

Algebra II

Minerva

2020-2nd

Contents

1	Module theory	4
1.1	Definition, examples and basis properties	4
1.1.1	Definition of module	4
1.1.2	Important examples	6
1.2	Free module	7
1.3	Direct limit and inverse limit	12
1.3.1	Definition	12
1.3.2	Examples	14
1.3.3	Stalk	15
1.4	Modules over a PID	15
1.5	Structure theorem for finite generated PID-modules and applications	20
1.5.1	Structure theorem for finite generated PID-module	20
1.5.2	Applications	21
1.6	Tensor product	24
1.7	Symmetric algebra	28
1.8	Modules of fractions	29
1.8.1	Definition and some property	29
1.8.2	Localization of prime ideal and maximal ideal	30
1.9	Noetherian modules	33
1.10	Primary decomposition	36
1.11	Nakayama's lemma & Artin-Rees lemma	40
1.12	Hilbert polynomial	44
1.13	Indecomposable module	47
1.13.1	Krull-Remak-Schmidt theorem	47
1.13.2	Commutative Artinian ring	50
2	Homological algebra	52
2.1	Projective, injective and flat module	52
2.2	Homology functor	58
2.3	Ext and Tor (I)	63
2.4	Ext and Tor (II) and an important application	68
2.4.1	group-module	68
2.4.2	resolution of \mathbb{Z}	69
2.4.3	Augmentation ideal	70
2.5	Koszul complex	72
2.5.1	Wedge product and Koszul complex	72

2.5.2	R -regular sequence	75
2.6	Extensions of abelian groups	76
2.7	$H^2(G, M)$ and $H^1(G, M)$	80
2.8	Applications	83
3	Representation theory	88
3.1	Semisimple modules	88
3.1.1	Semisimple modules	88
3.1.2	Matrix form of simple and semisimple modules	90
3.2	Semisimple rings	92
3.2.1	Semisimple rings	92
3.2.2	Product of ring	93
3.2.3	Radical	95
3.3	Simple rings	96
3.3.1	Simple rings and Artin-Wedderburn theorem	96
3.3.2	Matrix rings	98
3.3.3	Simple Algebra over a algebraically closed field	99
3.4	Representations and Semisimplicity	101
3.4.1	Definition-example	101
3.4.2	Complete reducibility	103
3.4.3	Application for semisimplicity	104
4	Presentation	107
5	Appendix	108
5.1	Definition of Categories and Functors	108
6	Homework	110
6.1	110
6.2	111
6.3	111
6.4	112
6.5	113
6.6	114
6.7	115
6.8	115
6.9	116
6.10	116
6.11	117
6.12	117
6.13	118
6.14	120
6.15	121
6.16	122
6.17	123
6.18	123
6.19	123

6.20	124
6.21	125
6.22	125
6.23	126

Chapter 1

Module theory

1.1 Definition, examples and basis properties

1.1.1 Definition of module

We give two definition to describe module. Actually, they are equivalent.

Definition 1.1.1 (module 1). Let A be a ring. A left A -module is an abelian group M (written additively) on which A acts linearly :
$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, x) & \longmapsto & ax \end{array} \text{ s.t.}$$

- M1 : $a(x + y) = ax + ay \ \forall a \in A, x \in M$
- M2 : $(a + b)x = ax + bx \ \forall a, b \in A, x \in M$
- M3 : $(ab)x = a(bx) \ \forall a, b \in A, x \in M$
- M4 : $1 \cdot x = x \ \forall x \in M$

Definition 1.1.2 (module 2). Let A be a ring. A left A -module is an abelian group M with a ring homomorphism $f : A \rightarrow \text{End}(M)$

Property 1.1.1. Two definition of module are equivalent.

Proof:

(1 \Rightarrow 2) Define
$$\begin{array}{ccc} f : & A & \longrightarrow \text{End}(M) \\ & a & \longmapsto f(a) : x \mapsto ax \end{array}$$

- M1 $\rightsquigarrow f(a)(x + y) = a(x + y) = ax + ay = f(a)(x) + f(a)(y) \rightsquigarrow f(a) \in \text{End}(M)$
- M2 $\rightsquigarrow f(a+b)(x) = (a+b)x = ax+bx = f(a)(x)+f(b)(x) = (f(a)+f(b))(x) \ \forall x \in M$
- M3: $f(ab)(x) = (ab)x = a(bx) = f(a)(bx) = f(a) \circ f(b)(x) \ \forall x \in M$
- M4: $f(1)(x) = 1 \cdot x = x \ \forall x \in M$

Hence, f is a ring homomorphism.

(2 \Rightarrow 1) Define $A \times M \longrightarrow M$
 $(a, x) \longmapsto f(a)x$ and reverse all in (1 \Rightarrow 2) which satisfy 4 law of module. \square

Remark 1.1.1. a left A -module = a representation of A

Remark 1.1.2.

- When A is commutative, a left module is a right module ($ax \leftrightarrow xa$)
pf. Only need to check M3: $(ab)x = a(bx) = a(xb) = (xb)a = x(ba) = x(ab)$
- The **opposite ring** of A : A° is a ring s.t. $(A^\circ, +) = (A, +)$ and (A°, \cdot) is defined by $a \cdot b = b \cdot a \ \forall a, b \in A$

A right A -module is an abelian group M with a ring homo. $g : A^\circ \longrightarrow \text{End}(M)$
 $a \longmapsto g(a) : z \mapsto xa$

$$M_3 : g(a \circ b)(x) = x(ba) = (xb)a = g(a)(xb) = g(a) \circ g(b)(x) \ \forall x \in M$$

Example 1.1.1.

- An abelian group G is a \mathbb{Z} -module

$$\forall m \in \mathbb{Z}, \forall x \in G, \text{ define } mx = \begin{cases} \underbrace{x + \cdots + x}_{m \text{ times}} & \text{if } m \geq 0 \\ \underbrace{(-x) + \cdots + (-x)}_{m \text{ times}} & \text{if } m < 0 \end{cases}$$

- A itself is an A -module
- A left(right) ideal I of A is a left(right) A -module

Property 1.1.2. Any left(right) A -submodule of A is a left(right) ideal of A

Definition 1.1.3. An A -module homo. $\varphi : M \rightarrow N$ is an additive group s.t.
 $\varphi(ax) = a\varphi(x) \ \forall a \in A, x \in M$

Property 1.1.3. $\ker \varphi$ is a submodule of M and $\text{Im } \varphi$ is a submodule of N

Definition 1.1.4. Let N be a submodule of M . The quotient modules is M/N :

$$\begin{aligned} A \times M/N &\longrightarrow M/N \\ (a, \bar{x}) &\longrightarrow \overline{ax} \end{aligned}$$

Well defined : $\overline{x_1} = \overline{x_2} \rightsquigarrow x_1 - x_2 \in N \rightsquigarrow ax_1 - ax_2 = a(x_1 - x_2) \in N \rightsquigarrow \overline{ax_1} = \overline{ax_2}$

Theorem 1.1.1. Basic theorems

- Factor thm. : Given $\varphi : M \rightarrow M'$ and $N \subseteq M$ s.t. $N \subseteq \ker \varphi$, then

$$\begin{array}{ccc} M/N & \xrightarrow{\exists! \bar{\varphi}} & M' \\ \swarrow \pi & & \nearrow \varphi \\ & M & \end{array}$$

- 1st isom.thm. : Given $\varphi : M \rightarrow N$, then $M/\ker \varphi \simeq \text{Im } \varphi$
- 2nd isom.thm. : Given $N_1, N_2 \subseteq M$, then $(N_1 + N_2)/N_1 \simeq N_1/(N_1 \cap N_2)$
- 3rd isom.thm. : Given $N \subseteq M$

$$\begin{array}{ccc} \{\text{submodules of } M/N\} & \longleftrightarrow & \{\text{submodules of } M \text{ containing } N\} \\ M'/N & \longleftrightarrow & M' \end{array}$$

$$\text{and } (M/N)/(M'/N) \simeq M/M'$$

Definition 1.1.5 (cokernel). $\text{coker } \varphi := N/\ker \varphi$

$$\rightsquigarrow \varphi \text{ is } 1-1 \iff \ker \varphi = \{0\}, \varphi \text{ is onto} \iff \text{coker } \varphi = \{0\}$$

1.1.2 Important examples

Homomorphism group

Definition 1.1.6 (Homomorphism group). $\text{Hom}_A(M, N)$ is the set of all A -module homomorphism $: M \rightarrow N$. Define

$$(f + g)(x) = f(x) + g(x) \quad \forall x \in M$$

then $\text{Hom}_A(M, N)$ has abelian group structure.

- When A is commutative, $\text{Hom}_A(M, N)$ has an A -module structure:
 - For $a \in A, f \in \text{Hom}_A(M, N)$, define $(af)(x) := f(ax) \quad \forall x \in M$
 - $af \in \text{Hom}_A(M, N)$:

$$\begin{aligned} (af)(x+y) &= f(a(x+y)) = f(ax+ay) = f(ax) + f(ay) = (af)(x) + (af)(y) \\ ((a+b)f)(x) &= f((a+b)x) = f(ax+bx) = f(ax) + f(bx) = (af)(x) + (bf)(x) \\ (bf)(x) &= (af+bf)(x) \end{aligned}$$
 - Module law : M1, M2, M4 is obvious.

$$\text{M3: } ((ab)f)(x) = f((ab)x) = f((ba)x) = f(b(ax)) = (bf)(ax) = (a(bf))(x)$$

Definition 1.1.7 (bimodule). If M is left A -module and right B -module and $(ax)b = a(xb)$, then we say ${}_A M_B$ is A, B -bimodule

- Given ${}_A M_B, {}_A N$, then $\text{Hom}_A(M, N)$ is a left B -module.

$$\forall b \in B, f \in \text{Hom}_A(M, N), \text{ define } (bf)(x) := f(xb) \quad \forall x \in M$$
 - $(bf)(ax) = f((ax)b) = f(a(xb)) = af(xb) = a(bf)(x)$
 - $((ab)f)(x) = f(x(ab)) = f((xa)b) = (bf)(xa) = (a(bf))(x)$
- Given ${}_A M_B, N_B$, then $\text{Hom}_B(M, N)$ is a right A -module.

$$\forall a \in A, f \in \text{Hom}_B(M, N), \text{ define } (fa)(x) := f(ax) \quad \forall x \in M$$
 - $(fa)(xb) = f(a(xb)) = f((ax)b) = f(ax)b = (fa)(x)b$
 - $(f(ab))(x) = f((ab)x) = f(a(bx)) = (af)(bx) = ((fa)b)(x)$

- Given ${}_A M, {}_A M_B$, $\text{Hom}_A(M, N)$ has a right B -module structure. $(fb)(x) = f(x)b$
- Given $M_B, {}_A M_B$, $\text{Hom}_B(M, N)$ has a left A -module structure. $(af)(x) = af(x)$

Vector space and polynomial

Let k be a field and V be a k -vector space, then V is a k -module.

$\forall T \in \text{Hom}_k(V, V) \rightsquigarrow V$ has a $k[x]$ -module structure corresponding to T . Define

$$\begin{aligned} \varphi : k[x] &\longrightarrow \text{End}(V) \\ f(x) &\longmapsto f(T) \end{aligned}$$

- $\varphi(f(x) + g(x)) = f(T) + g(T) = \varphi(f(x)) + \varphi(g(x))$
- $\varphi(f(x)g(x)) = f(T) \circ g(T) = \varphi(f(x)) \circ \varphi(g(x))$

representation of group

Let G be a finite group with $|G| = n$, say $G = \{g_1, \dots, g_n\}$

Consider $V = \mathbb{R}g_1 \oplus \dots \oplus \mathbb{R}g_n$ and define

$$\forall g \in G, \rho_g : \sum_{i=1}^n r_i g_i \longmapsto \sum_{i=1}^n r_i (gg_i) \rightsquigarrow \rho_g \in \text{GL}(V)$$

then $\varphi : \begin{matrix} G & \longrightarrow & \text{GL}(V) \\ g & \longmapsto & \rho_g \end{matrix}$ is the regular representation of G .

Definition 1.1.8 (group ring). $R[G] := \left\{ \sum_{g \in G}^{\text{finite}} a_g g : a_g \in R \right\}$ is called a **group ring** of G over R with

$$\begin{aligned} \sum a_g g + \sum b_g g &= \sum (a_g + b_g) g \\ \left(\sum a_g g \right) \left(\sum b_g g \right) &= \left(\sum_{g, g' \in G} a_g b_{g'} gg' \right) \end{aligned}$$

Example 1.1.2.

- $G = \langle g \rangle$ with $g^3 = e \implies \mathbb{C}[G] = \mathbb{C} \oplus \mathbb{C}g \oplus \mathbb{C}g^2 \simeq \mathbb{C}[x]/\langle x^3 - 1 \rangle$
- \mathbb{Z} is $\mathbb{Z}[x]$ -module : $\mathbb{Z} \simeq \mathbb{Z}[x]/\langle x \rangle$ is a $\mathbb{Z}[x]$ -module and thus $f(x) \cdot n := f(x)\bar{n} = \overline{f(0)n}$

1.2 Free module

Example 1.2.1. $A^n = A \times \dots \times A$ (n times) with

$$\begin{aligned} (a_1, \dots, a_n) + (b_1, \dots, b_n) &= (a_1 + b_1, \dots, a_n + b_n) \\ a(a_1, \dots, a_n) &= (aa_1, \dots, aa_n) \end{aligned}$$

is an A -module. Let $e_i = (0, \dots, 1, \dots, 0)$ (i -th entry is 1 and others are 0) $\forall i = 1, \dots, n$

Then $(a_1, \dots, a_n) = \sum_{i=1}^n a_i e_i$ and $\sum_{i=1}^n a_i e_i = 0 \iff a_i = 0 \forall i$

Definition 1.2.1 (basis). Given an A -module M . A nonempty set S is called a **basis** for M if S is linearly independent and generate M .

Property 1.2.1. If an A -module M has a basis $\{x_1, \dots, x_n\}$, then $M \simeq A^n$

Proof: Define $\varphi : A^n \longrightarrow M$
 $e_i \longmapsto x_i$ and extend by linearity

$$\sum_{i=1}^n a_i e_i \in \ker \varphi \iff \sum_{i=1}^n a_i e_i = 0 \iff a_i = 0 \forall i, \text{ so } \varphi \text{ is } 1-1 \rightsquigarrow M \simeq A^n \quad \square$$

By this Property, you may ask if $M \simeq N$ and M, N has a finite basis β_1, β_2 , respectively. Will it implies $|\beta_1| = |\beta_2|$ like we learn in vector space? In others word, does

$$A^n \simeq A^m \implies n = m$$

will holds? Actually, it doesn't hold forever. We see this example first.

Example 1.2.2. We construct a module A with $A^2 \simeq A$

Let V be a k -vector space with an infinite countable basis $\{e_1, e_2, \dots\}$

Let $A = \text{Hom}_k(V, V) \rightsquigarrow (A, +, \circ)$ forms a ring.

Define $\varphi : A \longrightarrow A \times A$
 $T \longmapsto (T_1, T_2)$, where $\begin{cases} T_1(e_k) = T(e_{2k-1}) \\ T_2(e_k) = T(e_{2k}) \end{cases}$

It is clear that φ is a module homomorphism.

- φ is $1-1 : T = 0 \iff T_1 = 0$ and $T_2 = 0$
- φ is onto : Given T_1, T_2 can decide unique T

Hence, $A \simeq A^2$

Remark 1.2.1. Similarly, $A \simeq A^n \forall n \in \mathbb{N} \rightsquigarrow A^n \simeq A^m \forall m, n \in \mathbb{N}$

Definition 1.2.2 (direct sum). Given a family of A -module $\{M_\lambda : \lambda \in \Lambda\}$, the **direct sum**

$$\coprod_{\lambda \in \Lambda} M_\lambda$$

of $\{M_\lambda : \lambda \in \Lambda\}$ is an A -module with injections $\rho_\lambda : M_\lambda \rightarrow \coprod_{\lambda \in \Lambda} M_\lambda \forall \lambda \in \Lambda$ s.t. $\forall N$ with A -module homo. $f_\lambda : M_\lambda \rightarrow N \forall \lambda \in \Lambda$, then $\exists!$ A -module homomorphism φ let the diagrams commute.

$$\begin{array}{ccc} \coprod_{\lambda \in \Lambda} M_\lambda & \xrightarrow{\exists! \varphi} & N \\ & \swarrow \rho_\lambda \quad \searrow f_\lambda & \\ & M_\lambda & \end{array} \quad \forall \lambda \in \Lambda$$

Property 1.2.2. $\coprod_{\lambda} M_\lambda$ is exists and unique up to isomorphism.

(unique be proved by universal property)

Proof: Define

$$\coprod_{\lambda} M_{\lambda} := \{(x_{\lambda})_{\lambda \in \Lambda} : x_{\lambda} \in M_{\lambda} \text{ and almost all of the } x_{\lambda} \text{ are zero}\}$$

and the operation on it.

- $(x_{\lambda})_{\lambda \in \Lambda} + (y_{\lambda})_{\lambda \in \Lambda} = (x_{\lambda} + y_{\lambda})_{\lambda \in \Lambda}$
- $a(x_{\lambda})_{\lambda \in \Lambda} = (ax_{\lambda})_{\lambda \in \Lambda}$

So it is a A -module.

- Define the injection $\rho_{\lambda} :$

$$\begin{aligned} \rho_{\lambda} : M_{\lambda} &\longrightarrow \coprod_{\lambda} M_{\lambda} \\ x_{\lambda} &\longmapsto (y_{\lambda'})_{\lambda' \in \Lambda} \end{aligned} \quad \text{with} \quad \begin{cases} y_{\lambda} = x_{\lambda} \\ y_{\lambda'} = 0 & \text{if } \lambda' \neq \lambda \end{cases}$$

- Given $f_{\lambda} : M_{\lambda} \rightarrow N$

$$\begin{array}{ccc} \rho_{\lambda}(x_{\lambda}) \in \coprod_{\lambda \in \Lambda} M_{\lambda} & \xrightarrow{\exists! \varphi} & N \ni f_{\lambda}(x_{\lambda}) \\ \swarrow \rho_{\lambda} & & \nearrow f_{\lambda} \\ & x_{\lambda} \in M_{\lambda} & \end{array}$$

define $\varphi((x_{\lambda})_{\lambda \in \Lambda}) = \sum_{\text{finite}} f_{\lambda}(x_{\lambda})$ is a module homomorphism.

□

Definition 1.2.3 (free module). An A -module F is said to be **free** on a nonempty set S if \exists a mapping $i : S \rightarrow F$ s.t. giving any mapping $j : S \rightarrow M$, where M is an A -module. Then $\exists!$ A -module homomorphism φ let the diagrams commute.

$$\begin{array}{ccc} F & \xrightarrow{\exists! \varphi} & M \\ \swarrow i & & \nearrow j \\ & S & \end{array}$$

Theorem 1.2.1. Given $S \neq \emptyset$, F exists and it is unique up to isomorphism.

Proof: Assume that $S = \{x_{\lambda} : \lambda \in \Lambda\}$. Consider $M_{\lambda} = Ax_{\lambda}$

Define $F = \coprod_{\lambda \in \Lambda} M_{\lambda}$. Given $j : S \rightarrow M$, define $f_{\lambda} : M_{\lambda} \longrightarrow M$
 $ax_{\lambda} \longmapsto aj(x_{\lambda})$

By the universal property of direct sum,

$$\begin{array}{ccc} i(x_{\lambda}) \in \coprod_{\lambda \in \Lambda} M_{\lambda} & \xrightarrow{\exists! \varphi} & N \ni j(x_{\lambda}) \\ \swarrow \rho_{\lambda} & & \nearrow f_{\lambda} \\ & M_{\lambda} & \\ \swarrow i & & \nearrow j \\ & x_{\lambda} \in S & \end{array}$$

Define $i(x_\lambda) = \rho(x_\lambda)$, then $\varphi \circ i = j$ is commute.

(Actually, we can choose $M_\lambda = A$ is also be a possible way.) \square

Theorem 1.2.2. Let A be a non-trivial commutative ring and $|S| < \infty$. Then all bases of F have the same number of element.

Proof: Let $S = \{x_1, \dots, x_n\}$. Then $F \simeq \prod_{i=1}^n Ax_i \simeq A^n$. For another basis $\{y_1, \dots, y_m\}$, then $F \simeq A^m$

Claim: $A^n \simeq A^m \iff n = m$
 $p.f.$ Let $e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}, f = \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{pmatrix}$, where $\{e_i\}, \{f_j\}$ be the standard basis for

A^n, A^m , respectively. Then $\begin{cases} f = Qe & \text{with } Q \in M_{m \times n}(A) \\ e = Pf & \text{with } P \in M_{n \times m}(A) \end{cases} \implies f = QPf \implies QP = I_m$, otherwise f_1, \dots, f_m will have non-trivial linearly relation.

Assume that $n < m$, set $Q_1 = \begin{pmatrix} Q & 0 \end{pmatrix}, P_1 = \begin{pmatrix} P \\ 0 \end{pmatrix} \implies Q_1 P_1 = (QP) = I_m \rightsquigarrow 0 = \det Q_1 \det P_1 = \det I_m = 1 \ (\rightarrow \leftarrow)$ \square

Definition 1.2.4. We say a ring A has **IBN**(invariant basis number) if every finitely generating free module F has fixed basis number.

Definition 1.2.5 (rank). If A has IBN and M is an A -module have a finite basis β , then we say M is **free of rank** n , where $n = |\beta|$.

Theorem 1.2.3. Let F be a free A -module. If F has an infinite basis S , then for any other basis S' of F , we have $|S| = |S'|$

Proof:

- $|S'| = \infty$: Assume that $|S'| < \infty$, say $S' = \{x'_1, \dots, x'_m\} \rightsquigarrow \exists \{x_1, \dots, x_n\} \subset S$ s.t. $S' \subseteq \langle x_1, \dots, x_n \rangle_A \rightsquigarrow F = \langle S' \rangle_A \subseteq \langle x_1, \dots, x_n \rangle_A \subseteq F \rightsquigarrow F = \langle x_1, \dots, x_n \rangle$. Since $|S| = \infty, \exists x \in S \setminus \{x_1, \dots, x_n\} \rightsquigarrow x \in \langle x_1, \dots, x_n \rangle_A$, but x, x_1, \dots, x_n are linearly independent. $(\rightarrow \leftarrow)$

- $|S| = \infty, |S'| = \infty$. Assume that $|S'| \leq |S|$

Recall that if $\mathcal{B} = \{T \subseteq S' : |T| < \infty\}$ and $|S'| = \infty$, then $|\mathcal{B}| = |S'|$

Let $T = \{y'_1, \dots, y'_k\} \subseteq S'$ and let $S_T = \{y \in S | y \in \langle T \rangle_A\}$

- $|S_T| < \infty$: $\langle T \rangle_A \subseteq \langle y_1, \dots, y_n \rangle_A$ for some $\{y_1, \dots, y_n\} \subset S$
 $\rightsquigarrow S_T \subseteq \langle T \rangle_A \subseteq \langle y_1, \dots, y_n \rangle_A$. By linear independence of S , $S_T \subseteq \{y_1, \dots, y_n\}$

- $|S| \leq |S'|$: Let $\mathcal{B} = \{T \subseteq S' : |T| < \infty\}$. Since $|S'| = \infty, |\mathcal{B}| = |S'|$

Define

$$f : \quad S \quad \longrightarrow \quad \mathcal{B}$$

$$\sum_{i=1}^k a_i y'_i = y \quad \longmapsto \quad \{y'_1, \dots, y'_k\}$$

which is well-defined since S' is linearly independent.

For $T \in \mathcal{B}$, $y \in f^{-1}(T) \iff y \in S_T \rightsquigarrow |f^{-1}(T)| < \infty$. Hence,

$$|S| = \left| \bigcup_{T \subseteq \mathcal{B}}^{\text{finite}} f^{-1}(T) \right| \leq |\mathcal{B}| \aleph_0 = |\mathcal{B}| = |S'|$$

□

Definition 1.2.6 (direct product). Given a family of A -modules $\{M_\lambda : \lambda \in \Lambda\}$, the **direct product** $\prod_{\lambda \in \Lambda} M_\lambda$ is an A -module with projections : $\pi_\lambda : \prod_{\lambda \in \Lambda} M_\lambda \rightarrow M_\lambda \forall \lambda$ s.t. for any A -module N with $h_\lambda : N \rightarrow M_\lambda \forall \lambda$, then $\exists!$ A -module homomorphism φ let the diagram commute.

$$\begin{array}{ccc} N & \xrightarrow{\exists! \varphi} & \prod_{\lambda \in \Lambda} M_\lambda \\ & \searrow h_\lambda & \swarrow \pi_\lambda \\ & M_\lambda & \end{array}$$

Definition 1.2.7. Define

$$\prod_{\lambda \in \Lambda} M_i = \{(x_\lambda)_{\lambda \in \Lambda} : x_\lambda \in M_\lambda \forall \lambda\}$$

and the operation on it.

- $(x_\lambda)_{\lambda \in \Lambda} + (y_\lambda)_{\lambda \in \Lambda} = (x_\lambda + y_\lambda)_{\lambda \in \Lambda}$
- $a(x_\lambda)_{\lambda \in \Lambda} = (ax_\lambda)_{\lambda \in \Lambda}$

So it is a A -module.

- Define the projection π_λ

$$\begin{array}{ccc} \pi_\lambda : & \prod_{\lambda} M_\lambda & \longrightarrow M_\lambda \\ & (x_\lambda)_{\lambda \in \Lambda} & \longmapsto x_\lambda \end{array}$$

- Given $h_\lambda : N \rightarrow M_\lambda$

$$\begin{array}{ccc} x \in N & \xrightarrow{\exists! \varphi} & \prod_{\lambda \in \Lambda} M_\lambda \\ & \searrow h_\lambda & \swarrow \pi_\lambda \\ & h_\lambda(x) \in M_\lambda & \end{array}$$

define $\varphi(x) = (h_\lambda(x))_{\lambda \in \Lambda}$ is a module homomorphism by checking every component independently.

Now, we can mix all together.

Property 1.2.3. By universal property, it is clear that (connected means isomorphism) and the last two will not isomorphism for general cases.

$$\begin{array}{cccc}
 \text{Hom}_A(\coprod_{\lambda} M_{\lambda}, N) & \text{Hom}_A(\prod_{\lambda} M_{\lambda}, N) & \text{Hom}_A(N, \coprod_{\lambda} M_{\lambda}) & \text{Hom}_A(N, \prod_{\lambda} M_{\lambda}) \\
 \searrow & & \downarrow & \downarrow \\
 \prod_{\lambda} \text{Hom}_A(M_{\lambda}, N) & \prod_{\lambda} \text{Hom}_A(M_{\lambda}, N) & \prod_{\lambda} \text{Hom}_A(N, M_{\lambda}) & \prod_{\lambda} \text{Hom}_A(N, M_{\lambda})
 \end{array}$$

1.3 Direct limit and inverse limit

1.3.1 Definition

Definition 1.3.1 (poset). (P, \leq) is called a poset if

- $a \leq a$
- If $a \leq b, b \leq a$, then $a = b$
- If $a \leq b, b \leq c$, then $a \leq c$

Definition 1.3.2 (directed set). A set I is called **directed set** if

- I is a poset
- $\forall i, j \in I \exists k \in I$ s.t. $i \leq k$ and $j \leq k$

Definition 1.3.3 (direct system). Let A be a ring, I be a directed set and $(M_i)_{i \in I}$ is a family of A -module. A collection of morphism $\{\mu_{ij}\}$ satisfy

- $\forall i \leq j, \mu_{ij} : M_i \rightarrow M_j$ is an A -module homomorphism
- $\mu_{ii} = \text{id}$
- $\forall i \leq j \leq k, \mu_{ik} = \mu_{jk} \circ \mu_{ij}$

is called a **direct system** over I and denote $((M_i)_{i \in I}, \mu_{ij})$

Definition 1.3.4 (direct limits).

Construction:

Let $C := \bigoplus_{i \in I} M_i$ and $D := A$ -module generate by all $x_i - \mu_{ij}(x_i)$, which is a submodule generate by the relation

$$M_i \ni x_i \sim x_j \in M_j \iff \exists k \in I \text{ s.t. } i \leq k, j \leq k, \mu_{ik}(x_i) = \mu_{jk}(x_j)$$

Then define

$$\varinjlim M_i := C/D$$

is an A -module. We further consider

$$M_i \xrightarrow{\text{injection}} C \xrightarrow{\text{can.}} \varinjlim M_i$$

and define $\mu_i : M_i \rightarrow \varinjlim M_i$, then $\mu_i = \mu_j \circ \mu_{ij}$

Universal Property

For all A -module N with module homomorphism $\alpha_i : M_i \rightarrow N$ s.t. $\alpha_i = \alpha_j \circ \mu_{ij}$ $\forall i \leq j$, then $\exists! \alpha : \varinjlim M_i \rightarrow N$ let the diagram commute.

$$\begin{array}{ccccc}
 & & N & & \\
 & \nearrow \alpha_i & \uparrow \exists! \alpha & \nwarrow \alpha_j & \\
 & \varinjlim M_i & & & \\
 \mu_i \nearrow & & & & \nwarrow \mu_j \\
 M_i & \xrightarrow{\mu_{ij}} & M_j & &
 \end{array} \quad \forall i \leq j$$

Construction of α

Define $\alpha : \varinjlim M_i \rightarrow N$ by

$$\alpha((x_i)_{i \in I} + D) = \sum_{i \in I}^{\text{finite}} \alpha_i(x_i)$$

First, We check that α is well-defined :

If $(x_i)_{i \in I} + D = (y_i)_{i \in I} + D \implies (x_i - y_i)_{i \in I} \in D$. By definition of D and I is directed set, we can find $k \in I$ s.t.

$$\sum_{i \in I}^{\text{finite}} \mu_{ik}(x_i - y_i) = 0$$

Take α_k in both side, then

$$\sum_{i \in I}^{\text{finite}} \alpha_i(x_i - y_i) = 0 \implies \alpha((x_i)_{i \in I} + D) = \alpha((y_i)_{i \in I} + D)$$

Second, we check that $\alpha_i = \alpha \circ \mu_i$: Trivial.

Definition 1.3.5 (inverse system). Let A be a ring, I be a directed set and $(M_i)_{i \in I}$ is a family of A -module. A collection of morphism $\{\pi_{ji}\}$ satisfy

- $\forall i \leq j, \pi_{ji} : M_j \rightarrow M_i$ is A -module homomorphism
- $\pi_{ii} = \text{id}$
- $\pi_{ki} = \pi_{ji} \circ \pi_{kj} \forall i \leq j \leq k$

is called a **inverse system** over I and denote $((M_i)_{i \in I}, \pi_{ij})$

Definition 1.3.6 (inverse limits).

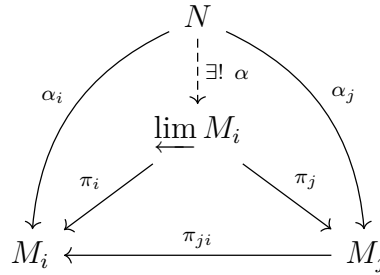
Construction

$$\varprojlim M_i := \left\{ (x_i)_{i \in I} \in \prod_{i \in I} M_i : \forall i \leq j, \pi_{ji}(x_j) = x_i \right\}$$

is an A -module. Define projections $\pi_i : \varprojlim M_i \rightarrow M_i$, then $\pi_i = \pi_{ji} \circ \pi_j \forall i \leq j$

Universal property

For any A -module N and $\alpha_i : N \rightarrow M_i$ with module homomorphism $\alpha_i = \pi_{ji} \circ \alpha_j \forall i \leq j$, then $\exists! \alpha : N \rightarrow \varprojlim M_i$ let the diagram commute.

**Construction α**

Define $\alpha : N \rightarrow \varprojlim M_i$ by

$$\alpha(x) = (\alpha_i(x))_{i \in I}$$

Since $\pi_{ji}(\alpha_j(x)) = \alpha_i(x) \forall i \leq j \implies (\alpha_i(x))_{i \in I} \in \varprojlim M_i$

And it is clear that $\pi_i \circ \alpha = \alpha_i \forall i$

1.3.2 Examples**Ring of p -adic number**

Define

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_i)_{i \in \mathbb{N}} \in \prod_{i=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \forall j \geq i, a_j - a_i \equiv 0 \pmod{p^i} \right\}$$

with

$$\begin{array}{ccc} \pi_{ji} : \mathbb{Z}/p^j\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^i\mathbb{Z} \\ \bar{a} & \longmapsto & \bar{a} \end{array}$$

is called **ring of p -adic number**

Now, consider $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ with $a \mapsto (a_i)_{i \in \mathbb{N}}$, where $a_n = \bar{a} \in \mathbb{Z}/p^n\mathbb{Z}$

- \mathbb{Z}_p is a domain
- $\mathbb{Q}_p := \text{Quot}(\mathbb{Z}_p)$ is a fraction field of \mathbb{Z}_p
- Define a metric d_p on \mathbb{Z}_p :

.. For $x = (x_n)_{n \in \mathbb{N}}, y = (y_n)_{n \in \mathbb{N}}$, define

$$d_p(x, y) = p^{-\max\{i | y_i - x_i \neq 0\}}$$

$$\dots d_p(a, b) = 0 \iff a_n = b_n \forall n \iff a = b$$

$$\dots d_p(a, b) = d_p(b, a)$$

$$\dots d_p(a, c) \leq \max\{d_p(a, b), d_p(b, c)\}$$

.. **Claim:** \mathbb{Z}_p is a completion of \mathbb{Z} under d_p

Given $\{x_n\}$ be a Cauchy sequence in \mathbb{Z}_p , which means $\forall \varepsilon > 0, \exists N \in \mathbb{N}$ s.t.

$$\forall n > m \geq N, d_p(x_n, x_m) < \varepsilon$$

Notice that

$$d_p(x_n, x_m) \leq \max\{d_p(x_n, x_{n-1}), \dots, d_p(x_{m+1}, x_m)\}$$

So we can rewrite the condition :

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \text{ s.t. } \forall n \geq N, d_p(x_{n+1}, x_n) < \varepsilon$$

Choose $\varepsilon = p^{-k}$, then exists $N(k) \in \mathbb{N}$ s.t. $\forall n \geq N, d_p(x_{n+1}, x_n) < p^{-k}$

Let a_n equal to the k -th term of $x_{N(k)}$, then $(x_n) \rightarrow (a_i)_{i \in \mathbb{N}}$. For $i < j$, there exists $x_n \in \{x_n\}$ s.t. x_n and $(a_i)_{i \in \mathbb{N}}$ have same first k -terms, so $(a_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p$

1.3.3 Stalk

Let X, Y be two topological space, for fix $x \in X$. We want to express a set of functions (denoted C_x) which are defined near a point x .

For a open set $U \subseteq X$, define $C(U) := \{f : U \rightarrow Y \text{ is continuous}\}$

$$I := \{U \subseteq X : x \in U\} \text{ with } U \leq V \iff V \subseteq U$$

open

Construct a direct system over $I : \forall u \leq v$

$$\begin{array}{ccc} r_{u,v} : C(u) & \longrightarrow & C(v) \\ f & \longmapsto & f|_v \end{array}$$

Let $C_x := \varinjlim C(u)$

The relation D for $\varphi_u \in C(u), \varphi_v \in C(v)$ is

$$\varphi_u \sim \varphi_v \iff \varphi_u|_w = \varphi_v|_w \text{ for some } w \in u \cap v$$

1.4 Modules over a PID

In this section, R is a PID.

Theorem 1.4.1. Any submodule of R^n is free of rank at most n .

Proof: By induction on n . $n = 1$: Submodule of a ring R is an ideal, say $0 \neq I \subseteq R \rightsquigarrow I = \langle a \rangle_R = Ra$, where $a \neq 0$. Consider $\begin{matrix} R & \longrightarrow & Ra \\ r & \longmapsto & ra \end{matrix}$, since R is integral domain, $ra = 0 \iff r = 0$. Hence, $Ra \simeq R$.

For $n > 1$, let N be a submodule of R^n . Consider the projection

$$P : \begin{matrix} R^n & \longrightarrow & R \\ (x_1, \dots, x_n) & \longmapsto & x_1 \end{matrix}$$

and $\bar{P} : N \rightarrow R$ is the restriction on N .

- Case1. : $\text{Im } \bar{P} = \{0\} \rightsquigarrow N \subseteq \ker P \simeq R^{n-1}$, by induction hypothesis, N is free of rank $\leq n - 1$
- Case2. : $\text{Im } \bar{P} \neq \{0\}$ is an ideal in R , write $\text{Im } \bar{P} = \langle a \rangle$ and $\bar{P}(x) = a$ for some $x \in N$

Claim: $N = \ker \bar{P} \oplus Rx$

$$\bullet \ker \bar{P} \cap Rx = \langle 0 \rangle : 0 = \bar{P}(rx) = r\bar{P}(x) = ra \in R \implies r = 0 \implies rx = 0$$

$$\bullet N = \ker \bar{P} + Rx : \forall y \in N, \bar{P}(y) = ra = \bar{P}(rx) \implies \bar{P}(y - rx) = 0 \implies y - rx \in \ker \bar{P} \implies y \in \ker \bar{P} + Rx$$

Since $N = \ker \bar{P} \oplus Rx$ and

$$\begin{cases} \ker \bar{P} \subseteq \ker P \simeq R^{n-1} \rightsquigarrow \ker \bar{P} \text{ is free of rank } \leq n - 1 \\ rx = 0 \iff 0 = \bar{P}(rx) = ra \in R \rightsquigarrow r = 0 \rightsquigarrow Rx \simeq R \text{ is free of rank } 1 \end{cases}$$

$\implies N$ at most free of rank n .

□

Observation: Let $M = \langle x_1, \dots, x_n \rangle_R$

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker f & \longrightarrow & R^n & \xrightarrow[e_i \mapsto x_i]{f} & M \longrightarrow 0 \\ & & \wr \downarrow & \nearrow T & & & \\ & & R^m & & & & \end{array}$$

$M \simeq R^n / \ker f$ and $(f_1 \ f_2 \ \dots \ f_m) = (e_1 \ e_2 \ \dots \ e_n) A$ for some $A \in M_{n \times m}(R)$, where $\{f_1, \dots, f_m\}$ is a basis for R^m .

Theorem 1.4.2. Let $A \in M_{n \times m}(R)$. Then $\exists P \in \text{GL}_n(R), Q \in \text{GL}_m(R)$ s.t.

$$PAQ = \begin{pmatrix} d_1 & & & & & & 0 \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{pmatrix}$$

with $d_i | d_{i+1}$

Before we prove the theorem, we give some notations.

Notation 1.4.1.

- $P_{ij} = I_n - e_{ii} - e_{jj} + e_{ij} + e_{ji} \rightsquigarrow \begin{cases} P_{ij}M : \text{exchange } i, j\text{-row} \\ MP_{ij} : \text{exchange } i, j\text{-column} \end{cases} \text{ and } P_{ij}^2 = I_n$
- $B_{ij}(a) = I_n + ae_{ij} \rightsquigarrow \begin{cases} B_{ij}(a)M : \text{add } a \text{ times } j\text{-row to } i\text{-row} \\ MB_{ij}(a) : \text{add } a \text{ times } i\text{-column to } j\text{-column} \end{cases} \text{ and } B_{ij}(a)^{-1} = B_{ij}(-a)$
- $D_i(a) = I_n - e_{ii} + ae_{ii} \ (a \neq 0)$

Proof: Define the length $\ell(a)$ of non-unit a to be r if $a = p_1 p_2 \cdots p_r$, p_i : prime (Since $\text{PID} \implies \text{UFD}$) and $\ell(a) = 0$ if a is a unit.

- (1) We may assume $a_{11} \neq 0$ and $\ell(a_{11}) \leq \ell(a_{ij}) \ \forall a_{ij} \neq 0$:

Let a_{st} is non-zero and having min length of $\{a_{ij} : \forall i, j\}$, then exchange 1-row, s -row and 1-column, t -column

- (2) We may assume $\begin{cases} a_{11}|a_{1k} & \forall k = 2, \dots, m \\ a_{11}|a_{k1} & \forall k = 2, \dots, n \end{cases}$:

If $a_{11} \nmid a_{1k}$, then exchange 2-column and k -column, we can assume $a_{11} \nmid a_{12}$. Let $a = a_{11}, b = a_{12}$ and $d = \gcd(a, b)$ i.e. $\langle d \rangle = \langle a, b \rangle \rightsquigarrow d = ax + by$ for some $x, y \in R$ and $\ell(d) < \ell(a)$. Let $a' = \frac{a}{d}, b' = \frac{b}{d}$, notice that

$$\begin{pmatrix} a' & b' \\ y & -x \end{pmatrix} \begin{pmatrix} x & b' \\ y & -a' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which means

$$\begin{pmatrix} x & b' & 0 \\ y & -a' & 0 \\ 0 & 0 & I \end{pmatrix} \text{ is invertible and } \begin{pmatrix} a & b \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x & b' & 0 \\ y & -a' & 0 \\ 0 & 0 & I \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix}$$

If exists a_{k1} s.t. $\ell(a_{k1}) < \ell(a_{11})$, we can do similarly way. We use this algorithm until $a_{11}|a_{1k}, a_{k1} \ \forall k$. Notice that the length of $(1, 1)$ -entry in every step will strictly decrease, after finite number of steps, we have $a_{11}|a_{1k}, a_{k1}$

- (3) After $B_{k1}(-\frac{a_{k1}}{a_{11}})(\)$ and $(\)B_{1k}(-\frac{a_{1k}}{a_{11}}) \ \forall k$, we have

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & \\ \vdots & \vdots & & \\ 0 & & & b_{nm} \end{pmatrix}$$

- (4) We may assume $a_{11}|b_{k\ell} \ \forall k, \ell$

If $a_{11} \nmid b_{k\ell}$, then we add the k -th row to the first row and using (2),(3), then the $(1, 1)$ -entry will strictly decreasing, after finite number of steps, we have $a_{11}|b_{k\ell}$

(5) Apply (1),(2),(3),(4) on $\begin{pmatrix} b_{22} & \cdots & b_{2m} \\ \vdots & & \\ b_{n2} & \cdots & b_{nm} \end{pmatrix}$ to get $\begin{pmatrix} b_{22} & & \\ & c_{ij} & \end{pmatrix}$ with $b_{22}|c_{33}$.

After finite step, we get $a_{11}|a_{22}|\cdots$

□

Remark 1.4.1. d_1, d_2, \dots, d_r are unique up to associates.

Proof: $\Delta_k(A) :=$ the gcd of all **k -th order minors** (Choose k rows and k columns, collect all intersection forms a submatrix and calculate the determinant) of A .

Let $P = (p_{ij})_{n \times m}$. Then

$$PA = \begin{pmatrix} \sum_{j=1}^n p_{1j} (a_{j1} \cdots a_{jm}) \\ \vdots \\ \sum_{j=1}^n p_{nj} (a_{j1} \cdots a_{jm}) \end{pmatrix}$$

and det of k -th order minors of PA is linear combination of some k -th order minor of A . Hence, $\Delta_k(A)|\Delta_k(PA)$. Similarly, $\Delta_k(A)|\Delta_k(AP)$. If $PAQ = B$, then $\Delta_k(A)|\Delta_k(B)$. In other hand, $P^{-1}BQ^{-1} = A$, then $\Delta_k(B)|\Delta_k(A)$, which means $\Delta_k(A) \simeq \Delta_k(B) = d_1 d_2 \cdots d_k$. Hence, $d_k \simeq \Delta_k(A)/\Delta_{k-1}(A)$ □

Goal: Let $M = \langle x_1, \dots, x_n \rangle_R \implies$

$$\begin{array}{ccccccc} 0 & \longrightarrow & R^m & \xrightarrow{T} & R^n & \xrightarrow{f} & M \longrightarrow 0 \\ & & f_i & & e_i & \longmapsto & x_i \end{array}$$

Recall: If $T(f_i) = \sum_{j=1}^n a_{ji} e_j$, then

$$(f_1 \cdots f_m) = (e_1 \cdots e_n) (a_{ij}) \implies A := (a_{ij}) = [T]_{\{f_i\}}^{\{e_i\}}$$

and

$$T\left(\sum_{i=1}^m x_i f_i\right) = \sum_{i=1}^m x_i T(f_i) = \sum_{i=1}^m \sum_{j=1}^n a_{ji} e_j = \sum_{j=1}^n \underbrace{\left(\sum_{i=1}^m x_i a_{ji}\right)}_{y_j} e_j \implies \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

By Theorem 1.4.2, $\exists P \in \text{GL}_n(R), Q \in \text{GL}_m(R)$ s.t.

$$PAQ = \begin{pmatrix} d_1 & & & & O \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ O & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \text{ with } d_i | d_{i+1} \forall i$$

Note $\because T$ is $1 - 1 \therefore m = \dim \text{Im } T = \text{rank } A = r$. Let

$$\begin{cases} \{u_1, \dots, u_m\} \text{ be a basis for } R^m \text{ s.t. } (u_1 \cdots u_m) = (f_1 \cdots f_m)Q & \rightsquigarrow Q = [\text{id}_{R^m}]_{\{u_i\}}^{\{f_i\}} \\ \{w_1, \dots, w_n\} \text{ be a basis for } R^n \text{ s.t. } (w_1 \cdots w_n) = (e_1 \cdots e_n)P^{-1} & \rightsquigarrow P = [\text{id}_{R^n}]_{\{e_i\}}^{\{w_i\}} \end{cases}$$

Hence, $B = PAQ = [T]_{\{u_i\}}^{\{w_i\}} \implies T(u_i) = d_i w_i \forall i = 1 \sim m$. So

$$M \simeq \bigoplus_{i=1}^n R w_i / \bigoplus_{i=1}^m R d_i w_i \simeq \left(\bigoplus_{i=1}^m R w_i / R d_i w_i \right) \oplus \left(\bigoplus_{i=m+1}^n R w_i \right)$$

Note that $R w_i \simeq R$, since R is integral domain. Consider

$$\begin{array}{ccccc} \varphi: & R & \rightarrow & R w_i & \rightarrow & R w_i / R d_i w_i \\ & r & \mapsto & r w_i & \mapsto & \overline{r w_i} \end{array}$$

$r \in \ker \varphi \iff r w_i = r' d_i w_i \iff r = r' d_i$, thus $\ker \varphi = \langle d_i \rangle$ and $R w_i / R d_i w_i \simeq R / \langle d_i \rangle$. Hence, $M \simeq R / \langle d_1 \rangle \oplus \cdots \oplus R / \langle d_m \rangle \oplus R^{n-m}$. If d_i is a unit, then $\langle d_i \rangle = R \rightsquigarrow R / \langle d_i \rangle \simeq \langle 0 \rangle$. Assume that d_1, d_2, \dots, d_k are units and d_{k+1}, \dots, d_m are not units, rewrite $d_{k+1} = a_1, \dots, d_m = a_\ell$. Then

$$M \simeq R / \langle a_1 \rangle \oplus \cdots \oplus R / \langle a_\ell \rangle \oplus R^{n-m}$$

Conclusion:

Theorem 1.4.3. M is finite generated over a PID R , then

$$M \simeq R / \langle a_1 \rangle \oplus \cdots \oplus R / \langle a_\ell \rangle \oplus R^s$$

with a_i are non-unit and $a_i | a_{i+1}$.

