Chapter 2

Modules

2.1 Modules, Homomorphisms, and Exact Sequences

(IV.1) Module over a ring $R$ is a generalization of abelian group. You may view an $R$-mod as a “vector space over $R$”.

**Def.** Let $R$ be a ring. A left $R$-module is an additive abelian group $A$ together with a function $R \times A \rightarrow A$ (by $(r,a) \mapsto ra$) such that for all $r,s \in R$ and $a,b \in A$:

1. $r(a + b) = ra + rb$.
2. $(r + s)a = ra + sa$.
3. $r(sa) = (rs)a$.

If $R$ has an identity $1_R$ and

4. $1_Ra = a$ for all $a \in A$,

then $A$ is said to be a unitary $R$-module. If $R$ is a division ring, then a unitary $R$-module is called a (left) vector space.

The right $R$-module are similarly defined.

In this chapter, we assume that $R$ is a ring with identity, and the $R$-modules refer to the left unitary $R$-modules.

**Ex.** A vector space $V$ over a field $F$ is a $F$-mod.

**Ex.** Abelian group $(G, +) \iff Z$-module $G$.

**Ex.** subring $S \leq R \iff R$ is a $S$-mod.
Ex. Suppose $I$ is a left ideal of $R$.

1. $I$ is a left $R$-mod under ring multiplication. In particular, $0$ and $R$ are $R$-mods.

2. $R/I$ is a left $R$-module with the multiplication $r(r_1 + I) := rr_1 + I$.

Ex. $\varphi : R \to S$ a ring homomorphism. Every $S$-module $A$ can be made into an $R$-module by $rx := \varphi(r)x$ for $x \in A$. The $R$-mod structure of $A$ is given by pullback along $\varphi$.

Ex. Let $R = C^{3 \times 3}$. Let $A = C^{3 \times 2}$. Then under matrix multiplication, $A$ is a left $R$-mod.

Ex. Let $A$ be an abelian group (resp. ring, vector space, module), and $\text{End} A$ its (corresponding) endomorphism ring. Then $A$ is a unitary $\text{End} A$-mod, with $fa := f(a)$ for $f \in \text{End} A$ and $a \in A$.

Def. A an $R$-module. A subset $B$ of $A$ is a submodule of $A$ (denoted by $B \leq R A$ or $B \leq A$) if $B$ is an additive subgroup of $A$ and $rb \in B$ for all $r \in R$, $b \in B$.

Ex. • A subspace of a vector space is a submodule.

• A subgroup $H$ of an abelian group $G$ is a $\mathbb{Z}$-submodule of $G$.

• Both $R[x]$ and $R[[x]]$ are $R$-modules, and $R[x]$ is an $R$-submodule of $R[[x]]$.

Lem 2.1. An $R$-mod. Then $B \subseteq A$ is an $R$-submod of $A$ iff:

1. $a - b \in B$ for all $a, b \in B$.

2. $ra \in B$ for all $r \in R$ and $a \in B$.

Thm 2.2. Let $A$ be an $R$-module, $\{B_i \mid i \in I\}$ a family of submodules of $A$. Then $\bigcap_{i \in I} B_i$ and $\sum_{i \in I} B_i$ are submodules of $A$.

Ex. Let $X$ be a subset of a $R$-mod $A$. The intersection of all submodules of $A$ containing $X$ is called the submodule generated by $X$.

Thm 2.3. Let $R$ be a ring with identity, $A$ a unitary left $R$-module.

1. Given $a \in A$, $Ra = \{ra \mid r \in R\}$ is the submodule of $A$ generated by $\{a\}$. It is called the cyclic submodule generated by $a$. 
2. Given a subset \( X \) of \( A \), the submodule generated by \( X \) is
\[
RX = \left\{ \sum_{i=1}^{s} r_i a_i \mid s \in \mathbb{N} \cup \{0\}; \ a_i \in X; \ r_i \in R \right\} = \sum_{x \in X} Rx
\]

Def. Let \( A \) and \( B \) be \( R \)-modules over \( R \). A function \( f: A \to B \) is an \( R \)-module homomorphism provided that for \( a, c \in A \) and \( r \in R \):
\[
f(a + c) = f(a) + f(c) \quad \text{and} \quad f(ra) = rf(a).
\]
If \( R \) is a division ring, then an \( R \)-mod hom is called a linear transformation.

