathrm{Hom}_R(M_3, X) \xrightarrow{g_X^*} \mathrm{Hom}_R(M_2, X) \xrightarrow{f_X^*} \mathrm{Hom}_R(M_1, X)$$

is exact, where f_X^* and g_X^* are defined in the 'obvious' way.

Problem 6: Let R be a ring and let $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be an exact sequence of left R-modules. Use the proceeding two exercises to prove that for every right R-module M, the sequence

$$M \otimes_R A \xrightarrow{1_M \otimes f} M \otimes_R B \xrightarrow{1_M \otimes g} M \otimes_R C \longrightarrow 0$$

is exact.

Problem 7: Let R be a commutative ring and let S be a multiplicative subset of R. Let R_S be the ring of fractions of R. Prove the following:

(a) For every R-module M, we have a natural isomorphism of R_S-modules $R_S \otimes_R M \xrightarrow{\sim} M_S$.

(b) R_S is a flat R-module. Then show that $\mathbb{Q}$ is flat over $\mathbb{Q}$ but is not projective over $\mathbb{Z}$.

Problem 8: Let R, S, and T be three rings and consider ${}_RA_S$ and ${}_SB_T$.

(i) Assume that B is a flat T-module and that A is a flat S-module. Prove that $A \otimes_S B$ is a flat T-module.

(ii) Assume that R is a commutative ring and that A and B are projective R-modules. Prove that $A \otimes_R B$ is a projective R-module too.

Problem 9: Let R be the following ring where the addition and multiplication are the usual addition and multiplication of matrices

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

and let

$$I = \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix},$$

where $a \in \mathbb{R}$.

(i) Show that as a right R-module, I is both a Noetherian and an Artinian module.

(ii) Show that as a left R-module, I is neither Noetherian nor Artinian.

(iii) Show that R is both right Noetherian and right Artinian ring, but neither a left Noetherian or left Artinian ring.

Problem 10: Let R be a ring. An idempotent $e \in R$ is *central* if $er = re$ for all $r \in R$. Let I be a two-sided ideal of R. Prove that $I = Re$ for some central idempotent e if and only if $R = I \oplus J$ for some two-sided ideal of J.

Problem 11: Prove that all the R-modules are free over a ring R if and only if R is a division ring.

Problem 12: Let S be a ring and let $R = M_n(S)$. Prove that all the ideals of R are of the form $M_n(I)$ for some $I \lhd S$.

Problem 13: Prove that a left artinian ring with no nonzero nilpotent elements and no nontrivial central idempotents is a division ring.

Problem 14: Let e and f be idempotents in a ring R. Prove the following:

(i) If M is a left R-module then we have an isomorphism of abelian groups $\mathrm{Hom}_R(Re, M) \cong eM$. Is this isomorphism natural?

(ii) Prove that $\mathrm{Hom}_R(Re, Rf) \cong eRf$. Show that if $e \neq 0$ then $\mathrm{End}_R(Re)$ is isomorphic as a ring to eRe.

Problem 15: Let $\mathbb{Z}$ denote the ring of integers and let $\mathbb{Q}$ denote the rational numbers. Show that $\mathbb{Q}/\mathbb{Z}$ is a torsion $\mathbb{Z}$-module.

Problem 16: Keeping the notation from the previous exercise, let M be the $\mathbb{Z}$-submodule of $\mathbb{Q}/\mathbb{Z}$ generated by all the elements of the form $1/p^n + \mathbb{Z}$ with n running over the set of *positive* integers.

(i) Prove that M is not a finitely generated $\mathbb{Z}$-module by showing that $\mathrm{ann}(M) = 0$ while $\mathrm{ann}(L) \neq 0$ for each finitely generated submodule L of M.

(ii) Conclude that M is not a noetherian module over the integers.

Problem 17: Keeping the notation from the previous two exercises, for each positive integer n, let M_n be the submodule of M generated by $1/p^n + \mathbb{Z}$. Prove the following:

(i) $M_1 \subset M_2 \subset M_3 \subset \cdots \subset M_n \subset \cdots$

(ii) $M_n \neq M_{n+1}$ for each $n = 1, 2, \cdots$.

(iii) M is the union of all the M_n.