Remark 1.4.2. In later section, we will prove that s is unique (then we called s is **rank** of M) and a_i are unique up to associate (we call a_i are **invariant factors**).

Observation: If M is finite generated over a PID, then $M \simeq R / \langle a_1 \rangle \oplus \cdots$, say $z \longleftrightarrow \bar{1} \in R / \langle a_1 \rangle$, then $a_1 z \longleftrightarrow a_1 \bar{1} = \overline{a_1} = \bar{0} \in R / \langle a_1 \rangle$, which means $a_1 z = 0$. Then it is naturally to research the property of $az = 0$.

Definition 1.4.1. Let M be a R -module

- $\text{ann}(z) := \{r \in R : rz = 0\}$ is a left ideal of R is called **annihilate** of z .
- z is called a **torsion element** if $\text{ann}(z) \neq \langle 0 \rangle$
- $\text{Tor}(M) = \{\text{torsion elements of } M\}$
- R is integral domain $\rightsquigarrow \text{Tor}(M)$ is a submodule of M (is called **torsion submodule** of M)
- If $r_1 z_1 = r_2 z_2 = 0$ with $r_1, r_2 \neq 0 \implies r_1 r_2 \neq 0, (r_1 r_2)(z_1 + z_2) = r_2 r_1 z_1 + 0 = 0$ and $\forall 0 \neq a \in R, ar_1 \neq 0$ and $r_1(az_1) = a(r_1 z_1) = 0$
- M is a **torsion module** if $\text{Tor}(M) = M$
- M is torsion free if $\text{Tor}(M) = \langle 0 \rangle$

(If M is finite generated over a PID, then $M = \text{Tor}(M) \oplus R^s$ and $M / \text{Tor}(M) \simeq R^s$ is free)

1.5 Structure theorem for finite generated PID-modules and applications

In this section, R is a PID and thus is a UFD.

1.5.1 Structure theorem for finite generated PID-module

Although we had proved the existence of Structure theorem, but we hadn't proved the uniqueness. We will prove it in this section.

Definition 1.5.1. Let p be a prime element in R .

- $M(p) := \{x \in M : p^k x = 0 \text{ for some } k \in \mathbb{N}\}$ is called **p -component**
- $M^{(1)}(p) := \{x \in M : px = 0\}$

Observation: $M^{(1)}(p)$ is a $R/\langle p \rangle$ -module. Note $\because R$ is a PID $\therefore \langle p \rangle$ is a prime ideal $\rightsquigarrow \langle p \rangle$ is a maximal ideal $\rightsquigarrow R/\langle p \rangle$ is a field $\rightsquigarrow M^{(1)}(p)$ is a $R/\langle p \rangle$ -vector space. Let $F = R/\langle p \rangle$

- If $N \simeq R/\langle d \rangle$ with $p|d$. Write $N = Ru$ with $\text{ann}(u) = \langle d \rangle$ and $d = pq$

•• $N^{(1)}(p) \simeq F :$

••• $N^{(1)}(p) = \langle q \rangle / \langle d \rangle :$

Since $r \in N^{(1)}(p) \rightsquigarrow rp = \bar{0}$ in $R/\langle d \rangle \rightsquigarrow rp = r'd = r'pq \rightsquigarrow r = r'q$

••• $\langle q \rangle / \langle d \rangle \simeq Rq/Rd \simeq R/\langle p \rangle :$ Consider

$$\begin{array}{ccccc} \varphi : R & \longrightarrow & Rq & \longrightarrow & Rq/Rd \\ r & \longmapsto & rq & \longmapsto & \overline{rq} \end{array}$$

$r \in \ker \varphi \iff rq = r'd \iff r = r'p$. Thus, $\ker \varphi = \langle p \rangle$

•• $pN = p \cdot R/\langle d \rangle \simeq (\langle p \rangle + \langle d \rangle) / \langle d \rangle \simeq \langle \gcd(p, d) \rangle / \langle d \rangle \simeq \langle p \rangle / \langle d \rangle \simeq R/\langle p \rangle \simeq Rq/Rpq \simeq R/\langle q \rangle$ (Recall that $I \cdot R/J \simeq (I + J)/J$)

•• $N/pN \simeq (R/\langle d \rangle) / (\langle p \rangle / \langle d \rangle) \simeq R/\langle p \rangle = F$

- If $N \simeq R/\langle d_1 \rangle \oplus R/\langle d_2 \rangle \oplus \cdots \oplus R/\langle d_\ell \rangle$ with $p|d_i \forall i = 1 \sim \ell$, then

•• $N^{(1)}(p) \simeq \bigoplus_{i=1}^{\ell} (R/\langle d_i \rangle)^{(1)}(p) \simeq F^\ell$

••

$$N/pN \simeq \left(\bigoplus_{i=1}^{\ell} R/\langle d_i \rangle \right) / \left(\bigoplus_{i=1}^{\ell} \langle p \rangle / \langle d_i \rangle \right) \simeq F^\ell$$

Theorem 1.5.1 (Structure theorem). R is a PID and M is a finite generated R -module. Then

$$M \simeq R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_\ell \rangle \oplus R^s \quad (*)$$

where a_i are non-zero and non-unit. Also, s is unique (which is called **rank** of M) and a_1, \dots, a_ℓ (called **invariant factor**) are unique up to associates. The form in $(*)$ is called **invariant factor form**.

Proof: Existence: done!

Uniqueness: Assume that

$$M \simeq R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_\ell \rangle \oplus R^s \simeq R/\langle b_1 \rangle \oplus \cdots \oplus R/\langle b_k \rangle \oplus R^t$$

with $a_i | a_{i+1}, b_i | b_{i+1}$

- $M/\text{Tor}(M) \simeq R^s \simeq R^t \implies s = t$
- $\text{Tor}(M) \simeq R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_\ell \rangle \simeq R/\langle b_1 \rangle \oplus \cdots \oplus R/\langle b_k \rangle$
- If $\text{Tor}(M) \ni x \longleftrightarrow x_1^{\in R/\langle a_1 \rangle} + \cdots + x_\ell$, then $x \in \text{Tor}(M)^{(1)}(p) \iff px_i = 0 \forall i$
 $\iff px_i \in \langle a_i \rangle \iff px_i = r_i a_i \rightsquigarrow p | r_i a_i \rightsquigarrow \begin{cases} p | r_i \rightsquigarrow a_i | x_i \rightsquigarrow x_i = 0 \text{ in } R/\langle a_i \rangle \\ p | a_i \end{cases}$
 Hence, $M^{(1)}(p) \simeq F^\mu$, where μ is the number of the $R/\langle a_i \rangle$ s.t. $p | a_i$
- $\forall p | a_1 \rightsquigarrow p | a_i \forall i = 1 \sim \ell \rightsquigarrow \dim_F M^{(1)}(p) = \ell$. Similarly, we can conclude that p must divide exactly ℓ elements b_j , so $\ell \leq k$. By symmetric, $k \leq \ell \implies k = \ell$.
- Moreover, we get that $\begin{cases} p | a_1 \rightsquigarrow p | b_1 \\ p | b_1 \rightsquigarrow p | a_1 \end{cases} \rightsquigarrow a_1, b_1 \text{ share the same prime divisor } p_1, \dots, p_\mu$. Write $a = up_1^{\alpha_1} \cdots p_\mu^{\alpha_\mu}$, $b_1 = vp_1^{\beta_1} \cdots p_\mu^{\beta_\mu}$. Assume $\alpha_1 < \beta_1$. Then

$$p_1^{\alpha_1} \text{Tor}(M) \simeq R/\langle q_1 \rangle \oplus \cdots \oplus R/\langle q_\ell \rangle \simeq R/\langle h_1 \rangle \oplus \cdots \oplus R/\langle h_\ell \rangle$$

where $q_i = a_i/p_1^{\alpha_1}, h_i = b_i/p_1^{\alpha_1}$ and $p \nmid q_1, p | h_1$ ($\rightarrow \leftarrow$)

So $\alpha_1 = \beta_1$. Similarly, $\alpha_i = \beta_i \rightsquigarrow a_i \sim b_i$

$$a_1 \text{Tor}(M) \simeq R/\langle a_2/a_1 \rangle \oplus \cdots \oplus R/\langle a_\ell/a_1 \rangle \simeq R/\langle b_2/b_1 \rangle \oplus \cdots \oplus R/\langle b_\ell/b_1 \rangle$$

By induction hypothesis, $a_i/a_1 \sim b_i/b_1 \forall i = 2, \dots, \ell \implies a_i \simeq b_i$

□

Property 1.5.1 (Elementary divisor form). Write $a_i = u_i p_1^{\alpha_{i1}} \cdots p_\mu^{\alpha_{i\mu}}$ with u_i : units, p_j : distinct prime and $0 \leq \alpha_{ik} \leq \alpha_{jk} \forall i < j$. By Chinese Remainder theorem,

$$\text{Tor}(M) \simeq \bigoplus_{i=1}^{\ell} \bigoplus_{j=1}^{\mu} R/\langle p_j^{\alpha_{ij}} \rangle \simeq \bigoplus_{j=1}^{\mu} \underbrace{\bigoplus_{i=1}^{\ell} R/\langle p_j^{\alpha_{ij}} \rangle}_{=M^{(1)}(p_j)}$$

1.5.2 Applications

1. finite generated abelian groups

finite generated abelian group \rightsquigarrow f.g. \mathbb{Z} -module \rightsquigarrow fundamental theorem of f.g. abelian group

Property 1.5.2. Let V be a n -dim vector space over k and $T \in \text{Hom}_k(V, V)$. Then V is a torsion $k[x]$ -module

Proof: Let $Z = Z(v; T)$ is T -cycle space generate by v is a subspace of V . Thus Z is finite dimensional vector space. Let $k = \dim Z$, then $\{v, xv, \dots, x^{k-1}v\}$ form a basis for $Z \implies x^k v + a_{k-1}x^{k-1}v + \dots + a_1 xv + v = 0$ for some $a_i \in k$. Hence, $v \in \text{Tor}(V)$ \square

Now, fix a basis $\{v_1, \dots, v_n\}$ for V over $k \rightsquigarrow V = \langle v_1, \dots, v_n \rangle_k = \langle x_1, \dots, x_n \rangle_{k[x]}$. Write $[T]_{\{v_i\}}^{\{v_i\}} = (c_{ij}) \implies T(v_i) = \sum_{j=1}^n c_{ji} v_j$ and consider

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker \varphi & \longrightarrow & k[x]^n & \xrightarrow{\varphi} & V \longrightarrow 0 \\ & & & & e_i & \longmapsto & v_i \end{array}$$

Property 1.5.3. $S := \left\{ f_i := xe_i - \sum_{j=1}^n c_{ji} e_j \mid i = 1, \dots, n \right\}$ forms a basis for $\ker \varphi$ over $k[x]$

Proof:

- $S \subset \ker \varphi : \varphi(f_i) = xv_i - \sum_{j=1}^n c_{ji} v_j = T(v_i) - T(v_i) = 0$
- S is linearly independent set over $k[x] : \text{If } \sum_{i=1}^n h_i(x) f_i = 0 \rightsquigarrow \sum_{i=1}^n h_i(x) x e_i = \sum_{i=1}^n \sum_{j=1}^n c_{ji} h_j(x) e_j \rightsquigarrow h_j(x) x = \sum_{i=1}^n c_{ji} h_j(x)$. If exists $h_j(x) \neq 0$ having max degree $\ell > 0 \rightsquigarrow \ell + 1 = \deg(h_j(x)x) = \deg(\sum_{i=1}^n c_{ji} h_j(x)) > \ell \ (\rightarrow \leftarrow)$
- $\ker \varphi \subseteq \langle S \rangle : xe_i = f_i + \sum_{j=1}^n c_{ji} h_j(x)$. For given $G \in k[x]^n$, write $G = \sum_{i=1}^n g_i(x) e_i$, then we can rewrite $G = \sum_{i=1}^n h_i f_i + \sum_{i=1}^n b_i e_i$. If $G \in \ker \varphi \rightsquigarrow \sum_{i=1}^n b_i e_i \in \ker \varphi \rightsquigarrow \sum_{i=1}^n b_i v_i = 0$. Which means $b_i = 0 \ \forall i = 1, \dots, n \implies G \in \langle S \rangle$.

\square

2. Rational canonical form of T

Let $\begin{array}{ccc} \ker \varphi & \xrightarrow{L} & k[x]^n \\ \{f_i\} & \longmapsto & \{e_i\} \end{array}$ and

$$[L]_{\{f_i\}}^{\{e_i\}} = \begin{pmatrix} x - c_{11} & -c_{12} & \cdots & -c_{1n} \\ -c_{21} & x - c_{22} & & \\ \cdots & & \ddots & \\ -c_{n1} & & & x - c_{nn} \end{pmatrix} =: A \in M_{n \times n}(k[x])$$

$\rightsquigarrow \exists P, Q \in \text{GL}_n(k[x])$ s.t.

$$PAQ = \begin{pmatrix} 1 & & & & O \\ & \ddots & & & \\ & & 1 & & \\ & & & d_1(x) & \\ O & & & & \ddots & \\ & & & & & d_r(x) \end{pmatrix} =: \text{diag}\{1, \dots, 1, d_1(x), \dots, d_r(x)\}$$

with $d_i(x) \mid d_{i+1}(x) \forall i = 1, \dots, r-1$, d_i : monic

$$\implies V \simeq k[x]/\langle d_1(x) \rangle \oplus \dots \oplus k[x]/\langle d_r(x) \rangle$$

Write $V \simeq V_1 \oplus \dots \oplus V_r$ and $k[x]/\langle d_i(x) \rangle \simeq V_i = k[x]v_i$. $\deg d_i = m_i \rightsquigarrow \dim V_i = m_i$

$$\begin{aligned} k[x]/\langle d_i(x) \rangle = k[x]\bar{1} &\longleftrightarrow k[x]v_i = V_i \\ \langle 1, x, \dots, x^{m_i-1} \rangle_k &\longleftrightarrow \langle v_i, xv_i, \dots, x^{m_i-1}v_i \rangle_k =: \beta_i \end{aligned}$$

Write $d_i(x) = x^{m_i} - b_{i,m_i-1}x^{m_i-1} - \dots - b_{i,1}x - b_{i,0}$

$$\implies [T|_{V_i}]_{\beta_i} = \begin{pmatrix} 0 & & & b_{i,0} \\ 1 & 0 & & b_{i,1} \\ & 1 & \ddots & \vdots \\ & & \ddots & 0 \\ & & & 1 & b_{i,m_i} \end{pmatrix}$$

Let $\beta = \bigsqcup_{i=1}^r \beta_i$, then

$$[T]_{\beta} = \begin{pmatrix} [T|_{V_1}]_{\beta_1} & & & \\ & [T|_{V_2}]_{\beta_2} & & \\ & & \ddots & \\ & & & [T|_{V_r}]_{\beta_r} \end{pmatrix}$$

Observation: $\det P \det A \det Q = d_1(x)d_2(x) \dots d_r(x)$. Since $\det P \det P^{-1} = \det Q \det Q^{-1} = 1 \rightsquigarrow \det P, \det Q$ are units $\rightsquigarrow \det P, \det Q \in R$ and thus $\det A =$

$ch_T(x) = d_1(x)d_2(x) \dots d_r(x)$. $\begin{cases} d_i(x)v_i = 0 \\ d_i \mid d_r \end{cases} \rightsquigarrow d_r(x)v_i = 0 \forall i = 1, \dots, r$ and thus

$d_r(T)v_i = 0$. For all $v \in V$, write $v = \sum_{i=1}^r g_i(x)v_i \rightsquigarrow d_r(x)v = \sum_{i=1}^r g_i(x)d_r(x)v_i = 0$.

Hence, $d_r(T) = 0 \implies ch_T(T) = 0$. Let $m_T(x)$ be the minimal polynomial of T , then $m_T \mid d_r$. Consider $(1, 1, \dots, 1) \leftrightarrow v$. Since $m_T(x)v = 0 \implies m_T(x)1 = 0$ in $R/\langle d_r \rangle \implies d_r \mid m_T$. Hence, $d_r = m_T$

Jordan canonical form of T

Assume V is a vector space over an algebraic closed field k . Consider the elementary divisor form of V

$$V \simeq \left(k[x] / \langle (x - \lambda)^{\alpha_{11}} \rangle \oplus \cdots \oplus k[x] / \langle (x - \lambda)^{\alpha_{\ell_1 1}} \rangle \right) \oplus \cdots \oplus \left(\cdots \right)$$

Let $\lambda = \lambda_i, \alpha = \alpha_{ji}, W \simeq k[x] / \langle (x - \lambda)^\alpha \rangle$, let $W = k[x]w$ with $\text{ann}(w) = \langle (x - \lambda)^\alpha \rangle$. Then $\beta = \{w, (x - \lambda)w, \dots, (x - \lambda)^{\alpha-1}w\}$ forms a basis for W over k . Then

$$[T|_W] = \begin{pmatrix} \lambda & & & O \\ 1 & \lambda & & \\ & 1 & \ddots & \\ O & & \lambda & \\ & & 1 & \lambda \end{pmatrix}$$

1.6 Tensor product

Definition 1.6.1. Let M be a right A -module and N be a left A -module

- Let G be an additive abelian group. An **A -biadditive** function is a function $f : M \times N \rightarrow G$ s.t.
 - $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$
 - $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$
 - $f(xa, y) = f(x, ay)$
- A **tensor product** of M and N is an abelian group $M \otimes_A N$ with an A -biadditive function $h : M \times N \rightarrow M \otimes_A N$ s.t. \forall abelian group G and $\forall A$ -biadditive function $f : M \times N \rightarrow G, \exists ! \mathbb{Z}$ -module homo. \tilde{f} let the diagram commute

$$\begin{array}{ccc} M \otimes_A N & \xrightarrow{\tilde{f}} & G \\ h \uparrow & \nearrow f & \\ M \times N & & \end{array}$$

Theorem 1.6.1. $M \otimes_A N$ exists and is unique up to isomorphism

Proof:

- Let F be the free abelian group on $M \times N$ i.e. $F = \coprod_{(x,y) \in M \times N} \mathbb{Z}(x, y)$
- Since we want to obtain the new structure, we consider an ideal I of F

$$I = \left\langle \begin{array}{l} (x_1 + x_2, y) - (x_1, y) - (x_2, y) \\ (x, y_1 + y_2) - (x, y_1) - (x, y_2) \\ (x, ay) - (x, a) \end{array} \middle| \begin{array}{l} x_1, x_2, x \in M \\ y_1, y_2, y \in N \\ a \in A \end{array} \right\rangle_{\mathbb{Z}}$$

and define $M \otimes_A N := F/I$. We denote the coset $(x, y) + I$ by $x \otimes y$.

- Define $h : M \times N \longrightarrow M \otimes_A N$ which is biadditive
 $(x, y) \longmapsto x \otimes y$
 - $(x_1 + x_2) \otimes y = (x_1 + x_2, y) + I = (x_1, y) + I + (x_2, y) + I = x_1 \otimes y + x_2 \otimes y$
 - $x \otimes (y_1 + y_2) = (x, y_1 + y_2) + I = (x, y_1) + I + (x, y_2) + I = x \otimes y_1 + x \otimes y_2$
 - $(xa) \otimes y = (xa, y) + I = (x, ay) + I = x \otimes (ay)$
- universal property :

$$\begin{array}{ccccc}
 M \times N & \longrightarrow & F & \twoheadrightarrow & F/I \\
 & \searrow f & \downarrow \exists f_1 & \nearrow \exists \tilde{f} & \\
 & & G & &
 \end{array}$$

By universal property of free module, $\exists!$ module homomorphism $f_1 : F \rightarrow G$ s.t. left diagram commute. It is clear that $I \subseteq \ker f_1$, by factor theorem (universal property of quotient), $\exists \mathbb{Z}$ -module $\tilde{f} : F/I \rightarrow G$

□

Remark 1.6.1.

- This yields

$$\{A\text{-biadditive functions } M \times N \rightarrow G\} \longleftrightarrow \{\mathbb{Z}\text{-module homo. } M \otimes_A N \rightarrow G\}$$

- Can we define left A -left A ? NO!

$$(a_1 a_2)x \otimes y = a_1(a_2 x) \otimes y = a_2 x \otimes a_1 y = x \otimes a_2 a_1 y. \text{ We need } A \text{ commutative.}$$

- Is $M \otimes_A N$ is an A -module ? NO!

Define $a(x \otimes y) = xa \otimes y = x \otimes ay$, then

$$(a_1 a_2)(x \otimes y) = a_1(a_2(x \otimes y)) = a_1(xa_2 \otimes y) = xa_2 \otimes a_1 y = x \otimes a_2 a_1 y$$

Theorem 1.6.2. Let M be a B - A bimodule and N be a left A -module. Then $M \otimes_A N$ is a left B module.

Proof: For fixed $b \in B$, define $\rho_b : M \longrightarrow M$
 $x \longmapsto bx$ is a right A -module homo.
 $\rho_b(xa) = b(xa) = (bx)a = \rho_b(x)a$ and

$$\begin{array}{ccc}
 \rho_b \otimes_A 1_N : M \otimes_A N & \longrightarrow & M \otimes_A N \\
 x \otimes_A y & \longmapsto & \rho_b(x) \otimes_A y
 \end{array}$$

is a group homo. (by the following property), then \exists a ring homo.

$$\begin{array}{ccc}
 f : B & \longrightarrow & \text{End } M \otimes_A N \\
 b & \longmapsto & \rho_b \otimes_A 1_N
 \end{array}$$

□

Property 1.6.1. $g : M \rightarrow M'$ is a right A -module homo., $h : N \rightarrow N'$ is a left A -module homo., then

$$\begin{aligned} g \otimes_A h : M \otimes_A N &\longrightarrow M' \otimes_A N' \\ x \otimes y &\longmapsto g(x) \otimes h(y) \end{aligned}$$

is a group homomorphism.

Proof: We only need to proof that

$$\begin{aligned} f; M \times N &\longrightarrow M' \otimes_A N' \\ (x, y) &\longmapsto g(x) \otimes h(y) \end{aligned}$$

is an A -biadditive. Which is trivial. \square

Corollary 1.6.1. R : commutative $\implies M \otimes_R N$: R -module

Definition 1.6.2. R : commutative and M, N, L : R -modules. $\varphi : M \times N \rightarrow L$ is **R -bilinear** if it is biadditive and $r\varphi(x, y) = \varphi(rx, y) = \varphi(x, ry)$

Then we have

$$\{R\text{-bilinear maps } M \times N \rightarrow L\} \longleftrightarrow \{R\text{-module homo. } M \otimes_R N \rightarrow L\}$$

Corollary 1.6.2. Let $f : A \rightarrow B$ be a ring homo.. Then B is an A -module and for M : left A -module, $B \otimes_A M$ is a left B -module

$$B \text{ is left } A\text{-module} : \begin{pmatrix} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & f(a)b \end{pmatrix}$$

$$B \text{ is right } A\text{-module} : \begin{pmatrix} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & bf(a) \end{pmatrix}$$

Example 1.6.1.

$$\bullet \mathbb{Z} \hookrightarrow \mathbb{Q}, \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0 \quad (\because q \otimes \bar{a} = \frac{q}{n} \cdot n \otimes \bar{a} = \frac{q}{n} \otimes n\bar{a} = \frac{q}{n} \otimes 0 = 0)$$

$$\bullet \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\gcd(m, n)\mathbb{Z} \text{ (let } d = \gcd(m, n)\text{)}$$

$$\bullet \bar{a} \otimes \bar{b} = ab(\bar{1} \otimes \bar{1}) \rightsquigarrow \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \otimes \bar{1} \rangle_{\mathbb{Z}}$$

$$\bullet m(\bar{1} \otimes \bar{1}) = \bar{0} \otimes \bar{1} = 0, n(\bar{1} \otimes \bar{1}) = \bar{1} \otimes \bar{0} = 0 \rightsquigarrow o(\bar{1} \otimes \bar{1}) | d$$

$$\bullet \begin{matrix} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/d\mathbb{Z} \\ (\bar{a}, \bar{b}) & \longmapsto & \bar{ab} \end{matrix} \text{ is } \mathbb{Z}\text{-bilinear} \rightsquigarrow \exists! \mathbb{Z}\text{-module homo.}$$

$$\begin{matrix} \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/d\mathbb{Z} \\ \bar{1} \otimes \bar{1} & \longmapsto & \bar{1} \end{matrix} \rightsquigarrow d | o(\bar{1} \otimes \bar{1})$$

Theorem 1.6.3. M, M' : right A -module, N : left A -module. Then

$$(M \oplus M') \otimes_A N \simeq (M \otimes_A N) \oplus (M' \otimes_A N)$$

Proof:

$$\begin{aligned} (M \oplus M') \times N &\longrightarrow (M \otimes_A N) \oplus (M' \otimes N) \text{ is } A\text{-biadditive} \\ ((x, x'), y) &\longmapsto (x \otimes y, x' \otimes y) \end{aligned}$$

$$\begin{aligned} \implies \exists! f : (M \oplus M') \otimes_A N &\longrightarrow (M \otimes_A N) \oplus (M' \otimes_A N) \\ (x, x') \otimes y &\longmapsto (x \otimes y, x' \otimes y) \end{aligned}$$

Conversely,

$$\begin{aligned} M \times N &\longrightarrow (M \oplus N) \otimes N \text{ is } A\text{-biadditive} \\ (x, y) &\longmapsto (x, 0) \otimes y \end{aligned}$$

$$\begin{aligned} \implies M \otimes_A N &\xrightarrow{\text{homo.}} (M \oplus M') \otimes N \\ x \otimes y &\longmapsto (x, 0) \otimes y \end{aligned}$$

Similarly,

$$\begin{aligned} \implies M' \otimes_A N &\xrightarrow{\text{homo.}} (M \oplus M') \otimes N \\ x' \otimes y &\longmapsto (0, x') \otimes y \end{aligned}$$

By universal property of direct sum,

$$\begin{aligned} \exists! g : (M \otimes_A N) \oplus (M' \otimes_A N) &\xrightarrow{\text{homo.}} (M \oplus M') \otimes_A N \\ (x \otimes y, x' \otimes y') &\longmapsto (x, 0) \otimes y + (0, x') \otimes y' \end{aligned}$$

Then we can check $f \circ g, g \circ f$ are identity. □

Theorem 1.6.4. $I \subseteq A, N$: left A -module. Then $A/I \otimes_A N \simeq N/IN$

Proof: Since $\begin{aligned} A/I \times N &\longrightarrow N/IN \\ (\bar{a}, \bar{x}) &\longmapsto \bar{a}\bar{x} \end{aligned}$ is A -biadditive

$$\begin{aligned} f : A/I \otimes N &\longrightarrow N/IN \\ \bar{a} \otimes x &\longmapsto \bar{a}\bar{x} \end{aligned}$$

Conversely, $\begin{aligned} g : N/IN &\longrightarrow A/I \otimes N \\ \bar{x} &\longmapsto \bar{1} \otimes x \end{aligned}$

• Well-defined : $x - x' \in IN$, say $x - x' = \sum a_i n_i$, then

$$\bar{1} \otimes (x - x') = \bar{1} \otimes \sum a_i n_i = \sum \bar{1} \otimes a_i n_i = \sum \bar{a}_i \otimes n_i = 0$$

• $g \circ f(\bar{a} \otimes x) = g(\bar{a}\bar{x}) = \bar{1} \otimes ax = \bar{a} \otimes x$

• $f \circ g(\bar{x}) = f(\bar{1} \otimes x) = \bar{x}$

Hence, $A/I \otimes_A N \simeq IN/N$. □

Remark 1.6.2. $A \otimes_A N \simeq N$.

1.7 Symmetric algebra

Let R be a commutative ring and M be a f.g. R -module. Note that in homework 5, we will prove $(M_1 \otimes M_2) \otimes M_3 = M_1 \otimes (M_2 \otimes M_3)$. So we can define

$$T^i(M) := \underbrace{M \otimes \cdots \otimes M}_{i \text{ times}} \text{ is a } R\text{-module, } T^0(M) := R$$

$$T(M) := R \oplus T^1(M) \oplus \cdots = \bigoplus_{k=0}^{\infty} T^k(M)$$

- $T(M)$ is a R -algebra, multiplication is defined by :

$$\underbrace{(x_1 \otimes \cdots \otimes x_i)}_{\in T^i(M)} \underbrace{(y_1 \otimes \cdots \otimes y_j)}_{\in T^j(M)} = x_1 \otimes \cdots \otimes x_i \otimes y_1 \otimes \cdots \otimes y_j \in T^{i+j}(M)$$

- universal property for $T(M)$: If A is any R -algebra and $\varphi : M \rightarrow A$ is an R -module homo., then $\exists! \tilde{\varphi} : T(M) \rightarrow A$ is an R -alg. homo.:

Define

$$\begin{aligned} f_k : M \times \cdots \times M &\longrightarrow A \\ (x_1, \dots, x_k) &\longmapsto \varphi(x_1)\varphi(x_2)\cdots\varphi(x_k) \end{aligned}$$

is a R -multilinear $\rightsquigarrow \exists! \tilde{f}_k : M \otimes \cdots \otimes M \rightarrow A$ is R -module homo.

By universal property of direct sum :

$$\begin{array}{ccc} \exists! \tilde{\varphi} : T(M) & \xrightarrow{\text{R-module homo.}} & A \\ & \nwarrow \rho_k \quad \nearrow \tilde{f}_k & \\ & T^k(M) & \end{array}$$

Also,

$$\begin{aligned} \tilde{\varphi}((x_1 \otimes \cdots \otimes x_i)(y_1 \otimes \cdots \otimes y_j)) &= \varphi(x_1)\cdots\varphi(x_i)\varphi(y_1)\cdots\varphi(y_j) \\ &= \tilde{\varphi}(x_1 \otimes \cdots \otimes x_i)\tilde{\varphi}(y_1 \otimes \cdots \otimes y_j) \end{aligned}$$

\implies The ring $T(M)$ is called the **tensor algebra** of M and the ring $R = \bigoplus_{k=1}^{\infty} M_i$ satisfy $M_i M_j \subseteq M_{i+j}$ is called **graded ring**.

Definition 1.7.1.

- $C(M)$ is the **graded ideal** generated by $x_1 \otimes x_2 - x_2 \otimes x_1 \in T^2(M) \forall x_1, x_2 \in M$ in $T(M)$
- $S(M) = T(M)/C(M)$ is called **symmetric algebraic** and

$$S(M) = T(M)/C(M) \simeq \bigoplus_{k=1}^{\infty} T^k(M)/C^k(M), \text{ where } C^k(M) = C(M) \cap T^k(M)$$

- $C^k(M) = \langle x_1 \otimes \cdots \otimes x_k - x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(k)} : \forall x_i \in M, \sigma \in S_n \rangle$
 eg. $x_1 \otimes x_2 \otimes x_3 - x_3 \otimes x_2 \otimes x_1 = x_1 \otimes (x_2 \otimes x_3 - x_3 \otimes x_2) + (x_1 \otimes x_3 - x_3 \otimes x_1) \otimes x_2$
 $\rightsquigarrow S^k(M) = \langle \overline{x_1} \otimes \cdots \otimes \overline{x_k} : x_i \in M \rangle$
- The universal property for $S(M)$: For any commutative R -alg A and $\varphi : M \rightarrow A$ is R -module homo. $\exists!$ $\tilde{\varphi}$ s.t.

$$\begin{array}{ccc}
 S(M) & \xrightarrow{\tilde{\varphi}} & A \\
 \uparrow & \swarrow \varphi & \nearrow \varphi \\
 T(M) & \leftarrow & M
 \end{array}$$

(We can consider the universal property of direct sum and quotient to get $\tilde{\varphi}$)

1.8 Modules of fractions

Let R be a commutative ring and $S \neq 0$ is multiplicatively closed in R . M be a R -module.

1.8.1 Definition and some property

Definition 1.8.1. $M_s := \{(x, t) | x \in M, t \in S\} / \sim$, where \sim is defined by

$$(x_1, t_1) \sim (x_2, t_2) \iff \exists u \in S \text{ s.t. } u(t_2x_1 - t_1x_2) = 0$$

- \sim is an equivalence relation
- $\frac{x}{t}$ = the equivalence class of (x, t)
- M_s is an R_s -module $\left(\frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}\right)$
- $f : M \rightarrow N$ is an R -module homo. \rightsquigarrow

$$\begin{array}{ccc}
 f_s : M_s & \rightarrow & N_s \\
 \frac{x}{t} & \mapsto & \frac{f(x)}{t}
 \end{array}$$

Well-defined :

$$\frac{x_1}{t_1} = \frac{x_2}{t_2} \rightsquigarrow \exists u \in S, ut_2x_1 = ut_1x_2 \rightsquigarrow ut_2f(x_1) = ut_1f(x_2) \rightsquigarrow \frac{f(x_1)}{t_1} = \frac{f(x_2)}{t_2}$$

Property 1.8.1. If $0 \rightarrow M \xrightarrow{f} N \xrightarrow{g} L \rightarrow 0$ is exact for R -modules, then $0 \rightarrow M_s \xrightarrow{f_s} N_s \xrightarrow{g_s} L_s \rightarrow 0$ is again exact. Hence, $(N/M)_s \sim N_s/M_s$

Proof:

- f_s is 1-1 :

$$f_s\left(\frac{x}{t}\right) = 0 \rightsquigarrow \exists u \in S, uf(x) = 0 \rightsquigarrow f(ux) = 0 \rightsquigarrow ux = 0 \rightsquigarrow \frac{x}{t} = 0$$

- g_s is onto : $\forall \frac{z}{t} \in L_s, \exists y \in N$ s.t. $g(y) = z \rightsquigarrow g_s(\frac{y}{t}) = \frac{z}{t}$
- $\text{Im } f_s \subseteq \ker g_s : g_s(f_s(\frac{x}{t})) = \frac{g(f(x))}{t} = \frac{0}{t} = 0$
- $\ker g_s \subseteq \text{Im } f_s : g_s(\frac{y}{t}) = 0 \rightsquigarrow \exists u \in S, ug(y) = 0 \rightsquigarrow uy = f(x) \rightsquigarrow \frac{y}{t} = \frac{f(x)}{ut} \in \text{Im } f_s$

□

Property 1.8.2. $R_s \otimes_R M = M_s$

Proof: Define $f : R_s \times M \longrightarrow M_s$
 $(\frac{a}{t}, x) \longmapsto \frac{ax}{t}$

Well-defined :

$$\frac{a_1}{t_1} = \frac{a_2}{t_2} \rightsquigarrow \exists u \in S \text{ s.t. } u(t_1 a_2 - t_2 a_1) = 0 \rightsquigarrow u(t_1 a_2 - t_2 a_1)x = 0 \rightsquigarrow \frac{a_1 x}{t_1} = \frac{a_2 x}{t_2}$$

$$\implies \tilde{f} : R_s \otimes M \longrightarrow M_s$$

$$\frac{a}{t} \otimes x \longmapsto \frac{ax}{t}$$

- \tilde{f} is onto : $\forall \frac{x}{t} \in M_s, \tilde{f}(\frac{1}{t} \otimes x) = \frac{x}{t}$
- \tilde{f} is 1-1 : Let $z = \sum_{i=1}^n \frac{a_i}{t_i} \otimes x_i \in R_s \otimes M$. Set $t = \prod t_i$ and $s_i = \frac{t}{t_i}$, then

$$z = \sum_{i=1}^n \frac{a_i s_i}{t} \otimes x_i = \sum_{i=1}^n \frac{1}{t} \otimes a_i s_i x_i = \frac{1}{t} \otimes \sum_{i=1}^n a_i s_i x_i = \frac{1}{t} \otimes x \text{ for some } x \in M$$

Now, if $\frac{1}{t} \otimes x \in \ker \tilde{f} \rightsquigarrow \frac{x}{t} = 0 \rightsquigarrow \exists u \in S, ux = 0 \rightsquigarrow \frac{1}{t} \otimes x = \frac{1}{ut} \otimes ux = 0$

□

1.8.2 Localization of prime ideal and maximal ideal

Definition 1.8.2. Let p be a prime ideal of R , then $S := R \setminus p$ is m.c. in R . Denote $R_p := R_{(S \setminus p)} \rightsquigarrow (R_p, p_p)$ is a local ring (since $R_p \setminus p_p = S_p = \{\text{unit of } R_s\}$)

Theorem 1.8.1. $M : R$ -module. TFAE

$$(1) M = 0 \quad (2) M_p = 0 \ \forall p \in \text{Spec } R \quad (3) M_m = 0 \ \forall m \in \text{Max } R$$

Proof: (1) \Rightarrow (2) \Rightarrow (3) : OK!

(3) \Rightarrow (1) : If $M \neq 0$ i.e. $\exists 0 \neq x \in M \rightsquigarrow \text{ann}(x) \neq R \rightsquigarrow \exists m_0 \in \text{Max } R$ s.t. $\text{ann}(x) \subseteq m_0$. But $M_{m_0} = 0, \frac{x}{1} = \frac{0}{1} \implies \exists u \notin m_0$ s.t. $ux = 0$. But $u \in \text{ann}(x) \subseteq m_0$ ($\rightarrow \leftarrow$) □

Corollary 1.8.1. Let $N \subseteq M$. Then TFAE

$$(1) M = N \quad (2) M_p = N_p \ \forall p \in \text{Spec } R \quad (3) M_m = N_m \ \forall m \in \text{Max } R$$

(Consider M/N is Theorem 1.8.1 and Property 1.8.1)

Corollary 1.8.2. Let R be an integral domain and $K = R_{(R \setminus \{0\})}$ be the field of fraction. Then $\forall m \in \text{Max } R, R \subset R_m \subset K$ and $R = \bigcap_{m \in \text{Max } R} R_m$

Proof: Let $R' = \bigcap_{m \in \text{Max } R} R_m \rightsquigarrow R \subset R' \subset R_m \implies R_m \subseteq R'_m \subseteq (R_m)_m = R_m$. So $R_m = R'_m \forall m \in \text{Max } R \rightsquigarrow R = R'$ \square

Corollary 1.8.3. Let $\varphi : M \longrightarrow N$ be an R -module homo.

- TFAE : (1) φ is 1 - 1 (2) φ_p is 1 - 1 $\forall p \in \text{Spec } R$ (3) φ_m is 1 - 1 $\forall m \in \text{Max } R$
- TFAE : (1) φ is onto (2) φ_p is onto $\forall p \in \text{Spec } R$ (3) φ_m is onto $\forall m \in \text{Max } R$
- (1) \implies (2) : $M \rightarrow N \rightarrow 0 \rightsquigarrow M_p \rightarrow N_p \rightarrow 0$
- (2) \implies (3) : OK!
- (3) \implies (1) : $M \xrightarrow{\varphi} N \longrightarrow \text{coker } \varphi \longrightarrow 0 \implies M_m \xrightarrow{\varphi_m} N_m \longrightarrow (\text{coker } \varphi)_m \longrightarrow 0 \implies (\text{coker } \varphi)_m = 0 \implies \varphi \text{ is onto.}$

Property 1.8.3. Let $\rho : R \rightarrow R_S, x \mapsto \frac{x}{1}$ is natural canonical map

$$\begin{array}{ccc} \text{Spec } R_S & \longleftrightarrow & \{P \in \text{Spec } R : P \cap S = \emptyset\} \\ Q & \longmapsto & \rho^{-1}(Q) \\ P_S & \longleftarrow & P \end{array}$$

Proof:

- If $t \in \rho^{-1}(Q) \cap S$, then $\frac{t}{1} = \rho(t) \in Q$ is a unit $\implies Q = R_S$ ($\rightarrow \leftarrow$)
- And it clear that $\rho^{-1}(Q)$ is a prime ideal of R .
- If $\frac{a}{t} \cdot \frac{b}{s} \in P_S \rightsquigarrow \frac{ab}{ts} = \frac{c}{v}, c \in P \rightsquigarrow \exists u \in S, uvab = utsc \in P$, since $c \in P$. Since $uv \in S$ and $S \cap P = \emptyset \rightsquigarrow ab \in P \rightsquigarrow a \in P$ or $b \in P$
- $(\rho^{-1}(Q))_S = Q$: (\subseteq) : By def.
- (\supseteq) : $\frac{a}{t} \in Q \implies \rho(a) = \frac{a}{1} = \frac{a}{t} \cdot \frac{t}{1} \in Q \implies a \in \rho^{-1}(Q)$
- $\rho^{-1}(P_S) = P$:
- (\supseteq) : By def. (\subseteq) : $\frac{a}{1} \in P_S \rightsquigarrow \frac{a}{1} = \frac{b}{t}, b \in P \rightsquigarrow \exists u \in S, uta = ub \in P \rightsquigarrow a \in P$

\square

Corollary 1.8.4. $P \in \text{Spec } R$

$$\text{Spec } R_P \longleftrightarrow \{q \in \text{Spec } R : q \subseteq P\}$$

Definition 1.8.3. Let M be a R -module, define $\text{Ann}_R(M) = \{a \in R : ax = 0 \forall x \in M\} \rightsquigarrow M$ is $R/\text{Ann}_R(M)$ -module

Theorem 1.8.2. M : f.g. R -module; S : m.c. in R . Then $(\text{Ann}_R(M))_S = \text{Ann}_{R_S}(M_S)$

Proof: Let $M = \langle x_1, \dots, x_n \rangle_R$. By induction on n .

$n = 1$: $M = Rx_1 \simeq R/\text{ann}(x_1)$.

Claim: $\text{Ann}_R(R/I) = I$

pf. (\supseteq) : OK! (\subseteq) : $\forall a \in \text{Ann}_R(R/I) \rightsquigarrow a(1+I) = I \rightsquigarrow a \in I$ □

So

$$\left(\text{Ann}_R \left(R/\text{ann}(x_1) \right) \right)_S = \text{ann}(x_1)_S = \text{Ann}_{R_S} \left(R_S/\text{ann}(x_1)_S \right) = \text{Ann}_{R_S} \left(\left(R/\text{ann}(x_1) \right)_S \right)$$

which means $(\text{Ann}_R(M))_S = \text{Ann}_{R_S}(M_S)$.

If $n > 1$, let $N = \langle x_1, \dots, x_{n-1} \rangle_R$. By induction hypothesis, $(\text{Ann}_R(N))_S = \text{Ann}_{R_S}(N_S)$. Since $M = N + Rx_n$, write $M' = Rx_n$. Then

$$\begin{aligned} (\text{Ann}_R(M))_S &= (\text{Ann}_R(N + M'))_S = (\text{Ann}_R(N) \cap \text{Ann}_R(M'))_S \\ &= (\text{Ann}_R(N))_S \cap (\text{Ann}_R(M'))_S = (\text{Ann}_{R_S}(N_S)) \cap (\text{Ann}_{R_S}(M'_S)) = (\text{Ann}_{R_S}(N_S) \cap \text{Ann}_{R_S}(M'_S)) \\ &= \text{Ann}_{R_S}(N_S + M'_S) = \text{Ann}_{R_S}((N + M')_S) = \text{Ann}_{R_S}(M_S) \end{aligned}$$

□

Definition 1.8.4. N, L are submodules of M .

Define $(N : L) := \{x \in R : xL \subseteq N\} = \text{Ann}_R \left((L + N)/N \right)$

Corollary 1.8.5. If L is a f.g. R -module, then $(N : L)_S = (N_S : L_S)$

Proof: $(L + N)/N \simeq L/(L \cap N)$ is a f.g. R -module, by Theorem 1.8.2

$$(N : L)_S = \text{Ann}_R \left((L + N)/N \right)_S = \text{Ann}_{R_S} \left((L + N)_S/N_S \right) = (L_S : N_S)$$

□

Definition 1.8.5. The **nilradical** of R is the ideal of **nilpotent element** ($a^n = 0$ for some n) in R , we usually denoted $\sqrt{\langle 0 \rangle}$ or \mathfrak{N}_R .

$$(x^n = 0, y^m = 0 \implies (x + y)^{n+m} = 0)$$

Property 1.8.4. $\sqrt{\langle 0 \rangle} = \bigcap_{P \in \text{Spec } R} P$

Proof: (\subseteq) : $x^n = 0 \in P \ \forall P \in \text{Spec } R \implies x \in P \ \forall P \in \text{Spec } R$

(\supseteq) : If $x \notin \sqrt{\langle 0 \rangle}$ i.e. $x^n \neq 0 \ \forall n > 0$, then consider

$$S = \{I \subseteq R : x^n \notin I \ \forall n > 0\} \neq \emptyset, \text{ since } \sqrt{\langle 0 \rangle} \in S$$

Define the partial order : $I_1 \leq I_2 \iff I_1 \subseteq I_2$. Let $T = (I_i)_{i \in \Lambda}$ be a chain in S . Set $I = \bigcup_{i \in \Lambda} I_i$ is a ideal and $x^n \notin I \ \forall n > 0 \rightsquigarrow I$ is a least upper bound for T . By Zorn's lemma, S has a maximal element. Say P .

Claim: $P \in \text{Spec } R$

pf. For $a, b \notin P$. $\langle a \rangle + P, \langle b \rangle + P \not\supseteq P$, so $\exists m, n > 0$ s.t. $\begin{cases} x^m \in P + \langle a \rangle \\ x^n \in P + \langle b \rangle \end{cases} \implies$

$$x^{m+n} \in P + \langle ab \rangle \implies P + \langle ab \rangle \notin S \implies ab \notin P. \quad \square$$

In particular, $x \notin P \in S$ □

Corollary 1.8.6. $(\mathfrak{N}_R)_S = \mathfrak{N}_{R_S}$

Proof: For $P \in \text{Spec } R$. If $P \cap S \neq \emptyset$, then $R_S = P_S$. If $P \cap S = \emptyset$, we have the corresponding $\text{Spec } R \ni P \longleftrightarrow P_S \in \text{Spec } R_S$. Then

$$(\mathfrak{N}_R)_S = \left(\bigcap_{P \in \text{Spec } R} P \right)_S = \bigcap_{P \in \text{Spec } R} P_S = \bigcap_{P_S \in \text{Spec } R_S} P_S = \mathfrak{N}_{R_S}$$

□

1.9 Noetherian modules

Definition 1.9.1. An (left) A -module M is said to be **Noetherian** if every ascending chain of submodule $M_i : M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ becomes stationary i.e. $\exists n \in \mathbb{N}$ s.t. $M_n = M_{n+1} = \dots$

(This condition is called **ascending chain condition** (ACC))

Property 1.9.1. TFAE

- (1) M is Noetherian
- (2) Any non-empty collection \mathcal{S} of submodules of M has a maximal member
- (3) Every submodule of M is f.g.