The kernel of \( f: A \to B \) is the following submodule of \( A \):
\[
\text{Ker } f = \{ a \in A \mid f(a) = 0 \} \leq A.
\]
The image of \( f \) is the following submodule of \( B \):
\[
\text{Im } f = \{ f(a) \mid a \in A \} \leq B.
\]

Likewise, we can define \( R \)-module
monomorphism \( \text{Ker } f = \{ 0_A \} \)
epimorphism \( \text{Im } f = B \)

isomorphism monomorphism + epimorphism

Ex. Let \( f: A \to B \) be a \( R \)-mod homom.
- If \( C \leq A \), then \( f(C) \leq B \).
- If \( D \leq B \), then \( f^{-1}(D) = \{ a \in A \mid f(a) \in D \} \leq A \).

Ex. An abelian group homomorphism \( f: A \to B \) is a \( \mathbb{Z} \)-mod homom.

Ex. Let \( A \) be a \( R \)-mod and \( a \in A \). The map \( \phi_a : R \to Ra \) given by \( \phi_a(r) = ra \) is an epimorphism. The kernel
\[
\text{Ker } \phi_a = \{ r \in R \mid ra = 0_A \} := \text{Ann}(a)
\]
is a left ideal of \( R \).

Thm 2.4. Let \( A \) be an \( R \)-mod and \( B \leq A \). Then the quotient group \( A/B \) is an \( R \)-module with
\[
r(a + B) = ra + B \quad \text{for} \quad r \in R, \ a \in A.
\]
The map \( \pi: A \to A/B \) given by \( a \mapsto a + B \) is an \( R \)-module epimorphism with kernel \( B \) (called canonical epimorphism or projection).
Similar to group and ring homomorphisms, we have three isomorphism theorem for $R$-module homomorphisms.

**Thm 2.5.** If $f : A \to A'$ is an $R$-mod homom, then $A/\text{Ker} f \simeq \text{Im} f$ as $R$-mods.

**Thm 2.6.** Let $B$ and $C$ be submods of an $R$-mod $A$.

1. $T B/(B \cap C) \simeq (B + C)/C$ as $R$-mods;

2. If $C \leq B$, then $B/C \leq A/C$, and $(A/C)/(B/C) \simeq A/B$ as $R$-mods.

(The constructions of isomorphisms are the same as those for groups.)

We define the **product** and **coproduct** of $R$-modules.

**Thm 2.7.** Let $R$ be a ring and $\{A_i \mid i \in I\}$ a nonempty family of $R$-modules, $\prod_{i \in I} A_i$ the direct product of the abelian groups $A_i$, and $\sum_{i \in I} A_i$ the direct sum of the abelian groups $A_i$.

1. $\prod_{i \in I} A_i$ is an $R$-module with the action of $R$ given by $r\{a_i\} = \{ra_i\}$.

2. $\sum_{i \in I} A_i$ is an submodule of $\prod_{i \in I} A_i$.

3. For each $k \in I$, we have the commutative diagram:

$$
\begin{array}{ccc}
A_k & \xrightarrow{id} & A_k \\
\downarrow{\iota_k} & & \downarrow{\pi_k} \\
\prod_{i \in I} A_i & \xrightarrow{\pi_k} & A_k
\end{array}
$$

where the canonical injection $\iota_k$ is an $R$-mod monomorphism, and the canonical projection $\pi_k$ is an $R$-mod epimorphism. Similarly, we have the commutative diagram for coproduct (direct sum) of $\{A_i \mid i \in I\}$:

$$
\begin{array}{ccc}
A_k & \xrightarrow{id} & A_k \\
\downarrow{\iota_k} & & \downarrow{\pi_k} \\
\sum_{i \in I} A_i & \xrightarrow{\pi_k} & A_k
\end{array}
$$

**Thm 2.8.** Let $R$ be a ring and $\{A_i \mid i \in I\}$ a family of $R$-modules.

1. If $C$ is an $R$-mod and $\{\varphi_i : C \to A_i \mid i \in I\}$ is a family of $R$-mod homoms, then there is a unique $R$-mod homom $\varphi : C \to \prod_{i \in I} A_i$
such that $\pi_k \circ \varphi = \varphi_k$ for all $k \in I$. The $R$-mod $\prod_{i \in I} A_i$ is uniquely determined up to isomorphism by this property.

\[
\begin{array}{ccc}
\prod_{i \in I} A_i & \xrightarrow{\varphi} & C \\
\downarrow{\pi_k} & & \downarrow{\varphi_k} \\
A_k & \rightarrow & \end{array}
\]

