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 $R \times A \to A$ (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. $1_R a = a$ *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* $\mathbf{F}$ *is a* $\mathbf{F}$*-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** *φ.*

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

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

$$RX = \{\sum_{i=1}^{s} r_i a_i \mid s \in \mathbf{N} \cup \{0\};\ a_i \in X;\ r_i \in R\} = \sum_{x \in X} Rx$$

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 $r \in R$:*

$$f(a + c) = f(a) + f(c) \qquad \text{and} \qquad f(ra) = rf(a).$$

If R is a division ring, then an R-mod homom is called a **linear transformation**.

The **kernel** *of $f : A \to B$ is the following submodule of A:*

$$Ker f = \{a \in A \mid f(a) = 0\} \leq A.$$

The **image** *of f is the following submodule of B:*

$$Im f = \{f(a) \mid a \in A\} \leq B.$$

Likewise, we can define R-module

monomorphism	$\operatorname{Ker} f = \{0_A\}$
epimorphism	$\operatorname{Im} f = B$
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 $\mathbf{Z}$-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*

$$Ker \phi_a = \{r \in R \mid ra = 0_A\} := Ann(a)$$

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*

$$r(a + B) = ra + B \qquad \text{for} \qquad r \in R,\ a \in A.$$

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 $A/Ker f \simeq Im f$ 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:*

$$A_k \overset{\iota_k}{\hookrightarrow} \prod_{i\in I} A_i \overset{\pi_k}{\twoheadrightarrow} A_k \quad (\pi_k \circ \iota_k = id)$$

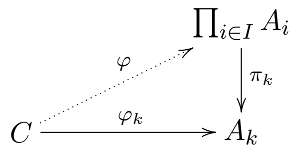
where the canonical injection ι_k is an R-mod monomorphism, and the canonical projection π_k is an R-mod epimorphism. Similarly, we have the commutative diagram for coproduct (direct sum) of $\{A_i \mid i \in I\}$:

$$A_k \overset{\iota_k}{\hookrightarrow} \sum_{i\in I} A_i \overset{\pi_k}{\twoheadrightarrow} A_k \quad (\pi_k \circ \iota_k = id)$$

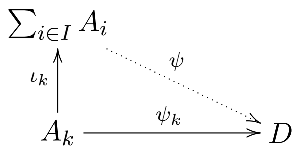
Thm 2.8. *Let R be a ring and $\{A_i \mid i \in I\}$ a family of R-modules.*

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.*



2. *If* D *is an R-mod and* $\{\psi_i : A_i \to D \mid i \in I\}$ *is a family of R-mod homoms, then there is a unique R-mod homom* $\psi : \sum_{i\in I} A_i \to D$ *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.*



(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* $A \simeq \sum_{i\in I} A_i$.

(exercise)

Def. *A pair of module homomorphisms* $A \xrightarrow{f} B \xrightarrow{g} C$ *is said to be* **exact** *at* B *provided* $Im\, f = Ker\, g$. *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* $Im\, f_i = Ker\, f_{i+1}$ *for all indices* i.

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

1. The sequence of R-mod homoms $0 \to A \xrightarrow{f} B$ is exact if and only if f is a monomorphism.

2. The sequence of R-mod homoms $B \xrightarrow{g} C \to 0$ is exact if and only if g is a epimorphism.

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

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

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

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

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

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

$$0 \to Ker\, f \to A \to Coim\, f \to 0$$
$$0 \to Im\, f \to B \to Coker\, f \to 0$$
$$0 \to Ker\, f \to A \xrightarrow{f} B \to Coker\, f \to 0$$

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

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

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

1. *α and γ are monomorphisms $\Longrightarrow$ β is a monomorphism;*

2. *α and γ are epimorphisms $\Longrightarrow$ β is a epimorphism;*

3. *α and γ are isomorphisms $\Longrightarrow$ β is a isomorphism;*

(proof)