Proof:

- (1) \Rightarrow (2) : If not, pick $M_1 \in \mathcal{S}$, for $M_1, \exists M_2 \in \mathcal{S}$ s.t. $M_1 \subsetneq M_2$. For $M_2, \exists M_3 \in \mathcal{S}$ s.t. $M_2 \subsetneq M_3 \rightsquigarrow M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \dots$ will stationary ($\rightarrow \leftarrow$)
- (2) \Rightarrow (3) : For $N \leq M$, consider $\mathcal{S} = \{\text{all f.g. submodules of } N\} \neq \emptyset$, since $\langle 0 \rangle \in \mathcal{S}$. Let N' be a max member of \mathcal{S} . If $N' \subsetneq N$, choose $x \in N \setminus N' \rightsquigarrow N' \subsetneq Ax + N' \subseteq N$, but $Ax + N'$ is also the f.g. ($\rightarrow \leftarrow$). That is $N = N' \in \mathcal{S}$ is f.g..
- (3) \Rightarrow (1) : $M_1 \subseteq M_2 \subseteq \dots$ in M . Let $N = \bigcup_{i=1}^{\infty} M_i$ which is a submodule of M , say $N = \langle x_1, \dots, x_k \rangle_R$ and $x_i \in M_{n_i}$. Let $n = \max_{1 \leq i \leq k} n_i \rightsquigarrow N \subseteq M_n \subseteq N \implies N = M_n$ and $M_n = M_{n+1} = \dots$

□

Definition 1.9.2. A ring A is (left) **Noetherian** if it is Noetherian as a left module over itself (i.e. $I \subseteq A$ is left ideal $\implies I$ is f.g.)

Theorem 1.9.1 (Hilbert basis theorem). If A is (left) Noetherian, then $A[x]$ is (left) also Noetherian.

(So $\mathbb{Z}, \mathbb{Z}[x], \mathbb{Z}[x, y], \dots, k[x_1, \dots, x_n]$ are all Noetherian, and we can find the **Gröbner basis** of their ideals.)

Proof: If not, \exists an (left) ideal J of $A[x]$ s.t. J is not f.g.. Choose $f_1 \in J$ s.t. f_1 is a poly. of least degree in J . $\exists f_2 \in J \setminus \langle f_1, f_2 \rangle$ s.t. f_2 is a poly. of least degree in $J \setminus \langle f_1, f_2 \rangle$. We can construct f_3, f_4, \dots and let $\deg f_i = n_i$, the leading coefficient is $a_i \rightsquigarrow n_1 \leq n_2 \leq \dots$.

Claim: $\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \dots$

pf. If $\exists m$ s.t. $\langle a_1, \dots, a_m \rangle = \langle a_1, \dots, a_{m+1} \rangle$, then $a_{m+1} = \sum_{i=1}^m r_i a_i$ and

$$\deg \left(\underbrace{f_{m+1}(x) - \sum_{i=1}^m x^{n_{m+1}-n_i} r_i f_i(x)}_{\in J \setminus \langle f_1, \dots, f_m \rangle} \right) < \deg f_{m+1} \quad (\rightarrow \leftarrow)$$

□

But A is Noetherian, $\{\langle a_1, \dots, a_n \rangle\}_{n \in \mathbb{N}}$ must be stationary $(\rightarrow \leftarrow)$

□

Property 1.9.2. $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ is exact for A -modules. Then M is Noetherian $\iff L, N$ are Noetherian

Proof:

(\implies) :

• $L_1 \subset L_2 \subset \dots$ in $L \rightsquigarrow f(L_1) \subset f(L_2) \subset \dots$ in $M \rightsquigarrow f(L_n) = f(L_{n+1}) = \dots$

Since f is 1-1, $L_n = L_{n+1} = \dots$

• $N_1 \subset N_2 \subset \dots$ in $N \simeq M/L$, by 3rd isom. thm., we have $N_i \longleftrightarrow M_i/L$ and $M_1 \subset M_2 \subset \dots$ in $M \rightsquigarrow M_n = M_{n+1} = \dots$ and thus $N_n = N_{n+1} = \dots$

(\impliedby) :

$M_1 \subset M_2 \subset \dots$ in M , then

$$\begin{cases} f(L) \cap M_1 \subset f(L) \cap M_2 \subset \dots \text{ in } f(L) \simeq L & \rightsquigarrow f(L) \cap M_r = f(L) \cap M_{r+1} = \dots \\ g(M_1) \subset g(M_2) \subset \dots \text{ in } N & \rightsquigarrow g(M_r) = g(M_{r+1}) = \dots \end{cases}$$

Claim: $M_r = M_{r+1}$

pf. $\forall x \in M_{r+1}, g(x) \in g(M_{r+1}) = g(M_r) \implies g(x) = g(y)$ for some $y \in M_r$
 $\implies (x - y) \in \ker g = \text{Im } f \in f(L) \implies x - y \in f(L) \cap M_{r+1} = f(L) \cap M_r \rightsquigarrow x \in M_r$ □

Corollary 1.9.1. M_r : Noetherian $\forall i = 1, \dots, r \implies \bigoplus_{i=1}^r M_i$ is Noetherian

Proof: By induction on r . $r = 1$ OK! $r = 2$: Since $0 \rightarrow M_1 \rightarrow M_1 \oplus M_2 \rightarrow M_2$ is exact and M_1, M_2 are Noeth $\implies M_1 \oplus M_2$ is Noeth.

If $r > 2$, $0 \rightarrow M_r \rightarrow \bigoplus_{i=1}^r M_i \rightarrow \bigoplus_{i=1}^{r-1} M_i \rightarrow 0 \implies \bigoplus_{i=1}^r M_i$ is Noeth. □

Corollary 1.9.2. A : Noetherian and $M = \langle x_1, \dots, x_n \rangle_A$ is a f.g. module, then M is Noetherian

Proof: Consider

$$\begin{array}{ccccccc} 0 & \rightarrow & \ker f & \rightarrow & A^n & \rightarrow & M \rightarrow 0 \\ & & & & e_i & \mapsto & x_i \end{array}$$

Then A^n is Noeth. $\implies M$ is Noeth. \square

Corollary 1.9.3. $f : A \rightarrow B$ is module homo. If A is Noetherian, then B is Noetherian.

Observation: R : commutative and M : R -module, $\forall 0 \neq x \in M \implies \text{ann}(x) \subsetneq R$
 If P is a maximal element in $\{\text{ann}(x) : x \in M\}$, say $P = \text{ann}(z) \implies P \in \text{Spec } R$
 $p.f.$ $p \subsetneq R$. If $ab \in P$ and $a \notin P$, then $abz = 0, az \neq 0 \implies b \in \text{ann}(az) \supseteq \text{ann}(z) \implies \text{ann}(az) = \text{ann}(z) \implies b \in P$.

Definition 1.9.3 (Associated prime).

$$\text{Ass}(M) := \{p \in \text{Spec } R : p = \text{ann}(x) \text{ for some } 0 \neq x \in M\}$$

$$\implies R/P \simeq Rx \subseteq M$$

Fact 1.9.1. If R is Noetherian and $M \neq 0$, then $\text{Ass}(M) \neq \emptyset$

$p.f.$ Let $\mathcal{S} = \{\text{ann}(x) | x \neq 0\} \neq \emptyset$. Since R is Noetherian $\rightsquigarrow \exists$ a maximal element in $\mathcal{S} \rightsquigarrow P \in \text{Ass}(M)$

Definition 1.9.4 (nilpotent).

- $a \in R$ is called **nilpotent** on M if $\exists n > 0$ s.t. $a^n M = 0$. In other word, $a^n \in \text{Ann}(M)$ i.e. $a \in \sqrt{\text{Ann}(M)}$
- $a \in R$ is called **locally nilpotent** on M if $\forall 0 \neq x \in M, \exists n(x) > 0$ s.t. $a^{n(x)}x = 0$. In other word, $a^{n(x)} \in \text{ann}(x) \forall x \in M$ i.e. $a \in \bigcap_{x \in M} \sqrt{\text{ann}(x)}$

Fact 1.9.2. M is f.g. R -module \rightsquigarrow “local nilpotent \implies nilpotent”

$p.f.$ Say $M = \langle x_1, \dots, x_k \rangle_R$ and $a^{n_i}x_i = 0$. Let $n = \max_{1 \leq i \leq k} n_i \rightsquigarrow a^n x_i = 0 \forall i \implies a^n M = 0$

Definition 1.9.5 (Support).

$$\text{Supp}(M) := \{p \in \text{Spec } R | M_p \neq 0\}$$

If $P \in \text{Supp}(M)$, which means there exists $\frac{x}{t} \neq 0 \in M_P$ for some $x \in M, t \notin P$. So we must have $\text{ann}(x) \subseteq P$ or we can say $(Rx)_P \neq 0$

Fact 1.9.3. $\text{Ass}(M) \subseteq \text{Supp}(M)$

$p.f.$ Since $\forall p \in \text{Ass}(M)$ is annihilate of element in M .

Property 1.9.3. a is locally nilpotent on $M \iff a \in \bigcap_{P \in \text{Supp}(M)} P$

Proof: (\Rightarrow) : Let a be locally nilpotent and $P \in \text{Supp}(M)$, say $\text{ann}(x) \subseteq P$. If $a^{n(x)}x = 0$, then $a^{n(x)} \in \text{ann}(x) \subseteq P \Rightarrow a \in P$

(\Leftarrow) : If a is not locally nilpotent, then $\exists 0 \neq x \in M$ s.t. $a^n x \neq 0 \forall n > 0$ i.e. $\{1, a, a^2, \dots\} \cdot x \cap \text{ann}(x) = \emptyset$. Let $\mathcal{S} = \{\text{ann}(x) \subseteq I \subseteq R : I \cap \mathcal{S} = \emptyset\} \neq \emptyset$, since $\text{ann}(x) \in \mathcal{S}$. By Zorn's lemma, \exists a max element $P \in \mathcal{S}$.

Claim: $P \in \text{Spec } R$

pf. $x, y \notin P \rightsquigarrow Rx + P, Ry + P \supseteq P \rightsquigarrow a^n \in Rx + P, a^m \in Ry + P \rightsquigarrow a^{n+m} \in Rxy + P \notin \mathcal{S} \Rightarrow xy \notin P$ \square

By Claim, $\text{ann}(x) \subseteq P \rightsquigarrow M_P \neq 0 \rightsquigarrow P \in \text{Supp}(M)$ and $a \notin P$ \square

Remark 1.9.1. Case of $M = R$ in Property 1.9.3 can be reduce to

- local nilpotent \Rightarrow global, since $a^n \cdot 1 = 0$ for some $n \Rightarrow a^n = 0$
- $\text{Supp}(M) = \text{Spec } R$, since $\frac{1}{1} \in M_P$

and by Property 1.8.4 we will get the result.

Property 1.9.4. Let R be Noetherian. Then $\bigcap_{P \in \text{Supp}(M)} P = \bigcap_{P \in \text{Ass}(M)} P$

Proof: (\subseteq) : By Fact 1.9.3

(\supseteq) : **Claim:** $\forall p \in \text{Supp}(M), \exists q \in \text{Ass}(M)$ s.t. $q \subseteq p$

pf. $\forall p \in \text{Supp}(M)$, $\exists 0 \neq x \in M$ s.t. $(Rx)_p \neq 0$ is a R_p -module

By Homework 7, R is Noetherian $\Rightarrow R_p$ is Noetherian $\forall p \in \text{Supp}(M)$

By Fact 1.9.1, $\exists q_p \in \text{Ass}((Rx)_p)$ i.e. $q_p = \text{ann}(\frac{rx}{t})$

Let $q = \langle a_1, \dots, a_m \rangle_R \rightsquigarrow \frac{a_i}{1} \cdot \frac{rx}{t} = 0 \rightsquigarrow \exists u_i \notin p$ s.t. $u_i a_i rx = 0$.

Let $u = u_1 \cdots u_m \notin p \rightsquigarrow a_i urx = 0 \forall i = 1, \dots, m \rightsquigarrow q \subseteq \text{ann}(urx)$

Conversely, if $a \in \text{ann}(urx) \rightsquigarrow \frac{au}{1} \in q_p$, say $\frac{au}{1} = \frac{b}{s}$ for some $b \in q$ and $s \notin p \rightsquigarrow \exists w \notin p$ s.t. $wsau = wb \in q \rightsquigarrow a \in q$, since $wsu \notin q$ \square

Theorem 1.9.2. $R, M \neq 0$: Noetherian $\Rightarrow \exists M = M_1 \supseteq M_2 \supseteq \dots \supseteq M_r = 0$ s.t. $M_i/M_{i+1} \simeq R/p_i$ for some $p_i \in \text{Spec } R$

Proof: Let $\mathcal{S} := \{N \subseteq M \mid N \text{ satisfies condition in above}\} \neq \emptyset$, since $\exists p \in \text{Ass}(M) \rightsquigarrow Rx \simeq R/p \in \mathcal{S}$. Since M is Noetherian, \exists a maximal element N in \mathcal{S} .

Claim: $N = M$

pf. If $N \subsetneq M$, then $M/N \neq 0$ and M/N is Noetherian $\Rightarrow \exists q \in \text{Ass}(M/N)$ and say $q = \text{ann}(y+N)$ i.e. $R\bar{y} = (Ry+N)/N \simeq R/q \rightsquigarrow N \subsetneq Ry+N \in \mathcal{S}(\rightarrow \leftarrow)$ \square

1.10 Primary decomposition

In this section, R is a commutative ring and M is an R -module

Definition 1.10.1. $a \in R$, define

$$\begin{aligned} a_M : M &\longrightarrow M \\ x &\longmapsto ax \end{aligned}$$

is a R -module homomorphism.

Fact 1.10.1. R is Noetherian, a_M is injective $\iff a \notin \bigcup_{p \in \text{Ass}(M)} p$

Proof: $(\implies) : \forall p \in \text{Ass}(M)$, say $p = \text{ann}(z)$ for some $z \neq 0$. If $a \in p \rightsquigarrow az = 0 \rightsquigarrow z \in \ker a_M = \{0\}$ $(\rightarrow \leftarrow)$

$(\impliedby) : a_M$ is not $1-1 \implies \exists 0 \neq x \in \ker a_M$ i.e. $ax = 0$. Since R is Noetherian, $\text{Ass}(M) \neq \emptyset$, we can choose $p \in \text{Ass}(M)$ s.t. $\text{ann}(x) \subseteq p$, then $a \in \bigcup_{p \in \text{Ass}(M)} p$ \square

Definition 1.10.2. a_M is called **(locally) nilpotent** if a is (locally) nilpotent on M .

Fact 1.10.2. R is Noetherian, then $\text{Ass}(M) = \{P\} \iff M \neq 0, \forall a \in R, a_M$ is injective or locally nilpotent.

Proof: $(\implies) : \text{If } a \in P \rightsquigarrow a_M \text{ is locally nilpotent. If } a \notin P \rightsquigarrow a_M \text{ is injective.}$

$(\impliedby) : R = \left(R \setminus \bigcup_{p \in \text{Ass}(M)} p \right) \cup \left(\bigcap_{p \in \text{Ass}(M)} p \right) \rightsquigarrow |\text{Ass}(M)| = 1$ \square

Definition 1.10.3.

- An ideal q of R is **primary** if $q \subsetneq R$ and

$$xy \in q, x \notin q \implies y^n \in q \text{ for some } n > 0$$

$(\iff R/q \neq 0 \text{ and the zero divisors in } R/q \text{ are nilpotent})$

If we say q is p -primary, which means q is primary and $\sqrt{q} = p$.

- R : Noetherian, a submodule N of M is **p -primary** if $\text{Ass}(M/N) = \{p\}$

Fact 1.10.3. $q \subset R$ is primary $\implies \sqrt{q}$ is the smallest prime ideal containing q .

Proof:

- If $xy \in \sqrt{q}, x \notin \sqrt{q} \implies x^n y^n \in q, (x^n)^m \neq q \text{ for all } m > 0 \implies y^n \in q \implies y \in \sqrt{q}$

- $\sqrt{q} = \bigcap_{q \subseteq P} P \implies \sqrt{q} \subset P \forall q \subseteq P$

(Note : R : Noetherian, then $\text{Ass}(R/q) = \{\sqrt{\langle 0 \rangle}\} = \{\sqrt{q}\}$) \square

From now on, R is Noetherian

Lemma 1.10.1. Let N_1 and N_2 be two p -primary submodules of M . Then $N_1 \cap N_2$ is a p -primary.

Proof: Since $M/N_1 \cap N_2 \hookrightarrow M/N_1 \oplus M/N_2$, by Homework 7.,

$$\emptyset \neq \text{Ass}(M/N_1 \cap N_2) \subset \text{Ass}(M/N_1 \oplus M/N_2) \subset \text{Ass}(M/N_1) \cup \text{Ass}(M/N_2) = \{p\}$$

Hence, $\text{Ass}(M/N_1 \cap N_2) = \{p\}$. \square

Definition 1.10.4. Let $N \subseteq M$

1. A **primary decomposition** of N is $N = N_1 \cap \cdots \cap N_r$ with N_i are primary.
2. It is **reduced** if no N_i can be omitted and the associated primes of M/N_i are all distinct.

(Note : Lemma 1.10.1 \implies any PD can be simplified to a RPD)

Lemma 1.10.2. If $N = N_1 \cap \cdots \cap N_r$ is a RPD and $\text{Ass}(M/N_i) = \{p_i\}$, then $\text{Ass}(M/N) = \{p_1, \dots, p_r\}$

Proof:

$$M/N \hookrightarrow \bigoplus_{i=1}^r M/N_i \implies \text{Ass}(M/N) \subseteq \bigcup_{i=1}^r \text{Ass}(M/N_i) = \{p_1, \dots, p_r\}$$

$$\begin{aligned} 0 \neq (N_2 \cap \cdots \cap N_r)/N &\simeq (N_1 + N_2 \cap \cdots \cap N_r)/N_1 \subseteq M/N_1 \\ \implies \text{Ass}\left((N_2 \cap \cdots \cap N_r)/N\right) &= \text{Ass}(M/N_1) = \{p_1\} \end{aligned}$$

Hence,

$$\{p_1\} = \text{Ass}\left((N_2 \cap \cdots \cap N_r)/N\right) \subseteq \text{Ass}(M/N)$$

□

Lemma 1.10.3. Let N be p -primary in M and $q \in \text{Spec } R$. Set $\rho : M \rightarrow M_q$, then

- $p \not\subseteq q \implies M_q = N_q$
- $p \subseteq q \implies \rho^{-1}(N_q) = N$ (sometimes we will denote $\rho^{-1}(N_q) = M \cap N_q$)

Proof:

- $M_q/N_q \simeq (M/N)_q$ and thus $\text{Ass}(M_q/N_q) = \text{Ass}(M/N) \cap \{q \supseteq P \in \text{Spec } R\} = \emptyset$. Hence, $M_q = N_q$.
- $\because \text{Ass}(M/N) = \{p\}$ and $p \subseteq q \therefore R \setminus q$ does not contain zero divisor of M/N . Consider $M/N \hookrightarrow (M/N)_q \simeq M_q/N_q$ i.e.

$$\begin{array}{ccccc} & & \varphi & & \\ & \nearrow & & \searrow & \\ M & \xrightarrow{\rho} & M_q & \xrightarrow{f} & M_q/N_q \text{ with} \end{array}$$

$$\begin{aligned} m \in \ker \varphi &\iff \frac{m}{1} = \frac{n}{s} \iff usm = un \in N \iff us(m+N) = 0 \iff \\ m+N &= 0 \iff m \in N, \text{ so } \ker \varphi = N \end{aligned}$$

In other hands, $\ker f = N_q$ and thus $\ker \varphi = \rho^{-1}(N_q)$, so $N = \rho^{-1}(N_q)$

□

Remark 1.10.1. $N = N_1 \cap \cdots \cap N_r$: RPD with $\text{Ass}(M/N_i) = \{p_i\}$. If p_1 is minimal in $\{p_1, \dots, p_r\} = \text{Ass}(M/N)$, then $N_{p_1} = (N_1)_{p_1} \cap \cdots \cap (N_r)_{p_1} = (N_1)_{p_1}$, then $N_1 = \rho^{-1}(N_{p_1})$ is determined by N and p_1

Theorem 1.10.1. $\forall p \in \text{Ass}(M), \exists N(p) \subset M$ with $\text{Ass}(M/N(p)) = \{p\}$ s.t.

$$\langle 0 \rangle = \bigcap_{p \in \text{Ass}(M)} N(p)$$

Proof: Fix $p \in \text{Ass}(M)$, say $p = \text{ann}(x)$. Consider $\mathcal{S} := \{N \subseteq M : p \notin \text{Ass}(N)\} \neq \emptyset$. Define a partial order on $\mathcal{S} : N_1 \leq N_2 \iff N_1 \subseteq N_2$. Since

$$\text{Ass}\left(\bigcup_{i \in \Lambda} N_i\right) = \bigcup_{i \in \Lambda} \text{Ass}(N_i) \not\ni p$$

By Zorn's lemma, \exists a maximal element $N(p)$ in \mathcal{S} .

Claim: $N(p)$ is a p -primary.

p.f. $p \in \text{Ass}(M)$ and $p \notin \text{Ass}(N(p)) \implies N(p) \neq M$

If $q \neq p$ and $q \in \text{Ass}(M/N(p))$, then $\exists M'/N(p) \subseteq M/N(p)$ s.t. $M'/N(p) \simeq R/q$
 $\rightsquigarrow \text{Ass}(M'/N(p)) = \{q\} \rightsquigarrow \text{Ass}(M') \subseteq \underbrace{\text{Ass}(N(p))}_{p \notin} \cup \underbrace{\text{Ass}(M'/N(p))}_{=\{q\}}$, so $p \notin \text{Ass}(M')$

and $M' \supsetneq N(p)$ ($\rightarrow \leftarrow$) □

Hence, $\text{Ass}(M/N(p)) = \{p\}$ and

$$\text{Ass}\left(\bigcap_{p \in \text{Ass}(M)} N(p)\right) = \bigcap_{p \in \text{Ass}(M)} \text{Ass}(N(p)) = \emptyset \implies \bigcap_{p \in \text{Ass}(M)} N(p) = \langle 0 \rangle$$

□

Corollary 1.10.1. If M is a f.g. R -module, then any submodule N of M has primary decomposition.

Proof: We have $|\text{Ass}(M/N)| < \infty$, say $\text{Ass}(M/N) = \{p_1, \dots, p_r\}$ and $p_i \longleftrightarrow N(p_i) = N_i/N$, then $\langle \bar{0} \rangle = \bigcap_{i=1}^r N_i/N \implies N = \bigcap_{i=1}^r N_i$

$$\text{Ass}(M/N_i) = \text{Ass}\left(M/N \big/ N_i/N\right) = \{p_i\} \rightsquigarrow N_i : p_i\text{-primary}$$

□

Corollary 1.10.2. In a Noetherian ring R , $I \subseteq R \rightsquigarrow I = q_1 \cap \cdots \cap q_r$ with $\sqrt{q_i} = p_i$, where $\{p_1, \dots, p_r\}$ are uniquely determined by I and if p_i is minimal, then q_i is uniquely determined.

We called p_i are **associated prime with I** or **belongs to I** and p_1 is called isolated and others are called **embedded**.

Example 1.10.1. $R = k[x, y]$, $I = \langle x^2, xy \rangle$. Let $p_1 = \langle x \rangle \in \text{Spec } R$, $p_2 = \langle x, y \rangle \in \text{Max } R$, then $I = p_1 \cap p_2^2$ is primary decomposition of I . (Here we use the fact in below). We find that $\sqrt{I} = \sqrt{p_1} \cap \sqrt{p_2^2} = p_1 \cap p_2 = p_1$ is prime, but I is not primary since $xy \in I$ and $x \notin I, y^n \notin I \forall n > 0$

Fact 1.10.4. If \sqrt{q} is max, then q is primary.

Proof: Let $\sqrt{q} = m$, which is the smallest prime ideal containing q , so $\text{Spec}(R/q) = \{m/q\}$ and $\mathfrak{N}_{R/q} = m/q$. So $R/q \setminus m/q = \{\text{units}\} \implies$ all zero divisors are nilpotent. \square

Remark 1.10.2.

- A prime-power is not necessarily primary :

$R = k[x, y, z]/\langle xy - z^2 \rangle = k[\bar{x}, \bar{y}, \bar{z}]$ and $p = \langle \bar{x}, \bar{z} \rangle \in \text{Spec } R$, since $R/p \simeq k[\bar{y}] = k[t]$ is integral domain. Now $\bar{x}\bar{y} = \bar{z}^2 \in p^2$, but $\bar{x} \notin p^2, \bar{y}^n \notin p^2 \forall n > 0$

- A max-power is primary : Say $q = m^n$, $m \supseteq \bigcap_{m^n \subseteq p} p = \sqrt{m^n} \supseteq m \implies m = \sqrt{m^n} = \sqrt{q}$. By Fact 1.10.4, q is primary.

- $m^n \subseteq q \subseteq m \rightsquigarrow m = \sqrt{m^n} \subseteq \sqrt{q} \subseteq \sqrt{m} = m \rightsquigarrow \sqrt{q}$ is max and thus q is primary.

- A primary ideal is not necessarily a prime power :

$R = k[x, y], q = \langle x, y^2 \rangle \implies \langle x, y \rangle^2 \subseteq q \subseteq \langle x, y \rangle \implies q$ is primary but is not prime power.

Example 1.10.2. $\mathbb{Z} \supseteq q = \langle a \rangle$ is primary $\rightsquigarrow \sqrt{q} = \langle p \rangle$. By def, $p^m \in \langle a \rangle$, say $p^m = ra$, since \mathbb{Z} is UFD $\implies a \sim p^n$, where $n \leq m \implies \langle a \rangle = \langle p^n \rangle$

Property 1.10.1. R : Noetherian, M : finitely generated. $\text{Ass}(M) = \{p\} \implies \text{Ann}(M)$ is p -primary

Proof: $\forall a \in R$, a_M is injective ($\leftrightarrow a \notin p$) or nilpotent ($\leftrightarrow a \in p$). So $\text{Ann}(M) \subseteq p$. If $ab \in \text{Ann}(M) \subseteq p$. If $a \in p \rightsquigarrow a^n M = 0 \rightsquigarrow a^n \in \text{Ann}(M)$. If $a \notin p \rightsquigarrow b \in p$ and by symmetric, $a^n \in \text{Ann}(M)$. Hence, $\text{Ann}(M)$ is p -primary. \square

1.11 Nakayama's lemma & Artin-Rees lemma

In this section, R is a commutative ring and M is R -module

Definition 1.11.1. The Jacobson radical of R is $J_R := \bigcap_{m \in \text{Max } R} m$

Property 1.11.1.

- $I \subsetneq R \implies \langle I, J_R \rangle \subsetneq R$:
 $p.f.$ $\exists m \in \text{max } R$ s.t. $I \subseteq m \implies \langle I, J_R \rangle \subseteq m$

- $\mathfrak{N}_R \subseteq J_R$
- $x \in J_R \iff 1 - rx$ is unit $\forall r \in R$:
 (\Rightarrow) If $1 - rx$ is not unit, then $\langle 1 - rx \rangle \subseteq m$ for some $m \in \max R \rightsquigarrow 1 \in m \implies m = R$ ($\rightarrow \leftarrow$)
 (\Leftarrow) : If $\exists m \in \max R$ s.t. $x \notin m \rightsquigarrow Rx + m = R$, say $rx + m_0 = 1 \rightsquigarrow m_0 = 1 - rx$ is unit $\implies m = R$ ($\rightarrow \leftarrow$)

Lemma 1.11.1 (Nakayama's lemma). If M is f.g. and $I \subseteq J_R$ s.t. $IM = M$, then $M = 0$

Proof: Assume $M \neq 0$ and $M = \langle x_1, \dots, x_n \rangle$, where n is the smallest integer s.t. M is generated by n elements. And $x_n \in M = IM$, say $x_n = a_1x_1 + \dots + a_nx_n$ with $a_i \in I$, then $(1 - a_n)x_n = a_1x_1 + \dots + a_{n-1}x_{n-1}$. Since $1 - a_n$ is unit, $x_n \in \langle x_1, \dots, x_{n-1} \rangle \implies M = \langle x_1, \dots, x_{n-1} \rangle$ ($\rightarrow \leftarrow$) \square

Corollary 1.11.1. M : f.g., $N \subseteq M$, $I \subseteq J_R$. Then $M = IM + N \implies M = N$.

Proof: M : f.g. $\implies M/N$ is f.g. and $I(M/N) = (IM + N)/N = M/N$. By Nakayama's lemma, $M/N = 0 \rightsquigarrow M = N$. \square

Corollary 1.11.2. (R, m) : local ring, M : f.g.. If $M/mM = \langle \bar{x}_1, \dots, \bar{x}_n \rangle_{R/m}$, where $\{\bar{x}_1, \dots, \bar{x}_n\}$ is a basis, then $M = \langle x_1, \dots, x_n \rangle_R$

Proof: Let $N = \langle x_1, \dots, x_n \rangle_R \rightsquigarrow (N + mM)/mM = \langle \bar{x}_1, \dots, \bar{x}_n \rangle_{R/m} = M/mM \rightsquigarrow N + mM = M$. By Corollary 1.11.2, $M = N$. \square

Corollary 1.11.3. (R, m) : local ring, M, N : f.g. and $f : M \rightarrow N$ is R -module homomorphism, Define $\bar{f} : M/mM \rightarrow N/mN$ by $\bar{f} : x + mM \mapsto f(x) + mN$

- \bar{f} is onto $\implies f$ is onto :

pf. $N/mN = \text{Im } \bar{f} = (f(M) + mN)/mN \implies N = mN + f(M) \rightsquigarrow N = f(M)$
i.e. f is onto.
- Assume M, N : free, then \bar{f} is $1 - 1 \implies f$ is $1 - 1$:

pf. Let $M = \langle v_1, \dots, v_\ell \rangle_R$ with $\{v_1, \dots, v_\ell\}$ is a basis and $w_i = f(v_i) \forall i$
By Corollary 1.11.2 and commutative ring has IBN, $M/mM = \langle \bar{v}_1, \dots, \bar{v}_\ell \rangle_{M/mM}$ and $\text{Im } \bar{f} = \langle \bar{w}_1, \dots, \bar{w}_\ell \rangle_{N/mN} \subseteq N/mN$. Since \bar{f} is $1 - 1$, $\dim \text{Im } \bar{f} = \ell \rightsquigarrow \{\bar{w}_1, \dots, \bar{w}_\ell\}$ is a basis for $\text{Im } \bar{f}$.
We can extend $\{\bar{w}_1, \dots, \bar{w}_\ell\}$ to a basis $\{\bar{w}_1, \dots, \bar{w}_\ell, \bar{w}_{\ell+1}, \dots, \bar{w}_k\}$ for N/mN . By Corollary 1.11.2, $\{w_1, \dots, w_k\}$ is a free basis for N .
Now $\forall x \in M, \exists! a_i$ s.t. $x = \sum_{i=1}^{\ell} a_i v_i$. If $x \in \ker f$ i.e. $0 = f(x) = \sum_{i=1}^{\ell} a_i w_i$. So $a_i = 0 \forall i$. Hence, f is $1 - 1$.
- Assume M, N : free. Then \bar{f} is isomorphism $\implies f$ is isomorphism.

Definition 1.11.2.

- A **filtration** of M is a descending sequence of submodules $M = M_0 \supseteq M_1 \supseteq \cdots$
- Let I be an ideal of R . $\{M_i\}_{i \geq 0}$ is said to be an **I -filtration** if $IM_n \subseteq M_{n+1} \forall n$
(e.g. $M_i := I^i M$, then $IM_n = M_{n+1}$)
- I -filtration is **stable** if $IM_n = M_{n+1} \forall n > N$

Fact 1.11.1. $\{M_i\}, \{M'_i\} : \text{stable } I\text{-filtration of } M \implies \exists d \in \mathbb{N} \text{ s.t.}$

$$M_{n+d} \subseteq M'_n, M'_{n+d} \subseteq M_n \forall n \geq 0$$

Proof: It is clear that $I^n M \subseteq M_n \forall n \geq 1$.

By stability, $\exists d_1 > 0$ s.t. $I^n M_{d_1} = M_{d_1+n} \forall n > 0 \rightsquigarrow M_{n+d_1} = I^n M_{d_1} \subseteq I^n M$.

And $I^{n+d_1} M \subseteq I^n M \subseteq M_n$. So it is true for the case of " $M'_n = I^n M$ ".

By symmetry, $\exists d_2 > 0$ s.t. $I^{n+d_2} M \subseteq M'_n$ and $M'_{d_2+n} \subseteq I^n M$.

Let $d = d_1 + d_2$, then

$$\begin{cases} M_{d+n} = M_{d_1+(d_2+n)} \subseteq I^{d_2+n} M \subseteq M'_n \\ M'_{d+n} = M'_{d_2+(d_1+n)} \subseteq I^{d_1+n} M \subseteq M_n \end{cases}$$

□

Recall that $R = \bigoplus_{i=0}^{\infty} R_i$ is graded ring if $R_i R_j \subseteq R_{i+j}$ and thus

- $R_0 R_0 \subseteq R_0 \implies R_0$ is subring.
- $R_0 R_i \subseteq R_i \implies R_i$ is R_0 -module.

$M = \bigoplus_{i=0}^{\infty} M_i$ is graded module if $R_i M_j \subseteq M_{i+j}$

Theorem 1.11.1. Let R be graded. Then $R : \text{Noetherian} \iff R_0 : \text{Noetherian}$ and $R = R_0[a_1, \dots, a_n]$ with $a_i \in R$

Proof: $(\Leftarrow) : R_0 : \text{Noetherian}$, by Hilbert basis theorem, $R_0[x_1, \dots, x_n] : \text{Noetherian}$
 $\rightsquigarrow R \simeq R_0[x_1, \dots, x_n]/I$ is Noetherian.

$(\Rightarrow) : \text{Let } R^+ = \bigoplus_{i=1}^{\infty} R_i \text{ is an ideal of } R \text{ and } R_0 \simeq R/R^+ \rightsquigarrow R_0 : \text{Noetherian. Since } R \text{ Noetherian, } R^+ = \langle z_1, \dots, z_m \rangle_R. \text{ Write } z_i = z_{i,1} + \cdots + z_{i,n_i}, \text{ where } z_{i,j} \in R_{n_{i,j}}, \text{ then } R^+ = \langle z_{i,j} : 1 \leq i \leq m, 1 \leq j \leq n_i \rangle = \langle a_1, \dots, a_n \rangle_R, \text{ where } a_i \in R_{d_i} \forall i = 1 \sim n$

Claim: $R_k \subseteq R_0[a_1, \dots, a_n] \forall k \geq 0$ and thus $R = R_0[a_0, \dots, a_n]$

pf. By induction on $k : k = 0 \rightsquigarrow R_0 \subseteq R_0[a_1, \dots, a_n]$.

For $k > 0$, $x \in R_k \subseteq R^+$, write $x = \sum_{i=1}^n r_i a_i$ where $a_i \in R_{d_i}$ and $r_i \neq 0$, then $r_i \in R_{k-d_i} \subseteq R_0[a_0, \dots, a_n]$ (by induction hypothesis). Hence, $x \in R_0[a_0, \dots, a_n]$ □

Theorem 1.11.2 (General form of Artin-Rees lemma). $R : \text{Noetherian}$, $I \subseteq R$, $M : \text{f.g. } R\text{-module with a stable } I\text{-filtration } \{M_i\}_{i \geq 0}$. If $N \subseteq M$ and $N_n := N \cap M_n$, then $\{N_n\}$ is a stable I -filtration of N .

Proof: First, $I(N \cap M_n) \subseteq IN \cap IM_n \subseteq N \cap M_{n+1} = N_{n+1} \rightsquigarrow \{N_n\}$ is I -filtration.

$$\text{Define } S = S_I(R) := \bigoplus_{n=0}^{\infty} I^n t^n \subseteq_{\text{subring}} R[t] = \bigoplus_{n=0}^{\infty} R t^n$$

($S_I(R)$ is called **Rees ring of R w.r.t. I**)

$\because R$: Noetherian (say $I = \langle a_1, \dots, a_n \rangle$) and $S = R[a_1 t, \dots, a_n t] \therefore S$ is Noetherian.

Define $\widetilde{M} := \bigoplus_{n=0}^{\infty} M_n t^n$ which is a graded S -module

(Since $(I^\ell t^\ell)(M_n t^n) = I^\ell M_n t^{\ell+n} \subseteq M_{\ell+n} t^{\ell+n}$) Let

$$L_m := \overbrace{M_0 \oplus \dots \oplus M_m t^m}^{U_m} \oplus I M_m t^{m+1} \oplus I^2 M_m t^{m+2} \oplus \dots = \langle U_m \rangle_S$$

is a S -submodule of \widetilde{M} . Since R : Noetherian and M : f.g. $\implies M$: Noetherian and thus M_i : f.g. R -module $\forall i \implies U_m$ is f.g. R -module (say $U_m = \langle f_1, \dots, f_p \rangle_R$) and thus L_m is f.g. S -module since $L_m = \langle f_1, \dots, f_p \rangle_S$. Also, $L_m \subseteq L_{m+1} \subseteq \dots$ and $\bigcup_{m=0}^{\infty} L_m = \widetilde{M}$. Since S is Noetherian, there exists N s.t. $L_N = L_{N+1} = L_{N+2} = \dots$

and thus \widetilde{M} is Noetherian and thus f.g. S -module. In fact, we have

$$\begin{aligned} \widetilde{M} \text{ is f.g. } S\text{-module} &\iff \widetilde{M} = L_{N_0} \text{ for some } N_0 \in \mathbb{N} \\ &\iff I^m M_{N_0} = M_{m+N_0} \quad \forall m \geq 0 \\ &\iff \{M_i\} \text{ is } I\text{-stable} \end{aligned}$$

$\because \widetilde{N} := \bigoplus_{n=0}^{\infty} N_n t^n$ is a S -submodule of $\widetilde{M} \therefore \widetilde{N}$ is a f.g. S -module and thus $\{N_i\}$ is I -stable. \square

Corollary 1.11.4 (Artin-Ress lemma). R : Noetherian, M : f.g. R -module, $I \subseteq R$, $N \subseteq M$. Then $\exists N_0 \in \mathbb{N}$ s.t.

$$I^{N_0+m} M \cap N = I^m (I^{N_0} M \cap N) \quad \forall m \geq 0$$

Proof: Let $M_n = I^n M \rightsquigarrow N_n = I^n M \cap N$. By general form of Artin-Ress lemma, $\{N_n\}$ is I -stable i.e. $\exists N_0 \in \mathbb{N}$ s.t. $I^m N_{N_0} = N_{m+N_0}$ \square

Remark 1.11.1. N_0 is Artin-Ress lemma is necessarily. Look at a example :

Let $R = k[x]$, $M = R$, $I = \langle x \rangle$, $N = \langle x \rangle$, then

$$\begin{aligned} I^2 M \cap N &= \langle x^2 \rangle \cap \langle x \rangle = \langle x^2 \rangle, \quad I^2 (M \cap N) = \langle x^2 \rangle \langle x \rangle = \langle x^3 \rangle \\ I^n (M^2 \cap N) &= \langle x^n \rangle \langle x^2 \rangle = \langle x^{n+2} \rangle, \quad I^{n+2} M \cap N = \langle x^{n+2} \rangle \cap \langle x \rangle = \langle x^{n+2} \rangle \end{aligned}$$

Theorem 1.11.3 (Krull theorem). R : Noetherian, $I \subseteq J_R$, M : f.g. R -module.

Then $\bigcap_{n=0}^{\infty} I^n M = \langle 0 \rangle$

Proof: Let $N = \bigcap_{n=0}^{\infty} I^n M \subseteq M$ is f.g. since M is Noetherian. And $N \cap I^n M = N \quad \forall n \geq 0$

By Artin-Ress lemma, $\exists N_0 \in \mathbb{N}$ s.t. $I^m (I^{N_0} M \cap N) = I^{N_0+m} M \cap N \quad \forall m \geq 0$.

$\implies IN = N$. By Nakayama's lemma, $N = 0$. \square

Corollary 1.11.5. $(R, m) : \text{Noetherian local}$, then $\bigcap_{n=0}^{\infty} m^n = 0$
 $(\forall x \in R, \exists k \text{ s.t. } x \in m^k \text{ but } x \notin m^{k+1} \text{ and we get a graded ring structure on } R)$

1.12 Hilbert polynomial

In this section, R is commutative and we will use the definition and result in Homework 09

Definition 1.12.1.

- Let G be an abelian group and $\varphi : \mathfrak{M}_R \rightarrow G$, where \mathfrak{M} collect all R -module. φ is called an **Euler-Poincaré mapping** if $\forall 0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$, $\varphi(M_2) = \varphi(M_1) + \varphi(M_3)$ and $\varphi(0) = 0$

- R : graded Noetherian, M : f.g. graded R -module. Say $R = R_0[a_1, \dots, a_n]$, where $a_i \in R_{d_i}$ and $M = \langle x_1, \dots, x_m \rangle_R$ with $x_i \in M_{\ell_i}$ and M_i : f.g. R_0 -module.

For given $\varphi : \mathfrak{M}_{R_0}^{<\infty} \rightarrow \mathbb{Z}$ is an Euler-Poincaré mapping, define **Poincaré series** of M is

$$P_{\varphi}(M, t) := \sum_{i=0}^{\infty} \varphi(M_i) t^i \in \mathbb{Z}[[t]]$$

- $p(z) \in \mathbb{Q}[z]$ is called a **numerical polynomial** if $P(n) \in \mathbb{Z}, \forall n \gg 0$

Property 1.12.1. If $p(z)$ is numerical, then $\exists c_0, c_1, \dots, c_r \in \mathbb{Z}$ s.t.

$$p(z) = c_0 \binom{z}{r} + c_1 \binom{z}{r-1} + \dots + c_{r-1} \binom{z}{1} + c_r, \text{ where } \binom{z}{k} = \frac{z(z-1)\dots(z-k+1)}{k!}$$

In particular, $p(n) \in \mathbb{Z} \forall n \in \mathbb{Z}$.

Proof: By induction on $\deg p : \deg p = 0 \rightsquigarrow p(z) = c \in \mathbb{Z}$ OK!

Since $\binom{z}{r} = \frac{z^r}{r!} + \dots, \binom{z}{0} = 1, \left\{ \binom{z}{r} : r \in \mathbb{Z}_{\geq 0} \right\}$ forms a basis for $\mathbb{Q}[z]$ over \mathbb{Q} . We can write $p(z) = \sum_{k=0}^r c_{r-k} \binom{z}{k}$ with $c_i \in \mathbb{Q}$. Note $\binom{z+1}{r} = \binom{z}{r} + \binom{z}{r-1}$
 $\rightsquigarrow p(z+1) - p(z) = \sum_{k=0}^{r-1} c_{r-1-k} \binom{z}{k}$ and $\deg(p(z+1) - p(z)) < \deg p(z)$. By induction hypothesis, $c_0, \dots, c_{r-1} \in \mathbb{Z}$. $c_r = P(n) - \left(c_0 \binom{n}{r} + \dots + c_{r-1} \binom{n}{1} \right) \in \mathbb{Z}$ for some $n \gg 1$ \square

Property 1.12.2. If $f : \mathbb{Z} \rightarrow \mathbb{Z}$ s.t. $f(n+1) - f(n) = Q(n)$ with Q : numerical $\forall n \gg 1$, then $f(n) = p(n) \forall n \gg 0$ for some numerical polynomial $p(z)$.

Proof: Write $Q(n) = \sum_{k=0}^r c_{r-k} \binom{z}{k}$ with $c_i \in \mathbb{Z}$. Let $\tilde{p}(z) = \sum_{k=0}^r c_{r-k} \binom{z}{k+1}$. Then $\tilde{p}(z+1) - \tilde{p}(z) = Q(z) \rightsquigarrow \tilde{p}(n+1) - f(n+1) = \tilde{p}(n) - \tilde{f}(n) \forall n \gg 0 \rightsquigarrow \tilde{p}(n) - f(n)$ is a constant $c_{r+1} \in \mathbb{Z} \forall n \gg 0$. Then $f(n) = \tilde{p}(n) - c_{r+1}$ is numerical polynomial. \square

Theorem 1.12.1 (Hilbert-Serre).

- (1) $P_\varphi(M, t) = \frac{f(t)}{\prod_{i=1}^n (1 - t^{d_i})}$ for some $f(t) \in \mathbb{Z}[t]$
- (2) If $d_i = 1 \forall i = 1 \sim n$, $P_\varphi(M, t) = \frac{h(t)}{(1-t)^d}$ for $(1-t) \nmid h(t)$, then $\exists! p(z) \in \mathbb{Q}[z]$ of $\deg = d-1$ s.t. $\varphi(M_n) = p(n) \forall n \gg 0$

Proof:

- (1) By induction of $n : n = 0 \rightsquigarrow R = R_0 \rightsquigarrow M : \text{f.g. } R_0\text{-module} \rightsquigarrow M_n = 0 \forall n \gg 0$. Then $P_\varphi(M, t) \in \mathbb{Z}[t]$ OK!

Now, let $n > 0$. Consider

$$0 \longrightarrow \ker(\cdot a_n) =: K_i \longrightarrow M_i \xrightarrow{\cdot a_n} M_{i+d_n} \longrightarrow \text{coker}(\cdot a_n) =: L_{i+d_n} \longrightarrow 0$$

Let $K = \bigoplus_{i=0}^{\infty} K_i \subseteq M, L = \bigoplus_{i=0}^{\infty} L_i = M / \sim : \text{f.g. } R\text{-module which are annihilated by } a_n$, so they are f.g. $R[a_1, \dots, a_{n-1}]$ -module. Also,

$$\begin{cases} 0 \rightarrow K_i \rightarrow M_i \rightarrow \text{Im}(\cdot a_n) \rightarrow 0 \\ 0 \rightarrow \text{Im}(\cdot a_n) \rightarrow M_{i+d_n} \rightarrow L_{i+d_n} \rightarrow 0 \end{cases}$$

Then $\varphi(K_i) - \varphi(M_i) + \varphi(M_{i+d_n}) - \varphi(L_{i+d_n}) = 0$, then

$$t^{d_n}(\varphi(K_i)t^i - \varphi(M_i)t^i) + \varphi(M_{i+d_n})t^{i+d_n} - \varphi(L_{i+d_n})t^{i+d_n} = 0 \quad (*)$$

Sum $(*)$ over i from 0 to ∞

$$t^{d_n}P_\varphi(K, t) - t^{d_n}P_\varphi(M, t) + P_\varphi(M, t) - P_\varphi(L, t) - g(t) = 0$$

for some $g(t) \in \mathbb{Z}[t]$. By induction hypothesis, $P_\varphi(K, t), P_\varphi(L, t)$ are form

$$\frac{h(t)}{\prod_{i=1}^{n-1} (1 - t^{d_i})}$$

and thus

$$P_\varphi(M, t) = \frac{1}{1 - t^{d_n}} (P_\varphi(L, t) - t^{d_n}P_\varphi(K, L) + g(t)) = \frac{f(t)}{\prod_{i=1}^n (1 - t^{d_i})}$$

for some $f(t) \in \mathbb{Z}[x]$

- (2) By (1), write $P_\varphi(M, t) = h(t)/(1-t)^d$ with $(1-t) \nmid h(t)$, $h(t) = \sum_{i=0}^N a_i t^i$, $a_i \in \mathbb{Z}$.