2. If $D$ is an $R$-mod and $\{\psi_i : A_i \rightarrow D \mid i \in I\}$ is a family of $R$-mod homoms, then there is a unique $R$-mod homom $\psi : \sum_{i \in I} A_i \rightarrow D$ such that $\psi \circ \iota_k = \psi_k$ for all $k \in I$. The $R$-mod $\sum_{i \in I} A_i$ is uniquely determined up to isomorphism by this property.

\[
\begin{array}{ccc}
\sum_{i \in I} A_i & \xrightarrow{\psi} & D \\
\uparrow{\iota_k} & & \uparrow{\psi_k} \\
A_k & \rightarrow & \end{array}
\]

(proof)

Thm 2.9. Let $R$ be a ring and $\{A_i \mid i \in I\}$ a family of submodules of an $R$-module $A$ such that

1. $A$ is the sum of the family $\{A_i \mid i \in I\}$;

2. for each $k \in I$, $A_k \cap A_k^* = \{0\}$, where $A_k^*$ is the sum of the family $\{A_i \mid i \neq k\}$. Then there is an isomorphism $A \cong \sum_{i \in I} A_i$.

(exercise)

Def. A pair of module homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ is said to be **exact** at $B$ provided $\text{Im } f = \text{Ker } g$. A sequence of module homomorphisms

\[
\cdots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \cdots
\]

is **exact** provided that $\text{Im } f_i = \text{Ker } f_{i+1}$ for all indices $i$.

Note that for any module $A$, there are unique module homomorphisms $0 \rightarrow A$ and $A \rightarrow 0$.

1. The sequence of $R$-mod homoms $0 \rightarrow A \xrightarrow{f} B$ is exact if and only if $f$ is a monomorphism.
2. The sequence of $R$-mod homoms $B \xrightarrow{g} C \rightarrow 0$ is exact if and only if $g$ is an epimorphism.

3. If $A \xrightarrow{f} B \xrightarrow{g} C$ is exact, then $gf = 0$.

An exact sequence of the form $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ is called a short exact sequence. In such a sequence,

$$A \simeq \text{Im } f = \text{Ker } g, \quad B/A \simeq B/\text{Ker } g \simeq \text{Im } g = C.$$ 

In general, if $A$ is a submod of $B$, then we have the exact sequence

$$0 \rightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} B/A \rightarrow 0$$

**Ex.** If $f : A \rightarrow B$ is an $R$-mod homom, then $A/\text{Ker } f$ is the coimage of $f$ (denoted $\text{Coim } f$), and $B/\text{Im } f$ is the cokernel of $f$ (denoted $\text{Coker } f$). We have the exact sequences:

$$0 \rightarrow \text{Ker } f \rightarrow A \rightarrow \text{Coim } f \rightarrow 0$$
$$0 \rightarrow \text{Im } f \rightarrow B \rightarrow \text{Coker } f \rightarrow 0$$

**Lem 2.10.** (The Short Five Lemma) Let $R$ be a ring and

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{\gamma} 0$$

a commutative diagram of $R$-mod homoms such that each row is a short exact sequence. Then

1. $\alpha$ and $\gamma$ are monomorphisms $\implies$ $\beta$ is a monomorphism;
2. $\alpha$ and $\gamma$ are epimorphisms $\implies$ $\beta$ is an epimorphism;
3. $\alpha$ and $\gamma$ are isomorphisms $\implies$ $\beta$ is an isomorphism;

(proof)

When $\alpha$, $\beta$, and $\gamma$ above are isomorphisms, the row short exact sequences are said to be isomorphic, and we have the commutative diagram:

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{\gamma} 0$$

$$0 \rightarrow A' \xrightarrow{f'} B' \xrightarrow{g'} C' \xrightarrow{\gamma^{-1}} 0$$
Thm 2.11. Let $R$ be a ring and $0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0$ a short exact sequence of $R$-mod homoms. Then the following conditions are equivalent:

1. There is a $R$-mod homom $h : A_2 \to B$ with $gh = 1_{A_2}$;
2. There is a $R$-mod homom $k : B \to A_1$ with $kf = 1_{A_1}$;
3. The given sequence is isomorphic to the direct sum short exact sequence $0 \to A_1 \xrightarrow{i_1} A_1 \oplus A_2 \xrightarrow{i_2} A_2 \to 0$; in particular $B \cong A_1 \oplus A_2$. We call such a sequence a split exact sequence.