When α, β, and γ above are isomorphisms, the row short exact sequences are said to be **isomorphic**, and we have the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle\alpha^{-1}} & & \uparrow{\scriptstyle\beta^{-1}} & & \uparrow{\scriptstyle\gamma^{-1}} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

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 $0 \to A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$; in particular $B \simeq A_1 \oplus A_2$. We call such a sequence a* **split exact sequence***.*

(proof)

2.2 Free Modules and Vector Spaces

(IV.2)

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 $r_i \in R$,*

$$r_1x_1 + \cdots + r_nx_n = 0 \quad \Longrightarrow \quad r_i = 0 \quad \text{for every } i.$$

- *X* **spans** *A if every $a \in A$ can be written as*

$$a = r_1x_1 + \cdots + r_nx_n \qquad \text{for} \qquad r_1, \cdots, r_n \in R, \quad x_1, \cdots, x_n \in X.$$

- *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 $\mathbf{Z}^n$. It is a free $\mathbf{Z}$-mod.*
2. *The vector space $\mathbf{K}^n$ for a field $\mathbf{K}$ is a free module of $\mathbf{K}$. It can be generated by n elements (i.e. $\dim_{\mathbf{K}} \mathbf{K}^n = n$). We can define linear independence, spanning set, basis, dimensions, etc, on $\mathbf{K}^n$.*
3. *$\mathbf{Z}_m$ for $m \in \mathbf{N}$ is not a free $\mathbf{Z}$-module.*
4. *$\mathbf{Q}$ is not a free $\mathbf{Z}$-mod. However, $\mathbf{Q}$ is a free $\mathbf{Q}$-mod. Similarly, $\mathbf{R}$ and $\mathbf{C}$ are not free $\mathbf{Z}$-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 $\overline{f}\iota = f$.*

(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 $\{x_1, \cdots, x_m\}$ of X that generates all elements of Y and thus generates F. Then every $x \in X - \{x_1, \cdots, x_m\}$ is a linear combination of $x_1, \cdots, x_m$, 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 $f : X \to K(Y)$ by $x \mapsto \{y_1, \cdots, y_n\}$, 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 $T \in \operatorname{Im} f$, order the elements of $f^{-1}(T)$, say $x_1, \cdots, x_n$, and define an injective map $g_T : f^{-1}(T) \to \operatorname{Im} f \times \mathbf{N}$ by $x_k \mapsto (T, k)$. Then we get an injective map $X \to \operatorname{Im} f \times \mathbf{N}$. Therefore,

   $$|X| \leq |\operatorname{Im} f \times \mathbf{N}| = |\operatorname{Im} f| \leq |K(Y)| = |Y|.$$

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

□

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-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. (exercise)*

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

(sketch of proof: 1. $\pi(X)$ generates F/IF. 2. $\pi(X)$ are linearly independent. 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.*

(Use Lemma 2.16 and $S \simeq R/I$ for $I := \operatorname{Ker} f \lhd R$.)

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-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-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,* $\dim_D W \leq \dim_D V$*; and if* $\dim_D W = \dim_D V$ *is finite, then* $W = V$.

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*

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

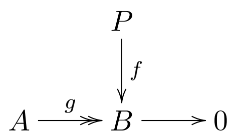
Precisely, if $\{s_i \mid i \in I\}$ is a basis of S over R, and $\{t_j \mid j \in J\}$ is a basis of T over S, then $\{s_i t_j \mid i \in I,\ j \in J\}$ is a basis of T over R.

2.3 Projective and Injective Modules

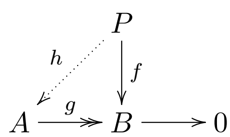
(IV.3)

2.3.1 Projective Modules

Def. *An R-mod P is* **projective** *if given any R-mod homom diagram*



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



Projective modules include all free modules:

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).)

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.