Since

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{-d}{k} (-t)^k = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k$$

The coefficient of t^n ($\forall n \geq N$) in $P_\varphi(M, t)$ is

$$\varphi(M_n) = \sum_{i=0}^N a_i \binom{d+n-i-1}{d-1} = \left(\sum_{i=0}^N a_i \right) n^{d-1} + \dots$$

and $\sum_{i=0}^N a_i = h(1) \neq 0 \rightsquigarrow$ it is a polynomial with degree $d-1$

□

Theorem 1.12.2. (R, m) : Noetherian, local, M : f.g. R -module, $k = R/m$. Then

- (1) $\dim_k \left(M/m^\ell M \right) < \infty$
- (2) Let d be the least number of generators of m . Then \exists a polynomial $g(z) \in \mathbb{Q}[z]$ of $\deg \leq d$ s.t. $g(n) = \dim_k \left(M/m^n M \right) \quad \forall n \gg 0$

Proof:

- (1) $M/m^\ell M$ can be regarded as a R/m -vector space. By Homework 9, $\text{gr}_m(M)$ is a f.g. graded $\text{gr}_m(R)$ -module and thus $m^\ell M/m^{\ell+1} M$ is a f.g. R/m -module ($\rightsquigarrow k$ -finite dimensional v.s.)

Claim: $\dim_k \left(M/m^\ell M \right) = \sum_{r=1}^{\ell} \dim_k \left(m^{r-1} M/m^r M \right) < \infty$

p.f. By induction on ℓ : $\ell = 1$ OK!

For $\ell > 1$,

$$\begin{aligned} 0 \rightarrow m^{\ell-1} M/m^\ell M \rightarrow M/m^\ell M \rightarrow M/m^{\ell-1} M \rightarrow 0 \\ \implies \dim_k \left(M/m^\ell M \right) = \dim_k \left(m^{\ell-1} M/m^\ell M \right) + \dim_k \left(M/m^{\ell-1} M \right) \\ = \sum_{r=1}^{\ell} \dim_k \left(m^{r-1} M/m^r M \right) \end{aligned}$$

- (2) Let $\langle a_1, \dots, a_d \rangle_R = m$. Then $\text{gr}_m(R) = R/m[\bar{a}_1, \dots, \bar{a}_d]$, where $\bar{a}_i \in m/m^2$. By Hilbert-Serre, $\exists!$ $p(z) \in \mathbb{Q}[z]$ of $\deg \leq d-1$ s.t.

$$p(n) = \dim_k \left(m^n M/m^{n+1} M \right) \quad \forall n \gg 0$$

$$\text{Thus, } \dim_k \left(M/m^{n+1} M \right) - \dim_k \left(M/m^n M \right) = \dim_k \left(m^n M/m^{n+1} M \right) = p(n)$$

$\forall n \gg 0$. By Property 1.12.2, $\exists g(z) \in \mathbb{Q}[z]$ with $\deg \leq d$ s.t.

$$g(n) = \dim_k \left(M/m^n M \right) \quad \forall n \gg 0$$

□

Definition 1.12.2.

- A chain $M = M_0 \supset M_1 \supset \cdots \supset M_r = 0$ is called a **composition series** if M_{i-1}/M_i is **simple** i.e. no submodule except 0 and itself.
- r is called the **length** of composition series.

The well-defined of length is by the following theorem.

Theorem 1.12.3 (Jordan-Hölder theorem). If M has a composition series, then two composition series have the same length and the same factors up to permutation. (By Butterfly lemma and Schreier refinement theorem)

Proposition 1.12.1. TFAE

- (1) M has a composition series
- (2) M is both Noetherian and **Artinian** (Have DCC)

Proof: (1) \Rightarrow (2) : Let $\ell(M) = n$. If $\exists 0 = N_1 \subsetneq N_2 \subsetneq \cdots$ in M , then

$$C : M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0 \text{ where } M_i = N_{n+1-i}$$

We know $\tilde{C} : a$ refinement of C s.t. \tilde{C} is a composition series $\rightsquigarrow \ell(\tilde{C}) = n = \ell(C) \rightsquigarrow C = \tilde{C}$, but $M/N_1 = M/N_n$ is not simple. ($\rightarrow \leftarrow$)

Similarly, it is also true for Artinian property.

(2) \Rightarrow (1) : $\because M$ is Noetherian $\therefore \exists$ a maximal proper submodule M_1 of $M \rightsquigarrow M/M_1$: simple and \exists a maximal proper submodule M_{i+1} of $M_i \rightsquigarrow M_i/M_{i+1}$: simple i.e. $M = M_0 \supsetneq M_1 \supsetneq \cdots$. Since M is Artinian, $\exists n$ s.t. $M_n = 0$ □

1.13 Indecomposable module

In this section, we want to decompose the module in suitable condition. So we see some property first.

1.13.1 Krull-Remak-Schmidt theorem

Let A be a ring and M be a Noetherian and Artinian A -module. Let $f \in \text{End}_A(M)$, then

$$\text{Im } f \supseteq \text{Im } f^2 \supseteq \cdots \xrightarrow{\text{Artinian}} \exists n \in \mathbb{N} \text{ s.t. } \text{Im } f^n = \text{Im } f^{n+1} = \cdots =: \text{Im } f^\infty$$

$$\ker f \subseteq \ker f^2 \subseteq \cdots \xrightarrow{\text{Noetherian}} \exists m \in \mathbb{N} \text{ s.t. } \ker f^m = \ker f^{m+1} = \cdots =: \ker f^\infty$$

Say $\text{Im } f^\infty = \text{Im } f^n$ and $\ker f^\infty = \ker f^n$ for some n .

Lemma 1.13.1 (Fitting lemma).

- (1) $M = \text{Im } f^\infty \oplus \ker f^\infty$
- (2) $f|_{\text{Im } f^\infty}$ is an automorphism
- (3) $f|_{\ker f^\infty}$ is nilpotent

Proof:

- (1) • If $x \in \text{Im } f^\infty \cap \ker f^\infty$, say $f^n(z) = x$ and $0 = f^n(x) = f^{2n}(z)$
 $\implies z \in \ker f^{2n} = \ker f^n \rightsquigarrow x = 0$
 • $\forall x \in M, f^n(x) \in \text{Im } f^n = \text{Im } f^{2n} \implies f^n(x) = f^n(y)$ for some $y \in \text{Im } f^n$
 $\implies x - y \in \ker f^n \rightsquigarrow x \in \ker f^n + \text{Im } f^n = \ker f^\infty + \text{Im } f^\infty$
- (2) $f|_{\text{Im } f^\infty} : \text{Im } f^\infty \rightarrow \text{Im } f^\infty$ is surjective. If $f^n(x) \in \ker f|_{\text{Im } f^\infty}$, then $f^{n+1}(x) = 0 \rightsquigarrow x \in \ker f^{n+1} = \ker f^n \rightsquigarrow f^n(x) = 0$
- (3) $f|_{\ker f^\infty} : \ker f^\infty \rightarrow \ker f^\infty, f^n(x) = 0 \forall x \in \ker f^\infty \rightsquigarrow f^n = 0$

□

Definition 1.13.1.

- M is **decomposable** if $M = M_1 \oplus M_2$ with $M_1, M_2 \subsetneq M$
- M is **indecomposable** if M is not decomposable.

Property 1.13.1. Let M be indecomposable and Noetherian + Artinian. Then

- (1) $\forall f \in \text{End}(M)$, f is either an auto. or a nilpotent.
- (2) $\text{End}(M)$ is a non-commutative local ring.
 (i.e. the set of non-unit is a two-side ideal)

Proof:

- (1) By Fitting lemma, one of $\ker f^\infty, \text{Im } f^\infty$ is 0. The former is auto, the latter is nilpotent.
- (2) Let $I = \text{End}(M) \setminus \{\text{unit}\}$. For $f \in I$, f is nilpotent i.e. $M = \ker f^\infty$.
 • $\forall g \in \text{End}(M)$. Notice that $\text{Im } f^n = 0 \iff \ker f^n = M$.
 • If $\ker f = M \rightsquigarrow (gf)(x) = 0 \forall x \in M \rightsquigarrow gf$ is not 1 $\rightsquigarrow gf \in I$
 If $\ker f^{n-1} \subsetneq \ker f^n = M \rightsquigarrow \text{Im } f^{n-1} \neq 0 \exists f^{n-1}(x) \neq 0$, then $gf(f^{n-1}(x)) = 0 \rightsquigarrow gf \in I$
 • $fg(M) \subseteq f(M) \neq M$, otherwise $f(M) = M \rightsquigarrow \text{Im } f = M$. By Fitting lemma, $\ker f^\infty = 0 \implies f$ is an auto. ($\rightarrow \leftarrow$). Hence, fg is not onto $\rightsquigarrow fg \in I$
 • $f_1, f_2 \in I$. If $f_1 + f_2$ is auto, then define $\begin{cases} h_1 = f_1(f_1 + f_2)^{-1} \\ h_2 = f_2(f_1 + f_2)^{-1} \end{cases} \implies h_1 + h_2 = 1$.
 Then $h_2 = 1 - h_1$ and $h_2^{-1} = 1 + h_1 + h_1^2 + \dots + h_1^{r-1}$ (if $h_1^r = 0$) $\rightsquigarrow h_2 \notin I$ ($\rightarrow \leftarrow$)

□

Property 1.13.2. Let M, N be A -modules and N indecomposable. If $f : M \rightarrow N$ and $g : N \rightarrow M$ s.t. gf is auto, then f, g are isomorphism.

Proof: It is clear that f is 1-1 and g is onto. Let $e = f(gf)^{-1}g \rightsquigarrow e^2 = f(gf)^{-1}gf(gf)^{-1}f = e \rightsquigarrow e(e-1) = 0$. If $e, 1-e \neq 0$, then $e(1-e) = 0$ and $1 = e + (1-e) \implies N = \text{Im } e \oplus \text{Im}(1-e) (\rightarrow \leftarrow)$. So $e = 0$ or $e = 1$. Also, $gef = gf(gf)^{-1}gf = gf$ is auto $\implies e \neq 0 \rightsquigarrow e = 1$. Hence, g is 1-1 and f is onto. □

Theorem 1.13.1 (Krull-Remak-Schmidt theorem). Let $M \neq 0$ be Noetherian and Artinian. Then $M = M_1 \oplus \cdots \oplus M_r$ with M_i : indecomposable and if

$$M = M_1 \oplus \cdots \oplus M_r = N_1 \oplus \cdots \oplus N_s$$

with M_i, N_j are indecomposable, then $r = s$ and $M_i \simeq N_i$ after rearrangement of indices.

Proof:

- **Existence:** If M is indecomposable, then done!

Otherwise, $M = E_1 \oplus E_2$. If E_1 is indecomposable, then done!

Otherwise, $E_1 = E_{11} \oplus E_{12}$. If E_{11} is indecomposable, then done!

Otherwise, $E_{11} = E_{21} \oplus E_{22}$. If E_{21} is indecomposable, then done! ...

Then $\exists M_1 \supsetneq E_1 \supsetneq E_{11} \supsetneq E_{21} \supsetneq \cdots$. Since M is Artinian, $\exists n$ s.t. E_n is indecomposable i.e. M contains an indecomposable component M_1 and $M = M_1 \oplus M'_1$. Similarly, M'_1 contains an indecomposable component M_2 and $M'_1 = M_2 \oplus M'_2$

Then $\exists M'_{r-1}$: indecomposable and $M = M_1 \oplus \cdots \oplus M_{r-1} \oplus M'_{r-1}$. Otherwise, $M_1 \subsetneq M_1 \oplus M_2 \subsetneq \cdots$ which is contradict to Noetherian.

- **Uniqueness:** Let $e_i : M \rightarrow M_i$, $p_j : M \rightarrow N_j$. Set $f_j = e_1 p_j$, $g_j = p_j e_1$, then $f_j g_j = e_1 p_j^2 e_1 = e_1 p_j e_1 \forall j$. So

$$\sum_{j=1}^s f_j g_j = e_1 \left(\sum_{j=1}^s p_j \right) e_1 = e_1^2 = e_1 \implies \left(\sum_{j=1}^s f_j g_j \right) \Big|_{M_1} = \text{id}_{M_1}$$

Since all nilpotent element will form an ideal, there exists j s.t. $(f_j g_j)|_{M_1}$ is an auto.

Notice that $g_j|_{M_1} = p_j|_{M_1}$ and $f_j|_{N_j} = e_1|_{N_j}$. We can let $N_j = N_1$ by renumbering. Then $g_1|_{M_1} : M_1 \rightarrow N_1, f_1|_{N_1} : N_1 \rightarrow M_1$ with $f_1|_{N_1} \circ g_1|_{M_1} = (f_1 g_1)|_{M_1}$ is auto. By Property 1.13.2, f_1 is isomorphism i.e. $M_1 \simeq N_1$.

Claim: $M = N_1 \oplus (M_2 \oplus \cdots \oplus M_r)$

$p f$. $\ker e_1 = M_2 \oplus \cdots \oplus M_r$ and $e_1|_{N_1}$ is 1-1 $\rightsquigarrow N_1 \cap \ker e_1 = \{0\}$

$\forall x \in M, e_1(x) \in M_1$ and by $e_1|_{N_1} : N_1 \xrightarrow{\sim} M_1, e(x) = e(y)$ for some $y \in N_1 \rightsquigarrow x - y \in \ker e_1 \rightsquigarrow x \in N_1 + \ker e_1$ \square

So $M = N_1 \oplus M_2 \oplus \cdots \oplus M_r = N_1 \oplus N_2 \oplus \cdots \oplus N_s$ and quotient N_1 in both side, then $M_2 \oplus \cdots \oplus M_r \simeq N_2 \oplus \cdots \oplus N_s$. By induction on $r, r - 1 = s - 1 \implies r = s$ and $M_i \simeq N_i \forall i = 2, \dots, r$ after rearrangement of $\{N_i\}$. \square

1.13.2 Commutative Artinian ring

Property 1.13.3.

(1) An Artinian domain R is a field.

pf. If $x \in R$, then $\langle x \rangle \supseteq \langle x^2 \rangle \supseteq \cdots \implies \langle x^n \rangle = \langle x^{n+1} \rangle$, say $x^n = yx^{n+1} \rightsquigarrow x^n(1 - yx) = 0 \rightsquigarrow yx = 1$

(2) If R is Artinian, then $\text{Max } R = \text{Spec } R$

pf. $\forall p \in \text{Spec } R, R/p$ is Artinian integral domain is a field, then $p \in \text{Max } R$

(3) If R is Artinian, then $|\text{Max } R| < \infty$

pf. Let $\mathcal{S} = \{\bigcap_{\text{finite}} m : m \in \text{Max } R\} \neq \emptyset$. Then \exists a minimal element say $m_1 \cap \cdots \cap m_r$. Now, for $m \in \text{Max } R, m \cap m_1 \cap \cdots \cap m_r = m_1 \cap \cdots \cap m_r \implies m \supseteq m_1 \cap \cdots \cap m_r$. By prime avoidance lemma, $m \supseteq m_i$ for some i .

(4) If R is Artinian and $\text{Max } R = \{m_1, \dots, m_\ell\}$, then $\exists n_1, \dots, n_\ell \in \mathbb{N}$ s.t.

$$\langle 0 \rangle = \prod_{i=1}^{\ell} m_i^{n_i} = \bigcap_{i=1}^{\ell} m_i^{n_i}$$

pf. $\sqrt{m_i^{n_i} + m_j^{n_j}} = \sqrt{\sqrt{m_i^{n_i}} + \sqrt{m_j^{n_j}}} = \sqrt{m_i + m_j} = \sqrt{R} = R \rightsquigarrow m_i^{n_i} + m_j^{n_j} = R$ for distinct i, j . So $m_i^{n_i}, m_j^{n_j}$ are coprime and thus

$$\prod_{i=1}^{\ell} m_i^{n_i} = \bigcap_{i=1}^{\ell} m_i^{n_i}$$

Since R is Artinian, $\forall i, \exists n_i$ s.t. $m_i^{n_i} = m_i^{n_i+1} = \cdots$.

If $m_1^{n_1} \cdots m_\ell^{n_\ell} \neq 0$, then $\mathcal{S} = \{J \subseteq R | Jm_1^{n_1} \cdots m_\ell^{n_\ell} \neq 0\} \neq \emptyset$ since $m_1 \in \mathcal{S}$. Let J_0 be a minimal element of \mathcal{S} . Pick $0 \neq x \in J_0$, then $\langle x \rangle \in \mathcal{S}$ and $\langle x \rangle \subseteq J_0 \implies \langle x \rangle = J_0$. Now, $xm_1^{n_1} \cdots m_\ell^{n_\ell} = xm_1^{n_1+1} \cdots m_\ell^{n_\ell+1} \implies \langle x \rangle \supseteq xm_1 \cdots m_\ell \in \mathcal{S} \rightsquigarrow xm_1 \cdots m_\ell = \langle x \rangle \rightsquigarrow (m_1 \cdots m_\ell)_{\subseteq J_R}(Rx) = Rx$. By Nakayama's lemma, $Rx = 0 \rightsquigarrow x = 0 (\rightarrow \leftarrow)$.

(5) R : Artinian, then

$$R = R/\langle 0 \rangle = R/m_1^{n_1} \cdots m_\ell^{n_\ell} \simeq \prod_{i=1}^{\ell} R/m_i^{n_i}$$

$\rightsquigarrow R/m_j^{n_j}$: Artinian and the only maximal ideal is $m_j/m_j^{n_j}$.

(Since $m/m_j^{n_j} \in \text{Max } R/m_j^{n_j} \rightsquigarrow m_j^{n_j} \subseteq m \in \text{Max } R \implies m = m_j$)

If we want to research the commutative Artinian ring, we only need to research the property of commutative local Artinian ring.

Chapter 2

Homological algebra

In this chapter, we will leave some check for Homework and will be use it in class naturally.

2.1 Projective, injective and flat module

Observation: $0 \rightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \rightarrow 0$ be exact in ${}_R\mathfrak{M}$. For $M, N \in {}_R\mathfrak{M}$,

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_R(M, M_1) & \xrightarrow{\bar{\alpha}} & \text{Hom}_R(M, M_2) & \xrightarrow{\bar{\beta}} & \text{Hom}_R(M, M_3) \text{ exact} \\ & & f & \longmapsto & \alpha \circ f & g & \longmapsto \beta \circ g \\ \\ 0 & \longrightarrow & \text{Hom}_R(M_3, N) & \xrightarrow{\bar{\beta}} & \text{Hom}_R(M_2, N) & \xrightarrow{\bar{\alpha}} & \text{Hom}_R(M_1, N) \text{ exact} \\ & & f & \longmapsto & f \circ \beta & g & \longmapsto g \circ \alpha \end{array}$$

For $M \in \mathfrak{M}_R$,

$$M \otimes_R M_1 \xrightarrow{1 \otimes \alpha} M \otimes_R M_2 \xrightarrow{1 \otimes \beta} M \otimes_R M_3 \longrightarrow 0 \text{ exact}$$

Those property in above please check by yourself.

Notice that it will not from a complete short exact sequence, we see some example.

Example 2.1.1.

- $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$ in $\mathfrak{M}_{\mathbb{Z}}$
 - $M = \mathbb{Z}/2\mathbb{Z}$: If $f \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q})$ and $f : \bar{1} \rightarrow x \rightsquigarrow 2x = 0 \rightsquigarrow x = 0 \rightsquigarrow f = 0$. But $0 \neq g : \bar{1} \rightarrow \bar{1}/2$ in $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ so it will not surjective.
 - $N = \mathbb{Z}$: If $f \in \text{Hom}(\mathbb{Q}, \mathbb{Z})$, since $f(\mathbb{Q}) \subseteq \mathbb{Z}$ is PID, say $f(\mathbb{Q}) = n\mathbb{Z}$ and $r \mapsto n \rightsquigarrow r/2 \mapsto n/2 \notin n\mathbb{Z}$ if $n \neq 0 \rightsquigarrow f = 0$. But $\text{Hom}(\mathbb{Z}, \mathbb{Z}) \neq 0$.
- $0 \rightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$
 - $M = \mathbb{Z}/2\mathbb{Z}$, then $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \xrightarrow{2 \otimes 1} \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}$ not injective since $0 \neq \bar{1} \otimes 1 \mapsto \bar{0} \otimes 1 = 0$

Definition 2.1.1.

- $M \in {}_R\mathfrak{M}$ is **projective** if $\text{Hom}(M, \cdot)$ preserves the right exactness.
- $N \in {}_R\mathfrak{M}$ is **injective** if $\text{Hom}(\cdot, N)$ preserves the right exactness
- $M \in \mathfrak{M}_R$ is **flat** if $M \otimes \cdot$ preserves the left exactness.

Fact 2.1.1.

- M is projective $\iff \forall M_2 \twoheadrightarrow M_3$ and $\forall f \in \text{Hom}(M, M_3)$ we have

$$\begin{array}{ccccc} & & M & & \\ & \swarrow \exists \tilde{f} & \downarrow f & & \\ M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$$

We called \tilde{f} is a lifting of f .

- N is injective $\iff \forall M_1 \hookrightarrow M_2$ and $\forall f \in \text{Hom}(M_1, N)$ we have

$$\begin{array}{ccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 \\ & & \downarrow f & \swarrow \exists \tilde{f} & \\ & & N & & \end{array}$$

We called \tilde{f} is an extension of f .

- free \implies projective

$$\begin{array}{ccccc} & & F & & \\ & \swarrow \exists \tilde{f} & \downarrow f & & \\ M_2 & \xrightarrow{g} & M_3 & \longrightarrow & 0 \end{array}$$

Let F be free on $X = \{x_i : i \in \Lambda\}$ and $f(x_i) = b_i$. Since g is surjective, $\exists a_i \in M_2$ s.t. $g(a_i) = b_i$. Then map $X \rightarrow M_2$ by $x_i \rightarrow a_i$ and by the universal property of free module, $\exists \tilde{f} : F \rightarrow M_2$ s.t. $\tilde{f}(x_i) = a_i$ and thus the diagram commute.

- free \implies flat : Say $F \simeq R^n$ where n may not be finite, then $0 \rightarrow M_1 \rightarrow M_2 \implies 0 \rightarrow M_1^{\oplus n} \rightarrow M_2^{\oplus n}$ and thus $0 \rightarrow R^n \otimes M_1 \rightarrow R^n \otimes M_2$.
- S : m.c. in R , $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ exact, then

$$0 \rightarrow (M_1)_S \rightarrow (M_2)_S \rightarrow (M_3)_S \rightarrow 0$$

and notice that $M_S = R_S \otimes_R M$, so R_S is flat R -module.

In particular, \mathbb{Q} is flat \mathbb{Z} -module.

Goal:

- It's known that for any $M = \langle X \rangle_R \in {}_R\mathfrak{M}$, $\exists F$: free on X and $\begin{array}{ccccc} F & \longrightarrow & M & \longrightarrow & 0 \\ e_i & \longmapsto & x_i \in X & & \end{array}$

- Now we want to do the “dual” version : for any $M \in {}_R\mathfrak{M}$, there exists injective R -module N s.t. $0 \rightarrow M \rightarrow N$

Theorem 2.1.1 (Baer’s criterion). N is injective \iff

$$\begin{array}{ccccc} \forall : 0 & \longrightarrow & I & \longrightarrow & R \\ & & \downarrow f & \swarrow \exists \tilde{f} & \\ & & N & & \end{array}$$

Proof: (\Rightarrow) : OK!

(\Leftarrow) : For given $0 \rightarrow M_1 \xrightarrow{\alpha} M_2$ and $g : M_1 \rightarrow N$, consider

$$\mathcal{S} := \{(M, \rho) : M \subseteq M_2, \rho \text{ extends } g\} \neq \emptyset$$

since $(M_1, g) \in \mathcal{S}$. By the routine argument of Zorn’s lemma, \exists a maximal element (M^*, μ) in \mathcal{S} .

Claim: $M^* = M_2$

p.f. Assume $M^* \subsetneq M_2$. Pick $x \in M_2 \setminus M^*$ and put $M' = M^* + Rx$. Let $I = \{r \in R : rx \in M^*\}$. Define $f : I \rightarrow N$ by $r \mapsto \mu(rx)$, then we can extend $f : I \rightarrow N$ to $h : R \rightarrow N$. Now, define

$$\begin{array}{ccc} \mu' : M' & \longrightarrow & N \\ z + rx & \longmapsto & \mu(z) + h(r) \end{array}$$

Well-defined : $z_1 + r_1x = z_2 + r_2x \implies z_1 - z_2 = (r_2 - r_1)x \rightsquigarrow (r_2 - r_1) \in I$
 $h(r_2) - h(r_1) = h(r_2 - r_1) = \mu((r_2 - r_1)x) = \mu(z_1 - z_2) = \mu(z_1) - \mu(z_2)$.

Then $(M', \mu') \geq (M^*, \mu)$ ($\rightarrow \leftarrow$). □

Property 2.1.1 (key property).

- Every injective module N over an integral domain R is **divisible** i.e. $\forall x \in N, r \in R \setminus \{0\}, \exists y \in N$ s.t. $x = ry$ i.e. $rN = N$
- Every divisible module N over a PID R is injective
(Over a PID, divisible \iff injective)

Proof:

- $\forall x_0 \in N, r_0 \in R \setminus \{0\}$, define $g : Rr_0 \rightarrow N$ which is well-defined by ID. By Baer’s criterion, $\exists h$ extends g :

$$\begin{array}{ccccc} 0 & \longrightarrow & Rr_0 & \longrightarrow & R \\ & & \downarrow g & \swarrow \exists h & \\ & & N & & \end{array}$$

let $y_0 = h(1) \rightsquigarrow r_0y_0 = r_0h(1) = h(r_0) = x_0$

- For given $I \subseteq R$ $f : I \rightarrow N$, say $I = \langle r_0 \rangle$ and $f : r_0 \mapsto x_0$. let $y_0 \in R$ s.t. $r_0 y_0 = x_0$. Define $h : R \rightarrow N$ by $h(1) = y_0$, then $h(rr_0) = rh(r_0) = rx_0 = g(rr_0)$ i.e. $h|_I = f$.

□

Theorem 2.1.2 (Main theorem). $\forall M \in {}_R\mathfrak{M}, \exists N \in {}_R\mathfrak{M} : \text{injective s.t. } M \hookrightarrow N$

Proof:

- We consider the case of \mathbb{Z} -module first :

$$0 \longrightarrow \ker f \longrightarrow F \xrightarrow{f} M \longrightarrow 0 \rightsquigarrow M \simeq F/\ker f$$

Say $F = \bigoplus_{i \in \Lambda} \mathbb{Z}e_i$. Consider $F' := \mathbb{Q} \otimes F = \bigoplus_{i \in \Lambda} \mathbb{Q}e_i$ which is injective \mathbb{Z} -module and $F'/\ker f$ is also injective, since $mF' = F'$ and $m(F'/\ker f) = F'/\ker f$ for all $m \in \mathbb{Z} \setminus \{0\}$. Then $M \simeq F/\ker f \hookrightarrow F'/\ker f$

- General R : As above, regard M as a abelian group, then $M \hookrightarrow N_0 : \text{injective } \mathbb{Z}\text{-module. Write } N = \text{Hom}_{\mathbb{Z}}(R, N_0) \text{ which is } R\text{-module.}$

Claim: N is injective

pf. Given $0 \rightarrow M_1 \rightarrow M_2$ with $f : M_1 \rightarrow N$, define $f' : M_1 \rightarrow N_0$ by $x \mapsto f(x)(1)$. By $N_0 : \text{injective}$, $\exists h' : M_2 \rightarrow N_0$ extends $f' : M_1 \rightarrow N_0$, then $h' \in \text{Hom}_{\mathbb{Z}}(M_2, N_0)$ has right R -module structure. Now define

$$\begin{aligned} h : M_2 &\longrightarrow N \\ x &\longmapsto h(x) : r \mapsto rh'(x) \end{aligned}$$

Finally, we will check those condition :

- $h(x) \in \text{Hom}_{\mathbb{Z}}(R, N_0)$

$$h(x)(r_1 + r_2) = (r_1 + r_2)h'(x) = r_1h'(x) + r_2h'(x) = h(x)(r_1) + h(x)(r_2)$$

- $h \in \text{Hom}_R(M_2, N)$

$$h(x_1+x_2)(r) = (x_1+x_2)h'(r) = h(x_1)(r) + h(x_2)(r) \forall r \rightsquigarrow h(x_1+x_2) = h(x_1) + h(x_2)$$

$$h(sx)(r) = rh'(sx) = r(h's)(x) = (h(x)s)(r)$$

- $h|_{M_1} = f : \text{Let } M_1 \xrightarrow{g} M_2 \text{ and } \forall x \in M_1$

$$\begin{aligned} h(g(x))(r) &= rh'(g(x)) = rf'(x) (\text{since } h' \circ g = f') \\ &= rf(x)(1) = f(x)(r) \forall r \in R \rightsquigarrow h \circ g = f \end{aligned}$$

□

Now, by $M \hookrightarrow N_0$ we have

$$M \simeq \text{Hom}_R(R, M) \hookrightarrow \text{Hom}_{\mathbb{Z}}(R, M) \hookrightarrow \text{Hom}_{\mathbb{Z}}(R, N_0) = N : \text{injective}$$

and get the goal.

□

Definition 2.1.2 (split). If $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ is called **split** if

$$M_2 = M_1 \oplus M_3$$

Note that $0 \rightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \rightarrow 0$ split if we can find a homomorphism $f' : M_1 \rightarrow M_2$ s.t. $f' \circ f = \text{id}_{M_1}$ or $g' : M_3 \rightarrow M_2$ s.t. $g \circ g' = \text{id}_{M_3}$.

Property 2.1.2 (Important property).

(1) TFAE

- (a) M is projective
- (b) $\forall 0 \rightarrow M_1 \rightarrow M_2 \rightarrow M \rightarrow 0$ split
- (c) $\exists M'$ s.t. $M \oplus M'$ is free

(2) TFAE

- (a) M is injective
- (b) $\forall 0 \rightarrow M \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ split exact

(3) projective \implies flat

Proof:

(1) • (a) \Rightarrow (b) : Since M is projective

$$\begin{array}{ccccc} & & M & & \\ & \swarrow \exists \mu & \downarrow \text{id} & & \\ M_2 & \xrightarrow{\beta} & M & \longrightarrow & 0 \end{array}$$

$$\text{s.t. } \beta \circ \mu = \text{id}$$

- (b) \Rightarrow (c) : $\exists F : \text{free s.t. } 0 \rightarrow \ker f \xrightarrow{f} M \rightarrow 0$. By assumption, $\ker f \oplus M \simeq F$ is free.
- (c) \Rightarrow (a) : For all $M_2 \rightarrow M_3 \rightarrow 0$ with $f : M \rightarrow M_3$. Since $M' \oplus M \simeq F : \text{free}$

$$\begin{array}{ccccccc} 0 & \longrightarrow & M' & \longrightarrow & F & \xrightarrow{\pi} & M \longrightarrow 0 : \text{split} \\ & & & & \downarrow \exists g & \swarrow f \circ \pi & \downarrow f \\ & & & & M_2 & \xrightarrow{\beta} & M_3 \longrightarrow 0 \end{array}$$

Since the above is split, $\exists \mu : M \rightarrow F$ s.t. $\pi \circ \mu = \text{id}_M$. Let $h := g \circ \mu$, then $\beta \circ h = f$

(2) • (a) \Rightarrow (b) : Since M is injective

$$\begin{array}{ccc} 0 & \longrightarrow & M \xrightarrow{\alpha} M_2 \\ & & \downarrow \text{id} \swarrow \exists \gamma \\ & & M \end{array}$$

s.t. $\gamma \circ \alpha = \text{id}_M$

- (b) \Rightarrow (a) : $\exists N$: injective s.t. $M \xrightarrow{i} N$ and consider $0 \rightarrow M \rightarrow N \rightarrow N/M \rightarrow 0$ is split, then $\exists \lambda : N \rightarrow M$ s.t. $\lambda \circ i = \text{id}_M$. Since N is injective, $\exists \tilde{f}_0$ extends f_0 . Let $\tilde{f} := \lambda \circ \tilde{f}_0$, then $\tilde{f} \circ \alpha = \lambda \circ f_0 = f$ i.e. $\tilde{f} : M_2 \rightarrow M$ is extension of $f : M_1 \rightarrow M$.

$$\begin{array}{ccc} 0 & \longrightarrow & M_1 \xrightarrow{\alpha} M_2 \\ & & \downarrow f \swarrow \exists \tilde{f} \\ & & M \\ & \nearrow f_0 & \downarrow i \swarrow \lambda \\ & & N \end{array}$$

(3) **Claim:** $\bigoplus_{i \in \Lambda} M_i$ is flat $\iff M_i$ is flat $\forall i$.

pf. For $\mathcal{C} : 0 \rightarrow N_1 \rightarrow N_2$,

$$\begin{aligned} \bigoplus_{i \in \Lambda} M_i \text{ is flat} &\iff 0 \rightarrow \left(\bigoplus_{i \in \Lambda} M_i \right) \otimes N_1 \rightarrow \left(\bigoplus_{i \in \Lambda} M_i \right) \otimes N_2 \quad \forall \mathcal{C} \\ &\iff \bigoplus_{i \in \Lambda} (M_i \otimes N_1) \rightarrow \bigoplus_{i \in \Lambda} (M_i \otimes N_2) \text{ is injective } \forall \mathcal{C} \\ &\iff M_i \otimes N_1 \rightarrow M_i \otimes N_2 \text{ is injective } \forall i \in \Lambda, \forall \mathcal{C} \\ &\iff M_i \text{ is flat } \forall i \in \Lambda \end{aligned}$$

□

Since $\exists M'$ s.t. $M \oplus M'$ is free and thus is flat, M is also flat by Claim.

□

Property 2.1.3. If $M_1, M_2, M_3 \in {}_R\mathfrak{M}$, then $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \rightarrow 0$: exact

$$\iff 0 \rightarrow \text{Hom}(M_3, N) \xrightarrow{\tilde{g}} \text{Hom}(M_2, N) \xrightarrow{\tilde{f}} \text{Hom}(M_1, N) : \text{exact } \forall N \in {}_R\mathfrak{M}$$

Proof: (\Rightarrow) : By observation.

(\Leftarrow) : We select specific R -module to get the conclusion.

- Let $N = M_3/g(M_2)$ and $i : M_3 \rightarrow N$, then $i \circ g = 0 \rightsquigarrow i = 0$ i.e. $M_3 = g(M_2) \rightsquigarrow g$ is onto.
- Let $N = M_3 \rightsquigarrow \text{id}_{M_3} \in \text{Hom}(M_3, N)$ and $0 = \tilde{f} \circ \tilde{g}(\text{id}_{M_3}) = g \circ f \rightsquigarrow \text{Im } f \subseteq \ker g$

- Let $N = M_2/f(M_1)$ and $i : M_2 \hookrightarrow N$, then $i \circ f = 0$ i.e. $i \in \ker \tilde{f} = \text{Im } \tilde{g}$, say $i = h \circ g$. If $x \in \ker g \rightsquigarrow x \in \ker i \rightsquigarrow x \in f(M_1) \rightsquigarrow \ker g \subseteq \text{Im } f$

□

Remark 2.1.1. Using Property 2.1.3 and the result in Homework 12-3, we can get tensor $(M \otimes \cdot)$ will preserve right exactness.

2.2 Homology functor

Definition 2.2.1.

- A **chain complex** C_\bullet of R -modules is a sequence and maps

$$C_\bullet : \cdots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \xrightarrow{d_1} C_0 \longrightarrow 0$$

s.t. $d_n d_{n+1} = 0 \rightsquigarrow \text{Im } d_{n+1} \subseteq \ker d_n$. It's closed to exact, but we want to know how close it between exact, so we define :

- $H_n(C_\bullet) := \ker d_n / \text{Im } d_{n+1}$ is called **n -th homology** of C_\bullet .
- $Z_n(C_\bullet) := \ker d_n$ is called **n cycle** and $B_n(C_\bullet) := \text{Im } d_n$ is called **n boundary**.

- A **cochain complex** C^\bullet of R -modules is a sequence and maps

$$C^\bullet : 0 \longrightarrow C^0 \xrightarrow{d_1} C^1 \xrightarrow{d_2} C^2 \cdots \longrightarrow C^m \xrightarrow{d_{n+1}} C^{n+1} \longrightarrow \cdots$$

s.t. $d_{n+1} d_n = 0 \rightsquigarrow \text{Im } d_n \subseteq \ker d_{n+1}$. Similarly, we define :

- $H^n(C^\bullet) := \ker d_{n+1} / \text{Im } d_n$ is called **n -th cohomology** of C^\bullet
- $Z^n(C^\bullet) := \ker d_n$ is called **n cocycle** and $B^n(C_\bullet) := \text{Im } d_n$ is called **n coboundary**.

- A **cochain homomorphism** $\varphi : C^\bullet \rightarrow \tilde{C}^\bullet$:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & C^0 & \xrightarrow{d_1} & C^1 & \longrightarrow & \cdots & \longrightarrow & C^{i-1} & \xrightarrow{d_i} & C^i & \xrightarrow{d_{i+1}} & C^{i+1} & \longrightarrow & \cdots \\ & & \varphi_0 \downarrow & & \varphi_1 \downarrow & & & & \varphi_{i-1} \downarrow & & \varphi_i \downarrow & & \varphi_{i+1} \downarrow & & \\ 0 & \longrightarrow & \tilde{C}^0 & \xrightarrow{\tilde{d}_1} & \tilde{C}^1 & \longrightarrow & \cdots & \longrightarrow & \tilde{C}^{i-1} & \xrightarrow{\tilde{d}_i} & \tilde{C}^i & \xrightarrow{\tilde{d}_{i+1}} & \tilde{C}^{i+1} & \longrightarrow & \cdots \end{array}$$

such that the diagram commutes.

We find that $\varphi_i(\ker d_{i+1}) \subseteq \ker \tilde{d}_{i+1}$ and $\varphi_i(\text{Im } d_i) \subseteq \text{Im } \tilde{d}_i$, so we can define

$$\begin{array}{ccc} \varphi_i^* : & H^i(C^\bullet) & \longrightarrow & H^i(\tilde{C}^\bullet) \\ & \underbrace{x}_{\in \ker d_{i+1}} + \text{Im } d_i & \longrightarrow & \underbrace{\varphi_i(x)}_{\in \ker \tilde{d}_i} + \text{Im } \tilde{d}_i \end{array}$$

which is well-defined. Then $\varphi^* : H^\bullet(C^\bullet) \rightarrow H^\bullet(\tilde{C}^\bullet)$ is a homomorphism of cohomology.

Similarly, we can define **chain homomorphism** and $\varphi_* : H_\bullet(C_\bullet) \rightarrow H_\bullet(\tilde{C}_\bullet)$

From now on, we consider the property of chain complex and it can do similar way in cochain complex.

Now, we want to know what kind of chain homomorphisms are “same”.

Definition 2.2.2. (homotopic)

- $f : C_\bullet \rightarrow \tilde{C}_\bullet$ is **null homotopic** is $\exists s_n : C_n \rightarrow \tilde{C}_{n+1}$ s.t. $f_n = \tilde{d}_{n+1}s_n + s_{n-1}d_n \forall n$

$$\begin{array}{ccccccc}
 \cdots & \longrightarrow & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} \longrightarrow \cdots \\
 & & \searrow \scriptstyle s_n & & \downarrow \scriptstyle f_n & & \nearrow \scriptstyle s_{n-1} \\
 \cdots & \longrightarrow & \tilde{C}_{n+1} & \xrightarrow{\tilde{d}_{n+1}} & \tilde{C}_n & \xrightarrow{\tilde{d}_n} & \tilde{C}_{n-1} \longrightarrow \cdots
 \end{array}$$

$$\begin{aligned}
 \implies f_* : H_n(C_\bullet) &\longrightarrow H_n(\tilde{C}_\bullet) \\
 x + \text{Im } d_{n+1} &\longrightarrow f_n(x) + \text{Im } \tilde{d}_{n+1} = \left(\tilde{d}_{n+1}s_n(x) + s_{n-1}d_n(x) \right) + \text{Im } \tilde{d}_{n+1} = \bar{0}
 \end{aligned}$$

- $f, g : C_\bullet \rightarrow \tilde{C}_\bullet$ are **homotopic** if $(f - g)$ is null homotopic i.e. $(f - g)_* = 0 \rightsquigarrow f_* = g_*$
- Let $M \in {}_R\mathfrak{M}$. A **projective resolution** of M is an exact sequence

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0, \text{ where } P_i : \text{projective}$$

Property 2.2.1. Every $M \in {}_R\mathfrak{M}$ has projective resolution.

Proof: We construct by induction. Let $P_0 = F_0$: free on M s.t. $F_0 \xrightarrow{\varepsilon} M \rightarrow 0$. Let $P_1 = F_1$: free on $\ker \varepsilon$ s.t. $F_1 \rightarrow \ker \varepsilon \rightarrow 0$,

$$\begin{array}{ccccccc}
 & & & & 0 & & \\
 & & & & \nearrow & & \\
 0 & \longrightarrow & \ker \varepsilon & \longrightarrow & F_0 & \longrightarrow & M \longrightarrow 0 \\
 & & \nearrow & & \nearrow \scriptstyle \exists d_1 & & \\
 & & F_1 & & & & \\
 & \nearrow & \nearrow & & & & \\
 & \ker d_1 & & & & &
 \end{array}$$

and notice that $\text{Im } d_1 = \ker \varepsilon$, so it is exact. Keep going to construct P_2, P_3, \dots and d_2, d_3, \dots . \square

Theorem 2.2.1 (Comparison theorem).

$$\begin{array}{ccccccc}
 \cdots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 \xrightarrow{\varepsilon} M \longrightarrow 0 & : \text{projective resolution} \\
 & & \downarrow \scriptstyle \exists f_2 & & \downarrow \scriptstyle \exists f_1 & & \downarrow \scriptstyle \exists f_0 & \downarrow \scriptstyle f \\
 \cdots & \longrightarrow & C_2 & \xrightarrow{d'_2} & C_1 & \xrightarrow{d'_1} & C_0 \xrightarrow{\varepsilon'} N \longrightarrow 0 & : \text{exact sequence}
 \end{array}$$

Then $\exists f_i : P_i \rightarrow C_i$ s.t. $\{f_i\}$ forms a chain maps s.t. diagram commute. Any two such chain maps are homotopic.

Proof: Existence: By induction on n : $n = 0$, $\exists f_0$ by projectivity of P_0 . For $n > 0$,

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_n & \xrightarrow{d_n} & P_{n-1} & \xrightarrow{d_{n-1}} & P_{n-2} \longrightarrow \\ & & \downarrow \exists f_n & & \downarrow f_{n-1} & & \downarrow f_{n-2} \\ \cdots & \longrightarrow & C_n & \xrightarrow{d'_n} & C_{n-1} & \xrightarrow{d'_{n-1}} & C_{n-2} \longrightarrow \end{array}$$

Claim: $\text{Im}(f_{n-1}d_n) \subseteq \text{Im } d'_n$

pf. Since $\text{Im } d'_n = \ker d'_{n-1}$ and $d'_{n-1}f_{n-1}d_n = f_{n-2}d_{n-1}d_n = 0$. □

By projectivity, there exists $f_n : P_n \rightarrow C_n$ such that the diagram commute

$$\begin{array}{ccc} P_n & \xrightarrow{d_n} & P_{n-1} \\ \downarrow \exists f_n & \searrow f_{n-1} \circ d_n & \downarrow f_{n-1} \\ C_n & \xrightarrow{d'_n} & \text{Im } d'_n \end{array}$$

Uniqueness: For another $\{g_i : P_i \rightarrow C_i\}$, we construct a homotopy by induction on n : Let $s_{-1} : 0 \rightarrow C_0$ be the zero map.

For $n > 0$.

$$\begin{array}{ccccc} P_{n+1} & \xrightarrow{d_{n+1}} & P_n & \xrightarrow{d_n} & P_{n-1} \\ & & \downarrow g_n - f_n & \swarrow s_{n-1} & \downarrow f_{n-1} \\ C_{n+1} & \xrightarrow{d'_{n+1}} & C_n & \xrightarrow{d'_n} & C_{n-1} \end{array}$$

$$\begin{aligned} d'_n(g_n - f_n - s_{n-1}d_n) &= d'_ng_n - d'_nf_n - d'_ns_{n-1}d_n \\ &= g_{n-1}d_n - f_{n-1}d_n - (g_{n-1} - f_{n-1} - s_{n-2}d_{n-1})d_n = 0 \\ &\implies \text{Im}(g_n - f_n - s_{n-1}d_n) \subseteq \ker d'_n = \text{Im } d'_{n+1} \end{aligned}$$

By projectivity, there exists $s_n : P_n \rightarrow C_{n+1}$ s.t. the following diagram commute

$$\begin{array}{ccccc} & & P_n & & \\ & \swarrow \exists s_n & \downarrow g_n - f_n - s_{n-1}d_n & & \\ C_{n+1} & \longrightarrow & \text{Im } d'_{n+1} & \longrightarrow & 0 \end{array}$$

□

Definition 2.2.3. Let $M \in {}_R\mathfrak{M}$ and $\cdots \rightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\bar{e}} M \rightarrow 0$ be a projective resolution of M (or simply $P_\bullet \rightarrow M \rightarrow 0$) $\rightsquigarrow P_M : P_\bullet \rightarrow 0$ is chain complex. Then for all $N \in {}_R\mathfrak{M}$,

$$0 \rightarrow \text{Hom}(P_0, N) \xrightarrow{\bar{d}_1} \text{Hom}(P_1, N) \xrightarrow{\bar{d}_2} \text{Hom}(P_2, N) \rightarrow \cdots$$

Notice that $\bar{d}_{i+1}\bar{d}_i(f) = f \circ d_i \circ d_{i+1} = 0$, so it form a cochain complex. Define

$$\text{Ext}_R^n(M, N) := H^n(\text{Hom}(P_M, N)) \quad \forall n \geq 0$$

$n = 0$: $\text{Ext}_R^0(M, N) = \ker \bar{d}_1 / 0 = \ker \bar{d}_1 = \text{Im } \bar{e} \simeq \text{Hom}(M, N)$ and

$$0 \rightarrow \text{Hom}(M, N) \xrightarrow{\bar{e}} \text{Hom}(P_0, N) \xrightarrow{\bar{d}_1} \text{Hom}(P_1, N) \rightarrow \cdots : \text{exact}$$

But our definition of Ext is depending on choice of P_\bullet . So we see this theorem.

Theorem 2.2.2 (Independency of the choice of projective resolution).