(proof)
2.2 Free Modules and Vector Spaces

**Def.** Let $A$ be an $R$-mod and $X$ a subset of $A$.

- $X$ is **linearly independent** if for distinct $x_1, \cdots, x_n \in X$ and $r_i \in R$, 
  \[ r_1 x_1 + \cdots + r_n x_n = 0 \implies r_i = 0 \text{ for every } i. \]

- $X$ spans $A$ if every $a \in A$ can be written as 
  \[ a = r_1 x_1 + \cdots + r_n x_n \text{ for } r_1, \cdots, r_n \in R, \ x_1, \cdots, x_n \in X. \]

- $X$ is a **basis** of $A$ if $X$ is linearly independent and $X$ spans $A$.

**Def.** A unitary $R$-mod $A$ with a nonempty basis $X$ is called a **free $R$-module** on the set $X$.

**Ex.**

1. A finitely generated free abelian group is isomorphic to $\mathbb{Z}^n$. It is a free $\mathbb{Z}$-mod.

2. The vector space $\mathbb{K}^n$ for a field $\mathbb{K}$ is a free module of $\mathbb{K}$. It can be generated by $n$ elements (i.e. $\dim_{\mathbb{K}} \mathbb{K}^n = n$). We can define linear independence, spanning set, basis, dimensions, etc, on $\mathbb{K}^n$.

3. $\mathbb{Z}_m$ for $m \in \mathbb{N}$ is not a free $\mathbb{Z}$-module.

4. $\mathbb{Q}$ is not a free $\mathbb{Z}$-mod. However, $\mathbb{Q}$ is a free $\mathbb{Q}$-mod. Similarly, $\mathbb{R}$ and $\mathbb{C}$ are not free $\mathbb{Z}$-mods.

5. A ring $R$ with no zero divisor is a free $R$-mod.

**Thm 2.12.** The following conditions on a unitary $R$-mod $F$ are equivalent:

1. $F$ has a nonempty basis;

2. $F$ is the internal direct sum of a family of cyclic $R$-mods, each of which is isomorphic as a left $R$-mod to $R$.

3. $F$ is isomorphic to a direct sum of copies of the left $R$-mod $R$;

4. there exists a nonempty set $X$ and a function $\iota : X \to F$ with the following property: given any unitary $R$-mod $A$ and function $f : X \to A$, there exists a unique $R$-mod homom $\overline{f} : F \to A$ such that $\overline{f}\iota = f$. 
2.2. FREE MODULES AND VECTOR SPACES

(proof)

Cor 2.13. Every unitary \( R \)-mod \( A \) is the homomorphic image of a free \( R \)-mod \( F \). If \( A \) is finitely generated, then \( F \) may be chosen to be finitely generated.

(proof)

Thm 2.14. Let \( R \) be a ring with identity and \( F \) a free \( R \)-mod with an infinite basis \( X \), then every basis of \( F \) has the same cardinality as \( X \).

Proof. Let \( Y \) be another basis of \( R \).

1. Claim: \( Y \) is infinite.

Suppose on the contrary, \( Y \) were finite. Since every element of \( Y \) is a linear combination of a finite number of elements of \( X \), there is a finite subset \( \{x_1, \ldots, x_m\} \) of \( X \) that generates all elements of \( Y \) and thus generates \( F \). Then every \( x \in X - \{x_1, \ldots, x_m\} \) is a linear combination of \( x_1, \ldots, x_m \), which contradicts the linear independence of \( X \). So \( Y \) is infinite.

2. Claim: \( Y \) has the same cardinality as \( X \).

Let \( K(Y) \) be the set of all finite subsets of \( Y \). Then \( |K(Y)| = |Y| \). Define a map \( f : X \rightarrow K(Y) \) by \( x \mapsto \{y_1, \ldots, y_n\} \), where \( x = r_1y_1 + \cdots + r_ny_n \) and \( r_i \neq 0 \) for all \( i \). It is well-defined since \( Y \) is a basis of \( F \).

For every \( T \in K(Y) \), \( f^{-1}(T) \) is a finite subset of \( X \) (by the similar argument as in the preceding paragraph). For each \( T \in \text{Im} \ f \), order the elements of \( f^{-1}(T) \), say \( x_1, \ldots, x_n \), and define an injective map \( g_T : f^{-1}(T) \rightarrow \text{Im} \ f \times \mathbb{N} \) by \( x_k \mapsto (T, k) \). Then we get an injective map \( X \rightarrow \text{Im} \ f \times \mathbb{N} \). Therefore,

\[
|X| \leq |\text{Im} \ f \times \mathbb{N}| = |\text{Im} \ f| \leq |K(Y)| = |Y|.
\]

Similar argument shows that \( |Y| \leq |X| \). Therefore, \( |Y| = |X| \).