(iv) For each n, M_n is isomorphic to $\mathbb{Z}/p^n/Z$.

Problem 18: Keeping the notation from the previous three exercises,

(i) Show that every non-zero element of M can be written as $m/p^n + \mathbb{Z}$ for some n, where p does not divide m.

(ii) Show that if p does not divide m, then M_n is the submodule of M generated by $m/p^n + \mathbb{Z}$.

(iii) Show that the M_n are the only nonzero proper submodules of M. Hence M has the property that every proper submodule is cyclic, even though M itself is infinitely generated.

(iv) Show that M is an artinian $\mathbb{Z}$-module which is not finitely generated; hence, it is not a noetherian module.

Problem 19:

(i) Let $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ be a series for a module M and assume that for each i the inclusion $M_i \subset M_{i+1}$ splits. Prove that

$$M \cong \bigoplus_{i=0}^{n-1} M_{i+1}/M_i$$

(ii) Assume that M is a semisimple module. Show that M is the direct sum of the factors in any composition series.

Problem 20: For which values of n is the ring $\mathbb{Z}/n\mathbb{Z}$ semisimple?

Problem 21: Let $0 \longrightarrow M_n \longrightarrow M_{n-1} \longrightarrow \cdots \longrightarrow M_1 \longrightarrow M_0 \longrightarrow 0$ be a long exact sequence of modules of finite length.

$$l(M_0) = \sum_{i=1}^{n} (-1)^{i+1} l(M_i)$$

where $l(M)$ denote the length of a module M.

Problem 22: Fittings Lemma: Let M be a module and let $f : M \to M$ be an endomorphism of M.

(i) If M is a noetherian module then $\ker f^n \cap \operatorname{im} f^n = 0$ for some integer n. Conclude that if f is surjective then it is an isomorphism.

(ii) If M is an artinian module, prove that $\operatorname{im} f^n + \ker f^n = M$ for some n. Conclude that f is an isomorphism if f is one-to-one.

(iii) If M is a module of finite length, prove that there is an integer n such that $M = \operatorname{im} f^n \oplus \ker f^n$.

Problem 23: Let R be a commutative local artinian ring with maximal ideal $\mathfrak{m}$. Let $\Bbbk$ denote the residue field $\Bbbk = R/\mathfrak{m}$. Assume also that there is a ring map $\Bbbk \to R$ such that the composition with the usual surjection $R \to \Bbbk$ is an isomorphism of $\Bbbk$. Show that for every module M of finite length we have

$$l(M) = \dim_{\Bbbk} M$$

where $\dim_{\Bbbk}$ denotes the dimension as a $\Bbbk$-vector space.

Problem 24: Let R be a left artinian ring and let I and J be two nilpotent left ideals in R. Prove that $I + J$ is also nilpotent.

Problem 25: Let R be a local commutative ring and let M and N be two finitely generated non-zero R-modules. Prove that $M \otimes_R N \neq 0$.

Problem 26: Let M be a module over a ring R and assume that M decomposes as a direct sum of submodules $L_1, L_2 \cdots, L_n$:

$$M = L_1 \oplus L_2 \oplus \cdots \oplus L_n.$$

Prove that there exist idempotent homomorphisms $e_i : M \to M$ for $i = 1, 2, \cdots, n$ such that for each $i \neq j$, we have $e_i e_j = 0$ and $1_M = e_1 + \cdots + e_n$.

Problem 27: Using the previous exercise, show that a nonzero module M is indecomposable if the only idempotent homomorphisms $M \to M$ are the zero homomorphism and 1_M.

Problem 28: Let M be a module and let K be a submodule. We say that K is *superfluous* in M, denoted $K \ll M$, if whenever $K + L = M$ for some $L \leq M$, then $L = M$. We say that an epimorphism $f : M \to N$ is superfluous if $\ker f \ll M$.

Prove that an epimorphism $f : M \to N$ is superfluous if and only if all homomorphisms h, fh is an epimorphism if and only if h is an epimorphism.

Problem 29: Let M be a module and let L, K be two submodules of M. Prove that $K \cap L \overset{\text{ess}}{\subset} M$ if and only if $K \overset{\text{ess}}{\subset} M$ and $L \overset{\text{ess}}{\subset} M$.