Proof:

- (1) Consider two projective resolution of M and \widetilde{M} and $F : M \rightarrow \widetilde{M}$. By comparison theorem, there exists $f = \{f_i\}$

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & M \longrightarrow 0 \\ & & \downarrow \exists f_1 & & \downarrow \exists f_0 & & \downarrow F \\ \cdots & \longrightarrow & \widetilde{P}_1 & \xrightarrow{\widetilde{d}_1} & \widetilde{P}_0 & \xrightarrow{\varepsilon'} & \widetilde{M} \longrightarrow 0 \end{array}$$

Take Hom functor on whole diagram, we get

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_R(P_0, N) & \xrightarrow{\widetilde{d}_1} & \text{Hom}_R(P_1, N) & \longrightarrow & \cdots \\ & & \uparrow \overline{f}_0 & & \uparrow \overline{f}_1 & & \\ 0 & \longrightarrow & \text{Hom}_R(\widetilde{P}_0, N) & \xrightarrow{\widetilde{d}_1} & \text{Hom}_R(\widetilde{P}_1, N) & \longrightarrow & \cdots \end{array}$$

Then $\overline{f}^* : \text{Ext}_R^\bullet(\widetilde{M}, N) \rightarrow \text{Ext}_R^\bullet(M, N)$. For another $g = \{g_i\}$, f and g are homotopic i.e. $\exists \{s_i\}$ s.t. $g_n - f_n = s_{n-1}d_n + \widetilde{d}_{n+1}s_n \rightsquigarrow \overline{g}_n - \overline{f}_n = \overline{s}_{n-1}\widetilde{d}_n + \widetilde{d}_{n+1}\overline{s}_n \rightsquigarrow \overline{f}^* = \overline{g}^*$

- (2) Let $\widetilde{M} = M$ and $f = \text{id}$

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow \exists g_0 & & \downarrow \text{id} & & \\ & \text{id} \left(& P'_0 & \longrightarrow & M & \longrightarrow & 0 \right. \\ & & \downarrow \exists f_0 & & \downarrow \text{id} & & \\ \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

$\rightsquigarrow \{f_i \circ g_i\}$ and $\{\text{id}_i\}$ are homotopic, so $\overline{g}^* \circ \overline{f}^* = (\text{id})^* = \text{id}$. By symmetry, $\overline{f}^* \circ \overline{g} = \text{id} \rightsquigarrow \overline{f}_i^* : H^i(\text{Hom}(P_\bullet, N)) \xrightarrow{\sim} H^i(\text{Hom}(\widetilde{P}_\bullet, N))$

□

Theorem 2.2.3 (Long exact sequence for Ext). If $0 \rightarrow L \rightarrow M \rightarrow K \rightarrow 0$ is exact for R -module, then

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}(K, N) & \longrightarrow & \text{Hom}(M, N) & \longrightarrow & \text{Hom}(L, N) \\ & & \searrow & & \searrow & & \\ & & \text{Ext}^1(K, N) & \longrightarrow & \text{Ext}^1(M, N) & \longrightarrow & \text{Ext}^1(L, N) \\ & & \searrow & & \searrow & & \\ & & \text{Ext}^2(K, N) & \longrightarrow & \text{Ext}^2(M, N) & \longrightarrow & \cdots \end{array}$$

We will use Horseshoe lemma and snake lemma in below, which will put the statement in Homework 13.

Proof: We choose $P_\bullet \rightarrow L$: proj. resol. of L and $\tilde{P}_\bullet \rightarrow K$: proj. resol. of K . By the Horseshoe lemma, $\exists \bar{P}_\bullet \rightarrow M \rightarrow 0$: proj. resol of M s.t.

$$\begin{array}{ccccccc}
 0 & \longrightarrow & P_\bullet & \longrightarrow & \bar{P}_\bullet & \longrightarrow & \tilde{P}_\bullet \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & K \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

Notice that \tilde{P}_i is projective, $0 \rightarrow P_i \rightarrow \bar{P}_i \rightarrow \tilde{P}_i \rightarrow 0$ is split, then $\bar{P}_i \simeq P_i \oplus \tilde{P}_i$ and thus $\text{Hom}(\bar{P}_i, N) \simeq \text{Hom}(P_i, N) \oplus \text{Hom}(\tilde{P}_i, N)$, then we have a exact sequence :

$$0 \rightarrow \text{Hom}(\tilde{P}_i, N) \rightarrow \text{Hom}(\bar{P}_i, N) \rightarrow \text{Hom}(P_i, N) \rightarrow 0$$

and thus

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \text{Hom}(\tilde{P}_1, N) & \longrightarrow & \text{Hom}(\bar{P}_1, N) & \longrightarrow & \text{Hom}(P_1, N) \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & \text{Hom}(\tilde{P}_0, N) & \longrightarrow & \text{Hom}(\bar{P}_0, N) & \longrightarrow & \text{Hom}(P_0, N) \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

Fact: $0 \rightarrow A^\bullet \xrightarrow{\alpha^\bullet} B^\bullet \xrightarrow{\beta^\bullet} C^\bullet \rightarrow 0$ exact, then

$$0 \rightarrow H^0(A^\bullet) \rightarrow H^0(B^\bullet) \rightarrow H^0(C^\bullet) \rightarrow H^1(A^\bullet) \rightarrow H^1(B^\bullet) \rightarrow H^1(C^\bullet) \rightarrow \dots$$

pf. Since $\text{Im } a_i = \ker a_{i+1} \subseteq A^i$ and by snake lemma we have

$$\begin{array}{ccccccc}
 \ker a_i & \longrightarrow & \ker b_i & \longrightarrow & \ker c_i & & \\
 \downarrow & & \downarrow & & \downarrow & & \\
 A^{i-1} & \longrightarrow & B^{i-1} & \longrightarrow & C^{i-1} & \longrightarrow & 0 \\
 \downarrow a_i & & \downarrow b_i & & \downarrow c_i & & \\
 0 & \longrightarrow & \ker a_{i+1} & \longrightarrow & \ker b_{i+1} & \longrightarrow & \ker c_{i+1} \\
 \downarrow & & \downarrow & & \downarrow & & \\
 & & H^i(A^\bullet) & \longrightarrow & H^i(B^\bullet) & \longrightarrow & H^i(C^\bullet)
 \end{array}$$

(Blue arrows in the original diagram indicate the snake lemma construction: a horizontal arrow from $\ker c_i$ to $\ker a_{i+1}$ and a horizontal arrow from $\ker a_i$ to $H^i(A^\bullet)$.)

By some discuss, we can get $0 \rightarrow \ker a_i / \operatorname{Im} a_{i-1} \rightarrow \ker b_i / \operatorname{Im} b_{i-1} \rightarrow \ker c_i / \operatorname{Im} c_{i-1}$. Now, we only need to prove that if $\lambda : \ker c_i \rightarrow H^i(A^\bullet)$ in the above diagram, then $\operatorname{Im} c_{i-1} \subseteq \ker \lambda$ and thus we can use factor theorem s.t. $\ker c_i / \operatorname{Im} c_{i-1} \rightarrow H^i(A^\bullet)$.

$$\ker \lambda = \beta_{i-1}(\ker b_i) = \beta_{i-1}b_{i-1}(B^{i-1}) = \operatorname{Im} c_{i-1}\beta_{i-2}(B^{i-1}) = \operatorname{Im} c_{i-1}(C^{i-1}) = \operatorname{Im} c_{i-1}$$

□

2.3 Ext and Tor (I)

For simplicity, R is commutative. But we still can discuss it when R is not commutative for somewhere.

Observation: Given $M, N \in \mathfrak{M}_R$, there are two ways to define $\operatorname{Ext}^n(M, N)$.

- Find any proj. resol. $P_\bullet \xrightarrow{\alpha} M \rightarrow 0$ and let $P_M : P_\bullet \rightarrow 0$ (complex). We define

$$\operatorname{Ext}_{proj}^n(M, N) = H^n(\operatorname{Hom}(P_M, N))$$

and

$$0 \xrightarrow{\bar{d}_0} \operatorname{Hom}(P_0, N) \xrightarrow{\bar{d}_1} \operatorname{Hom}(P_1, N) \rightarrow \dots$$

So $\ker \bar{d}_1 / \operatorname{Im} \bar{d}_0 = \ker \bar{d}_1 = \operatorname{Im} \bar{\alpha} = \operatorname{Hom}(M, N)$ which is well define.

- Find any injective resol. $0 \rightarrow N \xrightarrow{\beta} I^\bullet$ and let $I_N : 0 \rightarrow I^\bullet$ (complex). We define

$$\operatorname{Ext}_{inj}^n(M, N) = H^n(\operatorname{Hom}(M, I_N)) \rightsquigarrow \operatorname{Ext}_{inj}^0(M, N) = \operatorname{Hom}(M, N)$$

Theorem 2.3.1 (Equivalence of two definitions).

Proof:

- **Observation:** $M : \text{proj.} \implies 0 \rightarrow M \xrightarrow{\operatorname{id}} M \rightarrow 0 \rightsquigarrow \dots \rightarrow 0 \rightarrow M \rightarrow 0$ (complex), so $\operatorname{Ext}_{proj}^n(M, N) = 0 \forall n > 0$

$$N : \text{inj.} \implies \operatorname{Ext}_{inj}^n(M, N) = 0 \forall n > 0$$

- Recall the construction of projective resolution and injective resolution :

$$\begin{array}{ccccccc} \dots & \rightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 \longrightarrow M \longrightarrow 0 \\ & & \searrow & & \swarrow & & \swarrow \\ & & & & K_1 & & K_0 \\ & & \swarrow & & \searrow & & \searrow \\ 0 & & \nearrow & & 0 & & 0 \end{array}$$

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & I^0 & \longrightarrow & I^1 \longrightarrow I^2 \longrightarrow \dots \\ & & & & \searrow & & \swarrow \\ & & & & L^1 & & L^2 \\ & & \swarrow & & \searrow & & \searrow \\ 0 & & \nearrow & & 0 & & 0 \end{array}$$

For $0 \rightarrow K_0 \rightarrow P_0 \rightarrow M \rightarrow 0$ and $0 \rightarrow N \rightarrow I^0 \rightarrow L^1 \rightarrow 0$, by long exact of Ext, we have

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 \rightarrow & \text{Hom}(M, N) & \rightarrow & \text{Hom}(M, I^0) & \xrightarrow{\varphi} & \text{Hom}(M, L^1) & \rightarrow \text{Ext}_{inj}^1(M, N) \rightarrow \text{Ext}_{inj}^1(M, I^0) \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 \rightarrow & \text{Hom}(P_0, N) & \rightarrow & \text{Hom}(P_0, I^0) & \xrightarrow{\sigma} & \text{Hom}(P_0, L^1) & \longrightarrow 0 \\
 & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & \\
 0 \rightarrow & \text{Hom}(K_0, N) & \rightarrow & \text{Hom}(K_0, I^0) & \xrightarrow{\tau} & \text{Hom}(K_0, L^1) & \rightarrow \text{Ext}_{inj}^1(K_0, N) \rightarrow \text{Ext}_{inj}^1(K_0, I^0) \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & \text{Ext}_{proj}^1(M, N) & & 0 & & \text{Ext}_{proj}^1(M, L^1) & \\
 & \downarrow & & & & \downarrow & \\
 & \text{Ext}_{proj}^1(P_0, N) & & & & \text{Ext}_{proj}^1(P_0, L^1) &
 \end{array}$$

where blue modules are 0 by above observation and red are 0 by the property of projective and injective. So

$$\begin{aligned}
 \text{Ext}_{proj}^1(M, N) &= \text{coker } \alpha & \text{Ext}_{inj}^1(M, N) &= \text{coker } \varphi \\
 \text{Ext}_{proj}^1(M, L^1) &= \text{coker } \gamma & \text{Ext}_{inj}^1(K_0, N) &= \text{coker } \tau
 \end{aligned}$$

Apply snake lemma for (α, β, γ) ,

$$\text{Hom}(M, I^0) \xrightarrow{\varphi} \text{Hom}(M, L^1) \rightarrow \text{coker } \alpha \rightarrow 0$$

and thus $\text{coker } \alpha \simeq \text{coker } \varphi$ i.e. $\text{Ext}_{proj}^1(P_0, N) \simeq \text{Ext}_{inj}^1(M, N)$.

Also, $\text{Im } \gamma = \gamma(\text{Hom}(P_0, L^1)) = \gamma(\sigma(\text{Hom}(P_0, I^0))) = \tau(\beta(\text{Hom}(P_0, I^0))) = \text{Im } \tau \rightsquigarrow \text{coker } \gamma = \text{coker } \tau \rightsquigarrow \text{Ext}_{proj}^1(M, L^1) = \text{Ext}_{inj}^1(K_0, N)$.

Similarly using on $0 \rightarrow K_j \rightarrow P_j \rightarrow K_{j-1} \rightarrow 0$ and $0 \rightarrow L^i \rightarrow I^i \rightarrow L^{i+1} \rightarrow 0$, we can get

$$\text{Ext}^1(K_{j-1}, L^{i+1}) \simeq \text{Ext}^1(K_j, L^i) \quad (K_{-1} := M, L^0 := N)$$

(Notice that we had proved two definition of Ext^1 are equivalent)

Observe that $0 \rightarrow L^{n-1} \rightarrow I^{n-1} \xrightarrow{\bar{d}_n} I^n \xrightarrow{\bar{d}_{n+1}} I^{n+1} \rightarrow \dots$ is inj. resol. of L^{n-1}

$$\implies \text{Ext}^1(M, L^{n-1}) \simeq \ker \bar{d}_{n+1} / \ker \bar{d}_n \simeq \text{Ext}_{inj}^n(M, N)$$

Similarly, by $\dots \rightarrow P_n \rightarrow P_{n-1} \rightarrow K_{n-2}$, $\text{Ext}_{proj}^n(M, N) \simeq \text{Ext}_{proj}^1(K_{n-2}, N)$. Hence,

$$\begin{aligned}
 \text{Ext}_{inj}^n(M, N) &\simeq \text{Ext}^1(M, L^{n-1}) \simeq \text{Ext}^1(K_0, L^{n-2}) \\
 &\simeq \dots \simeq \text{Ext}^1(K_{n-2}, L^0) \simeq \text{Ext}_{proj}^n(M, N) \quad \forall n \geq 2
 \end{aligned}$$

□

Definition 2.3.1. Let $P_\bullet \rightarrow M \rightarrow 0$ be a projective resol. and $N \in \mathfrak{M}_R$. Define

$$\mathrm{Tor}_n(M, N) = H_n(P_M \otimes N) \quad \forall n \geq 0 \quad (\mathrm{Tor}_0(M, N) \simeq M \otimes_R N)$$

Fact 2.3.1. $\mathrm{Tor}_n(U, N) = 0 \quad \forall n > 0, \forall N \in \mathfrak{M}_R$

Proof: Let F, F' be free s.t. $0 \rightarrow \ker \varepsilon \rightarrow F \xrightarrow{\varepsilon} U$ and $0 \rightarrow \ker \varepsilon' \rightarrow F' \xrightarrow{\varepsilon'} N$, apply snake lemma on (α, β, γ) ,

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ \ker \varepsilon \otimes \ker \varepsilon' & \longrightarrow & F \otimes \ker \varepsilon' & \longrightarrow & U \otimes \ker \varepsilon' & \longrightarrow & 0 \\ \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 \longrightarrow & \ker \varepsilon \otimes F' & \longrightarrow & F \otimes F' & \longrightarrow & U \otimes F' & \longrightarrow 0 \\ \downarrow & & \downarrow & & \downarrow \varepsilon' & & \\ \ker \varepsilon \otimes N & \longrightarrow & F \otimes N & \xrightarrow{\varepsilon} & U \otimes N & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 & & 0 & & 0 & & \end{array}$$

$$0 = \ker \gamma \rightarrow \mathrm{coker} \alpha \rightarrow \mathrm{coker} \beta \rightarrow \mathrm{coker} \gamma \rightarrow 0$$

and $\mathrm{coker} \alpha = \ker \varepsilon \otimes N$, $\mathrm{coker} \beta = F \otimes N$, $\mathrm{coker} \gamma = U \otimes N$. But

$$\mathrm{Tor}_1(U, N) \rightarrow \ker \varepsilon \otimes N \rightarrow F \otimes N \rightarrow U \otimes N \rightarrow 0 \implies \mathrm{Tor}_1(U, N) = 0$$

We induct $\mathrm{Tor}_n(U, N) = 0 \quad \forall n > 0$ on n . If $n = 1$: OK!. If $n > 1$, notice that $\mathrm{Tor}_n(F, N) = 0 \quad \forall n > 0$ since F is projective. By long exact sequence for Tor (Homework 14),

$$0 = \mathrm{Tor}_n(F, N) \rightarrow \mathrm{Tor}_n(U, N) \rightarrow \mathrm{Tor}_{n-1}(\ker \varepsilon, N) \rightarrow \mathrm{Tor}_{n-1}(F, N) = 0$$

So $\mathrm{Tor}_n(U, N) = \mathrm{Tor}_{n-1}(\ker \varepsilon, N)$. For all $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$,

$$\begin{array}{ccccccc} & & \textcolor{red}{0} & & \textcolor{red}{0} & & \\ & & \downarrow & & \downarrow & & \\ \textcolor{blue}{\mathrm{Tor}_1(U, M')} & \longrightarrow & \ker \varepsilon \otimes M' & \longrightarrow & F \otimes M' & \longrightarrow & U \otimes M' \longrightarrow 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \textcolor{blue}{\mathrm{Tor}_1(U, M)} & \longrightarrow & \ker \varepsilon \otimes M & \longrightarrow & F \otimes M & \longrightarrow & U \otimes M \longrightarrow 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \varepsilon' \\ \textcolor{blue}{\mathrm{Tor}_1(U, M'')} & \longrightarrow & \ker \varepsilon \otimes M'' & \longrightarrow & F \otimes M'' & \xrightarrow{\varepsilon} & U \otimes M'' \longrightarrow 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

Red zeros by flat and blue zeros by $\text{Tor}_1(\text{flat}, N) = 0$. By nine lemma,

$$0 \rightarrow \ker \varepsilon \otimes N' \rightarrow \ker \varepsilon \otimes N \rightarrow \ker \varepsilon \otimes N'' \rightarrow 0$$

i.e. $\ker \varepsilon$ is flat. By induction hypothesis, $\text{Tor}_{n-1}(\ker \varepsilon, N) = 0 \implies \text{Tor}_n(U, N) = 0$. \square

Property 2.3.1 (Tor for flat resolutions). Let $U_\bullet \rightarrow M \rightarrow 0$ be a flat resolution of M . Then

$$\text{Tor}_n(M, N) \simeq H_n(U_M \otimes N) \quad \forall n > 0$$

Proof:

- $n = 0$: $\because U_1 \otimes N \xrightarrow{\bar{d}_1} U_0 \otimes N \rightarrow M \otimes N \rightarrow 0$ exact $\rightsquigarrow U_1 \otimes N \xrightarrow{\bar{d}_1} U_0 \otimes N \rightarrow 0$ complex $\therefore H_0(U_M \otimes N) = U_0 \otimes N / \text{Im } \bar{d}_1 \simeq M \otimes N = \text{Tor}_0(M, N)$
- $n = 1$: Let $W_i = \ker d_i$ and consider

$$\begin{array}{ccccccc} \cdots & \rightarrow & U_2 & \xrightarrow{\quad} & U_1 & \xrightarrow{\quad} & U_0 \rightarrow M \rightarrow 0 \\ & & \searrow & & \searrow & & \nearrow \\ & & & W_1 & & & W_0 \\ & & \nearrow & & \searrow & & \searrow \\ 0 & & & & 0 & & 0 \end{array}$$

By long exact sequence for Tor on $0 \rightarrow W_0 \rightarrow U_0 \rightarrow M \rightarrow 0$,

$$\begin{array}{ccccc} & & \text{Tor}_2(U_0, N) & \longrightarrow & \text{Tor}_2(M, N) \\ & \searrow & & & \nearrow \\ \text{Tor}_1(W_0, N) & \longrightarrow & \text{Tor}_1(U_0, N) & \longrightarrow & \text{Tor}_1(M, N) \\ & \searrow & & & \nearrow \\ W_0 \otimes N & \xrightarrow{i \otimes 1} & U_0 \otimes N & \xrightarrow{\epsilon \otimes 1} & M \otimes N \longrightarrow 0 \end{array}$$

where the blue one is 0 by U_0 is flat. So $\text{Tor}_2(M, N) \simeq \text{Tor}_1(W_0, N)$ and $\text{Tor}_1(M, N) \simeq \ker(i \otimes 1)$. In the other hand,

$$\begin{array}{ccccc} U_2 \otimes N & \xrightarrow{d_2 \otimes 1} & U_1 \otimes N & \xrightarrow{d_1 \otimes 1} & U_0 \otimes N \\ & & \searrow & \nearrow i \otimes 1 & \uparrow \overline{d_1 \otimes 1} \\ & & W_0 \otimes N & \xrightarrow{\sim} & U_1 \otimes N / \text{Im}(d_2 \otimes 1) \\ & & & \searrow & \\ & & & & 0 \end{array}$$

Thus,

$$\text{Tor}_1(M, N) \simeq \ker(i \otimes 1) = \ker \overline{d_1 \otimes 1} = \ker(d_1 \otimes 1) / \text{Im}(d_2 \otimes 1) = H_1(U_M \otimes N)$$

- $n > 1$: $\text{Tor}_2(M, N) \simeq \text{Tor}_1(W_0, N) = H_1(U_{W_0} \otimes N) = H_2(U_M \otimes N)$. In general, $\text{Tor}_n(M, N) \simeq \text{Tor}_{n-1}(W_0, N) \simeq H_{n-1}(U_{W_0} \otimes N) \simeq H_n(U_M \otimes N)$ by induction hypothesis.

□

Example 2.3.1. For any abelian group G , determine $\text{Tor}_n(\mathbb{Q}/\mathbb{Z}, G)$:

- Consider the flat resolution : $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$ (Recall that R_S is R flat module). Let $0 \xrightarrow{\bar{d}_2} \mathbb{Z} \otimes_{\mathbb{Z}} G \xrightarrow{\bar{d}_1} \mathbb{Q} \otimes_{\mathbb{Z}} G \rightarrow 0$ is a complex. Then

$$\text{Tor}_1(\mathbb{Q}/\mathbb{Z}, G) = \ker \bar{d}_1 / \text{Im } \bar{d}_2 = \ker \bar{d}_1. \text{ Since } \mathbb{Q} \otimes_{\mathbb{Z}} G \simeq G_{\mathbb{Z} \setminus \{0\}} \text{ and } \mathbb{Z} \otimes_{\mathbb{Z}} G \simeq G,$$

$$g \in \ker \bar{d}_1 \iff \frac{g}{1} = 0 \text{ in } G_{\mathbb{Z} \setminus \{0\}} \iff \exists m \in \mathbb{Z} \setminus \{0\} \text{ s.t. } mg = 0 \iff g \in \text{Tor}(G)$$

$$\text{So } \text{Tor}_1(\mathbb{Q}/\mathbb{Z}, G) = \text{Tor}(G)$$

- Since $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0 \rightsquigarrow \dots \rightarrow 0 \rightarrow 0 \rightarrow \mathbb{Z} \otimes G \rightarrow \mathbb{Q} \otimes G \rightarrow \mathbb{Q}/\mathbb{Z} \otimes G \rightarrow 0$ is a complex and thus $\text{Tor}_n(\mathbb{Q}/\mathbb{Z}, G) = 0 \forall n \geq 2$.

Proposition 2.3.1. TFAE

- (1) M is flat
- (2) $\text{Tor}_1(M, R/I) = 0 \forall I \subseteq R$
- (3) $\forall 0 \rightarrow I \rightarrow R \implies 0 \rightarrow M \otimes I \rightarrow M \otimes R$ exact
- (4) $M^* := \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is an injective R -module

Proof:

- (2) \iff (3) : For $0 \rightarrow I \rightarrow R \rightarrow R/I \rightarrow 0$, by long exact sequence for Tor ,

$$0 = \text{Tor}_1(R, M) \rightarrow \text{Tor}_1(R/I, M) \rightarrow I \otimes M \xrightarrow{f} R \otimes M \rightarrow R/I \otimes M \rightarrow 0$$

By Homework 14, we will prove that if R is commute, then $\text{Tor}_n(M, N) = \text{Tor}_n(N, M)$. So (2) $\iff f$ injective \iff (3)

- (1) \iff (4) : $\forall 0 \rightarrow N' \rightarrow N$: exact, by Homework 12, we have

$$\text{Hom}_R(N, M^*) \simeq \text{Hom}_{\mathbb{Z}}(M \otimes N, \mathbb{Q}/\mathbb{Z}) = (M \otimes N)^*$$

$$\text{Hom}_R(N', M^*) \simeq \text{Hom}_{\mathbb{Z}}(M \otimes N', \mathbb{Q}/\mathbb{Z}) = (M \otimes N')^*$$

Fact:

- $A^* = 0 \iff A = 0$

pf. (\Leftarrow) : OK! (\Rightarrow) : If $\exists 0 \neq a \in A$, let $f : \langle a \rangle_{\mathbb{Z}} \rightarrow \mathbb{Q}/\mathbb{Z}$ by $a \mapsto o(a)^{-1} + \mathbb{Z}$ or $a \mapsto 1 + \mathbb{Z}$ (if $o(a) = \infty$). Since \mathbb{Q}/\mathbb{Z} is injective and $0 \rightarrow \langle a \rangle \rightarrow A$, there exists $\tilde{f} : A \rightarrow \mathbb{Q}/\mathbb{Z}$ is \mathbb{Z} -module homomorphism i.e. $A^* \neq 0$ ($\rightarrow \Leftarrow$)

- $0 \rightarrow B \xrightarrow{f} C \iff C^* \xrightarrow{f^*} B^* \rightarrow 0$
 $pf. 0 \rightarrow \ker f \rightarrow B \xrightarrow{f} C \rightarrow 0 \rightsquigarrow C^* \xrightarrow{f^*} B^* \rightarrow (\ker f)^* \rightarrow 0$ by \mathbb{Q}/\mathbb{Z} is injective.
 So $\ker f = 0 \iff \text{coker } f^* \simeq (\ker f)^* = 0$

Hence,

$$\begin{aligned} & M^* \text{ is injective} \\ \iff & (M \otimes N)^* \rightarrow (M \otimes N')^* \rightarrow 0 \text{ exact } \forall 0 \rightarrow N' \rightarrow N \\ \iff & 0 \rightarrow M \otimes N' \rightarrow M \otimes N \text{ exact } \forall 0 \rightarrow N' \rightarrow N \iff M \text{ is flat} \end{aligned}$$

- (4) \iff (3) : M^* is injective $\xleftrightarrow{\text{bear's criterion}} (M \otimes R)^* \rightarrow (M \otimes I)^* \rightarrow 0 \forall I \subseteq R$
 $R \iff 0 \rightarrow M \otimes I \rightarrow M \otimes R \forall I \subseteq R$

□

2.4 Ext and Tor (II) and an important application

2.4.1 group-module

Definition 2.4.1. Let M be an abelian group and G be a group. We say

$$G \curvearrowright M \iff \exists \text{ a group homo. } (G, \cdot) \rightarrow (\text{Aut}(M), \circ)$$

and extend to a ring homo.

$$\mathbb{Z}[G] \rightarrow (\text{Aut}(M), +, \circ) \implies M : \text{left } \mathbb{Z}[G]\text{-module}$$

- $H^n(G, M) := \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, M)$, here $G \curvearrowright \mathbb{Z}$ trivially i.e. $\forall g \in G, \forall n \in \mathbb{Z}, gn = n$
- $H_n(G, M) := \text{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M) \simeq \text{Tor}_n^{\mathbb{Z}[G]}(M, \mathbb{Z})$

But M is only left $\mathbb{Z}[G]$ -module, we need to give M the right $\mathbb{Z}[G]$ -module structure. We will complete the definition in remark.

Remark 2.4.1. Since G is may not abelian, $\mathbb{Z}[G]$ may not be commutative ring. But $\mathbb{Z}[G]$ is a group ring have some good structure, we can define the right $\mathbb{Z}[G]$ -module structure on M . Define

$$\begin{aligned} \rho : \mathbb{Z}[G] &\longrightarrow \mathbb{Z}[G] \\ g &\longmapsto g^{-1} \end{aligned}$$

Then ρ is additive homo. and $\rho(ab) = \rho(b)\rho(a)$ (we called it **antiautomorphism**) or say $\rho : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]^o$ is an isomorphism. By

$$\mathbb{Z}[G]^o \xrightarrow{\rho^{-1}} \mathbb{Z}[G] \rightarrow \text{Aut}(M)$$

gives M a right $\mathbb{Z}[G]$ -module structure, denote M^r .

Similarly. For given N be a left $\mathbb{Z}[G]$ module,

$$\mathbb{Z}[G] \xrightarrow{\rho} \mathbb{Z}[G]^o \rightarrow \text{Aut}(M)$$

gives N a left $\mathbb{Z}[G]$ -module structure, denote N^ℓ and $\forall x \in N^\ell, a \in \mathbb{Z}[G], a \cdot x := x\rho(a)$
 So we can extend the definition of Tor.

- Two left $\mathbb{Z}[G]$ -module M, N . Define $M \otimes_{\mathbb{Z}[G]} N := M^r \otimes_{\mathbb{Z}[G]} N$. Then

$$\mathrm{Tor}_n^{\mathbb{Z}[G]}(M, N) := \mathrm{Tor}_n^{\mathbb{Z}[G]}(M^r, N), \quad \mathrm{Tor}_n^{\mathbb{Z}[G]}(N, M) := \mathrm{Tor}_n^{\mathbb{Z}[G]}(N^r, M)$$

- $\mathrm{Tor}_n^{\mathbb{Z}[G]}(M, N) \simeq \mathrm{Tor}_n^{\mathbb{Z}[G]}(N, M) :$
 - P is a projective right $\mathbb{Z}[G]$ -module $\iff P^\ell$ is a projective left $\mathbb{Z}[G]$ -module :
 - $\rho(a \cdot b) = \rho(b\rho(a)) = \rho^2(a) \cdot \rho(b) = a\rho(b)$. So $\mathbb{Z}[G] \xrightarrow{\rho} \mathbb{Z}[G]$ as left $\mathbb{Z}[G]$ module.
 - $(\mathbb{Z}[G]^{\oplus n})^\ell \simeq \mathbb{Z}[G]^{\oplus n}$.
 - p is projective $\iff \exists p'$ s.t. $p \otimes p' = \mathbb{Z}[G]^{\oplus n}$

$$\iff p^\ell \oplus (p')^\ell \simeq (p \oplus p')^{\oplus n} \simeq (\mathbb{Z}[G]^{\oplus n})^\ell \simeq \mathbb{Z}[G]^{\oplus n}$$

$$\iff p^\ell \text{ is projective}$$
 - $P_\bullet \rightarrow M^r : \text{right projective resolution} \iff P_\bullet^\ell \rightarrow (M^r)^\ell = M : \text{left projective resolution of } M$.

2.4.2 resolution of \mathbb{Z}

- **The bar resolution of \mathbb{Z} :** $B[G] : \cdots \rightarrow B_n \xrightarrow{d_n} B_{n-1} \rightarrow \cdots \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0$
 - $B_0 = \mathbb{Z}[G][\]$ and $\varepsilon : [\] \mapsto 1$ i.e. $\varepsilon(\sum \lambda_g g) = \sum \lambda_g$, where $[\]$ just a generator for convenient symbol in later.
 - $B_n = \bigoplus_{x_i \in G} \mathbb{Z}[G][x_1|x_2|\cdots|x_n]$ and define

$$d_n : [x_1|x_2|\cdots|x_n] \mapsto x_1[x_2|\cdots|x_n] + \sum_{i=1}^{n-1} (-1)^i [x_1|\cdots|x_i x_{i+1}|\cdots|x_n] + (-1)^n [x_1|\cdots|x_{n-1}]$$

For example,

- $d_1[x] = x[\] - [\]$
- $d_2[x|y] = x[y] - [xy] + [x]$
- $d_3[x|y|z] = x[y|z] - [xy|z] + [x|yz] - [x|y]$
- It is clear that B_i are free, but it not easy to check that $B[G]$ is projective resolution. We will using another resolution to prove it.

- **The homogeneous resolution of \mathbb{Z} :** $P(G) : \cdots \rightarrow P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon'} \mathbb{Z} \rightarrow 0$
 - $P_n = \bigoplus_{x_i \in G} \mathbb{Z}(x_0, \dots, x_n)$ and $G \curvearrowright P_n$ by

$$x(x_0, \dots, x_n) = (xx_0, \dots, xx_n)$$

$$\text{So } P_n = \bigoplus_{x_i \in G} \mathbb{Z}[G](1, x_1, \dots, x_n)$$

- $\varepsilon' : (x_0) \mapsto 1 \rightsquigarrow \varepsilon' = \varepsilon$, since $P_0 \simeq P[G](1)$
- $\partial_n : (x_0, \dots, x_n) \mapsto \sum_{i=0}^n (-1)^i (x_0, \dots, \hat{x}_i, \dots, x_n)$
- $P(G) \simeq B(G)$: Consider

$$\begin{array}{ccccccccccc}
 \longrightarrow & P_{n+1} & \xrightarrow{\partial_{n+1}} & P_n & \xrightarrow{\partial_n} & P_{n-1} & \xrightarrow{\partial_{n-1}} & \dots & \longrightarrow & P_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & \downarrow \tau_{n+1} & & \downarrow \tau_n & & \downarrow \tau_{n-1} & & & & \downarrow \tau_0 & & \downarrow \text{id} & & \\
 \longrightarrow & B_{n+1} & \xrightarrow{d_{n+1}} & B_n & \xrightarrow{d_n} & B_{n-1} & \longrightarrow & \dots & \xrightarrow{d_{n-1}} & B_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
 \end{array}$$

and define $\tau_n : (x_0, \dots, x_n) \mapsto x_0[x_0^{-1}x_1|x_1^{-1}x_2|\dots|x_{n-1}^{-1}x_n]$, then we can check that τ_n is \mathbb{Z} -module homomorphism and $\tau_{n-1} \circ \partial_n = d_n \circ \tau_n$.

So $\tau_n^{-1} : [x_1|\dots|x_n] \mapsto (1, x_1, x_1x_2, \dots, x_1x_2 \dots x_n)$ and $\tau_n \circ \tau_n^{-1} = \text{id}_{B_n}$, $\tau_n^{-1} \circ \tau_n = \text{id}_{P_n}$.

- $P(G)$ is exact : Define $s_{-1} : \mathbb{Z} \rightarrow P_0$ by $1 \mapsto (1)$ and

$$\begin{array}{ccc}
 s_n : & P_n & \longrightarrow & P_{n+1} \\
 & (x_0, \dots, x_n) & \longmapsto & (1, x_0, \dots, x_n)
 \end{array}$$

are \mathbb{Z} -module homomorphism. Notice that $1_{P_n} = s_{n-1} \circ \partial_n + \partial_{n+1} \circ s_n$, which means $\text{id} : P(G) \rightarrow P(G)$ and $0 : P(G) \rightarrow P(G)$ are homotopic $\rightsquigarrow H_n(P(G)) = 0 \forall n \rightsquigarrow P(G)$ is exact.

- So $P(G), B(G)$ are free resolution of \mathbb{Z} .

- **Normalized bar resolution of \mathbb{Z} :** $B^*(G) : \dots \rightarrow B_2^* \xrightarrow{d_2^*} B_1^* \xrightarrow{d_1^*} B_0^* \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0$

- Let $U_n = \bigoplus_{\substack{x_i \in G \\ \exists x_i = 1}} \mathbb{Z}[G][x_1|\dots|x_n]$, then $B_n^* := B_n/U_n \simeq \bigoplus_{1 \neq x_i \in G} \mathbb{Z}[G][x_1|\dots|x_n]$
and $B_0^* = B_0$.

- Define $[x_1|\dots|x_n]^* := [x_1|\dots|x_n] + U_n \in B_n^*$
- Construct $d_n^* : [x_1|\dots|x_n] + U_n \mapsto d_n([x_1|\dots|x_n]) + U_{n-1}$, since $d_n(U_n) \subseteq U_{n-1}$ by Homework 15.
- $B^*(G)$ is exact : Define $t_n := \tau_{n+1} \circ s_n \circ \tau_n^{-1}$ i.e.

$$\begin{array}{ccc}
 t_n : & B_n & \longrightarrow & B_{n+1} \\
 & x[x_1|\dots|x_n] & \longmapsto & [x|x_1|\dots|x_n]
 \end{array}$$

By $t_n(U_n) \subseteq U_{n+1}$, we can define $t_n^* : B_n^* \longrightarrow B_{n+1}^*$ by $x[x_1|\dots|x_n]^* \mapsto [x|x_1|\dots|x_n]^*$. Notice that $1_{B_n^*} = d_{n+1}^* t_n^* + t_{n-1}^* d_n^* \rightsquigarrow B^*(G)$ is exact.

2.4.3 Augmentation ideal

The first part of resolution (ε) is essential to calculate H^1 .

Definition 2.4.2. Define **augmentation ideal**

$$IG := \ker \varepsilon = \left\{ \sum \lambda_g g \in \mathbb{Z}[G] : \sum \lambda_g = 0 \right\}$$

is two-side ideal of $\mathbb{Z}[G]$, and say ε is the **augmentation map**.

- $\mathbb{Z}[G]/IG \simeq \mathbb{Z}$ as $\mathbb{Z}[G]$ -module isomorphism, since $\mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0$.
- $IG = \langle g-1 : g \in G \rangle_{\mathbb{Z}} : \sum \lambda_g g \in \ker \varepsilon \iff \sum \lambda_g = 0 \iff \sum \lambda_g g = \sum \lambda_g (g-1)$
- IG is \mathbb{Z} -free : If $\sum_{g \neq 1} r_g (g-1) = 0 \rightsquigarrow \sum_{g \neq 1} r_g g - \left(\sum_{g \neq 1} r_g \right) \cdot 1 = 0 \rightsquigarrow r_g = 0 \forall g \in G$.
- For given $f \in \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$, say $f : 1 \mapsto x$, then x is G -invariant. So
 $H^0(G, M) = \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \simeq M^G = \{x \in M : gx = x \forall g \in G\} = \{x \in M : IGx = 0\}$ is $\mathbb{Z}[G]/IG$ -module and $G \curvearrowright M^G$ trivially.
- $H_0(G, M) = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M \simeq \mathbb{Z}[G]/IG \otimes_{\mathbb{Z}[G]} M \simeq M/IGM =: M_G$ is the largest quotient of M , which G acts trivially.
p.f. $N \subseteq M$, $G \curvearrowright M/N$ trivially $\iff gx + N = x + N \forall g \in G, x \in M \iff (g-1)x \in N \forall g \in G, \forall x \in M \iff (IG)M \subseteq N$
- $H^0(G, \mathbb{Z}) = \mathbb{Z}^G = \mathbb{Z}$, $H_0(G, \mathbb{Z}) = \mathbb{Z}_G = \mathbb{Z}$
- $H^0(G, \mathbb{Z}[G]) = \mathbb{Z}[G]^G = \begin{cases} \mathbb{Z} & , \text{if } |G| < \infty \\ 0 & , \text{if } |G| = \infty \end{cases}$
p.f. $\forall g' \in G$, $g'(\sum \lambda_g g) = \sum (\lambda_g g) \rightsquigarrow \lambda_g = \lambda_{g'g} \rightsquigarrow$ all λ_g are the same, say λ .
 If $|G| \leq \infty$, then $\sum_{g \in G} \lambda_g g = \lambda \sum_{g \in G} g \rightsquigarrow \mathbb{Z}[G]^G = \left\langle \sum_{g \in G} g \right\rangle_{\mathbb{Z}} \simeq \mathbb{Z}$.
 If $|G| = \infty \rightsquigarrow \lambda = 0$ i.e. $\mathbb{Z}[G]^G = 0$
- $H_0(G, \mathbb{Z}[G]) = \mathbb{Z}[G]_G \simeq \mathbb{Z}[G]/IG\mathbb{Z}[G] = \mathbb{Z}[G]/IG \simeq \mathbb{Z}$
- $H_1(G, \mathbb{Z}[G]) = 0$, since $\mathbb{Z}[G] \simeq \bigoplus_{g \in G} \mathbb{Z}g$ is free and thus flat.
- $H_1(G, \mathbb{Z}) : 0 \rightarrow IG \rightarrow \mathbb{Z}[G] \rightarrow \mathbb{Z} \rightarrow 0$, then

$$\begin{array}{c} H_1(G, \mathbb{Z}[G]) \longrightarrow H_1(G, \mathbb{Z}) \\ \searrow \hspace{10em} \nearrow \\ \mathbb{Z} \otimes_{\mathbb{Z}[G]} IG \xrightarrow{g} \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \xrightarrow{f} \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z} \longrightarrow 0 \end{array}$$

where the blue one is 0.

$f : n \otimes \sum \lambda_g g \mapsto n \otimes \sum \lambda_g = n \otimes (\sum \lambda_g g) \cdot 1 = (\sum \lambda_g g) \cdot n \otimes 1$ and $n \otimes \lambda_g g = (\sum \lambda_g g) \cdot n \otimes 1$, so f is id and thus $g = 0$, so $H_1(G, \mathbb{Z}) \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} IG \simeq \mathbb{Z}[G]/IG \otimes_{\mathbb{Z}[G]} IG \simeq IG/(IG)^2$.

Claim: $G/[G, G] \simeq IG/(IG)^2$, where $[G, G]$ is commutator of G .

proof: Define $\varphi : \begin{array}{ccc} G & \longrightarrow & IG/(IG)^2 \\ g & \longmapsto & (g-1) + (IG)^2 \end{array}$

- $\text{Homo} : \varphi(g_1 g_2) = \overline{g_1 g_2 - 1} = \overline{(g_1 - 1)(g_2 - 1) + g_1 - 1 + g_2 - 1} = \varphi(g_1) + \varphi(g_2)$
- $\because IG/(IG)^2$ is abelian as addition $\therefore [G, G] \leq \ker \varphi \rightsquigarrow \bar{\varphi} : G/[G, G] \longrightarrow IG/(IG)^2$
- Define $\psi : IG \longrightarrow G/[G, G]$
 $g - 1 \longmapsto g[G, G]$
Subclaim: $(IG)^2 \subseteq \ker \psi (\rightsquigarrow \bar{\psi} : IG/(IG)^2 \longrightarrow G/[G, G])$
subproof: $u = (\sum m_i(x_i - 1))(\sum n_j(y_j - 1)) = \sum m_i n_j (x_i - 1)(y_j - 1) = \sum m_i n_j (x_i y_j - 1 + x_i - 1 + y_j - 1) \rightsquigarrow \psi(u) = \prod (x_i y_j x_i^{-1} y_j^{-1})^{m_i n_j} [G, G] = 0$
- Finally, $\bar{\varphi} \circ \bar{\psi}, \bar{\psi} \circ \bar{\varphi}$ are identity, so $G/[G, G] \simeq IG/(IG)^2$

2.5 Koszul complex

When we calculate the Ext or Tor, it is necessary to find a good resolution which is easier to realize the structure and calculate the homology, cohomology.

2.5.1 Wedge product and Koszul complex

Assume R : commutative with $\text{char} R \neq 2$ and $M \in \mathfrak{M}_R$

Goal: To construct a free resolution of R/I .

Definition 2.5.1. Recall that $T^k(M) = M \otimes \cdots \otimes M$ (k times), $T(M) = \bigoplus_{k=0}^{\infty} T^k(M)$

- $A(M) = \langle x \otimes x : x \in M \rangle_{T(M)} \rightsquigarrow A^k(M) := A(M) \cap T^k(M)$ is the submodule of $T^k(M)$ generated by all $x_1 \otimes \cdots \otimes x_k$ with $x_i = x_j$ for some distinct i, j .

- $\bigwedge(M) = T(M)/A(M) = \bigoplus_{k=0}^{\infty} \bigwedge^k(M)$

$$\bigwedge^k(M) = T^k(M)/A^k(M) = \langle \overline{x_1 \otimes \cdots \otimes x_k} : x_i \in M \rangle$$

denote $\overline{x_1 \otimes \cdots \otimes x_k} = x_1 \wedge \cdots \wedge x_k$. Notice that $(x_1 + x_2) \wedge (x_1 + x_2) = 0$ and thus

$$x_1 \wedge x_1 + w_1 \wedge x_2 + w_2 \wedge x_1 + w_2 \wedge x_2 = 0 \implies x_1 \wedge x_2 = -x_2 \wedge x_1$$

which is satisfy concept of notation of differential form.

- $f : M \times \cdots \times M \rightarrow L$ is an **alternating** k -mutilinear map if $f(x_1, \dots, x_m) = 0 \forall x_i \in M$ with $x_i = x_j$ for distinct i, j .
- **Universal property** : If A is an R -algebra with $a^2 = 0 \forall a \in A$, and $\varphi : M \rightarrow A$ is a R -module homomorphism. Then there exists a unique R -algebra homomorphism ψ such that

$$\begin{array}{ccc} M & \longrightarrow & \bigwedge(M) \\ & \searrow \varphi & \downarrow \exists \psi \\ & & A \end{array}$$

commute.

Goal: Let $f : M \rightarrow R$ be an R -module homomorphism, consider

$$\begin{aligned} M^n &\longrightarrow \bigwedge^{n-1} M \\ (x_1, \dots, x_n) &\longmapsto \sum_{i=1}^n (-1)^{i+1} f(x_i) x_1 \wedge \dots \wedge \widetilde{x_i} \wedge \dots \wedge x_n \end{aligned}$$

which is an alternating. By universal property,

$$\begin{aligned} \exists d_f : \quad \bigwedge^n M &\longrightarrow \bigwedge^{n-1} M \\ x_1 \wedge \dots \wedge x_n &\longmapsto \sum_{i=1}^n (-1)^{i+1} f(x_i) x_1 \wedge \dots \wedge \widetilde{x_i} \wedge \dots \wedge x_n \end{aligned}$$

By Homework 16, $d_f \circ d_f = 0$. Then we get a **Koszul complex** :

$$K_\bullet(f) : \dots \longrightarrow \bigwedge^n M \xrightarrow{d_f} \bigwedge^{n-1} M \xrightarrow{d_f} \dots \xrightarrow{d_f} \bigwedge^2 M \xrightarrow{d_f} \bigwedge M \xrightarrow{f} R \rightarrow 0$$

where $f \circ d_f : x \wedge y \mapsto f(x)y - f(y)x \mapsto f(x)f(y) - f(y)f(x) = 0$, so $K_\bullet(f)$ is a complex. Note : $d_f : \bigwedge M \rightarrow \bigwedge M$ is graded R -algebra of $\deg -1$.

Definition 2.5.2. Let $(C_\bullet, d), (C'_\bullet, d')$ be two chain complexes of R -modules, then

$$(C_\bullet \otimes C'_\bullet)_n := \bigoplus_{i=0}^n (C_i \otimes_R C'_{n-i})$$

and

$$\begin{aligned} d \otimes d' : (C_\bullet \otimes C'_\bullet)_n &\longrightarrow (C_\bullet \otimes C'_\bullet)_{n-1} \\ \sum_{i=0}^n x_i \otimes y_{n-i} &\longmapsto \sum_{i=0}^n dx_i \otimes y_{n-i} + (-1)^i x_i \otimes d'y_{n-i} \end{aligned}$$

$$\rightsquigarrow (d \otimes d') \circ (d \otimes d') = 0$$

- Let $M_1, M_2 \in \mathfrak{M}_R$, $f_1 \in \text{Hom}_R(M_1, R)$, $f_2 \in \text{Hom}_R(M_2, R)$. Define $f = f_1 + f_2 : M_1 \oplus M_2 \rightarrow R$ with $(x, y) \mapsto f_1(x) + f_2(y)$. Then

$$K_\bullet(f_1) \otimes K_\bullet(f_2) \simeq K_\bullet(f)$$

and

$$\bigoplus_{i=0}^n \left(\bigwedge^i M_1 \otimes \bigwedge^{n-i} M_2 \right) \simeq \bigwedge^n (M_1 \oplus M_2)$$

Actually, $(\bigwedge^i M_1) \wedge (\bigwedge^{n-i} M_2) \simeq \bigwedge^i M_1 \otimes \bigwedge^{n-i} M_2$, since M_1, M_2 haven't common non-zero element. And

$$(d_{f_1} \otimes d_{f_2})(x \otimes y) = d_{f_1}(x) \otimes y + (-1)^{\deg x} x \otimes d_{f_2}(y)$$

We will check in Homework 16 that $d_{f_1} \otimes d_{f_2} = d_f$ under the above isomorphism.