\( \square \)

Theorem 2.14 works only on free \( R \)-mods with infinite cardinality bases. For finitely generated \( R \)-modules, we consider the rings \( R \) with invariant dimension property.
Def. Suppose ring \( R \) satisfies that any two bases of any free \( R\text{-mod} \) \( F \) have
the same cardinality. Then \( R \) is said to have the invariant dimension
property (IDP) and the cardinality number of any basis of \( F \) is called the
dimension (or rank) of \( F \) over \( R \).

Prop 2.15. Let \( E \) and \( F \) be free mods over a ring \( R \) with the IDP. Then
\( E \simeq F \) if and only if \( E \) and \( F \) have the same dimension. \((\text{exercise})\)

Lem 2.16. \( R \) a ring with identity. \( I \triangleleft R \). \( F \) a free \( R\text{-mod} \) with basis \( X \).
\( \pi : F \to F/IF \) the canonical projection. Then \( F/IF \) is a free \( R/I\text{-mod} \) with
basis \( \pi(X) \) and \( |\pi(X)| = |X| \).

\((\text{sketch of proof: } 1. \, \pi(X) \text{ generates } F/IF. \, 2. \, \pi(X) \text{ are linearly inde-
pendent. } 3. \, |\pi(X)| = |X|.\)\)

Prop 2.17. Let \( f : R \to S \) be a nonzero epimorphism of rings with identity.
If \( S \) has the IDP, then so does \( R \).

\((\text{Use Lemma 2.16 and } S \simeq R/I \text{ for } I := \ker f \triangleleft R.)\)

Ex. Some examples of rings with IDP

1. If \( R \) is a ring with identity that has a homomorphic image which is a
division ring, then \( R \) has the IDP. In particular, every commutative
ring with identity has the IDP.

2. Every division ring \( D \) has IDP. In fact, every \( D\text{-mod} \) \( V \) is free. \( V \) is
called a vector space over \( D \).

Prop 2.18. Let \( V \) be a vector space over a division ring \( D \).

1. \( V \) always has a basis and is a free \( D\text{-mod} \).

2. Every maximal linearly independent subset \( X \) of \( V \) is a basis of \( V \).

3. If \( Y \) is a subset of \( V \) that spans \( V \), then \( Y \) contains a basis of \( V \).

4. Every two bases of \( V \) have the same cardinality.

Prop 2.19. Let \( V \) be a vector space over a division ring \( D \). Let \( W \) and \( U \)
be subspaces of \( V \).

1. \( \dim_D V = \dim_D W + \dim_D (V/W) \). In particular, \( \dim_D W \leq \dim_D V \); \( \text{and if } \dim_D W = \dim_D V \text{ is finite, then } W = V. \)
2.2. FREE MODULES AND VECTOR SPACES

2. $\dim_D U + \dim_D W = \dim_D (U + W) + \dim_D (U \cap W)$.

(Proof by constructing the bases.)

The following result would be used in Galois Theory.

**Thm 2.20.** Let $R, S, T$ be division rings such that $R \subset S \subset T$. Then

$$\dim_R T = (\dim_S T)(\dim_R S).$$

Precisely, if $\{s_i \mid i \in I\}$ is a basis of $S$ over $R$, and $\{t_j \mid j \in J\}$ is a basis of $T$ over $S$, then $\{s_i t_j \mid i \in I, j \in J\}$ is a basis of $T$ over $R$. 
2.3 Projective and Injective Modules

(IV.3)

2.3.1 Projective Modules

Def. An $R$-mod $P$ is \textbf{projective} if given any $R$-mod homom diagram

\[
\begin{array}{ccc}
P & \xrightarrow{f} & A \\
\downarrow & & \downarrow \\
B & \xrightarrow{g} & 0
\end{array}
\]

with bottom row exact (i.e. $g$ an epimorphism), there exists an $R$-mod homom $h : P \to A$ such that $g \circ h = f$:

\[
\begin{array}{ccc}
P & \xrightarrow{f} & A \\
\downarrow{h} & & \downarrow{g} \\
B & \xrightarrow{g} & 0
\end{array}
\]

Projective modules include all free modules:

\textbf{Thm 2.21.} Every free $R$-module is projective.

(Proof: Suppose $F$ is a free module with a basis $X$. We construct the commutative diagram on $X$ first. Then apply Theorem 2.12 (4).)

\textbf{Cor 2.22.} Every module $A$ is the homomorphic image of a projective $R$-module.