Thm 2.23. *The following condition on an R-mod P are equivalent:*

1. *P is projective;*
2. *Every short exact sequence $0 \to A \overset{f}{\hookrightarrow} B \overset{g}{\twoheadrightarrow} P \to 0$ is split exact (hence $B \simeq A \oplus P$);*
3. *there is a free module F and an R-module K such that $F \simeq K \oplus P$.*

(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 $R = \mathbf{Z}_6$. Then $\mathbf{Z}_6 \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_3$ as $\mathbf{Z}_6$-modules. So both $\mathbf{Z}_2$ and $\mathbf{Z}_3$ are projective $\mathbf{Z}_6$-modules, although they are not free $\mathbf{Z}_6$-modules.*

Ex. *$\mathbf{Z}_2$ is NOT a projective $\mathbf{Z}_4$-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:*

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

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

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \overset{g}{\hookrightarrow} & B \\ & & {\scriptstyle f}\downarrow & \swarrow {\scriptstyle h} & \\ & & J & & \end{array}$$

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 $0 \to J \overset{f}{\hookrightarrow} B \overset{g}{\twoheadrightarrow} C \to 0$ is split exact (hence $B \simeq J \oplus C$).*

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* $\mathbf{Z}$*-module) is isomorphic to* $\mathbf{Z}^r \bigoplus_{i=1}^{k} \mathbf{Z}_{p_i^{s_i}}$ *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* $\operatorname{rank} G \leq \operatorname{rank} F$*.*

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 $\{x_i \mid i < j\}$. Let $G_j = G \cap F_j$.

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* $\mathcal{O}_a = \{r \in R \mid ra = 0\}$*.*

1. $\mathcal{O}_a$ *is an ideal of* R *for each* $a \in A$*.*

2. $A_t = \{a \in A \mid \mathcal{O}_a \neq 0\}$ *is a submodule of* A*, the* **torsion submodule** *of* A*. Indeed,* $\mathcal{O}_{ra} \supset \mathcal{O}_a$ *and* $\mathcal{O}_{a+b} \supset \mathcal{O}_a \cap \mathcal{O}_b$ *for* $r \in R - \{0\}$ *and* $a, b \in A$*.*

3. *For each* $a \in A$ *there is an isomorphism of left modules*

$$R/\mathcal{O}_a \simeq Ra = \{ra \mid r \in R\}.$$

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* **Z***-module* **Q** *is a counter-example. See theorem below for the finitely generated case.*

3. *Given* $a \in A$*, suppose that* $\mathcal{O}_a = (r)$ *for* $r \in R$*. Then*

$$Ra \simeq R/\mathcal{O}_a = R/(r)$$

is said to be **cyclic of order** r*.*

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

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 $S = \{x_1, \cdots, x_k\}$ be a maximal subset of X such that

$$r_1x_1 + \cdots + r_kx_k = 0 \quad \Longrightarrow \quad r_1 = \cdots = r_k = 0.$$

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 $r_1, \cdots, r_k \in R$ 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. □

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 invesetigate the torsion part of A.

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 $\mathcal{O}_a = (r)$ and $r = p_1^{n_1} \cdots p_k^{n_k}$. Let $r_i \in R$ satisfy that $r = p_i^{n_i} r_i$. 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 $\mathcal{O}_{a_i} = (r_i)$. 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 $A \simeq \bigoplus_{i=1}^{k} R/(p^{n_i})$ 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*

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

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

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

Verify that ϕ 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, ϕ 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.*

1.

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

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

2.

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

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

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

$$A \simeq \mathbf{Z}^6 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{2^2} \oplus \mathbf{Z}_{2^3} \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_{3^2} \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_7 \oplus \mathbf{Z}_7$$

We work out the following table:

		p			t_j
$p_i^{s_i}$	2^3	3^2	5	7	2520
	2^2	3		7	84
	2	3			6
	2				2
	2				2

Therefore, A has another classification into cyclic modules:

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

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).*