- Let $M = Re_1 \oplus \dots \oplus Re_n$ be free R -module and $\underline{x} = x_1, \dots, x_n$ with $x_i \in R \forall i = 1, \dots, n$. We associate (M, \underline{x}) with $f : M \rightarrow R$, $e_i \mapsto x_i$. Let

$$\begin{aligned} f_i : Re_i &\longrightarrow R \\ e_i &\longmapsto x_i \end{aligned}$$

Then $K_\bullet(f) \simeq K_\bullet(f_1) \otimes \cdots \otimes K_\bullet(f_n)$. Consider the Koszul complex for $(\cdot x_i)$

$$\begin{array}{ccccccc} K_\bullet(x_i) : 0 & \longrightarrow & R & \xrightarrow{\cdot x_i} & R & \longrightarrow & 0 \\ & & r & \longmapsto & rx_i & & \end{array}$$

Then $K_\bullet(x) \simeq K_\bullet(x_1) \otimes \cdots \otimes K_\bullet(x_n)$.

Therefore we see a Koszul complex of a free module can be decomposed into n lines.

Property 2.5.1. Let $x \in R$ and (C_\bullet, ∂) be a chain complex of R -modules. Then \exists two chain maps ρ, π s.t.

$$0 \rightarrow C_\bullet \xrightarrow{\rho} C_\bullet \otimes K_\bullet(x) \xrightarrow{\pi} C_\bullet(-1) \rightarrow 0$$

is exact, where $(C_\bullet(-1))_n = C_{n-1}$

Proof: Since $K_\bullet : 0 \rightarrow R \xrightarrow{1} R \xrightarrow{x} R \rightarrow 0$, $(C_\bullet \otimes K_\bullet(x))_n = (C_n \otimes R) \oplus (C_{n-1} \otimes R)$

$$\begin{array}{ccc} d_n : (C_n \otimes R) \oplus (C_{n-1} \otimes R) & \longrightarrow & (C_{n-1} \otimes R) \oplus (C_{n-2} \otimes R) \\ (z_1 \otimes r_1, z_2 \otimes r_2) & \longmapsto & (\partial z_1 \otimes r_1 + (-1)^{n-1} z_2 \otimes r_2 x, \partial z_2 \otimes r_2) \end{array}$$

Under isomorphism $C_n \otimes_R R \simeq C_n$, we get

$$\begin{array}{ccc} d_n : C_n \oplus C_{n-1} & \longrightarrow & C_{n-1} \oplus C_{n-2} \\ \begin{pmatrix} r_1 z_1 \\ r_2 z_2 \end{pmatrix} & \longmapsto & \begin{pmatrix} \partial & (-1)^{n-1} x \\ 0 & \partial \end{pmatrix} \begin{pmatrix} r_1 z_1 \\ r_2 z_2 \end{pmatrix} \end{array}$$

Let $\rho_n : C_n \rightarrow C_n \oplus C_{n-1}$ be inclusion and $\pi_n : C_n \oplus C_{n-1} \rightarrow C_{n-1}$ be projection. Then

$$\begin{array}{ccccccc} 0 & \longrightarrow & C_n & \xrightarrow{\rho_n} & C_n \oplus C_{n-1} & \xrightarrow{\pi_n} & C_{n-1} \longrightarrow 0 \\ & & \partial_n \downarrow & & \downarrow d_n & & \downarrow \partial_{n-1} \\ 0 & \longrightarrow & C_{n-1} & \xrightarrow{\rho_{n-1}} & C_{n-1} \oplus C_{n-2} & \xrightarrow{\pi_{n-1}} & C_{n-2} \longrightarrow 0 \end{array}$$

is commute. □

Corollary 2.5.1. This induces a long exact sequence :

$$\cdots \rightarrow H_n(C_\bullet) \xrightarrow{\rho_*} H_n(C_\bullet \otimes K_\bullet(x)) \xrightarrow{\pi_*} H_n(C_\bullet(-1)) \xrightarrow{(-1)^{n-1}x} H_{n-1}(C_\bullet) \rightarrow \cdots$$

For the map $\pm x$: Given $z \in C_{n-1}$ with $\partial(z) = 0$

$$z \xrightarrow{\pi^{-1}} (0, z) \xrightarrow{d} ((-1)^{n-1}xz, 0) \xrightarrow{\rho^{-1}} (-1)^{n-1}xz$$

Definition 2.5.3. x is C_\bullet -regular if x is not a zero divisor of $C_n \forall n$ and $C_n/xC_n \neq 0 \forall n$.

Property 2.5.2. If x is C_\bullet -regular, then $H_n(C_\bullet \otimes K_\bullet(x)) \simeq H_n(C_\bullet/xC_\bullet) \forall n \geq 0$.

Proof: Let

$$\begin{array}{ccc} \phi_n : C_n \oplus C_{n-1} & \longrightarrow & C_n/xC_n \\ (z_1, z_2) & \longmapsto & \bar{z}_1 \end{array}$$

Then

$$\begin{array}{ccc} C_n \oplus C_{n-1} & \longrightarrow & C_n/xC_n \\ d_n \downarrow & & \downarrow \bar{\partial}_n \\ C_{n-1} \oplus C_{n-2} & \longrightarrow & C_{n-1}/xC_{n-1} \end{array}$$

will commute $\rightsquigarrow \{\phi_n\}$ is a chain map. Therefore there induce the homomorphism

$$H_n(C_\bullet \otimes K_\bullet(x)) \xrightarrow{\phi_*} H_n(C_\bullet/xC_\bullet) \quad \forall n \geq 0$$

- ϕ_* is onto : Given $\bar{z} \in \ker \bar{\partial}_n$ i.e. $\partial(z) \in xC_{n-1}$, say $\partial z = xz'$, where $z' \in C_{n-1}$

$$d(z, (-1)^n z') = (\partial z + (-1)^{n-1} (-1)^n xz', (-1)^n \partial z') = (0, (-1)^n \partial z')$$

Since $0 = \partial \partial z = x \partial z' \implies \partial z' = 0$ (x is not zero divisor) $\rightsquigarrow (z, (-1)^n z') \in \ker d$ and $\phi(z, (-1)^n z') = \bar{z}$

- ϕ_* is 1 - 1 : Let $(z, z') \in \ker d_n$ with $\phi_n(z, z') = \bar{z} \in \text{Im } \bar{\partial}_{n+1} \subseteq C_n/xC_n$, say $\bar{z} = \bar{\partial} z''$ with $z'' \in C_{n+1} \rightsquigarrow z - \partial z'' = xz'''$ for $z''' \in C_n$.

On the other hand, $0 = d_n(z, z') = (\partial z + (-1)^{n-1} xz, \partial z') \rightsquigarrow \partial z = (-1)^n xz', \partial z' = 0$. Consider $d_{n+1}(z'', (-1)^n z''') = (\partial z'' + xz''', (-1)^n \partial z''') = (z, (-1)^n \partial z''')$.

$\therefore z - \partial z'' = xz''' \therefore \partial z = x \partial z'''$ and $\partial z = (-1)^n xz' \implies (-1)^n z' = \partial z'''$, since x is not zero divisor. So $(z, z') = d_{n+1}(z'', (-1)^n z''') \in \text{Im } d_{n+1}$

□

2.5.2 R -regular sequence

Definition 2.5.4. $\{a_1, \dots, a_n\} \subset R$ is called an R -regular sequence if

- $\langle a_1, \dots, a_n \rangle_R \neq R$
- For $i = 0, \dots, n-1$, a_{i+1} is not a zero divisor of $R/\langle a_1, \dots, a_i \rangle$

Note : Second condition is different to the linearly independent and depends on the order of a_i . For example, $R = k[x, y, z]$, where k is a field. Then $x, y(1-x), z(1-x)$ is regular but $y(1-x), z(1-x), x$ is not.

Theorem 2.5.1. If $\underline{x} = x_1, \dots, x_n$ is a R -regular sequence, then $K_\bullet(x)$ is a free resolution of $R/\langle x_1, \dots, x_n \rangle$.

Proof: By induction on n : $n = 1$: $0 \rightarrow R \xrightarrow{x} R \rightarrow R/xR \rightarrow 0$. For $n > 1$, we assume that $\underline{x}' = x_1, \dots, x_{n-1}$ and

$$K_\bullet(\underline{x}') \rightarrow R/\langle x_1, \dots, x_{n-1} \rangle \rightarrow 0 : \text{exact}$$

i.e. $H_i(K_\bullet(\underline{x})) = 0 \forall i > 0$. We have $K_\bullet(\underline{x}) = K_\bullet(\underline{x}') \otimes K_\bullet(x_n)$ and $\forall i > 1$

$$\cdots \rightarrow H_i(K_\bullet(\underline{x}')) \rightarrow H_i(K_\bullet(\underline{x})) \rightarrow H_i(K_\bullet(\underline{x}')(-1)) \xrightarrow{(-1)^{i-1}x_i} H_{i-1}(K_\bullet(\underline{x}')) \rightarrow \cdots$$

By induction hypothesis, $H_i(K_\bullet(\underline{x}')) = 0$ and $H_i(K_\bullet(\underline{x}')(-1)) = H_{i-1}(K_\bullet(\underline{x}')) = 0$, so $H_i(K_\bullet(\underline{x})) = 0 \forall i > 1$. For $i = 1$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_1(K_\bullet(\underline{x})) & \longrightarrow & H_0(K_\bullet(\underline{x}')) & \xrightarrow{\frac{x_1}{1-1}} & H_0(K_\bullet(\underline{x}')) \\ & & & & \parallel & & \parallel \\ & & & & R/\langle x_1, \dots, x_{n-1} \rangle & & R/\langle x_1, \dots, x_{n-1} \rangle \end{array}$$

Hence, $H_1(K_\bullet(\underline{x})) = 0$. □

2.6 Extensions of abelian groups

Definition 2.6.1. Let $M \triangleleft E$ and $G \simeq E/M$. We call E an extension of M by G and denoted by $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$.

Note: We will using addition for some times and we will replace 1 by 0.

Goal: When M and G are given, try to obtain all extensions of M by G , where we assume M : abelian, G : arbitrary.

Definition 2.6.2. ℓ is called a **lifting** of p if $\ell(1) = 1$ and

$$1 \longrightarrow M \longrightarrow E \xrightleftharpoons[\ell]{p} G \longrightarrow 1$$

such that $p \circ \ell = \text{id}_G$. Note : $G \simeq E/M$, $p \circ \ell(\bar{x}) = xM = \ell(\bar{x})M$ and a lifting is an assignment of representation for cosets of M .

Property 2.6.1. For a lifting ℓ ,

$$\begin{array}{ccc} \exists \theta : & G & \longrightarrow \text{Aut}(M) \\ & \bar{x} & \longmapsto \theta_{\bar{x}} : a \mapsto \ell(\bar{x})a\ell(\bar{x})^{-1} \end{array}$$

is a group homo. ($\rightsquigarrow G \curvearrowright M$) and θ is independent of the choice of ℓ .

Proof:

- For another ℓ' , $\because \ell'(\bar{x})M = xM = \ell(\bar{x})M \therefore \ell'(\bar{x}) = \ell(\bar{x})b$ for some $b \in M$. $\forall a \in M$

$$\ell'(\bar{x})a\ell'(\bar{x})^{-1} = \ell(\bar{x})bab^{-1}\ell(\bar{x})^{-1} = \ell(\bar{x})bb^{-1}a\ell(\bar{x})^{-1}$$

- $\theta_{\overline{xy}}(a) = \ell(\overline{xy})a\ell(\overline{xy})^{-1}$, $\theta_{\bar{x}} \circ \theta_{\bar{y}}(a) = \ell(\bar{x})\ell(\bar{y})a\ell(\bar{y})^{-1}\ell(\bar{x})^{-1}$.

$p(\ell(\overline{xy})) = p(\ell(\bar{x}))p(\ell(\bar{y})) = xy \therefore \ell(\bar{x})\ell(\bar{y})$ is a lifting of \overline{xy} so $\ell_{\overline{xy}} = \theta_{\bar{x}} \circ \theta_{\bar{y}}$. □

Definition 2.6.3. $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ splits if \exists a lifting $\ell : G \rightarrow E$ is a group homomorphism.

Definition 2.6.4. $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ is splits $\iff \exists$ a subgroup $K \leq E$ s.t. $K \simeq G$ and $K \cap M = \{1\}$, $KM = E \rightsquigarrow \varphi : G \rightarrow \text{Aut}(M)$, $E \simeq M \rtimes_{\varphi} K$.

Proof: (\Rightarrow) : Let $K = \text{Im } \ell$ which is a subgroup of E since ℓ is a group homomorphism.

- $\ell : G \rightarrow K$. If $\ell(\bar{x}) = \ell(\bar{y}) \rightsquigarrow p(\ell(\bar{x})) = p(\ell(\bar{y})) \rightsquigarrow \bar{x} = \bar{y}$ so $\ell : G \simeq K$
- $E = KM : \forall x \in E, \ell(p(x)) = y \in K \rightsquigarrow p\ell(p(x)) = p(y) \rightsquigarrow y^{-1}x \in \ker p = M$
- $K \cap M = \{1\} : a = \ell(\bar{x}) \in K \cap M \rightsquigarrow 1 = p(a) = p(\ell(\bar{x})) = \bar{x} \rightsquigarrow a = \ell(\bar{1}) = 1$

(\Leftarrow) :

- $p|_K : K \rightarrow G$ is a isomorphism :
 - Onto : $p(K) = p(KM) = p(E) = G$
 - 1-1 : $\ker(p|_K) = M \cap K = \{1\}$
- $\ell := (p|_K)^{-1}$ is a lifting and also is a group homomorphism.

□

Observation: Given $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ for $\bar{x}, \bar{y} \in G$,

$$p(\ell(\bar{x}\bar{y})) = xy, \quad p(\ell(\bar{x})\ell(\bar{y})) = xy$$

Then $M\ell(\bar{x})\ell(\bar{y}) = M\ell(\bar{x}\bar{y}) \rightsquigarrow \exists f(x, y) \in M$ s.t. $\ell(\bar{x})\ell(\bar{y}) = f(\bar{x}, \bar{y})\ell(\bar{x}\bar{y})$. Then $f : G \times G \rightarrow M$ is called the **obstruction of ℓ** being a group homomorphism.

Property 2.6.2.

- $\forall \bar{x}, \bar{y} \in G, f(\bar{x}, \bar{1}) = f(\bar{1}, \bar{y}) = 1$
 $p f. \ell(\bar{1})\ell(\bar{y}) = f(1, \bar{y}\ell(\bar{y})) \rightsquigarrow \ell(\bar{1}, \bar{y}) = 1$
- (**Cocycle identity**) By associativity, $\forall \bar{x}, \bar{y}, \bar{z} \in G$
 $(\ell(\bar{x})\ell(\bar{y}))\ell(\bar{z}) = f(\bar{x}, \bar{y})\ell(\bar{x}\bar{y})\ell(\bar{z}) = f(\bar{x}, \bar{y})f(\bar{x}\bar{y}, \bar{z})\ell(\bar{x}\bar{y}\bar{z})$
 $\ell(\bar{x})(\ell(\bar{y})\ell(\bar{z})) = \ell(\bar{x})f(\bar{y}, \bar{z})\ell(\bar{y}\bar{z}) = \ell(\bar{x})f(\bar{y}, \bar{z})\ell(\bar{x})^{-1}\ell(\bar{x})\ell(\bar{y}\bar{z}) = \theta_{\bar{x}}(f(\bar{y}, \bar{z}))f(\bar{x}, \bar{y}\bar{z})\ell(\bar{x}\bar{y}\bar{z}).$

Hence,

$$f(\bar{x}, \bar{y})f(\bar{x}\bar{y}, \bar{z}) = \theta_{\bar{x}}(f(\bar{y}, \bar{z}))f(\bar{x}, \bar{y}\bar{z})$$

and the additive version

$$f(\bar{x}, \bar{y}) + f(\bar{x}\bar{y}, \bar{z}) = \bar{x} \cdot f(\bar{y}, \bar{z}) + f(\bar{x}, \bar{y}\bar{z})$$

where \cdot is a kind of group action $(G \curvearrowright M)$.

The function $f : G \times G \rightarrow M$ satisfy above property is called a **factor set w.r.t. ℓ** .

Theorem 2.6.1. Let $\sigma : G \rightarrow \text{Aut } M$ be a group homomorphism and $f : G \times G \rightarrow M$ satisfy two condition in Property 2.6.2. Then $\exists 1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ and $\ell : G \rightarrow E$ be a lifting s.t. $\theta = \sigma$ and f is corresponding factor set w.r.t. ℓ .

Proof:

- Define $E(M, G, f, \sigma) =: E := M \times G$ equipped with the operation

$$(a, x)(b, y) = (a\sigma_x(b)f(x, y), xy) \quad (\text{Note: } f = 1 \rightsquigarrow E = M \rtimes_{\varphi} G)$$

- associativity :

$$((a, x)(b, y))(c, z) = (a\sigma_x(b)f(x, y), xy)(c, z) = (a\sigma_x(b)f(x, y)\sigma_{xy}(c)f(xy, z), xyz)$$

$$\begin{aligned} (a, x)((b, y)(c, z)) &= (a, x)(b\sigma_y(c)f(y, z), yz) = (a\sigma_x(b\sigma_y(c)f(y, z))f(x, yz), xyz) \\ &= (a\sigma_x(b)\sigma_{xy}(c)\sigma_x(f(y, z))f(x, yz), xyz) \end{aligned}$$

- identity : $(1, 1)$

$$(a, x)^{-1} : (a, x)(\sigma_{x^{-1}}(a^{-1}f(x, x^{-1})), x^{-1}) = (a\sigma_x(\sigma_{x^{-1}}(a^{-1}f(x, x^{-1})))f(x, x^{-1}), 1) = (1, 1)$$

$$\begin{aligned} \bullet \bullet \quad p : \quad E &\longrightarrow G \\ (a, x) &\longmapsto x \end{aligned} \text{ is a group homomorphism.}$$

$$\bullet \bullet \quad i : \quad M \longrightarrow E \\ a \longmapsto (a, 1) \text{ is a group homomorphism.}$$

$$(a, 1)(b, 1) = (a\sigma_1(b)f(1, 1), 1) = (ab, 1)$$

- $\ker p = \text{Im } i$

- Let $\ell : \begin{array}{ccc} G & \longrightarrow & E \\ x & \longmapsto & (1, x) \end{array}$ be a lifting. For $a \in M, x \in G$,

$$\begin{aligned} \theta_x(a) &= \ell(x)(a, 1)\ell(x)^{-1} = (1, x)(a, 1)(\sigma_{x^{-1}}(f(x, x^{-1})^{-1}), x^{-1}) \\ &= (\sigma_x(a)f(x, 1), x)(\sigma_{x^{-1}}(f(x, x^{-1})^{-1}), x^{-1}) \\ &= (\sigma_x(a)\sigma_x(\sigma_{x^{-1}}(f(x, x^{-1})^{-1}))f(x, x^{-1}), 1) = (\sigma_x(a), 1) \end{aligned}$$

- $\ell(x)\ell(y)\ell(xy)^{-1} = f(x, y)$

$$\begin{aligned} \ell(x)\ell(y)\ell(xy)^{-1} &= (1, x)(1, y)(\sigma_{(xy)^{-1}}(f(xy, (xy)^{-1})^{-1}), (xy)^{-1}) \\ &= (f(x, y), xy)(\sigma_{(xy)^{-1}}(f(xy, (xy)^{-1})^{-1}), (xy)^{-1}) \\ &= (f(x, y)\sigma_{xy}(\sigma_{(xy)^{-1}}(f(xy, (xy)^{-1})^{-1}))f(xy, (xy)^{-1}), 1) \\ &= (f(x, y), 1) \end{aligned}$$

□

Observation: Let $1 \rightarrow M \rightarrow E \xrightarrow{p} G \rightarrow 1$ and $\ell : G \rightarrow E$ be a lifting, then θ is independent of ℓ and f depends on ℓ . Since $E = \bigsqcup_{x \in G} M\ell(\bar{x})$, construct

$$\begin{aligned} \varphi : E &\longrightarrow E(M, G, f, \theta) \\ a\ell(\bar{x}) &\longmapsto (a, \bar{x}) \end{aligned}$$

Then

$$\begin{aligned} \varphi((a\ell(\bar{x}))(b\ell(\bar{y}))) &= \varphi(a\theta_{\bar{x}}(b)f(\bar{x}, \bar{y})\ell(\bar{x}\bar{y})) = (a\theta_{\bar{x}}(b)f(\bar{x}, \bar{y}), \bar{x}\bar{y}) \\ \varphi(a\ell(\bar{x}))\varphi(b\ell(\bar{y})) &= (a, \bar{x})(b, \bar{y}) = (a\theta_{\bar{x}}(b)f(\bar{x}, \bar{y}), \bar{x}\bar{y}) \end{aligned}$$

So φ is group homomorphism and it clear that is isomorphism.

Definition 2.6.5. Two extensions are **equivalent** if $\exists \varphi$ s.t.

$$\begin{array}{ccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G \longrightarrow 1 \\ & & \downarrow 1_M & & \downarrow \wr \varphi & & \downarrow 1_G \\ 1 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G \longrightarrow 1 \end{array}$$

Theorem 2.6.2.

$$\begin{array}{ccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G \longrightarrow 1 \\ & & \downarrow 1_M & & \downarrow \wr \varphi & & \downarrow 1_G \\ 1 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G \longrightarrow 1 \end{array}$$

are equivalent \iff They associate the same action $\theta : G \rightarrow \text{Aut}(M)$ and \exists liftings

$$\begin{cases} \ell : G \rightarrow E \\ \ell' : G \rightarrow E' \end{cases} \quad \text{s.t. } \exists h : G \rightarrow M \text{ with } h(1) = 1 \text{ and}$$

$$f'(\bar{x}, \bar{y})f(\bar{x}, \bar{y})^{-1} = \theta_{\bar{x}}(h(\bar{y}))h(\bar{x}\bar{y})^{-1}h(\bar{x})$$

Proof: (\Rightarrow) : Choose a lifting $\ell : G \rightarrow E$ and $\ell' = \varphi \circ \ell$

• $\forall a \in M$,

$$\begin{aligned} \ell'(\bar{x})a\ell'(\bar{x})^{-1} &= \varphi(\ell(\bar{x}))a(\varphi \circ \ell(\bar{x}))^{-1} = \varphi(\ell(\bar{x}))\varphi(a)\varphi(\ell^{-1}(\bar{x})) \\ &= \varphi(\underbrace{\ell(\bar{x})a\ell^{-1}(\bar{x})}_{\in M}) = \ell(\bar{x})a\ell^{-1}(\bar{x}) \end{aligned}$$

•

$$\begin{aligned} f'(\bar{x}, \bar{y})f(\bar{x}, \bar{y})^{-1} &= \ell'(\bar{x})\ell'(\bar{y})\ell'(\bar{x}\bar{y})f(\bar{x}, \bar{y})^{-1} \\ &= \varphi(\ell(\bar{x}))\varphi(\ell(\bar{y}))\varphi(\ell(\bar{x}\bar{y})^{-1})f(\bar{x}, \bar{y})^{-1} \\ &= \varphi(\underbrace{f(\bar{x}, \bar{y})}_{\in M})f(\bar{x}, \bar{y})^{-1} = 1 \end{aligned}$$

Let $h = 1$ and get the result.

- By observation

$$\begin{array}{ccccccc}
 1 & \rightarrow & M & \longrightarrow & E & \longrightarrow & G \rightarrow 1 \\
 & & \text{id} \downarrow & & \wr \downarrow \varphi & & \downarrow \text{id} \\
 1 & \rightarrow & M & \rightarrow & E(M, G, f, \theta) & \rightarrow & G \rightarrow 1
 \end{array}
 \quad
 \begin{array}{ccccccc}
 1 & \rightarrow & M & \longrightarrow & E' & \longrightarrow & G \rightarrow 1 \\
 & & \text{id} \downarrow & & \wr \downarrow \varphi & & \downarrow \text{id} \\
 1 & \rightarrow & M & \rightarrow & E(M, G, f', \theta) & \rightarrow & G \rightarrow 1
 \end{array}$$

Define

$$\begin{aligned}
 \bar{\varphi} : E(M, G, f', \theta) &\longrightarrow E(M, G, f, \theta) \\
 (a, \bar{x}) &\longmapsto (ah(\bar{x}), \bar{x})
 \end{aligned}$$

- $\bar{\varphi}$ is a group homomorphism :

$$\bar{\varphi}((a, \bar{x})(b, \bar{y})) = \varphi(a\theta_{\bar{x}}(b)f'(\bar{x}, \bar{y}), \bar{xy}) = (a\theta_{\bar{x}}(b)f'(\bar{x}, \bar{y})h(\bar{xy}), \bar{xy})$$

$$\bar{\varphi}(a, \bar{x})\bar{\varphi}(b, \bar{y}) = (ah(\bar{x}), x)(bh(\bar{y}), \bar{y}) = (ah(\bar{x})\theta_x(bh(\bar{y})f(\bar{x}, \bar{y})), \bar{xy})$$

Since M is abelian and $f'(\bar{x}, \bar{y})f(\bar{x}, \bar{y})^{-1} = \theta_{\bar{x}}(h(\bar{y}))h(\bar{xy})^{-1}h(\bar{x})$, we have $\bar{\varphi}$ is homomorphism.

- $1 - 1 : (ah(\bar{x}), \bar{x}) = (1, 1) \rightsquigarrow \bar{x} = 1 \rightsquigarrow a = 1$
- Onto : $E(M, G, f', \theta) = \bigcup_{x \in G} M\ell'(\bar{x}) \rightsquigarrow \bar{\varphi}(E(M, G, f', \theta)) = \bigcup_{x \in G} Mh(\bar{x})\ell(\bar{x}) = \bigcup_{x \in G} M\ell(\bar{x}) = E(M, G, f, \theta)$

□

Definition 2.6.6.

- $e(G, M) :=$ equivalence classes of extensions of M by G
- $Z^2(G, M) :=$ the abelian group of all factor sets $f : G \times G \rightarrow M$ satisfies $f(\bar{x}, \bar{1}) = f(\bar{1}, \bar{y}) = 1$ and cocycle identity.
- $B^2(G, M) :=$ the abelian of all functions $f : G \times G \rightarrow M$ such that $\exists h : G \rightarrow M$ with $h(1) = 1$ and

$$f(x, y) = \sigma_x(h(y))h(xy)^{-1}h(x)$$

Then by Homework 17, $B^2(G, M) \leq Z^2(G, M)$ and thus

$$Z^2(G, M)/B^2(G, M) \simeq e(G, M)$$

2.7 $H^2(G, M)$ and $H^1(G, M)$

Recall: The normalized bar resolution of \mathbb{Z} :

$$\cdots \rightarrow B_3^* \xrightarrow{d_3^*} B_2^* \xrightarrow{d_2^*} B_1^* \xrightarrow{d_1^*} B_0^* \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0$$

$$\rightsquigarrow 0 \rightarrow \text{Hom}(B_0^*, M) \xrightarrow{\bar{d}_1^*} \text{Hom}(B_1^*, M) \xrightarrow{\bar{d}_2^*} \text{Hom}(B_2^*, M) \xrightarrow{\bar{d}_3^*} \text{Hom}(B_3^*, M) \rightarrow \cdots$$

Observation: As we fix $G \overset{\sigma}{\curvearrowright} M$

- $f \in \ker \overline{d}_3^*$
 - $f : B_2/U_2 \rightarrow M \rightsquigarrow f([x|1]) = f([1|y]) = 0$
 - $f \circ d_3 = 0 \rightsquigarrow 0 = f \circ d_3([x|y|z]) = f(x[y|z] - [xy|z] + [x|yz] - [x|y]) = xf([y|z]) - f([xy|z]) + f([x|yz]) - f(x|y)$

Consider the corresponding $f([x|y]) \longleftrightarrow f(x, y)$, then f is satisfy the condition of factor set. Hence, $\ker \overline{d}_3^* = Z^2(G, M)$.

- $g \in \text{Im } \overline{d}_2^* \rightsquigarrow g = h \circ d_2^*$
 - $g([x|y]) = h \circ d_2([x|y]) = h(x[y] - [xy] + [x]) = xh([y]) - h([xy]) + h([x])$
 - $h : B_1/U_1 \rightarrow M \rightsquigarrow h([1]) = 1$

Hence, $\text{Im } \overline{d}_2^* = B^2(G, M)$

- Hence, $H^2(G, M) \simeq Z^2(G, M) / B^2(G, M) \simeq e(G, M)$

$$\begin{array}{ccc}
 Z^2(G, M) / B^2(G, M) & \longleftrightarrow & e(G, M) \\
 \overline{f} & \longrightarrow & [1 \rightarrow M \rightarrow E(M, G, f, \sigma) \rightarrow G \rightarrow 1] \\
 \overline{f} & \longrightarrow & [1 \longrightarrow M \longrightarrow E \xrightarrow{\ell} G \longrightarrow 1] \\
 \overline{0} & \longleftrightarrow & [1 \rightarrow M \rightarrow M \rtimes_{\sigma} G \rightarrow G \rightarrow 1]
 \end{array}$$

- $f \in \ker \overline{d}_2^*$
 - $f : B/U_1 \rightarrow M \rightsquigarrow f(1) = 0$
 - $f \circ d_2 = 0 \rightsquigarrow 0 = f \circ d_2([x|y]) = f(x[y] - [xy] + [x]) \rightsquigarrow f([xy]) = xf([y]) + f([x])$

i.e. $f : G \rightarrow M$ satisfies

$$(1) \quad f(1) = 0$$

$$(2) \quad f(xy) = xf(y) + f(x) = xf(y) + f(x)y, \text{ where } M \curvearrowright G \text{ trivially.}$$

and called f is a **derivation** and denote $\text{Der}(G, M)$ is a group of all derivation $f : G \rightarrow M$.

- $g \in \text{Im } \overline{d}_1^*$
 - $g = h \circ d_1 \rightsquigarrow h([]) = a_0 \in M$
 - $g[x] = h \circ d_1([x]) = h(x[] - []) = xa_0 - a_0$

and called g is a **principle derivation** and denote $\text{PDer}(G, M)$ is a group of all principle derivation $f : G \rightarrow M$.

- $H^1(G, M) \simeq \text{Der}(G, M) / \text{PDer}(G, M)$

Definition 2.7.1.

- $\varphi \in \text{Aut}(E)$ is **stabilizes** $1 \rightarrow M \rightarrow E \rightarrow G$ if

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow 1_M & & \downarrow \varphi & & \downarrow 1_G & & \\ 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

commute.

- $\text{Stab}_E(G, M) = \{\text{stabilizing automorphism}\} \leq \text{Aut}(E)$

Theorem 2.7.1. Let $1 \rightarrow M \rightarrow E \xrightarrow{p} G \rightarrow 1$ and $\ell : G \rightarrow E$ be a lifting. Then $\forall \varphi \in \text{Stab}_E(G, M)$, $\exists d : G \rightarrow M$ s.t. $\varphi(a\ell(x)) = ad(x)\ell(x) \forall a \in M, x \in G$ and d is independent of the choice of ℓ and $d(xy) = xd(y) + d(x) \forall x, y \in G$. Conversely, such d defines an $\varphi \in \text{Stab}_E(G, M)$.

Proof:

- By diagram chasing,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \xrightarrow{a \mapsto a} & E & \xrightarrow{\ell(x) \mapsto x} & G & \longrightarrow & 1 \\ & & \downarrow 1_M & & \downarrow \varphi & & \downarrow 1_G & & \\ 1 & \longrightarrow & M & \xrightarrow{a \mapsto a} & E & \xrightarrow{\varphi(\ell(x)) \mapsto x} & G & \longrightarrow & 1 \end{array}$$

we have $\varphi(a) = a \forall a \in M$, $M\ell(x) = M\varphi(\ell(x)) \rightsquigarrow \varphi(\ell(x)) = d(x)\ell(x)$ for some $d(x) \in M$. Hence, $\varphi(a\ell(x)) = ad(x)\ell(x)$.

- For another $\ell' : G \rightarrow E$, say $\ell'(x) = g(x)\ell(x)$ for some $g(x) \in M$. Then

$$\begin{aligned} d'(x) &= \varphi(\ell'(x))\ell'(x)^{-1} = \varphi(g(x)\ell(x))(g(x)\ell(x))^{-1} \\ &= g(x)d(x)\ell(x)\ell^{-1}(x)g(x)^{-1} = d(x) \end{aligned}$$

Since $g(x), d(x), g(x)^{-1} \in M$ and M is abelian.

- Check $d : G \rightarrow M$ is derivation :

$$\begin{aligned} d(xy) &= \varphi(\ell(xy))\ell(xy)^{-1} = \varphi(f(x, y)^{-1}\ell(x)\ell(y))(f(x, y)^{-1}\ell(x)\ell(y))^{-1} \\ &= f(x, y)^{-1}d(x)\ell(x)d(y)\ell(y)\ell(y)^{-1}\ell(x)^{-1}f(x, y) \\ &= f(x, y)^{-1}d(x)(x \cdot d(y))f(x, y) = d(x)(x \cdot d(y)) \end{aligned}$$

In additive version : $d(xy) = d(x) + xd(y)$

- Conversely, define $\varphi(a\ell(x)) = ad(x)\ell(x) \forall a \in M, x \in G$ and well define by $E = \bigcup_{x \in G} M\ell(x)$.

- In additive version, $d(1) = 1 \cdot d(1) + d(1) \rightsquigarrow d(1) = 0$, in multiplicative version, $d(1) = 1$.

- $\forall a \in M, \varphi(a) = \varphi(al(1)) = ad(1)\ell(1) = a$
- $p(\varphi(al(x))) = p(ad(x)\ell(x)) = p(al(x))$
- Check $\varphi \in \text{Aut}(E)$:

$$\begin{aligned}\varphi((al(x))(bl(y))) &= \varphi(a(x \cdot b)f(x, y)\ell(xy)) = a(x \cdot b)f(x, y)d(xy)\ell(xy) \\ \varphi(al(x))\varphi(bl(y)) &= (ad(x)\ell(x))(bd(y)\ell(y)) = ad(x)(x \cdot bd(y))f(x, y)\ell(xy) \\ &= ad(x)(x \cdot b)(x \cdot d(y))f(x, y)\ell(xy)\end{aligned}$$

By $d(xy) = xd(y) + d(x)$ and M is abelian, $\varphi((al(x))(bl(y))) = \varphi(al(x))\varphi(bl(y))$

Hence, $\varphi \in \text{Stab}_E(G, M)$.

□

Definition 2.7.2.

$$\text{Inn}_E(G, M) = \left\{ \varphi \in \text{Stab}_E(G, M) \mid \begin{array}{ccc} E & \longrightarrow & E \\ z & \longmapsto & a_0 z a_0^{-1} \end{array} \text{ for some } a_0 \in M \right\}$$

Remark 2.7.1. Let $\varphi \in \text{Inn}_E(G, M)$, say $\varphi(z) = a_0 z a_0^{-1}$ with $a_0 \in M$

$$\varphi(\ell(x)) = d(x)\ell(x) \rightsquigarrow d(x) = a_0 \ell(x) a_0^{-1} \ell(x)^{-1} = a_0(x \cdot (a_0^{-1}))$$

In additive version : $d(x) = a_0 - x a_0$

Theorem 2.7.2. $H^1(G, M) \simeq \text{Stab}_E(G, M) / \text{Inn}_E(G, M)$ (Similar to Theorem 2.7.1)

Theorem 2.7.3. Let L/K be a finite Galois extension with $G = \text{Gal}(L/K) \rightsquigarrow G \curvearrowright L^\times$. Then $H^1(G, L^\times) = 0$

Proof: Let $d : G \rightarrow L^\times$ be a derivation i.e. $d(\sigma\tau) = (\sigma d(\tau))d(\sigma)$

Claim: $\exists b \in L^\times$ s.t. $d(\sigma) = b\sigma(b)^{-1}$ ($\rightsquigarrow d$ is principle)

pf. By linear independent of automorphism $\exists c \in L^\times$ s.t.

$$b = \sum_{\tau \in G} d(\tau)\tau(c) \neq 0 \rightsquigarrow b \in L^\times$$

$$\forall \sigma \in G, \sigma(b) = \sum_{\tau \in G} \sigma(d(\tau))(\sigma(\tau(c))) = \sum_{\tau \in G} d(\sigma\tau)d(\sigma)^{-1}((\sigma\tau)(c)) = d(\sigma)^{-1}b$$

□

2.8 Applications

G : a finite group, M : abelian, $G \curvearrowright M$

Definition 2.8.1. The norm map define by

$$\begin{array}{ccc} N : M & \longrightarrow & M \\ a & \longmapsto & N(a) = \sum_{x \in G} x \cdot a \end{array}$$

Observation:

$$\forall y \in G \begin{cases} yN(a) = \sum_{x \in G} (yx)a = N(a) \rightsquigarrow \text{Im } N \subseteq M^G \\ (y-1) \cdot a \in IGM \text{ and } N((y-1)a) = N(ya) - N(a) = 0 \rightsquigarrow IGM \subseteq \ker N \end{cases}$$

- Let $M = \mathbb{Z}[G]$, recall $\mathbb{Z}[G]^G = \mathbb{Z} \cdot \left(\sum_{x \in G} x \right)$ and denote $N = \sum_{x \in G} x \in \mathbb{Z}[G]$

•• $\text{Im } N = \mathbb{Z}[G]^G = \mathbb{Z}N :$

$$(\supseteq) : \forall a \in \mathbb{Z}[G]^G = \mathbb{Z}N, \text{ say } a = nN = \sum_{x \in G} nx = \sum_{x \in G} n(x \cdot 1_G) = \sum_{x \in G} x(n \cdot 1_G) = N(n \cdot 1_G) \in \text{Im } N$$

•• $IGM = \ker N :$

$$(\supseteq) : 0 = N\left(\sum_{x \in G} n_x x\right) = \sum_{x \in G} n_x N(x) = \left(\sum_{x \in G} n_x\right) N \rightsquigarrow \sum_{x \in G} n_x = 0 \text{ i.e. } \sum_{x \in G} n_x x \in IGM.$$

$$\text{Hence, } 0 \rightarrow IG \xrightarrow{i} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}N \rightarrow 0$$

- $G = C_n = \langle \sigma \rangle$ with $o(\sigma) = n \rightsquigarrow N = 1 + \sigma + \dots + \sigma^{n-1}$ and $(\sigma - 1)N = \sigma^n - 1 = 0 \rightsquigarrow \text{Im } N \subseteq \ker(\sigma - 1)$.

Property 2.8.1. $0 \rightarrow \mathbb{Z} \cdot N \xrightarrow{i} \mathbb{Z}[C_n] \xrightarrow{\sigma-1} IC_n \rightarrow 0$ is exact.

Proof:

- $(\sigma - 1)N = 0 \rightsquigarrow \text{Im } i \subseteq \ker(\sigma - 1)$
- $a \in \ker(\sigma - 1) \rightsquigarrow (\sigma - 1)a = 0 \rightsquigarrow \sigma(a) = a \rightsquigarrow \sigma^i(a) = a \forall i = 0, \dots, n-1$ i.e. $a \in \mathbb{Z}[C_n]^{C_n} = \mathbb{Z}N$
- $IC_n = \langle \sigma^i - 1 : i = 1, \dots, n-1 \rangle_{\mathbb{Z}[C_n]}$ and $\sigma^i - 1 = (\sigma - 1)(\sigma^{i-1} + \dots + 1) \in \text{Im}(\sigma - 1)$.

□

Now, we get two exact sequence, combine them we have

- a periodic $\mathbb{Z}[C_n]$ -free resolution of \mathbb{Z}

$$\begin{array}{ccccccc} \cdots & \rightarrow & \mathbb{Z}[C_n] & \xrightarrow{\sigma-1} & \mathbb{Z}[C_n] & \xrightarrow{N} & \mathbb{Z}[C_n] & \xrightarrow{\sigma-1} & \mathbb{Z}[C_n] & \xrightarrow{\varepsilon} & \mathbb{Z} & \rightarrow & 0 \\ & & \searrow & & \swarrow & & \searrow & & \swarrow & & & & \\ & & IC_n & & \mathbb{Z} \cdot N & & IC_n & & & & & & \\ & \nearrow & & \searrow & & \nearrow & & \searrow & & \nearrow & & & \\ 0 & & & & 0 & & 0 & & 0 & & 0 & & 0 \end{array}$$

- Let $C_n \curvearrowright M$, take $\cdot \otimes_{\mathbb{Z}[C_n]} M$ functor on above resolution,

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \mathbb{Z}[C_n] \otimes M & \xrightarrow{(\sigma-1)_*} & \mathbb{Z}[C_n] \otimes M & \xrightarrow{N_*} & \mathbb{Z}[C_n] \otimes M & \xrightarrow{(\sigma-1)_*} & \mathbb{Z}[C_n] \otimes M & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\ & & M & \xrightarrow{\text{---}\sigma-1\text{---}} & M & \xrightarrow{\text{---}N\text{---}} & M & \xrightarrow{\text{---}\sigma-1\text{---}} & M & & \end{array}$$

So we get the red exact sequence with natural maps and thus

$$H_0(C_n, M) \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} M \simeq \mathbb{Z}[G]/IC_n \otimes_{\mathbb{Z}[C_n]} M \simeq M/IC_n M =: M_{C_n}$$

$$H_1(C_n, M) \simeq \ker(\sigma - 1)/\text{Im } N \simeq M^{C_n}/NM \simeq H_{\text{odd}}(C_n, M)$$

$$H_2(C_n, M) \simeq \ker N / \text{Im}(\sigma - 1) \simeq \ker N / (\sigma - 1)M \simeq H_{\text{even}}(C_n, M)$$

- Let $C_n \curvearrowright M$, take $\text{Hom}_{\mathbb{Z}[C_n]}(\cdots, M)$ functor on above resolution,

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_{\mathbb{Z}[C_n]}(\mathbb{Z}[C_n], M) & \xrightarrow{(\sigma-1)^*} & \text{Hom}_{\mathbb{Z}[C_n]}(\mathbb{Z}[C_n], M) & \xrightarrow{N^*} & \text{Hom}_{\mathbb{Z}[C_n]}(\mathbb{Z}[C_n], M) \xrightarrow{(\sigma-1)^*} \cdots \\ & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr \\ & & M & \xrightarrow[\text{red}]{\sigma-1} & M & \xrightarrow[\text{red}]{N} & M \end{array}$$

For $f \in \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[C_n], M)$, $(\sigma - 1)^*(f) : 1 \mapsto f(\sigma - 1) = (\sigma - 1)f(1)$. So we get the red exact sequence with natural maps and thus

$$H^0(C_n, M) = M^{C_n}$$

$$H^1(C_n, M) = \ker N / \text{Im}(\sigma - 1) = \ker N / (\sigma - 1)M \simeq H^{\text{odd}}(C_n, M).$$

$$H^2(C_n, M) = \ker(\sigma - 1) / \text{Im } N = M^{C_n}/NM \simeq H^{\text{even}}(C_n, M)$$

Theorem 2.8.1 (Hilbert theorem 90). Let L/K be a cyclic extension with $G = \text{Gal}(L/K) = \langle \sigma \rangle$ and $\sigma^n = 1$. Then

$$N(x) = 1 \iff \exists y \in L^\times \text{ s.t. } x = \sigma y / y$$

Proof: By Theorem 2.7.3 $0 = H^1(C_m, L^\times) = \ker N / \text{Im}(\sigma - 1) \rightsquigarrow \ker N = \text{Im}(\sigma - 1)$. Then $N(x) = 1 \iff \exists y \in L^\times \text{ s.t. } x = \sigma y / y$ for some $y \in L^\times$. \square

Recall : $\text{Im } N \subseteq M^G$, $IGM \subseteq \ker N$, we have

$$\begin{array}{ccccccc} & & M & & & & \\ & & \downarrow \pi & \searrow N & & & \\ 0 & \longrightarrow & \ker N / IGM & \xrightarrow{i} & M / IGM & \xrightarrow[\text{blue}]{\bar{N}} & M^G \xrightarrow{\pi} M^G / NM \longrightarrow 0 \\ & & \downarrow \wr & & \downarrow \wr & & \\ & & H_0(G, M) & \xrightarrow[\text{red}]{N} & H^0(G, M) & & \end{array}$$

The blue one is by factor theorem and we get red exact sequence

$$0 \rightarrow \ker N / IGM \rightarrow H_0(G, M) \xrightarrow{N} H^0(G, M) \rightarrow M^G / NM \rightarrow 0$$

Let $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ be exact in $\mathfrak{M}_{\mathbb{Z}[G]}$, then apply general snake lemma on (N, N, N)

$$\begin{array}{ccccccc} \cdots & \longrightarrow & H^1(G, M_3) & \longrightarrow & H_0(G, M_1) & \longrightarrow & H_0(G, M_2) \longrightarrow H_0(G, M_3) \longrightarrow 0 \\ & & \downarrow N & & \downarrow N & & \downarrow N \\ 0 & \longrightarrow & H^0(G, M_1) & \longrightarrow & H^0(G, M_2) & \longrightarrow & H^0(G, M_3) \longrightarrow H^1(G, M_1) \longrightarrow \cdots \end{array}$$

We get

$$\begin{array}{ccccccc}
 \cdots & \longrightarrow & H_1(G, M_3) & \longrightarrow & \ker_{M_1} N / IG \cdot M_1 & \longrightarrow & \ker_{M_2} N / IG \cdot M_2 \longrightarrow \ker_{M_3} N / IG \cdot M_3 \\
 pt & & & & \searrow & & \nearrow \\
 & & & & M_1^G / NM_1 & \longrightarrow & M_2^G / NM_2 \longrightarrow M_3^G / NM_3 \longrightarrow H^1(G, M_1) \longrightarrow \cdots
 \end{array}$$

Define **Tate cohomology group** by

$$\widehat{H}^n(G, M) = \begin{cases} H^n(G, M) & , \text{ if } n \geq 1 \\ \text{coker } N = M^G / NM & , \text{ if } n = 0 \\ \text{ker } N = \text{ker}_M N / IG \cdot M & , \text{ if } n = -1 \\ H_{-(n+1)}(G, M) & , \text{ if } n \leq -2 \end{cases}$$

Then $\forall -\infty < n < \infty$,

$$\cdots \rightarrow \widehat{H}^n(G, M_1) \rightarrow \widehat{H}^n(G, M_2) \rightarrow \widehat{H}^n(G, M_3) \rightarrow \widehat{H}^{n+1}(G, M_1) \rightarrow \cdots$$

Example 2.8.1. $G \simeq C_n$

$$\begin{array}{ccccc}
& \widehat{H}^0(C_m, M_2) & \longrightarrow & \widehat{H}^0(C_m, M_3) & \\
& \nearrow & & \searrow & \\
\widehat{H}^0(C_m, M_1) & & & & \widehat{H}^1(C_m, M_1) \\
& & & & \parallel \\
& & & & \widehat{H}^{-1}(C_m, M_1) \\
& \nwarrow & & \swarrow & \\
& \widehat{H}^{-1}(C_m, M_3) & \longleftarrow & \widehat{H}^{-1}(C_m, M_2) &
\end{array}$$

For red isomorphism :

$$\widehat{H}^{-1}(C_m, M_1) \simeq \ker_{M_1} N / IC_n \cdot M_1 = \ker_{M_1} N / (\sigma - 1) \cdot M_1 \simeq \widehat{H}^1(C_m, M_1)$$

Example 2.8.2. $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{1, a, b, c\}$, $M = \mathbb{Z}/2\mathbb{Z}$

Since $\text{Aut}(M) = \{\text{id}\} \implies G \curvearrowright M$ trivially i.e. $ax = x \ \forall a \in G, x \in M$.