(Proof: Recall that if $X$ generates $A$, then $A$ is the homomorphic image of the free module generated by $X$.)

Projective modules are characterized by the important theorem below.

\textbf{Thm 2.23.} The following condition on an $R$-mod $P$ are equivalent:

1. $P$ is projective;

2. Every short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ is split exact (hence $B \simeq A \oplus P$);

3. there is a free module $F$ and an $R$-module $K$ such that $F \simeq K \oplus P$. 
2.3. PROJECTIVE AND INJECTIVE MODULES

(Proof: $1 \to 2$, $2 \to 3$, $3 \to 1$.)

So a module is projective if and only if it is the direct sum component of a free module.

**Ex.** Let $R = \mathbb{Z}_6$. Then $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ as $\mathbb{Z}_6$-modules. So both $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are projective $\mathbb{Z}_6$-modules, although they are not free $\mathbb{Z}_6$-modules.

**Ex.** $\mathbb{Z}_2$ is NOT a projective $\mathbb{Z}_4$-module.

**Thm 2.24.** A direct sum of $R$-mods $\bigoplus_{i \in I} P_i$ is projective if and only if each $P_i$ is projective.

(Proof)

2.3.2 Injective Modules

Injectivity is the dual notation to projectivity.

**Def.** An $R$-mod $J$ is injective if given any $R$-mod homom diagram:

$$
\begin{array}{ccc}
0 & \longrightarrow & A \\
& & \downarrow g \\
& & B \\
& & \downarrow f \\
& & J \\
\end{array}
$$

with top row exact (i.e. $g$ a monomorphism), there exists an $R$-mod homom $h : B \to J$ such that $h \circ g = f$:

$$
\begin{array}{ccc}
0 & \longrightarrow & A \\
& & \downarrow g \\
& & B \\
& & \downarrow f \\
& & J \\
& & \downarrow h \\
\end{array}
$$

There is a dual result to Cor 2.22 for injective modules:

**Prop 2.25.** Every $R$-mod $A$ may be embedded in an injective $R$-module.

(The proof is complex and we skip it.)

**Thm 2.26.** The following conditions on an $R$-mod $J$ are equivalent:

1. $J$ is injective;

2. every short exact sequence $0 \to J \xrightarrow{f} B \xrightarrow{g} C \to 0$ is split exact (hence $B \cong J \oplus C$).
3. \( J \) is a direct summand of any module \( B \) of which \( J \) is a submodule.

(proof)

The dual result to Thm 2.24 for injective module is:

**Thm 2.27.** A direct product of \( R \)-mods \( \prod_{i \in I} J_i \) is injective if and only if \( J_i \) is injective for every \( i \in I \).

(exercise)
2.4 Modules over a Principal Ideal Domain

(IV.6) In this section, the ring \( R \) is a principal ideal domain (PID).

**Ex.** An finitely generated abelian group (i.e. a finitely generated \( \mathbb{Z} \)-module) is isomorphic to \( \mathbb{Z}^r \oplus \bigoplus_{i=1}^k \mathbb{Z}_{p_i^{s_i}} \) for (not necessary distinct) primes \( p_i \) and integers \( r, k, s_i \).

**Thm 2.28.** Let \( R \) be a PID, \( F \) a free \( R \)-module, and \( G \) a submodule of \( F \). Then \( G \) is a free \( R \)-mod and rank \( G \) \( \leq \) rank \( F \).

**Proof.** Let \( \{ x_i \mid i \in I \} \) be a basis of \( F \). Choose a well ordering \( \leq \) of \( I \) (Introduction, Section 7), and denote the immediate successor of \( i \) by \( i + 1 \) (Introduction, Ex 7.7). Choose \( \alpha \notin I \). Let \( J = I \cup \{ \alpha \} \) and let \( i < \alpha \) for all \( i \in I \). For each \( j \in J \) Let \( F_j \) be the submodule generated by \( \{ x_i \mid i < j \} \).

1. \( F_{i+1}/F_i \simeq Rx_i \simeq R \) (apply 3rd Isomorphism Thm on the canonical projection \( F_{i+1} \to Rx_i \)).

2. \( G_i = G_{i+1} \cap F_i \).

3. \( G_{i+1}/G_i = G_{i+1}/(G_{i+1} \cap F_i) \simeq (G_{i+1} + F_i)/F_i \).

But \( (G_{i+1} + F_i)/F_i \) is a submodule of \( F_{i+1}/F_i \simeq R \), and every submodule of \( R \) is an ideal and is of the form \( Rc \) for some \( c \in R \). So \( G_{i+1}/G_i \) is free of rank 0 or 1. Then \( 0 \to G_i \to G_{i+1} \to G_{i+1}/G_i \to 0 \) is split exact. So \( G_{i+1} = G_i \oplus Rb_i \) for \( b_i = 0 \) or \( b_i \in G_{i+1} - G_i \). Let \( B = \{ b_i \mid b_i \neq 0, i \in I \} \). Then \( |B| \leq |I| \). We can show that \( B \) is a basis of \( G \) (Exercise).

Likewise, if every ideal of a generic ring \( R \) is finitely generated (for example, if \( R \) is a Noetherian Ring), then every submodule of a finitely generated \( R \)-module is finitely generated.

**Cor 2.29.** Let \( R \) be a PID. If \( A \) is a finitely generated \( R \)-mod generated by \( n \) elements, then every submodule of \( A \) may be generated by \( m \) elements with \( m \leq n \).

**Cor 2.30.** A module \( A \) over a PID \( R \) is free if and only if \( A \) is projective.

**Lem 2.31.** Let \( A \) be a left module over a PID \( R \) and for each \( a \in A \) let \( O_a = \{ r \in R \mid ra = 0 \} \).

1. \( O_a \) is an ideal of \( R \) for each \( a \in A \).
2. \( A_t = \{ a \in A \mid O_a \neq 0 \} \) is a submodule of \( A \), the **torsion submodule** of \( A \). Indeed, \( O_{ra} \supseteq O_a \) and \( O_{a+b} \supseteq O_a \cap O_b \) for \( r \in R - \{0\} \) and \( a, b \in A \).

3. For each \( a \in A \) there is an isomorphism of left modules

\[
R/O_a \simeq Ra = \{ ra \mid r \in R \}.
\]

**Remark.**

1. \( A \) is a **torsion module** if \( A = A_t \); \( A \) is **torsion-free** if \( A_t = 0 \).

2. Every free module is torsion-free. However, a torsion-free (not finitely generated) module may not be free. The \( \mathbb{Z} \)-module \( \mathbb{Q} \) is a counterexample. See theorem below for the finitely generated case.

3. Given \( a \in A \), suppose that \( O_a = (r) \) for \( r \in R \). Then

\[
Ra \simeq R/O_a = R/(r)
\]

is said to be **cyclic of order** \( r \).

**Ex.** Let \( A \) be an abelian group (i.e. \( \mathbb{Z} \)-module). If the group theoretic order of \( a \in A \) is \( n \in \mathbb{N} \), then \( \mathbb{Z}a \simeq \mathbb{Z}/(n) \) as \( \mathbb{Z} \)-mod; if \( a \) has infinite order, then \( \mathbb{Z}a \simeq \mathbb{Z}/(0) \simeq \mathbb{Z} \).

**Thm 2.32.** A finitely generated torsion-free module \( A \) over a PID \( R \) is free.

**Proof.** Let \( X \) be a set of elements that generate \( A \). Let \( S = \{ x_1, \ldots, x_k \} \) be a maximal subset of \( X \) such that

\[
r_1x_1 + \cdots + r_kx_k = 0 \quad \Rightarrow \quad r_1 = \cdots = r_k = 0.
\]

Then \( S \) is nonempty. Let \( F \) be the submodule generated by \( S \). Then \( F \) is a free submodule of \( A \). Given \( y \in X - S \), there exists \( r_y \neq 0 \) and \( r_1, \ldots, r_k \in R \) such that \( r_y y + r_1x_1 + \cdots + r_kx_k = 0 \). Then \( r_y y \in F \). This shows that there exists \( r = \prod_{y \in X - S} r_y \neq 0 \), such that \( rX \leq F \). Then \( X \simeq rX \) is free. \( \square \)

**Thm 2.33.** If \( A \) is a finitely generated module over a PID \( R \), then \( A = A_t \oplus F \), where \( F \) is a free \( R \)-module of finite rank and \( F \simeq A/A_t \).

Let us investigate the torsion part of \( A \).
2.4. MODULES OVER A PRINCIPAL IDEAL DOMAIN

Lem 2.34. Let $A$ be a torsion module over a PID $R$ and for each prime $p \in R$ let $A(p) = \{ a \in A \mid a \text{ has order a power of } p \}$.

1. $A(p)$ is a submodule of $A$ for each prime $p \in R$;

2. $A = \bigoplus A(p)$, where the sum is over all primes $p \in R$. If $A$ is finitely generated, only finitely many of the $A(p)$ are nonzero.