Calculate $H^2(G, M)$:

$$\mathrm{Hom}_{\mathbb{Z}[G]}(B_2^*, M) = \mathrm{Func}((G \setminus \{1\})^2, M) \rightsquigarrow \# = 2^9.$$

If $f \in Z^2(G, M)$, then f must satisfy cocycle identity i.e.

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz) \quad \forall x \in G \setminus \{1\}.$$

Then

$$f(x, y) + f(xy, z) + f(y, z) + f(x, yz) = 0$$

$$x = y : f(x, x) + f(x^2, z) + f(x, z) + f(x, xz) = 0 \rightsquigarrow f(x, a) + f(x, b) + f(x, c) = 0.$$

If we fix $f(a, a) = \alpha, f(a, b) = \beta, f(b, a) = \delta, f(b, b) = \varepsilon$. Then other value can be uniquely decided. So $|Z^2(G, M)| \leq 2^4$.

Now, if $f \in B^2(G, M)$, then $\exists h : G \rightarrow M$ s.t. $f(x, y) = h(y) - h(xy) + h(x) \forall x, y \in G$.

$$x = y : f(x, x) = h(x) + h(x^2) + h(x) = 0$$

$$x \neq y : f(x, y) = h(a) + h(b) + h(c) \rightsquigarrow |B^2(G, M)| = 2 \text{ and thus } |H^2(G, M)| \leq 8.$$

In this case, $E \simeq (\mathbb{Z}/2\mathbb{Z})^3, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_4, Q_8$.

- $E \simeq (\mathbb{Z}/2\mathbb{Z})^3$, then $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ splits $\rightsquigarrow f = 0 \in H^2(G, M)$

- $E \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, M = \langle x^2 \rangle$: Then we have
 $\quad \quad \quad = \langle x \rangle \quad \quad = \langle y \rangle$

$$Mx = \{x, x^3\}, Mxy = \{xy, x^3y\}, My = \{y, x^2y\}$$

with order 4, 4, 2 respectively. One of $\ell(a), \ell(b), \ell(c)$ has order 2 and others are 4. So we have 3 inequivalent extensions.

- $E \simeq D_4 = \langle x, y : x^4 = y^2 = e, yx = x^{-1}y \rangle, M = \langle x^2 \rangle$: Then we have

$$Mx = \{x, x^3\}, My = \langle y, x^2y \rangle, Mxy = \{xy, x^3y\}$$

with order 4, 2, 2 respectively. One of $\ell(a), \ell(b), \ell(c)$ has order 4 and others are 2. So we have 3 inequivalent extensions.

- $E \simeq Q_8, M = \langle 1, -1 \rangle$: Then we have

$$Mi = \langle \pm i \rangle, Mj = \langle \pm j \rangle, Mk = \langle \pm k \rangle$$

with order 4. So we have 1 inequivalent extensions.

So $|H^2(G, M)|$ is exactly 8.

Calculate $H^1(G, M) \simeq \text{Der}(G, M) / \text{PDer}(G, M)$:

If $d \in \text{Der}(G, M) : d(xy) = xd(y) + d(x)y = d(x) + d(y)$ which is group homomorphism.

If $d \in \text{PDer}(G, M) : d(x) = xv - v = v - v = 0$

So $H^1(G, M) \simeq \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \rightsquigarrow |H^1(G, M)| = 4$

Chapter 3

Representation theory

3.1 Semisimple modules

In this section, A may not be commute and M be a left A -module.

3.1.1 Semisimple modules

Definition 3.1.1. Let A be a ring and M be a left A -module

- M is **simple** if $M \neq 0$ and it has no nontrivial proper submodule.
- M is **semisimple** if $M = \bigoplus_{i \in \Lambda} M_i$ with M_i : simple submodules of $M \forall i$

Lemma 3.1.1 (Schur's lemma). Let M, N be two simple A -modules. Then $\forall 0 \neq f \in \text{Hom}_A(M, N)$, f is an isomorphism, In particular, M : simple $\implies \text{End}_A(M)$ is a division ring. Sometimes we will denote $\text{End}_A(M)$ by $A'(M)$ or A' .

Proof: $\because \ker f \leq M$ and $\text{Im } f \leq N \therefore \ker f = 0$ or M and $\text{Im } f = 0$ or N . If $\ker f = M$ or $\text{Im } f = 0$, then $f = 0$ ($\rightarrow \leftarrow$). So $\ker f = 0$, $\text{Im } f = N \rightsquigarrow f$ is isomorphism. \square

Property 3.1.1. TFAE

- (1) M is semisimple
- (2) $\forall 0 \neq N \subseteq M, \exists N' \leq M$ s.t. $M = N \oplus N'$
- (3) $M = \sum_{i \in J} M_i$ with M_i : simple in M .

Proof: Before proof TFAE, we see the key lemma.

Key lemma: If $M = \sum_{i \in J} M_i$ with M_i : simple, then $\exists I \subseteq J$ s.t. $M = \bigoplus_{i \in I} M_i$
pf. Let $\mathcal{S} = \{I' \subseteq J : \sum_{i \in I'} M_i \text{ is direct}\} \neq \emptyset$ and $\{I_i\}_{i \in \Lambda}$ be a chain in \mathcal{S} .

Consider $I' = \bigcup_{i \in \Lambda} I_i$ which is lies in \mathcal{S} , since if $x \in M_k \cap \left(\bigoplus_{j \in I' \setminus \{k\}} M_j \right) \rightsquigarrow x \in$

$M_k \cap \bigoplus_{j \in J'} M_j$ for some finite subsets J' of $I \setminus k$ and $\{k\} \cup J' \subseteq I_i$ for some $i \rightsquigarrow x = 0$. By Zorn's lemma, \exists a maximal I in \mathcal{S} . We claim that $M = \bigoplus_{i \in I} M_i$. For $j \in J \setminus I$, consider $M_j \cap \left(\bigoplus_{i \in I} M_i \right) \leq M_j$. By M_j is simple, $M_j \cap \left(\bigoplus_{i \in I} M_i \right) = 0$ or M_j . For former, $I \subseteq \{j\} \cup I \in \mathcal{S} (\rightarrow \leftarrow)$. For latter, $M_j \subseteq \bigoplus_{i \in I} M_i$. \square

Back to origin problem.

- (3) \Rightarrow (1) : By key lemma.
- (1) \Rightarrow (2) : Let $M = \bigoplus_{i \in J} M_i$. Consider

$$\mathcal{S} = \left\{ I' \subseteq J \mid N + \left(\bigoplus_{i \in I'} M_i \right) \text{ is direct} \right\}.$$

By Zorn's lemma, \exists a maximal element $I \in \mathcal{S}$. We claim that $M = N \oplus \left(\bigoplus_{i \in I} M_i \right)$. $\forall j \in J \setminus I$, $M_j \subseteq \text{RHS}$ (by similar reason in above).

- (2) \Rightarrow (3) : First, we prove if M satisfy the assumption, then M contain a simple submodule : Let $0 \neq x \in M$ and $\varphi : A \rightarrow Ax \rightsquigarrow \ker \varphi$ is a proper left ideal of A . By Zorn's lemma, \exists a left maximal ideal \mathfrak{m} in A s.t. $\ker \varphi \subseteq \mathfrak{m} \rightsquigarrow \mathfrak{m}x \rightsquigarrow \mathfrak{m}x$ is a maximal proper submodule of $Ax \subseteq Mx$. By assumption, $M = \mathfrak{m}x \oplus M' \rightsquigarrow Ax \rightsquigarrow Ax = \mathfrak{m}x \oplus (M' \cap Ax)$.

Claim : $M' \cap Ax$ is a simple submodule of M .

.. $\mathfrak{m}x \subsetneq Ax \rightsquigarrow M' \cap Ax \neq 0$

.. If $M' \cap Ax$ has a nontrivial proper submodule N , then $\mathfrak{m}x \subsetneq \mathfrak{m}x \oplus N \subsetneq Ax$

Let $M_0 = \sum_{\substack{\text{simple} \\ M_i \subseteq M}} M_i$. If $M \neq M_0$, then $M = M_0 \oplus M'_0$ with $M'_0 \neq 0$. Notice that M'_0 also satisfy the assumption, so \exists a simple submodule $N \leq M'_0 (\rightarrow \leftarrow)$. \square

Theorem 3.1.1. If $M \simeq M_1^{\oplus n_1} \oplus \dots \oplus M_r^{\oplus n_r} \simeq N_1^{\oplus m_1} \oplus \dots \oplus N_s^{\oplus m_s}$ with N_i, M_j : simple and $M_i \neq M_j, N_i \neq N_j \forall i \neq j$. Then $r = s$ and $M_i \simeq N_i \forall i$ after rearrangement of indices and $n_i = m_i$.

Proof: Let $f_{ij} : M_i \xrightarrow{\rho_i} M \xrightarrow{\pi_j} N_j$. By Schur's lemma, $\forall i, f_{ij} = 0$ or isomorphism. $\forall j$, if $\forall i, f_{ij} = 0 \rightsquigarrow \rho_i : M_i \rightarrow M$ is zero map $\forall i \rightsquigarrow M_i = 0 (\rightarrow \leftarrow)$. So $\exists!$ j s.t. f_{ij} is isom. and thus $M_i \simeq N_j$ (otherwise $N_{j_1} \simeq M_i \simeq N_{j_2}$ for distinct j_1, j_2). Thus $r \leq s$. By symmetry, $r = s$. Finally, $M_i^{\oplus n_i} \simeq N_i^{\oplus m_i} \rightsquigarrow n_i = m_i$. \square

3.1.2 Matrix form of simple and semisimple modules

Observation:

- $M = N^{\oplus n}$ with N : simple. Let $\varphi \in \text{Hom}_A(M, M)$ and $\rho_i : N \hookrightarrow M, \pi_i : M \rightarrow N$ be inclusion from i -th N to M and projection from M to i -th N .

Define $\varphi_{ij} = \pi_i \circ \varphi \circ \rho_j : N \rightarrow N$, then $\varphi_{ij} \in \text{End}_A(N) =: D'$ and for $x = (x_1, \dots, x_n) \in M$ with $x_i \in N \forall i$

$$\begin{aligned} \varphi(x) &= \varphi \left(\sum_{j=1}^n \rho_j(x_j) \right) = \sum_{j=1}^n \varphi(\rho_j(x_j)) \\ &= \left(\pi_1 \left(\sum_{j=1}^n \varphi \circ \rho_j(x_j) \right), \dots, \pi_n \left(\sum_{j=1}^n \varphi \circ \rho_j(x_j) \right) \right) \\ \implies \varphi(x) &= \begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n} \\ \varphi_{21} & \ddots & & \dots \\ \vdots & & & \\ \varphi_{n1} & \varphi_{n2} & \cdots & \varphi_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \end{aligned}$$

Hence, $\varphi \longleftrightarrow (\varphi_{ij}) \in M_{n \times n}(D')$ and we leave the checking

$$\text{End}_A(M) \simeq M_{n \times n}(D') \text{ as a ring}$$

in Homework 20.

- $M = N_1^{\oplus m_1} \oplus \dots \oplus N_r^{\oplus m_r}$: For all $\varphi \in \text{End}_A(M)$, we have the corresponding

$$\varphi \longleftrightarrow \begin{pmatrix} \left(\varphi|_{N_1^{\oplus m_1}} \right) & & & \\ & \left(\varphi|_{N_2^{\oplus m_2}} \right) & & \\ & & \ddots & \\ & & & \left(\varphi|_{N_r^{\oplus m_r}} \right) \end{pmatrix}$$

where $(\varphi|_{N_i^{\oplus m_i}}) \in M_{m_i \times m_i}(D'_i)$ and $D'_i = \text{End}_A(N_i)$. Notice that others blocks are all zero, for example $(m_1 + 1, 1)$ -entry is $\pi_{m_1+1} \circ \varphi \circ \rho_1 : N_1 \rightarrow N_2$ which is not isomorphism and thus is zero map. This give us

$$\text{End}_A(M) \simeq M_{m_1 \times m_1}(D'_1) \oplus \dots \oplus M_{m_r \times m_r}(D'_r) \text{ as a ring}$$

which leave it at Homework 20.

- Let M be a semisimple A -module and $A' = \text{End}_A(M)$, consider

$$\begin{aligned} A' \times M &\longrightarrow M \\ (\varphi, x) &\longmapsto \varphi(x) \end{aligned}$$

So M is an A' -module i.e. M is a module over a division ring.

Now, consider $\forall a \in A$,

$$\begin{aligned} f_a : M &\longrightarrow M \\ x &\longmapsto ax \end{aligned}$$

- f_a is not always A -homomorphism, since in general the equality will not hold. It need A is commutative.

$$f_a(bx) = (ab)x \neq (ba)x = bf_a(x)$$

- However, f_a is A' -homomorphism

$$f_a(\varphi(x)) = a\varphi(x) = \varphi(ax) = \varphi(f_a(x))$$

So $f_a \in \text{End}_{A'}(M)$ and denote $\text{End}_{A'}(M)$ by A'' . This give as a ring homomorphism $A \rightarrow A''$, but it will not always a ring isomorphism.

Theorem 3.1.2 (Jacobson theorem). If $M = N_1^{\oplus m_1} \oplus \dots \oplus N_r^{\oplus m_r}$ with N_i : simple and let $A' = \text{End}_A(M)$. Then

- (1) If $f \in A'' = \text{End}_{A'}(M)$ and $x_1, \dots, x_n \in M$, then $\exists a \in A$ s.t. $f(x_i) = f_a(x_i) \forall i$
- (2) If $M = \langle x_1, \dots, x_n \rangle_{A'}$, then
$$\begin{array}{ccc} A & \longrightarrow & A'' \\ a & \longmapsto & f_a \end{array}$$

Proof:

- (1) First, we prove the cases $n = 1$: Write $M = Ax \oplus M'$, since M is semisimple. Let $\pi : M \rightarrow Ax$ be the projection $\rightsquigarrow \pi \in A'$. By $f \in \text{End}_{A'}(M)$, we have

$$f(x) = f(\pi(x)) = \pi(f(x)) \in Ax \rightsquigarrow \exists a \in A \text{ s.t. } f(x) = ax$$

For $n > 1$: It's the most trick part, consider

$$\begin{array}{ccc} f^{\oplus n} : & M^{\oplus n} & \longrightarrow & M^{\oplus n} \\ & (y_1, \dots, y_n) & \longmapsto & (f(y_1), \dots, f(y_n)) \end{array}$$

Then we can write as the matrix version :

$$\begin{pmatrix} f & & \\ & \ddots & \\ & & f \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Notice that we always can write $\text{End}_A(M^{\oplus n})$ as $M_n(A')$.

Claim: $f^{\oplus n} \in \text{End}_{\text{End}_A(M^{\oplus n})}(M^{\oplus n})$

pf. Write it as matrix version. For all $\varphi_{ij} \in \text{End}_{A'}(M)$, we have

$$(\delta_{ij}f)(\varphi_{ij}) = (f\varphi_{ij}) = (\varphi_{ij}f) = (\varphi_{ij})(\delta_{ij}f).$$

The red equality is from $f \in \text{End}_{A'}(M)$. □

Apply the cases $n = 1$ on $f^{\oplus n}$, let $\bar{x} = (x_1, \dots, x_n)$, there $\exists a \in A$ s.t. $f^{\oplus n}(\bar{x}) = a\bar{x}$ i.e. $f(x_i) = ax_i \forall i = 1, \dots, n$.

- (2) Apply (1), $\forall f \in A'' \exists a \in A$ s.t. $f(x_i) = f_a(x_i) \forall i \rightsquigarrow f = f_a$. □

Theorem 3.1.3 (Wedderburn's theorem). Let M be a simple **faithful** ($\text{def} : \text{Ann}(M) = 0$) module over A . Let $D = \text{End}_A(M)$ and M be finite dimensional n over D . Then $A \simeq M_n(D^\circ)$.

Proof: Let $M = \langle x_1, \dots, x_n \rangle_D$, by Jacobson theorem,

$$\begin{array}{ccccc} A & \rightarrow & \text{End}_D(M) & \simeq & M_n(\text{End}_D(D)) \simeq M_n(D^\circ) \\ a & \mapsto & f_a & & \end{array}$$

Now, if $f_a = f_b$ for some $a, b \in A$, then $ax = bx \ \forall x \in M \rightsquigarrow (a - b) \in \text{Ann}_A(M) \rightsquigarrow a = b$. Hence, $A \simeq M_n(D^\circ)$ \square

3.2 Semisimple rings

3.2.1 Semisimple rings

Definition 3.2.1. A ring R is semisimple if $R \neq 0$ and it is semisimple as a left R -module. (or denoted by ${}_R R$)

Property 3.2.1. R is semisimple $\iff \forall M \in {}_R \mathfrak{M}, M$ is semisimple.

Proof: (\Leftarrow) : OK!

(\Rightarrow) : R is semisimple \rightsquigarrow any free R -module is semisimple. Since any R -module is a quotient of free R -module and thus it is semisimple. \square

Property 3.2.2. Any semisimple ring R is a finite direct sum of minimal left ideals and every simple R -module is isomorphic to one of them. In particular, it is left Artinian and Noetherian.

Proof:

- Let $R = \bigoplus_{i \in \Lambda} I_i$ with I_i : minimal left ideal of $R \ \forall i$,

$$\because 1 \in R \therefore 1 = x_1 + \dots + x_n \text{ with } x_k \in I_{i_k} \ \forall k \rightsquigarrow R \subseteq \bigoplus_{k=1}^n I_{i_k} \text{ and thus } R = \bigoplus_{k=1}^n I_{i_k}$$

- Let M be a simple R -module and $0 \neq x \in M \rightsquigarrow M = Rx$. Consider

$$\begin{array}{ccc} \varphi : R & \longrightarrow & M \\ r & \longmapsto & rx \end{array} \text{ and } \varphi|_{I_{i_k}} : I_{i_k} \longrightarrow M$$

Then $\varphi|_{I_{i_k}} = 0$ or isomorphism. Since $\varphi \neq 0 \rightsquigarrow \exists k$ s.t. $\varphi|_{I_{i_k}} \neq 0 \rightsquigarrow \varphi|_{I_{i_k}} : I_{i_k} \xrightarrow{\sim} M$

- Let $J_r = \bigoplus_{k=1}^r I_k \rightsquigarrow R = J_n \supseteq J_{n-1} \subseteq \dots \subseteq J_1 \subseteq J_0 = 0$ and $J_k/J_{k-1} \simeq I_k$: simple.

So R has a finite composition series $\rightsquigarrow R$ is Artinian and Noetherian. \square

Theorem 3.2.1 (Artin-Wedderburn theorem). A semisimple ring R is a finite direct product of matrix rings over division rings.

Proof: Let $R = I_1 \oplus \cdots \oplus I_n$ with I_i : minimal left ideal of R . Rewrite R as $I_{i_1}^{\oplus s_1} \oplus \cdots \oplus I_{i_t}^{\oplus s_t}$ with $I_{i_p} \not\cong I_{i_q}$ for distinct p, q . Let $D_j = \text{End}_R(I_{i_j})$, then

$$\text{End}_R(R) \simeq M_{s_1 \times s_1}(D_1) \oplus \cdots \oplus M_{s_t \times s_t}(D_t) \text{ as rings}$$

- Define $f_a : R \rightarrow R$ by $1 \mapsto a \rightsquigarrow f_a : r \mapsto ra$. Then $f_a \circ f_b(r) = f_a(rb) = r(ba) \rightsquigarrow \text{End}_R(R) \simeq R^\circ$ and thus

$$R \simeq (R^\circ)^\circ \simeq \bigoplus_{i=1}^t (M_{s_i}(D_i))^\circ$$

- $\forall i$ define $\psi : (M_n(D_i))^\circ \longrightarrow M_n(D_i^\circ)$
 $A = (a_{ij}) \longmapsto A^t = (a'_{ij})$, where $a'_{ij} = a_{ji}$ (In below, we use \cdot represent the opposite multiplication). Then

$$\begin{aligned} \psi(A \cdot B) &= \psi(BA) = (BA)^t = \left(\sum_{k=1}^n b_{ik} \cdot a_{kj} \right)^t = \left(\sum_{k=1}^n b_{jk} \cdot a_{ki} \right) \\ &= \left(\sum_{k=1}^n a_{ki} b_{jk} \right) = \left(\sum_{k=1}^n a'_{ik} b'_{kj} \right) = A^t B^t = \psi(A) \psi(B) \end{aligned}$$

Combine with D_i : division $\rightsquigarrow D_i^\circ$: division, we have

$$R \simeq \bigoplus_{i=1}^t M_{s_i}(D_i^\circ)$$

i.e. R is a finite direct product of matrix rings over division rings.

□

3.2.2 Product of ring

Before we move forward, We check something about product, so that we can use them freely after.

Observation:

- $R \simeq R_1 \times \cdots \times R_n$ with R_i : ring $\forall i$. Let $I_i \longleftrightarrow (0, \dots, 0, R_i, 0, \dots, 0)$.
- I_i is two-sided ideal with $I_i \simeq R_i$ as rings.
- $I_i I_j = 0$ for all $i \neq j$
- $R = \sum_{i=1}^n I_i = \bigoplus_{i=1}^n I_i$ (Note : I_i is a ring but not a subring of R if $n \geq 2$)

- Conversely, if $\exists \{I_i\}_{i \in \Lambda}$ s.t. $\begin{cases} I_i : \text{two-sided ideal } \forall i \text{ and } R = \sum_{i \in \Lambda} I_i \\ I_i I_j = 0 \text{ for all } i \neq j \end{cases}$, then

•• $|\Lambda| = n < \infty$

•• I_i is a ring R_i s.t. $R \simeq R_1 \times \cdots \times R_n$

proof:

•• Let $1 = \sum_{i \in \Lambda} e_i$ with $e_i = 0$ for almost all i .

For $x \in I_i$, $x = x \cdot 1 = x e_i$. If $e_j = 0 \rightsquigarrow I_j = 0$ and thus $|\Lambda| = n < \infty$.

•• $I_i : \text{two-sided ideal} \rightsquigarrow \begin{cases} I_i \text{ is closed under } “+ , \cdot” \\ x e_i = e_i x \forall x \in I_i \rightsquigarrow e_i \text{ is identity for } I_i \end{cases}$
 $\rightsquigarrow I_i$ is a ring R_i .

•• $R = \sum_{i=1}^n I_i$ is direct : If $x \in I_i \cap \left(\sum_{j \neq i} I_j \right) \rightsquigarrow x = e_i x = 0$

•• $R \simeq R_1 \times \cdots \times R_n$: Given $x = \sum_{i=1}^n x_i, y = \sum_{i=1}^n y_i \rightsquigarrow xy = \sum_{i=1}^n x_i y_i$, since $x_i y_j = 0$ for $i \neq j$.

- If $R = R_1 \times \cdots \times R_n$, then a simple left R -module M is a simple left R_i -module for some i .

proof:

•• $\sum_{i=1}^n R_i M = \left(\sum_{i=1}^n R_i \right) M = RM = M \neq 0 \rightsquigarrow R_i M \neq 0$ for some i .

Since $R_i R_j = 0$ for $i \neq j$, $R_i M = R R_i M \rightsquigarrow R_i M$ is a left R -submodule of M
 $\rightsquigarrow R_i M = M \rightsquigarrow R_j M = R_j R_i M = 0 \forall j \neq i$.

•• Let e_j be the identity of $R_j \forall j = 1, \dots, n \rightsquigarrow 1 = \sum_{j=1}^n e_j \rightsquigarrow \forall x \in M, x = 1 \cdot x = \sum_{j=1}^n e_j x = e_i x \rightsquigarrow M$ is an R_i -module.

•• N is R_i -simple : If N is an R_i -submodule of M , then $RN = \left(\sum_{j=1}^n R_j \right) N = R_i N = N \rightsquigarrow N$ is an R -submodule of $M \rightsquigarrow N = 0$ or M .

- Conversely, M is a simple R_i -module, then by $R_j M = 0 \forall j \neq i$, M is a R -module. If N is a R -submodule of M , then $R_i N = \left(\sum_{j=1}^n R_j \right) N = RN \subseteq N$ i.e. N is an R_i -submodule of $M \rightsquigarrow N = 0$ or M .

From now on, the concept of direct sum and direct product has a correspondence and we will feel free using those.

3.2.3 Radical

In this subsection, we try to transfer useful properties in commutative algebra to non-commutative algebra. For example : basis property of Jacobson radical and Nakayama's lemma. We leave it in Homework 21 and we will use it unreservedly.

Definition 3.2.2. Let A be a ring. The **(Jacobson) radical** of A , denoted by $r(A)$ is the intersection of all max left ideals of A . (Note : the existence of max left ideals is by Zorn's lemma, which may not assume A is commutative)

Property 3.2.3. $r(A) = \bigcap_{M: \text{ simple}} \text{Ann}(M)$ is a two-sided ideal.

Proof:

- $\text{RHS} = \bigcap_{M: \text{ simple}} \bigcap_{x \in M \setminus \{0\}} \text{ann}(x)$. For $x \in M \setminus \{0\}$, $\text{ann}(x) \neq A \rightsquigarrow \exists$ a max left ideal \mathfrak{m} s.t. $\text{ann}(x) \subseteq \mathfrak{m}$ (By Zorn's lemma).
 $\therefore M = Ax \simeq A/\text{ann}(x) \supsetneq \mathfrak{m}/\text{ann}(x) \implies \mathfrak{m}/\text{ann}(x) = 0$ i.e. $\mathfrak{m} = \text{ann}(x) \implies r(A) \subseteq \bigcap_{M: \text{ simple}} \text{Ann}(M)$
- Let \mathfrak{m} be a maximal left ideal of A , then A/\mathfrak{m} is simple A -module and $\mathfrak{m} = \text{ann}(\bar{1})$ with $\bar{1} \in A/\mathfrak{m} \implies \text{RHS} \subseteq r(A)$.

□

Definition 3.2.3. Given a ring A and I is a ideal of A . Then

- I is **nil ideal** if $\forall a \in I, a^n = 0$ for some $n \in \mathbb{N}$ depend on a .
- I is **nilpotent ideal** if $\exists n \in \mathbb{N}$ s.t. $I^n = 0$.

Property 3.2.4. Any nil ideal I is contained in $r(A)$.

Proof: $\forall a \in I \forall y \in A, ya \in I$, say $(ya)^n = 0$, then

$$(1 - ya)^{-1} = 1 + ya + \cdots + (ya)^{n-1}$$

i.e. $\forall y \in A, 1 - ya$ is unit in $A \rightsquigarrow a \in r(A)$.

□

Property 3.2.5. Let R be a left Artinian. Then $r(R)$ is the largest nilpotent ideal in R .

Proof: $r(R) \subseteq r(R)^2 \subseteq \cdots \rightsquigarrow r(R)^m = r(R)^{m+1} = \cdots =: I \rightsquigarrow I^2 = I$.

Assume that $I \neq 0$. Let $\mathcal{S} = \{J \subseteq R : IJ \neq 0\} \neq \emptyset$, since $I \in \mathcal{S}$. Since R is Artinian, $\exists J_0$ is minimal element in \mathcal{S} i.e. $IJ_0 \neq 0$. Pick $a \in J_0$ s.t. $Ia \neq 0 \rightsquigarrow I(Ra) \neq 0$ and $Ra \subseteq J_0 \rightsquigarrow J_0 = Ra$ is f.g. And $0 \neq IJ_0 = I(IJ_0) \rightsquigarrow J_0 \supseteq IJ_0 \in \mathcal{S} \implies IJ_0 = J_0$. By Nakayama's lemma, $J_0 = 0$ ($\rightarrow \leftarrow$).

So $I = 0 \implies r(R)^m = 0$ i.e. $r(R)$ is nilpotent ideal.

Finally, $\forall J : \text{left nilpotent ideal} \implies J$ is nil ideal. By Property 3.2.4, $J \subseteq r(R)$.

□

Property 3.2.6. R : left Artinian $\rightsquigarrow r(R) = \bigcap_{i=1}^n m_i$ with m_i : maximal left ideal.

Proof: Let $\mathcal{S} = \{\text{finite intersection of maximal left ideals}\} \neq \emptyset$ by Zorn's lemma. Since R is Artinian $\rightsquigarrow \bigcap_{i=1}^n m_i$ is minimal in \mathcal{S} . Then for all m : maximal left ideal of A , $m \cap \left(\bigcap_{i=1}^n m_i\right) = \bigcap_{i=1}^n m_i \rightsquigarrow r(R) = \bigcap_{i=1}^n m_i$. \square

Theorem 3.2.2. TFAE

- (1) R is semisimple.
- (2) R is Artinian and $r(R) = 0$.

Proof:

- (1) \Rightarrow (2) : By Property 3.2.2, R is Artinian. Let $R = \bigoplus_{i=1}^n I_i \implies 0 = \text{Ann}_R(R) = \bigcap_{i=1}^n \text{Ann}_R(I_i) = r(R)$, since every simple R -module will be isomorphic to I_k for some k .
- (2) \Rightarrow (1) : Since R is left Artinian, $r(R) = \bigcap_{i=1}^n m_i$ for some m_i : maximal left ideal. By Chinese remainder theorem,

$$R \simeq R/r(R) \simeq R/\bigcap_{i=1}^n m_i \simeq R/m_1 \times \cdots \times R/m_n$$

So R is semisimple. \square

3.3 Simple rings

3.3.1 Simple rings and Artin-Wedderburn theorem

Definition 3.3.1. R is **simple** if R is semisimple and has no two-sided ideals other than 0 and R .

Property 3.3.1 (key property). Let R be a semisimple ring. Then R is simple \iff all simple R -module are isomorphic.

Proof:

- (\Rightarrow) : Recall $R = \bigoplus_{i=1}^n I_i$, I_i : minimal left ideal of R . If M is a simple R -module, then $M \simeq I_j$ for some j . Pick a minimal left ideal of R , say I . For $0 \neq a \in I$,

$Ra = I$ by minimality of I . The two-sided RaR is nonzero, so $RaR = R$. That is $R = \sum_{b \in R} Rab$.

Claim: $Rab = 0$ or $Rab \simeq Ra = I$.

p.f. Consider $\rho_b : \begin{matrix} R & \longrightarrow & R \\ r & \longmapsto & rb \end{matrix} \rightsquigarrow \rho_b(r'r) = (r'r)b = r'(rb) = r'\rho_b(r) \rightsquigarrow \rho_b \in \text{End}_R({}_R R)$. It is clear that $Rab = \rho_b(Ra) \simeq Ra / \ker \rho_b|_{Ra}$.

Since Ra is minimal, $\ker \rho_b|_{Ra} = 0$ or $Ra \rightsquigarrow Rab \simeq Ra$ or 0 □

By Claim, if $Rab \neq 0$, then Rab is a minimal left ideal. So $R = \bigoplus_{i=1}^n Rab_i$ and $Rab_i \simeq I$. By recall, every simple R -module will isomorphic to I .

- (\Leftarrow) : By assumption, $R \simeq I^{\oplus n}$ with I : minimal left ideal. So $R^\circ \simeq \text{End}_R({}_R R) \simeq M_n(D)$, where $D = \text{End}_R(I)$. Since I is simple, D is a division ring. So $R \simeq M_n(D^\circ)$ and D° also is a division ring. By Homework 20, the only two-sided ideals of matrix ring over division ring are 0 and itself. Hence, R is simple. □

Theorem 3.3.1 (Artin-Wedderburn theorem). R is simple $\iff R \simeq M_n(D)$ with D : division ring.

Proof:

- (\Rightarrow) : By the proof of key property $R \simeq M_n(D)$, where $D = (\text{End}_R(I))^\circ$
- (\Leftarrow) : First, we study “ $M_n(D)$ ”.
- $\bullet \exists$ a composition series (\rightsquigarrow Artinian) : Let $e_{ij} \in M_n(R)$ s.t. only (i, j) -entry is 1, and others are 0. Observe that

$$M_n(D) = M_n(D)e_{11} \oplus \cdots \oplus M_n(D)e_{nn}$$

Claim: $M_n(D)e_{ii}$ is a minimal left ideal of $M_n(D)$

p.f. Let $0 \neq I \subseteq M_n(D)e_{ii}$ and $0 \neq \sum_{j=1}^n a_j e_{ji}$, say $a_k \neq 0$, then

$$I \ni a_k^{-1} e_{ik} \sum_{j=1}^n a_j e_{ji} = \sum_{j=1}^n a_k^{-1} a_j e_{ik} e_{ji} = e_{ii} \implies I = M_n(D)e_{ii}$$

□

Let $C_j = \bigoplus_{i=1}^j M_n(D)e_{ii} \rightsquigarrow C_j/C_{j-1} \simeq M_n(D)e_{jj}$: simple. So

$$M_n(D) = C_n \supset C_{n-1} \supset \cdots \supset C_1 \supset C_0 = 0 \text{ is a composition series}$$

Hence, $\ell(M_n(D)) = n$.

- \therefore radical is the intersection of all maximal left ideal $\therefore r(M_n(D)) \subsetneq M_n(D)$.
- $\therefore M_n(D)$ has no two-sided ideal other than 0 and $M_n(D)$ and radical is two-sided ideal $\therefore r(M_n(D)) = 0$.

Hence, $M_n(D)$ is semisimple. Finally, the only two-sided ideal of $M_n(D)$ are 0 and $M_n(D)$, so $M_n(D)$ is simple.

□

Example 3.3.1. M is simple faithful A -module. Then $D = \text{End}_A(M)$ is division ring and $M \in {}_D\mathfrak{M}$. If $\dim_D M = n$, by Wedderburn's theorem, $A \simeq M_n(D^\circ)$. So $A \simeq M_n(D^\circ)$ is a simple ring.

Conversely, If M is simple A -module and A is simple, then M is faithful A -module. *pf.* If $0 \neq a \in \text{Ann}(M)$, then $A = AaA$ and $M = AM = AaAM = AaM = 0$ ($\rightarrow \leftarrow$).

3.3.2 Matrix rings

Theorem 3.3.2. If $R = M_n(D)$ with D : division ring and N is the unique simple R -module, then $D \simeq (\text{End}_R(N))^\circ$. Which means D is unique determined by R .

Proof: We can choose $N = M_n(D)e_{11}$. For $a \in D$, define

$$\begin{aligned} \rho_a : N &\longrightarrow N \\ U &\longmapsto U(ae_{11}) \end{aligned}$$

- $\rho_a \in \text{End}_R(N) : \forall U, V \in M_n(D), \rho_a(VU) = (VU)(ae_{11}) = V(U(ae_{11})) = V\rho_a(U)$
- Now, we have the correspondence between D and $\text{End}_R(N)$. Based on previous experience, we found that this correspondence is anti-homomorphism. So we define

$$\begin{aligned} \varphi : D^\circ &\longrightarrow \text{End}_R(N) \\ a &\longmapsto \rho_a \end{aligned}$$

- φ is a ring homo : $\varphi(a \cdot b) = \varphi(ba) = \rho_{ba}$

$$\rho_{ba}(U) = U((ba)e_{11}) = (Ube_{11})(ae_{11}) = \rho_a(Ube_{11}) = \rho_a\rho_b(U)$$

- φ is $1 - 1$: $\rho_a(U) = 0 \rightsquigarrow U(ae_{11}) = 0 \forall U$. If $a \neq 0$, then $U = a^{-1}e_{11} \in N$ and $U(ae_{11}) = e_{11} \neq 0$ ($\rightarrow \leftarrow$).

- φ is onto : For $f \in \text{End}_R(N)$. Let $f(e_{11}) = \sum_{i=1}^n a_i e_{i1}$. Since f is R -linear,

$$f(e_{11}) = f(e_{11}^2) = e_{11}f(e_{11}) = e_{11} \left(\sum_{i=1}^n a_i e_{i1} \right) = a_1 e_{11} = \rho_{a_1}(e_{11})$$

Then $(f - \rho_{a_1})$ has nontrivial kernel i.e. $(f - \rho_{a_1})$ is not an isomorphism. Since N is simple module, by Schur's lemma, $f - \rho_{a_1} = 0$ i.e. $f = \rho_{a_1}$.

Hence, $\varphi : D^\circ \xrightarrow{\sim} \text{End}_R(N) \rightsquigarrow D \simeq (\text{End}_R(N))^\circ$.

□

Corollary 3.3.1. If $M_{n_1}(D_1) \simeq M_{n_2}(D_2)$, where $n_i \in \mathbb{N}$ and D_i : division ring $\forall i$. Then $n_1 = n_2$, $D_1 \simeq D_2$.

Proof:

- Since $M_{n_1}(D_1)$ and $M_{n_2}(D_2)$ have the same length, so $n_1 = n_2$.
- Let $R \simeq M_{n_1}(D_1) \simeq M_{n_2}(D_2)$. By Theorem 3.3.2, $D_1 \simeq \text{End}_R(N)^\circ$, $D_2 \simeq \text{End}_R(N)^\circ$, where N is unique simple R -module. So $D_1 \simeq D_2$.

□

Observation: Now, we want to given a division ring D , is there a relation between ${}_D\mathfrak{M}$ and ${}_{M_n(D)}\mathfrak{M}$. Obviously, we can have the correspondence with the constraint of n .

- $M \in {}_D\mathfrak{M}$ and $\dim_D M = n \rightsquigarrow \text{End}_D(M) \simeq M_n(D)$. Since $M \in {}_{\text{End}_D(M)}\mathfrak{M} \rightsquigarrow M \in {}_{M_n(D)}\mathfrak{M}$.

Claim: M is simple $M_n(D)$ -module.

pf. $\forall v \in M$, we can extend $\{v\}$ to a basis $\{v, v_2, \dots, v_n\}$ for M over D . Since $\forall w \in M$, $\exists \varphi \in M_n(D)$ s.t. $\varphi(v) = w$. That is M cannot have any $M_n(D)$ -invariant subspace other than 0 and M .

- $N \in {}_{M_n(D)}\mathfrak{M}$
 - $M_n(D)$ is simple $\rightsquigarrow N$ is semisimple over $M_n(D)$
 - Define

$$\begin{array}{ccc} D & \hookrightarrow & M_n(D) \\ a & \mapsto & aI_n \end{array} \text{ as rings}$$

So we can regard D as a subring of $M_n(D)$ and thus $N \in {}_D\mathfrak{M}$.

- Let S be the unique simple $M_n(D)$ -module. ($S \simeq M_n(D)e_{11}$ and $\dim_D S = n$) Since N is semisimple over $M_n(D)$, we can write $M = \bigoplus_{i \in \Lambda} S$. In particular, if

$$N = \bigoplus_{i=1}^n S, \text{ then } \dim_D N = mn.$$

- Hence, if $M, N \in {}_{M_n(D)}\mathfrak{M}$ and $\dim_D M = \dim_D N$, then $M \simeq N$ in ${}_{M_n(D)}\mathfrak{M}$, since $n \dim_D(M) = \dim_{M_n(D)} M$.

3.3.3 Simple Algebra over a algebraically closed field

In this subsection, we require more algebra structure to our ring.

Theorem 3.3.3 (Burnside's theorem). Let $k = \bar{k}$ and $\dim_k V = n$. If R is a subalgebra of $\text{End}_k(V)$ and V is simple over R , then $R = \text{End}_k(V) (\simeq M_n(k))$.

Proof:

- $V \in {}_R\mathfrak{M} : R \subseteq \text{End}_k(V) \curvearrowright V \implies R \curvearrowright V$

- $V : \text{simple}/R \rightsquigarrow R' = \text{End}_R(V)$ is a division ring.
- Since R contains identity which can be regard as the identity in k , so $k \subset R$. Then $R' = \text{End}_R(V) \subseteq \text{End}_k(V)$ as k -subspaces.
- $\forall 0 \neq \alpha \in R'$, since R' is division $\rightsquigarrow k(\alpha)$ is a field and $k(\alpha) \subseteq R' \subseteq \text{End}_k(V)$ as k -module and notice that $\dim_k \text{End}_k(V) = n^2 < \infty \rightsquigarrow k(\alpha)/k$ is finite extension i.e. α algebraic over $k \rightsquigarrow \alpha \in k$, since $\bar{k} = k$. So $R' = k$
- Let $V = \langle v_1, \dots, v_n \rangle_k = \langle v_1, \dots, v_n \rangle_{R'}$. By Jacobson theorem, $R \twoheadrightarrow R'' = \text{End}_{R'}(V) = \text{End}_k(V) \rightsquigarrow R \subseteq \text{End}_k(V)$. Hence, $R = \text{End}_k(V)$.

□

Corollary 3.3.2. Let R be a simple algebra over algebraically closed field k and $\dim_k R < \infty$. Then $R \simeq M_n(k)$.

Proof:

- Since R is simple ring, let S be the unique minimal left ideal of R and $D = \text{End}_R(S)$ be the corresponding division ring. Then $R \simeq S^{\otimes n} \rightsquigarrow R \simeq M_N(D^\circ)$.
- Since S is an ideal of R , $RS \subseteq S \rightsquigarrow kS \subseteq S$ i.e. S is a k -subspace of R . Then $\dim_k R < \infty \implies \dim_k S < \infty$, say $\dim_k S = m$.
- **Claim:** R can be regarded as a subalgebra of $\text{End}_k(S)$

pf. Define

$$\begin{aligned} \varphi : R &\longrightarrow \text{End}_k(S) \\ a &\longmapsto \left(\begin{array}{ccc} T_a : S & \rightarrow & S \\ x & \mapsto & ax \end{array} \right) \end{aligned}$$

- $T_a \in \text{End}_k(S) : \forall r \in k, T_a(rx) = a(rx) = (ar)x = (ra)x = rT_a(x)$. For red equality is by k is commutative.
- $T_a \circ T_b(x) = T_a(bx) = a(bx) = (ab)x = T_{ab}(x) \rightsquigarrow \varphi$ is a k -algebra homo.

$\therefore R : \text{simple}$ and $S : \text{simple}/R \therefore S : \text{faithful}/R \rightsquigarrow \varphi : R \hookrightarrow \text{End}_k(S)$. □

- By Burnside's theorem, $R \simeq \text{End}_k(S) \simeq M_m(k)$. Since D°, k is division ring and $M_n(D^\circ) \simeq M_m(k)$, we have $n = m$ and $D^\circ \simeq k$. Hence, $R \simeq M_n(k)$.

□

Finally, given $R : \text{semisimple algebra over a algebraically closed field } k$. By Artin-Wedderburn theorem,

$$R \simeq M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

Let $R_i \subseteq R$ be the two-sided ideal such that $R_i \longleftrightarrow M_{n_i}(D_i)$, then $M_{n_i}(D_i)$ is simple algebraic over k . By Corollary 3.3.2, $R_i \simeq M_{n_i}(k)$. That is

$$R \simeq M_{n_1}(k) \times \cdots \times M_{n_r}(k)$$

Remark 3.3.1.

- R is right-semisimple if R° is left-semisimple. Since we have the correspondent of right ideals of R and left ideals of R° , so this definition is reasonable.
- R is semisimple $\iff R \simeq \prod_{i=1}^r M_{n_i}(D_i) \iff R^\circ \simeq \prod_{i=1}^r M_{n_i}(D_i^\circ) \simeq R^\circ$ is semisimple. Hence, left semisimple \iff right semisimple.

3.4 Representations and Semisimplicity

Let G be a finite group and F be a field. If V is a vector space over F , then $\text{GL}(V)$ is the group of nonsingular linear transformations : $V \rightarrow V$.

3.4.1 Definition-example

Definition 3.4.1. A group homomorphism $\begin{matrix} G & \longrightarrow & \text{GL}(V) \\ s & \longmapsto & \rho_s = \rho(s) \end{matrix}$ is called a linear representation of G .

- ρ is called **faithful** if it is injective.
- V is called a **representation space** of G and $\dim V$ is called the degree of ρ .
- $\rho : G \rightarrow \text{GL}(V)$ and $\rho' : G \rightarrow \text{GL}(V)$ are **isomorphic** if \exists a F -linear isomorphism $\tau : V \rightarrow V'$ s.t.

$$\tau \circ \rho_s = \rho'_s \circ \tau \quad \forall s \in G \quad \text{i.e.} \quad \begin{array}{ccc} V & \xrightarrow{\rho_s} & V \\ \tau \downarrow & & \downarrow \tau \\ V & \xrightarrow{\rho'_s} & V \end{array} \text{ commute}$$

- For a subspace $W \subset V$, W is **invariant** under G if $\forall s \in G, \rho_s(W) \subseteq W$. Then

$$\rho|_W : G \longrightarrow \text{GL}(W) \text{ is a } \mathbf{subrepresentation} \text{ of } \rho$$

- ρ is **irreducible** if ρ has no proper nontrivial subrepresentation.

As we do in group extension, given a group G acts on a module M . Since M is a abelian group i.e. a \mathbb{Z} -module, we can given M a $\mathbb{Z}[G]$ -module structure. Now, we want to similar way on V , recall : $F[G] = \{ \sum_{g \in G} \alpha_g g \mid \alpha_g \in F \}$ and see the key property in below.

Property 3.4.1 (key properties).

- $\{V : \text{an } F[G]\text{-module}\} \longleftrightarrow \{\rho : G \rightarrow \text{GL}(V)\}$
- $\{W \subset V : \text{an } F[G]\text{-submodule}\} \longleftrightarrow \{W \subseteq V : \text{a } G\text{-invariant subspace}\}$

- V is a simple $F[G]$ -module $\iff \rho$ is an irreducible representation
- ρ, ρ' are isomorphism $\iff V \simeq V'$ as $F[G]$ -modules.

Example 3.4.1.

- **(Regular representation)** $V = F[G] = \bigoplus_{g \in G} Fg$, define

$$\begin{aligned} \rho^{\text{reg}} : G &\longrightarrow \text{GL}(V) \\ s &\longmapsto \rho_s^{\text{reg}} : \sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g (sg) \end{aligned}$$

Notice that $\{sg : g \in G\} = \{g : g \in G\}$, so ρ_s^{reg} can be regarded as exchange the coefficient of the basis $\{g : g \in G\}$ i.e. $[\rho_s^{\text{reg}}]_G$ is a matrix with every column, row has exactly one entry is 1 and others are 0.