Proof. 1. Easy.

2. Given $a \in A$, suppose $O_a = (r)$ and $r = p_1^{n_1} \cdots p_k^{n_k}$. Let $r_i \in R$ satisfy that $r = p_1^{n_1} r_i$. Then $\gcd(r_1, \cdots, r_k) = 1$ and there exist $s_1, \cdots, s_k \in R$ such that $s_1 r_1 + \cdots + s_k r_k = 1$. Then $a = s_1 r_1 a + \cdots + s_k r_k a$ and $s_i r_i a \in A(p_i)$. So $A = \sum A(p)$. Now for any prime $p$, we set $A_p := \sum_{q \neq p} A(q)$. Verify that $A(p) \cap A_p = \{0\}$. Then $A = \bigoplus A(p)$.

If $A = \langle a_1, \cdots, a_n \rangle$. Let $O_{a_i} = (r_i)$. Let $q_1, \cdots, q_\ell$ be all distinct primes (up to associate) that divides one of $r_1, \cdots, r_n$. Then $A = \bigoplus_{i=1}^\ell A(q_i)$.

Lem 2.35. Let $R$ be a PID and $p \in R$ be a prime. Let $A$ be a fin gen $R$-mod such that every nonzero element of $A$ has order a power of $p$. Then

$A \simeq \bigoplus_{i=1}^k R/(p_i^{n_i})$ for some $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$.

(The proof is skipped here.)

Lem 2.36. If $r = p_1^{n_1} \cdots p_k^{n_k}$ where $p_i$ are distinct primes, then

$R/(r) \simeq \bigoplus_{i=1}^k R/(p_i^{n_i})$ as left $R$-modules.

Proof. Define $\phi : R/(r) \to \bigoplus_{i=1}^k R/(p_i^{n_i})$ by

$\phi(a + (r)) = (a + (p_1^{n_1}), a + (p_2^{n_2}), \cdots, a + (p_k^{n_k}))$.

Verify that $\phi$ is a well-defined $R$-mod monomorphism. Let $A_i = (p_i^{n_i})$ in $R$. Then $A_i + A_j = R$ for $i \neq j$. By Chinese Remainder Theorem, $\phi$ is an epimorphism.

The classification theorem of finitely generated modules over a PID is:

Thm 2.37. Let $A$ be a finitely generated module over a PID $R$. 
CHAPTER 2. MODULES

1.

$$A \cong R^r \bigoplus_{i=1}^{k} R/(p_i^{s_i}),$$

where $r \in \mathbb{N}$, $p_1, \ldots, p_k$ are (not necessary distinct) primes in $R$ and $s_1, \ldots, s_k$ are (not necessary distinct) positive integers. The elements $p_1^{s_1}, \ldots, p_k^{s_k}$ are called the **elementary divisors** of $A$. The rank $r$ and the list of ideals $(p_1^{s_1}), \ldots, (p_k^{s_k})$ are uniquely determined by $A$.

2.

$$A \cong R^r \bigoplus_{j=1}^{t} R/(r_j)$$

where $r \in \mathbb{N}$, $r_1, \ldots, r_t$ are (not necessary distinct) nonzero nonunit elements of $R$ such that $r_1 \mid r_2 \mid \cdots \mid r_t$. The elements $r_1, \ldots, r_t$ are called the **invariant factors** of $A$. The rank $r$ and the list of ideals $(r_1), \ldots, (r_t)$ are uniquely determined by $A$.

**Ex.** The $\mathbb{Z}$-mod $A = \mathbb{Z}^6 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{14} \oplus \mathbb{Z}_{18} \oplus \mathbb{Z}_{24}$ is classified by

$$A \cong \mathbb{Z}^6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_84 \oplus \mathbb{Z}_{2520}$$

We work out the following table:

<table>
<thead>
<tr>
<th>$p_i^{s_i}$</th>
<th>$p$</th>
<th>$t_j$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2^4</td>
<td>2^4</td>
<td>5</td>
</tr>
<tr>
<td>2^2</td>
<td>2^2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Therefore, $A$ has another classification into cyclic modules:

$$A \cong \mathbb{Z}^6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{84} \oplus \mathbb{Z}_{2520} \quad \text{where} \quad 2 \mid 2 \mid 6 \mid 84 \mid 2520$$

**Cor 2.38.** Two finitely generated modules $A$ and $B$ over a PID are isomorphic if and only if $A/A_t$ and $B/B_t$ have the same rank and $A$ and $B$ have the same invariant factors (resp. elementary divisors).