- **(Permutation representation)** Let $V = \bigoplus_{i=1}^n F e_i$ and consider

$$\begin{aligned} \rho : S_n &\longrightarrow \text{GL}(V) \\ \sigma &\longmapsto \rho_\sigma : \sum_{i=1}^n \alpha_i e_i \mapsto \sum_{i=1}^n \alpha_i e_{\sigma(i)} \end{aligned}$$

For example : $G = S_3$, then $\dim_F V = 3$. Let $\sigma = (1\ 2)$, then $\rho_\sigma : \begin{cases} e_1 \mapsto e_2 \\ e_2 \mapsto e_1 \\ e_3 \mapsto e_3 \end{cases}$

Note : By Cayley theorem, $G \hookrightarrow S_n$ for some n . Restrict ρ on G , then we get a linear representation $\rho|_G : G \longrightarrow \text{GL}(V)$. Actually, $\rho|_G$ is isomorphic to regular representation of G .

- Unfortunately, those two representation are all not the irreducible when $n \geq 2$, the reason is below :

- For the permutation representation :

$N = \{\alpha_1 e_1 + \cdots + \alpha_n e_n : \alpha_1 = \alpha_2 = \cdots = \alpha_n\}$ is an S_n -invariant subspace which is called the **trace submodule** of V over $F[S_n]$ and $\dim_F N = 1$.

$I = \{\alpha_1 e_1 + \cdots + \alpha_n e_n : \alpha_1 + \cdots + \alpha_n = 0\}$ is also S_n -invariant

which is called the **augmentation submodule** of V over $F[S_n]$ and $\dim_F I = n - 1$.

- For the regular representation : Let $n = |G|$

$N = \{\alpha_1 g_1 + \cdots + \alpha_n g_n : \alpha_1 = \alpha_2 = \cdots = \alpha_n\}$ is an G -invariant subspace which is called the **trace ideal** of $F[G]$ and $\dim_F N = 1$.

$I = \{\alpha_1 g_1 + \cdots + \alpha_n g_n : \alpha_1 + \cdots + \alpha_n = 0\}$ is also G -invariant

which is called the **augmentation ideal** of $F[G]$ and $\dim_F I = n - 1$.

And both N, I are two-sided ideals of $F[G]$.

Now, we know how to divide the representation to some smaller subrepresentation. So we may ask how to piece some representation together into larger representation. We introduce two operations on representation : Given $\rho_1 : G \rightarrow \text{GL}(V_1)$, $\rho_2 : G \rightarrow \text{GL}(V_2)$ with $\dim_F V_1 = n, \dim_F V_2 = m$ and $\beta_1 = \{v_1, \dots, v_n\}, \beta_2 = \{w_1, \dots, w_m\}$ be the basis for V_1, V_2 respectively. Construct

- (Direct sum)

$$\begin{aligned} \rho_1 \oplus \rho_2 : G &\longrightarrow \text{GL}(V_1 \oplus V_2) \\ s &\longmapsto (\rho_1 \oplus \rho_2)_s = ((\rho_1)_s, (\rho_2)_s) \end{aligned}$$

Then the degree of $\rho_1 \oplus \rho_2$ is $\dim_F(V_1 \oplus V_2) = m + n$ and $[(\rho_1 \oplus \rho_2)_s]_{\beta_1 \cup \beta_2}$ is form

$$\begin{pmatrix} [(\rho_1)_s]_{\beta_1} & O \\ O & [(\rho_2)_s]_{\beta_2} \end{pmatrix}$$

- (Tensor product)

$$\begin{aligned} \rho_1 \otimes \rho_2 : G &\longrightarrow \text{GL}(V_1 \otimes_F V_2) \\ s &\longmapsto (\rho_1 \otimes \rho_2)_s = (\rho_1)_s \otimes (\rho_2)_s : v \otimes w \mapsto (\rho_1)_s(v) \otimes (\rho_2)_s(w) \end{aligned}$$

Then the degree of $\rho_1 \otimes \rho_2$ is $\dim_F(V_1 \otimes V_2) = mn$, since $\{v_i \otimes w_j\}$ form a basis.

3.4.2 Complete reducibility

Theorem 3.4.1 (Maschke's theorem). Assume $\text{char } F \nmid |G|$. Let $\rho : G \rightarrow \text{GL}(V)$ and W be a subrepresentation of G in V . Then $\exists W' \subset V$ s.t. W' is G -invariant and $W \oplus W' = V$ as $F[G]$ -modules.

Proof: First, pick arbitrary W_1 s.t. $V = W \oplus W_1$ and let $\pi : V \rightarrow W$ be the projection. Notice that W_1 may not be G -invariant, so π may not be a $F[G]$ -module homomorphism. To get a $F[G]$ -module homomorphism, we have the common method : take average. Under this ideal, define

$$\pi' = \frac{1}{|G|} \sum_{s \in G} \rho_s^{-1} \circ \pi \circ \rho_s : V \longrightarrow W$$

Since W is G -invariant, $\pi'(V) \subseteq W$. Notice that W is G -invariant, so $\forall w \in W$, $\rho_s(w) \in W \rightsquigarrow \pi \circ \rho_s(w) = \rho_s(w) \rightsquigarrow \rho_s^{-1} \circ \pi \circ \rho_s(w) = w$. Then $\sum_{s \in G} \rho_s^{-1} \circ \pi \circ \rho_s(w) =$

$|G| \cdot w$. So the assumption of $\text{char } F \nmid |G|$ is necessary, otherwise it will be the zero map (before divide $|G|$). Hence, $\pi'(w) = w \implies \pi'(V) = W$.

Claim: π' is an $F[G]$ -module epimorphism.

pf. We need to prove “ $\rho_s \circ \pi' = \pi' \circ \rho_s \forall s \in G$ ”. For all $v \in V$

$$\begin{aligned} \pi(\rho_s(v)) &= \frac{1}{|G|} \sum_{t \in G} \rho_t^{-1} \circ \pi \circ \rho_t \circ \rho_s(v) \\ &= \frac{1}{|G|} \sum_{t \in G} \rho_s \circ \rho_s^{-1} \circ \rho_t^{-1} \circ \pi \circ \rho_t \circ \rho_s(v) \\ &= \frac{\rho_s}{|G|} \sum_{t \in G} \rho_t^{-1} \circ \pi \circ \rho_t(v) = \rho_s \circ \pi'(v) \end{aligned}$$

□

By Claim, $W' := \ker \pi'$ is an $F[G]$ -submodule of V i.e. W is G -invariant. Since V is a F -vector space, $0 \rightarrow W' \rightarrow V \rightarrow W \rightarrow 0$ splits i.e. thus $V = W \oplus W'$. □

Theorem 3.4.2. Assume $\text{char } F \nmid |G|$. Every representation of G of finite degree is a direct sum of irreducible representations.

Proof: Let $\rho : G \rightarrow \text{GL}(V)$ with $\dim_F V = n$. We need to prove that V is semisimple over $F[G]$. By induction on $\dim V$, if V is simple, then done! Otherwise, \exists a nontrivial proper $F[G]$ -submodule W of V . By Maschke's theorem, $\exists W'$ which is also an $F[G]$ -submodule s.t. $V = W \oplus W'$ as $F[G]$ -modules. By induction hypothesis, W, W' are direct sums of simple $F[G]$ -submodules, hence so is V . □

3.4.3 Application for semisimplicity

Observation: G : finite group; F : field with $\text{char } F \nmid |G|$.

- We can interpret the regular representation of G as

“ $F[G]$ is a left module over itself”

- By Maschke's theorem, $F[G]$ can be decomposed into a direct sum of simple $F[G]$ -modules $\rightsquigarrow F[G]$ is a semisimple algebra/ F .
- $\mathbb{C}[G]$ is a semisimple algebra/ \mathbb{C} , then by Corollary of Burnside theorem,

$$\mathbb{C}[G] \simeq M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

By this isomorphism, we have

- $\mathbb{C}[G]$ has exactly r distinct isomorphic types of simple modules.
- $|G| = \sum_{i=1}^r n_i^2$ by comparing the \dim / \mathbb{C} on both sides.
- $\dim_{\mathbb{C}} Z(\mathbb{C}[G]) = r$, since $Z(M_{n_i}(\mathbb{C})) = \mathbb{C} \cdot I_{n_i}$.

Property 3.4.2. $r = \#$ of conjugacy classes of G .

Proof: Let K_1, \dots, K_ℓ be distinct conjugacy classes of G . Set

$$x_i = \sum_{g \in K_i} g \in \mathbb{C}[G]$$

Then x_i, x_j have no common terms for $i \neq j \rightsquigarrow x_i$'s are linearly indep./ \mathbb{C} . Also, $\forall g \in G, gx_i g^{-1} = g \rightsquigarrow x_i \in Z(\mathbb{C}[G])$. Conversely, $\forall x \in Z(\mathbb{C}[G])$, say $x = \sum_{g \in G} \alpha_g g$.

$$\because \forall h \in G, h^{-1} x h = x \rightsquigarrow \sum_{g \in G} \alpha_g h^{-1} g h = \sum_{g \in G} \alpha_g g \text{ in } \mathbb{C}[G] \rightsquigarrow \alpha_{hgh^{-1}} = \alpha_g \quad \forall h \in G$$

$$\therefore x = \sum_{i=1}^{\ell} \alpha_i x_i \rightsquigarrow Z(\mathbb{C}[G]) = \langle x_1, \dots, x_\ell \rangle_{\mathbb{C}}$$

Hence, $r = \dim_{\mathbb{C}} Z(\mathbb{C}[G]) = \ell$. □

In above, since we choose a algebraically closed field so we have Burnside theorem. In general, By Artin-Wedderburn theorem, we only have

$$F[G] \simeq M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

with division ring D_i . Then we have

- Let I_{n_i} be the identity in $M_{n_i}(D_i)$, and let $z_i \longrightarrow (0, \dots, 0, I_{n_i}, 0, \dots, 0)$ under the isomorphism. Then
 - $z_i^2 = z_i$, $z_i z_j = 0$ for all $i \neq j$
 - $\sum_{i=1}^r z_i = 1$
 - $z_i F[G] \simeq M_{n_i}(D_i)$
 - $z_i \in Z(F[G])$

Here z_1, \dots, z_r are called the **primitive central idempotents** of $F[G]$.

- M : simple $F[G]$ -module $\rightsquigarrow M$: simple $M_{n_i}(D_i)$ -module for some i . So M can be uniquely determined $(M_{n_i}(D_i)e_{11})$. Now, we give a method to find i :

$M = 1 \cdot M = (z_1 + \cdots + z_r)M = z_1M + \cdots + z_rM$. Actually, it will be direct, since if $y \in z_1M \cap (z_2M + \cdots + z_rM)$, say $y = z_1x = z_2x_2 + \cdots + z_rx_r$, then $y = z_1x = z_1^2x = z_1(z_2x_2 + \cdots + z_rx_r) = 0$. Since M is simple, $M = z_iM$ for some i .

Example 3.4.2. Find all irreducible representations of $G = S_3$:

Conjugacy classes : $\{e\}, \{(1\ 2), (1\ 3), (2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}$.

Notice that $|G| = 6 = 1^2 + 1^2 + 2^2$ is unique solution for $|G| = \sum_{i=1}^3 n_i^2$. So

$$\mathbb{C}[S_3] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$$

ρ : irreducible representation $\longleftrightarrow S$: simple/ $\mathbb{C}[S_3] \rightsquigarrow S$: simple/ \mathbb{C} or simple/ \mathbb{C} or simple/ $M_2(\mathbb{C})$. So there have three different irreducible representation.

Recall the permutation representation of S_3 , then $V = \langle e_1, e_2, e_3 \rangle_{\mathbb{C}}$ have two non-trivial proper submodule.

- $\rho_1 \longleftrightarrow$ trace submodule $W_1 = \{\alpha e_1 + \alpha e_2 + \alpha e_3 : \alpha \in \mathbb{C}\}$ of V . So $\rho_1 : \sigma \mapsto \text{id}$ is trivial representation.
- Let $W_2 = \{\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3\}$ be the augmentation submodule of V . It's clear that W_2 is simple over $\mathbb{C}[S_3]$ and $V = W_1 \oplus W_2$.

$$\rho_2 \longleftrightarrow W_2$$

- For last one, we have

$$\begin{array}{rcl} \rho_3 : & S_3 & \longrightarrow \mathbb{C}^* \simeq \text{GL}(\mathbb{C}) \\ & \text{even} & \longmapsto 1 \\ & \text{odd} & \longmapsto -1 \end{array}$$

As you see, if we only using the technology in this section, it is not enough to clearly understand all irreducible representation. We will introduce more powerful technology in later sections.

Chapter 4

Presentation

Chapter 5

Appendix

5.1 Definition of Categories and Functors

Definition 5.1.1. A **category** C consists of :

- $\text{Ob}(C)$: a **class** of object
- Set of morphisms : $C(X, Y)$ for order pair (X, Y)
- Composition of morphisms : $\forall (X, Y, Z)$: ordered pair

$$\begin{array}{ccc} C(X, Y) \otimes C(Y, Z) & \longrightarrow & C(X, Z) \\ (f, g) & \longmapsto & g \circ f \end{array}$$

satisfies associativity and $\forall X \in \text{Ob}(C) \exists 1_X \in C(X, X)$ s.t. $f \circ 1_X = f, 1_X \circ g = g$.

Remark 5.1.1. C is called a small cat. if $\text{Ob}(C)$ is a set. Otherwise, we called it large cat.

Definition 5.1.2. For $X, Y \in C$, $f : X \rightarrow Y$ is called an **isomorphism** if $\exists g : Y \rightarrow X$ s.t. $f \circ g = 1_Y$ and $g \circ f = 1_X$.

Example 5.1.1.

- Set with functions between them.
- Topological space with continuous map.
- poset with $X \rightarrow Y \iff x \leq Y$, then it form a small cat.

Definition 5.1.3. Let C, D : category. A **covariant functor** $F : C \rightarrow D$ consists of

- $F : \text{Ob}(C) \rightarrow \text{Ob}(D)$
- $F : C(X, Y) \rightarrow D(F(X), F(Y))$

which satisfies

- $\forall X \in C, F(1_X) = 1_{F(X)}$
- $F(g \circ f) = F(g) \circ F(f)$ which is called **functoriality**

We say $F : C \rightarrow D$ is a **contravariant functor** if we change the condition to

- $F : C(X, Y) \rightarrow D(F(Y), F(X))$
- $F(g \circ f) = F(f) \circ F(g)$

Example 5.1.2. $\text{Hom}(_, N) : M \mapsto \text{Hom}(M, N)$ is a covariant functor and $_ \otimes N : M \rightarrow M \otimes N$ is a contravariant functor.

Definition 5.1.4. For given C is a category, define **opposite category** of C by

- $\text{Ob}(C^{op}) = \text{Ob}(C)$
- $C^{op}(Y, X) = C(X, Y)$

So F is contravariant functor if F is covariant functor define on C^{op} .

Chapter 6

Homework

6.1

Problem 6.1.1. Let A be a ring and M be a left A -module.

- (a) For any left ideal I of A , define

$$IM = \left\{ \sum_{\text{finite}} a_i x_i \mid a_i \in I, x_i \in M \right\}$$

Show that IM is a submodule of M .

- (b) Let $N_1 \subset N_2 \subset \cdots$ be an ascending chain of submodules of M . Show that $\bigcup_{i=1}^{\infty} N_i$ is a submodule of M .

Problem 6.1.2. Let $k = \mathbb{R}$ and $V = \mathbb{R}^2$.

- (a) Let T be the rotation clockwise about the origin by $\pi/2$ radians. We know that the linear transformation T gives rise to a $k[x]$ -submodules for this T . Show that V and 0 are the only $k[x]$ -submodules for this T .
- (b) Let T be the projection onto the y -axis. Show that $V, 0$, the x -axis and the y -axis are the only $k[x]$ -submodules for this T .
- (c) Let T be the rotation clockwise about the origin by π radians. Show that every subspace of V is a $k[x]$ -submodule for this T .

Problem 6.1.3.

- (a) Show that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/\gcd(m, n)\mathbb{Z}$
- (b) Let A be a commutative ring and M be an A -module. Show that $\text{Hom}_A(A, M) \simeq M$ as left A -modules.
- (c) Let A be a commutative ring. Show that $\text{Hom}_A(A, A) \simeq A$ as a ring.

6.2

Problem 6.2.1. Construct a ring A such that for all $m, n \in \mathbb{N}$, $A^n \simeq A^m$

Problem 6.2.2. If A is a division ring, then A has IBN.

Problem 6.2.3. Let I be an ideal of A .

- (a) Let M be an A -module. Show that M/IM has an A/I -module structure.
- (b) Show that if I is proper and A/I has IBN, then A also has IBN.
- (c) Show that if $f : B \rightarrow A$ is a ring epimorphism and A is a division ring, then B has IBN.

Problem 6.2.4. Let $\{M_i\}$ be a directed family of modules over a ring. For any module N show that

$$\varprojlim \text{Hom}(H, M_i) = \text{Hom}(N, \varprojlim M_i)$$

6.3

Problem 6.3.1. Let G be an abelian group and

$$\begin{aligned} G = \langle x, y, z, u, v \mid x - 7y + 14z - 21u &= 5x - 7y - 2z + 10u - 15v \\ &= 3x - 3y - 2z + 6u - 9v = x - y + 2z - 3v = 0 \rangle \end{aligned}$$

Please write G as a direct sum of cyclic groups.

Problem 6.3.2. Let R be a PID and M be a finitely generated R -module with rank n . Show that if N is a submodule of M and has rank m , then M/N has rank $n - m$.

Problem 6.3.3. Let A be an additive subgroup of Euclidean space \mathbb{R}^n , and assume that in every bounded region of space, there is only a finite number of elements of A . Show that A is a free abelian group on $\leq n$ generators.

Hint: Induction on the maximal number of linearly independent elements of A over \mathbb{R} . Let v_1, \dots, v_m be a maximal set of such elements, and let A_0 be the subgroup of A contained in the \mathbb{R} -space generated by v_1, \dots, v_{m-1} . By induction, one may assume that any element of A_0 is a linear integral combination of v_1, \dots, v_{m-1} . Let S be the subset of elements $v \in A$ of the form $v = a_1 v_1 + \dots + a_m v_m$ with real coefficients a_i satisfying

$$\begin{cases} 0 \leq a_i < 1 & \text{if } i = 1, \dots, m-1 \\ 0 \leq a_m \leq 1 \end{cases}$$

If v'_m is an element of S with the smallest $a_m \neq 0$, show that $\{v_1, \dots, v_{m-1}, v'_m\}$ is a basis of A over \mathbb{Z} .

Note: The above exercise is applied in algebraic number theory to show that the group of units in the ring of integers of a number field modulo torsion is isomorphic to a lattice in a Euclidean space.

Problem 6.3.4. Let M be a finitely generated abelian group. By a **seminorm** on M we mean a real-value function $v \rightarrow |v|$ satisfying the following properties :

$$|V| \geq 0 \text{ for all } v \in M$$

$$|nv| = |n||v| \text{ for } n \in \mathbb{Z}$$

$$|v + W| \leq |v| + |W| \text{ for all } v, w \in M$$

By the kernel of the seminorm we mean the subset of elements v such that $|v| = 0$.

- (a) Let M_0 be the kernel. Show that M_0 is a subgroup. If $M_0 = \{0\}$, then the seminorm is called a **norm**.
- (b) Assume that M has rank r . Let $v_1, \dots, v_r \in M$ be linearly independent over $\mathbb{Z} \bmod M_0$. Prove that there exists a basis $\{w_1, \dots, w_r\}$ of M/M_0 such that

$$|w_i| \leq \sum_{j=1}^i |v_j|$$

(**Hint** : An explicit version of the proof of Theorem 7.8 gives the result. Without loss of generality, we can assume $M_0 = \{0\}$. Let $M_1 = \langle v_1, \dots, v_r \rangle$. Let d be the exponent of M/M_1 . Then dM has a finite index in M_1 . Let $n_{j,j}$ be the smallest positive integer such that there exist integers $n_{j,1}, \dots, n_{j,j-1}$ satisfying

$$n_{j,1}v_1 + \dots + n_{j,j-1}v_{j-1} = dw_j \text{ for some } w_j \in M$$

Without loss of generality we may assume $0 \leq n_{j,k} \leq d-1$. Then the elements w_1, \dots, w_r form the desired basis.)

6.4

Problem 6.4.1.

- (a) Let $k = \mathbb{C}$. Find the Jordan canonical form J of

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix}$$

and the matrix Q such that $J = Q^{-1}AQ$

(b) Let $k = \mathbb{R}$. Find the Rational canonical form C of

$$A = \begin{pmatrix} 0 & -7 & 14 & -6 \\ 1 & -4 & 6 & -3 \\ 0 & -4 & 9 & -4 \\ 0 & -4 & 11 & -5 \end{pmatrix}$$

and the matrix Q such that $J = Q^{-1}AQ$

Problem 6.4.2. Let R be a PID and M be a finitely generated R -module. Show that if $M \simeq Rz_1 \oplus \cdots \oplus Rz_r$ with $\text{ann}(z_i) = \langle d_i \rangle \neq R$ and $d_i | d_{i+1}$ for all $i = 1, \dots, r-1$, then the ring $(\text{Hom}_R(M, M), +, \circ)$ is isomorphic to S/I where S is the ring of matrices $B \in M_{r \times r}(R)$ for which there exists a $C \in M_{r \times r}(R)$ such that $\text{diag}\{d_1, \dots, d_r\}C = B \text{diag}\{d_1, \dots, d_r\}$ and I is the ideal of matrices of the form $\text{diag}\{d_1, \dots, d_r\}Q$, $Q \in M_{r \times r}(R)$.

Problem 6.4.3. Let $A \in M_{n \times n}(k)$ with k being a field. Assume that $d_1(x), \dots, d_r(x)$ are the non-unit monic invariant factors of $(xI_n - A)$ with $\deg d_i(x) = n_i > 0$. Show that

$$\dim_k \{B \in M_{n \times n}(k) : BA = AB\} = \sum_{j=1}^r (2r - 2j + 1)n_j$$

6.5

Problem 6.5.1.

(a) Let M be a right A -module, N an A - B bimodule and L a left B -module. Show that

$$(M \otimes_A N) \otimes_B L \simeq M \otimes_A (N \otimes_B L)$$

(b) Let R be a commutative ring and M, N be two R -modules. Show that

$$M \otimes_R N \simeq N \otimes_R M$$

Problem 6.5.2. Justify your answers.

- (a) Compute $\dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ and $\dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.
- (b) Compute $\dim_{\mathbb{C}} \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ and $\dim_{\mathbb{C}} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.
- (c) Compute $\dim_{\mathbb{C}} \mathbb{C}[x]/\langle x^2 + x + 1 \rangle \otimes_{\mathbb{R}} \mathbb{R}[z]/\langle z + 1 \rangle$
- (d) Let V and W be two k -vector spaces with $\dim_k V = n$ and $\dim_K W = m$. Compute $\dim_k V \otimes_k W$

Problem 6.5.3. Let $R = \bigoplus_{k=0}^{\infty} R_k$ be a graded ring with $R_i R_j \subset R_{i+j}$ and I be an ideal of R generated by some homogeneous elements. Show that the quotient ring R/I has a natural graded ring structure via $R/I = \bigoplus_{k=0}^{\infty} R_k / (R_k \cap I)$.

Problem 6.5.4. Let R be a commutative ring.

- (a) Let F be a free R -module of rank n . Show that

$$S(F) \simeq R[x_1, \dots, x_n]$$

- (b) Let $F = F_1 \oplus F_2$ be a direct sum on finite free R -modules. Show that

$$S^n(F) \simeq \bigoplus_{p+q=n} S^p(F_1) \otimes S^q(F_2)$$

6.6

Problem 6.6.1. Let N, L be two R -submodules of M and S be a multiplicatively closed set in the commutative ring R . Show that

- (a) $(N + L)_S = N_S + L_S$
 (b) $(N \cap L)_S = N_S \cap L_S$
 (c) $(M/N)_S \simeq M_S/N_S$

Problem 6.6.2. Let R be a commutative ring. Show that

- (a) If M is a proper ideal of R such that for all $x \in R - M$ are units in R , then R is a local ring.
 (b) If M is a maximal ideal of R such each element of $1 + M$ is a unit in R , then R is a local ring.

Problem 6.6.3 (Prime avoidance lemma). Let R be a commutative ring. Show that

- (a) If $P_1, \dots, P_n \in \text{Spec } R$ and I is an ideal of R contained in $\bigcup_{i=1}^n P_i$, then there exists an P_k such that $I \subseteq P_k$.
 (b) If I_1, \dots, I_n are ideals of R and $P \in \text{Spec } R$ containing $\bigcap_{i=1}^n I_i$, then there exists an I_k such that $P \supseteq I_k$.

Problem 6.6.4. Let R be a commutative ring and I be an ideal of R . Define

$$\sqrt{I} := \{x \in R : x^n \in I \text{ for some } n > 0\}$$

Show that

- (a) $\sqrt{\sqrt{I}} = \sqrt{I}$
 (b) For another ideal J , $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
 (c) For another ideal J , $\sqrt{I + J} = \sqrt{(\sqrt{I} + \sqrt{J})}$
 (d) $\sqrt{I} = \bigcap_{I \subseteq P \in \text{Spec } R} P$

6.7

Problem 6.7.1. Show that if A is a (left) Noetherian ring, then the formal power series ring $A[[x]]$ is (left) Noetherian.

Problem 6.7.2. Let R be a commutative Noetherian ring and S be a multiplicatively closed set in R .

- (a) Show that R_S is Noetherian
- (b) Show that if M is an R -module, then

$$\text{Ass}_R(M_S) = \text{Ass}_R(M) \cap \{P \in \text{Spec } R : P \cap S = \emptyset\}$$

Problem 6.7.3. Let R be a commutative ring. Show that if $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ is an exact sequence of R -modules, then

$$\text{Ass}(M_1) \subset \text{Ass}(M_2) \subset \text{Ass}(M_1) \cup \text{Ass}(M_3)$$

Problem 6.7.4. Let R be a commutative Noetherian ring and M be a finitely generated R -module. Show that $\text{Ass}(M)$ is a finite set.

6.8

Problem 6.8.1. Show that if A is a commutative Noetherian ring, then the set of zero-divisors in A is the set-theoretical union of all primes belongs to primary ideals in a reduced primary decomposition of $\langle 0 \rangle$.

Problem 6.8.2.

- (a) Let \mathfrak{p} be a prime ideal, and $\mathfrak{a}, \mathfrak{b}$ ideals of A . If $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, show that $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.
- (b) Let \mathfrak{q} be a primary ideal. Let $\mathfrak{a}, \mathfrak{b}$ be ideals, and assume $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. Assume that \mathfrak{b} is finitely generated. Show that $\mathfrak{a} \subseteq \mathfrak{p}$ or there exists some positive integer n such that $\mathfrak{b}^n \subseteq \mathfrak{p}$.

Problem 6.8.3. Let A be Noetherian, and let \mathfrak{q} be a \mathfrak{p} -primary ideal. Show that there exists some $n \geq 1$ such that $\mathfrak{p}^n \subseteq \mathfrak{q}$.

Problem 6.8.4.

- (a) Let A be an arbitrary commutative ring and let S be a multiplicative subset. Let \mathfrak{p} be a prime ideal and let \mathfrak{q} be a \mathfrak{p} -primary ideal. Then \mathfrak{p} intersects S if and only if \mathfrak{q} intersects S . Furthermore, if \mathfrak{q} does not intersect S , then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$ -primary in $S^{-1}A$.

- (b) Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ be a reduced primary decomposition of an ideal. Assume that $\mathfrak{q}_1, \dots, \mathfrak{q}_i$ do not intersect S , but that \mathfrak{q}_j intersects S for $j > i$. Show that

$$S^{-1}\mathfrak{a} = S^{-1}\mathfrak{q}_1 \cap \cdots \cap S^{-1}\mathfrak{q}_i$$

is a reduced primary decomposition of $S^{-1}\mathfrak{a}$.

6.9

Problem 6.9.1. Let R be a commutative ring and I be an ideal of R .

- (a) Show that $\text{gr}_I(R) := \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$ has a graded ring structure.
- (b) Show that if M is an R -module, then $\text{gr}_I(M) := \bigoplus_{n=0}^{\infty} I^n M/I^{n+1} M$ has a graded $\text{gr}_I(R)$ -module structure.

Problem 6.9.2. Let $\varphi : S_I(R) \rightarrow \text{gr}_I(R)$ be additive such that $\varphi(a_i t^i) = a_i + I^{i+1}$. Show that

- (a) φ is a graded ring homomorphism.
- (b) φ is onto.
- (c) $\ker \varphi = IS_I(R)$ and thus $S_I(R)/IS_I(R) \simeq \text{gr}_I(R)$.

Problem 6.9.3. Show that $\text{gr}_I(M) \simeq S_I(R)M/IS_I(R)M$
(Here, $S_I(R)M = M \oplus IMt \oplus I^2Mt^2 \oplus \cdots$)

Problem 6.9.4. Show that if R is Noetherian and M is a finitely generated R -module, then $\text{gr}_I(M)$ is a finitely generated $\text{gr}_I(R)$ -module.

6.10

Problem 6.10.1. Let (R, m) be a Noetherian local ring and Q be an m -primary ideal.

- (1) Show that R/Q is an Artinian R -module and thus $\ell(R/Q)$ is well-defined.
- (2) Show that $\ell(Q^i/Q^{i+1})$ is well-defined for all $i = 1, 2, \dots$ and

$$\ell(R/Q^n) = \sum_{i=0}^{n-1} \ell(Q^i/Q^{i+1})$$

- (3) Show that there exists $\chi_Q^R(t) \in \mathbb{Q}[t]$ such that

$$\ell(R/Q^n) = \chi_Q^R(n)$$

for sufficiently large n .

- (4) Show that \deg_Q^R is independent of the choice of Q , that is, it is an invariant of (R, m) .

Remark 6.10.1.

- We call χ_Q^R is the **characteristic polynomial** of R relative to Q .
- $d(R) := \deg \chi_Q^R$.

6.11

Problem 6.11.1. Let A, B be local rings with maximal ideals $\mathfrak{m}_A, \mathfrak{m}_B$, respectively. Let $f : A \rightarrow B$ be a homomorphism. We say that f is **local** if $f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$. Suppose this is the case. Assume A, B are Noetherian, and assume that :

- (1) $A/\mathfrak{m}_A \rightarrow B/\mathfrak{m}_B$ is an isomorphism
- (2) $\mathfrak{m}_A \rightarrow \mathfrak{m}_B/\mathfrak{m}_B^2$ is surjective
- (3) B is a finite A -module, via f .

Prove that f is surjective.

Problem 6.11.2. Let A be a Noetherian local ring. Let E be a finite A -module. Assume that A has no nilpotent elements. For each prime ideal \mathfrak{p} of A , let $k(\mathfrak{p})$ be the residue class field. If $\dim_{k(\mathfrak{p})}(E_{\mathfrak{p}}/\mathfrak{p}E_{\mathfrak{p}})$ is constant for all \mathfrak{p} , show that E is free.

Problem 6.11.3. Let R be a commutative ring. Show that R is Artinian if and only if R is Noetherian and $\text{Spec } R = \text{Max } R$.

Problem 6.11.4. Let (R, \mathfrak{m}) be an Artinian local ring. Show that TFAE :

- (1) R is a PID
- (2) \mathfrak{m} is principal
- (3) $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \leq 1$

6.12

Problem 6.12.1. Show that for a short exact sequence of R -modules

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$$

the following are equivalent :

- (a) $M_2 = \alpha(M_1) \oplus N$ with $N \simeq M_3$.
- (b) $\exists \lambda : M_3 \rightarrow M_2$ such that $\beta \circ \lambda = \text{id}_{M_3}$.

(c) $\exists \mu : M_2 \rightarrow M_1$ such that $\mu \circ \alpha = \text{id}_{M_1}$

(In this case, this sequence is said to be split exact)

Problem 6.12.2. Show that for a short exact sequence of R -modules

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$$

(a) For all $M : R$ -modules,

$$0 \rightarrow \text{Hom}_R(M, M_1) \rightarrow \text{Hom}_R(M, M_2) \rightarrow \text{Hom}_R(M, M_3) \text{ is exact.}$$

(b) For all $N : R$ -modules,

$$0 \rightarrow \text{Hom}_R(M_3, N) \rightarrow \text{Hom}_R(M_2, N) \rightarrow \text{Hom}_R(M_1, N) \text{ is exact.}$$

(c) For all $M : \text{right } R$ -modules,

$$M \otimes_R M_1 \rightarrow M \otimes_R M_2 \rightarrow M \otimes_R M_3 \rightarrow 0 \text{ is exact.}$$

Problem 6.12.3. Show that if M is S - R bimodule, $A \in {}_R\mathfrak{M}, B \in {}_S\mathfrak{M}$, then

$$\text{Hom}_S(M \otimes_R A, B) \simeq \text{Hom}_R(A, \text{Hom}_S(M, B))$$

6.13

Problem 6.13.1.

- (a) State the property of morphisms being homotopic in the case of cochain complexes.
- (b) Let $M \in {}_R\mathcal{M}$. Show that there exists an injective resolution of M

$$0 \rightarrow M \xrightarrow{\mu} I^0 \xrightarrow{d_1} I^1 \xrightarrow{d_2} I^2 \xrightarrow{d_3} \dots$$

Problem 6.13.2. State and show the dual version of Comparison theorem for injective resolutions.

Problem 6.13.3.

(a) (Snake Lemma) Suppose the following diagram commutes in \mathcal{M}_R

$$\begin{array}{ccccccc} M_1 & \xrightarrow{\alpha_1} & M_2 & \xrightarrow{\beta_1} & M_3 & \longrightarrow & 0 \\ \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{\alpha_2} & N_2 & \xrightarrow{\beta_2} & N_3 \end{array}$$

Show that there exists a long exact sequence (in blue color):

$$\begin{array}{ccccccc}
 0 & \dashrightarrow & \ker f_1 & \longrightarrow & \ker f_2 & \longrightarrow & \ker f_3 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & M_1 & \longrightarrow & M_2 & \longrightarrow & M_2 \longrightarrow 0 \\
 & & \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 \\
 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \operatorname{coker} f_1 & \longrightarrow & \operatorname{coker} f_2 & \longrightarrow & \operatorname{coker} f_3 \dashrightarrow 0
 \end{array}$$

(A blue path connects the kernels and cokernels, starting from the first 0, going right through the kernels, then down to the cokernels, and finally right to the last 0.)

Furthermore, if those two exact sequences are short exact sequence:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & M_1 & \xrightarrow{\alpha_1} & M_2 & \xrightarrow{\beta_1} & M_3 \longrightarrow 0 \\
 & & \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 \\
 0 & \longrightarrow & N_1 & \xrightarrow{\alpha_2} & N_2 & \xrightarrow{\beta_2} & N_3 \longrightarrow 0
 \end{array}$$

Then we can extend the blue exact sequence by adding two red “0” on it.

- (b) Show the Horseshoe Lemma: Let two projective resolutions of L and N respectively combined with a short exact sequence as follows:

$$\begin{array}{ccccccc}
 \vdots & & \vdots & & & & \\
 \downarrow & & \downarrow & & & & \\
 p_1 & & \widetilde{p}_1 & & & & \\
 \downarrow d_1 & & \downarrow \widetilde{d}_1 & & & & \\
 p_0 & & \widetilde{p}_0 & & & & \\
 \downarrow \epsilon & & \downarrow \widetilde{\epsilon} & & & & \\
 0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0 & \text{exact} & & & & & \\
 \downarrow & & \downarrow & & & & \\
 0 & & 0 & & & &
 \end{array}$$

then there is a projective resolution of M :

$$\cdots \rightarrow \bar{p}_1 \xrightarrow{\bar{d}_1} \bar{p}_0 \xrightarrow{\bar{\epsilon}} M \rightarrow 0$$

such that the completed diagram

$$\begin{array}{ccccccc}
 & \vdots & & \vdots & & \vdots & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & p_1 & \longrightarrow & \overline{p_1} & \longrightarrow & \widetilde{p_1} \longrightarrow 0 \\
 & & \downarrow d_1 & & \downarrow \bar{d}_1 & & \downarrow \tilde{d}_1 \\
 0 & \longrightarrow & p_0 & \longrightarrow & \overline{p_0} & \longrightarrow & \widetilde{p_0} \longrightarrow 0 \\
 & & \downarrow \epsilon & & \downarrow \bar{\epsilon} & & \downarrow \tilde{\epsilon} \\
 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

commutes, and horizontal sequences are all short exact sequences.

Problem 6.13.4 (standard complex). Let S be a set. For $i = 0, 1, 2, \dots$ let E_i be the free module over \mathbb{Z} generated by $(i+1)$ -tuples (x_0, \dots, x_i) with $x_0, \dots, x_i \in S$. Thus such $(i+1)$ -tuples form a basis of E_i over \mathbb{Z} . There is a unique homomorphism

$$d_{i+1} : E_{i+1} \rightarrow E_i$$

such that

$$d_{i+1}(x_0, \dots, x_{i+1}) = \sum_{j=0}^{i+1} (-1)^j (x_0, \dots, \hat{x}_j, \dots, x_{i+1})$$

where the symbol \hat{x}_j means that this term is to be omitted. For $i = 0$, we define $d_0 : E_0 \rightarrow \mathbb{Z}$ to be the unique homomorphism such that $d_0(x_0) = 1$. The map d_0 is sometimes called the **augmentation**, and is also denoted by ϵ . Check that

$$\dots \rightarrow E_{i+1} \rightarrow E_i \rightarrow \dots \rightarrow E_0 \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0$$

is a resolution of \mathbb{Z} by the complex.

6.14

Problem 6.14.1.

- (a) Let $P_\bullet \rightarrow M \rightarrow 0$ be a projective resolution of M . Show that for $N \in \mathfrak{M}_R$, the definition

$$\mathrm{Tor}_n(M, N) := H_n(P_M \otimes N) \quad \text{for } n \geq 0$$

is independent of the choices of projective resolutions.

- (b) For $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ exact in \mathfrak{M}_R , show that we have the long exact sequence :

$$\begin{array}{ccccccc}
 \cdots & \longrightarrow & \mathrm{Tor}_2(M_1, N) & \longrightarrow & \mathrm{Tor}_2(M_2, N) & \longrightarrow & \mathrm{Tor}_2(M_3, N) \\
 & & & & \searrow & & \\
 & & & & \mathrm{Tor}_1(M_1, N) & \longrightarrow & \mathrm{Tor}_1(M_2, N) \longrightarrow \mathrm{Tor}_1(M_3, N) \\
 & & & & & & \searrow \\
 & & & & & & M_1 \otimes N \xrightarrow{i \otimes 1} M_2 \otimes N \xrightarrow{\epsilon \otimes 1} M_3 \otimes N \longrightarrow 0
 \end{array}$$

- (c) If M is flat, show that $\mathrm{Tor}_n(M, N) = 0 \ \forall n > 0, N \in \mathfrak{M}_R$

Problem 6.14.2. Show that

- (a) $\mathrm{Ext}^1(M, N) = 0 \ \forall N \iff M$ is projective.
 (b) $\mathrm{Ext}^1(M, N) = 0 \ \forall M \iff N$ is injective.
 (c) $\mathrm{Tor}_1(M, N) = 0 \ \forall N \iff M$ is flat.

Problem 6.14.3. Show that the two ways to define $\mathrm{Tor}_n(M, N)$ with $M, N \in \mathfrak{R}$ (by $H_n(P_M \otimes N)$ and by $H_n(M \otimes P_N)$) are equivalent.

Problem 6.14.4. Let R be an integral domain and Q be its field of fractions. Show that

- (a) if M is a torsion R -module, then $\mathrm{Tor}_1(Q/R, M) \simeq M$.
 (b) for any $M \in \mathfrak{M}_R$, $\mathrm{Tor}_n(Q/R, M) = 0 \ \forall n \geq 2$ and $\mathrm{Tor}_1(Q/R, M) \simeq \mathrm{Tor}(M)$.
 (c) if M is torsion-free, then $\mathrm{Tor}_1(Q/R, M) \simeq 0$.

6.15

Problem 6.15.1.

- (a) Show that $B(G)$ is a chain complex.
 (b) Show that in $P(G)$, ∂_n is a $\mathbb{Z}[G]$ -module homomorphism.
 (c) Show that $P(G)$ is a chain complex.

Problem 6.15.2.

- (a) Show that τ_n and τ_n^{-1} are $\mathbb{Z}[G]$ -module homomorphisms.
 (b) Show that $\tau = \{\tau_n\}$ is a chain map from $P(G)$ to $B(G)$.
 (c) Show that $\tau^{-1} = \{\tau_n^{-1}\}$ is a chain map from $B(G)$ to $P(G)$

- (d) Show that for $P(G)$, there is $s_n : P_n \rightarrow P_{n+1}$ such that

$$1_{P_n} = s_{n-1} \circ \partial_n + \partial_{n+1} \circ s_n$$

Problem 6.15.3.

- (a) Show that $d_n(U_n) \subseteq U_{n+1}$ for the normalized bar resolution of \mathbb{Z} .
 (b) Show that $B^*(G)$ is a chain complex.
 (c) Show that there is $t_n^* : B_n^* \rightarrow B_{n+1}^*$ such that

$$1_{B_n^*} = t_{n-1}^* d_n^* + d_{n+1}^* t_n^*$$

and $B^*(G)$ is an exact sequence.

Problem 6.15.4.

- (a) Show that if $G = \langle g_1, \dots, g_n \rangle$, then $IG = \langle g_1 - 1, \dots, g_n - 1 \rangle_{\mathbb{Z}[G]}$
 (b) Show that $H_1(G, \mathbb{Z}/m\mathbb{Z}) \simeq G/[G, G]G^m$, where $G^m = \langle g^m : g \in G \rangle$.
 (For $H_1(G, \mathbb{Z}/m\mathbb{Z})$, G acts on $\mathbb{Z}/m\mathbb{Z}$ trivially.)

6.16

Problem 6.16.1.

- (a) For $f : M \rightarrow R$, show that $d_f \circ d_f = 0$.
 (b) For two chain complexes of R -modules $(C_\bullet, d), (C'_\bullet, d')$, show that $(d \circ d') \circ (d \circ d') = 0$.
 (c) Let $M_1, M_2 \in \mathfrak{M}_R$, $f_1 \in \text{Hom}_R(M_1, R)$, $f_2 \in \text{Hom}_R(M_2, R)$. Show that $df_1 \otimes df_2 = df$ with $f = f_1 + f_2 \in \text{Hom}_R(M_1 \oplus M_2, R)$ under the isomorphism

$$\bigoplus_{i=0}^n \bigwedge^i M_1 \otimes \bigwedge^{n-i} M_2 \simeq \bigwedge^n (M_1 \oplus M_2) \quad \forall n.$$

Problem 6.16.2. Let $\{a_1, \dots, a_n\}$ be an R -regular sequence and $I = \langle a_1, \dots, a_n \rangle \subseteq R$. Show that

- (a) I/I^2 is free of rank n over R/I .
 (b) $\text{gr}_I(R) \simeq R/I[x_1, \dots, x_n]$ as graded rings.

Problem 6.16.3. Let $\{a_1, \dots, a_n\}$ be an R -regular sequence and $I = \langle a_1, \dots, a_n \rangle \subseteq R$. Show that R/I does not have any projective resolution of length shorter than n .

Problem 6.16.4. Let $\{x_1, x_2, x_3\}$ be an R -regular sequence. Write down explicitly

$$K_\bullet(\underline{x}) \rightarrow R/\langle x_1, x_2, x_3 \rangle \rightarrow 0$$

where $\underline{x} = x_1, x_2, x_3$.

6.17

Problem 6.17.1. Let a group G act on an abelian group M . Show that $B^2(G, M) \leq Z^2(G, M)$.

Problem 6.17.2. Let $1 \rightarrow M \rightarrow E \xrightarrow{p} G \rightarrow 1$ with two liftings $\ell_1 : G \rightarrow E, \ell_2 : G \rightarrow E$, whose corresponding factor sets are f_1, f_2 , respectively. Show that there is $h : G \rightarrow M$ with $h(1) = 1$ and for all $\bar{x}, \bar{y} \in G$,

$$f_2(\bar{x}, \bar{y})f_1(\bar{x}, \bar{y})^{-1} = \theta_{\bar{x}}(h(\bar{y}))h(\bar{x}\bar{y})^{-1}h(\bar{x})$$

Problem 6.17.3. Show that there are inequivalent extensions of M by G with isomorphic middle group.

6.18

Problem 6.18.1. Two group-homomorphism liftings $\ell_1, \ell_2 : G \rightarrow E$ are *M-conjugate* if there is an $a \in M$ such that $(a, 1)\ell_1(x)(a, 1)^{-1} = \ell_2(x) \forall x \in G$. Show that

$$H^1(G, M) \longleftrightarrow \{M\text{-conjugacy classes of group-homomorphism liftings}\}$$

Problem 6.18.2. Let $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ be split and $\ell : G \rightarrow E, \ell' : G \rightarrow E$ be two liftings with $K = \ell(G), K' = \ell'(G)$. Show that if $H^1(G, M) = H^2(G, M) = 0$, then K and K' are conjugate in E .

Problem 6.18.3.

- (a) Let $d|m$ and N be a $\mathbb{Z}/m\mathbb{Z}$ -module. Compute

$$\text{Ext}_{\mathbb{Z}/m\mathbb{Z}}^n(\mathbb{Z}/d\mathbb{Z}, N), \quad \forall n \geq 0$$

- (b) Compute $\text{Ext}_{\mathbb{Z}/p^2\mathbb{Z}}^n(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}), \quad \forall n \geq 0$.

6.19

Problem 6.19.1. Let $M = \mathbb{Z}/4\mathbb{Z}$ and $G = \mathbb{Z}/2\mathbb{Z}$.

- (a) Find all linear actions of G on M .
- (b) For each such action, compute $H^2(G, M)$.
- (c) For each such action, describe all extensions of M by G .
- (d) For each extension E of M by G , compute $\text{Stab}_E(G, M)/\text{Inn}(G, M)$.

Problem 6.19.2. Compute

- (a) $H_n(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) \forall n \geq 0$.
- (b) $H^n(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) \forall n \geq 0$.

Problem 6.19.3.

- (a) Show that if G acts on M trivially, then

$$H^1(G, M) \simeq \text{Der}(G, M) \simeq \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M).$$

- (b) Let $C_2 = \langle \sigma \rangle$ with $\sigma^2 = 1$ and act on \mathbb{Z} by $\sigma \cdot n = -n$.
Compute $\text{Der}(C_2, \mathbb{Z})$, $\text{PDer}(C_2, \mathbb{Z})$ and $H^1(C_2, \mathbb{Z})$.

Problem 6.19.4. Define $\text{Ind}^G(M) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$ and $\text{CoInd}^G(M) = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)$ which have natural $\mathbb{Z}[G]$ -module structure.

- (a) Compute $H^n(G, \text{CoInd}^G(M))$ and $H_n(G, \text{Ind}^G(M))$ for every $n \geq 0$.
- (b) Let $|G| < \infty$. Show that

$$\text{CoInd}^G(M) \simeq \text{Ind}^G(M)$$

as $\mathbb{Z}[G]$ -modules.

6.20

Problem 6.20.1. Let M be a semisimple A -module and N be a submodule of M . Show that N and M/N are also semisimple.

Problem 6.20.2. Let A be a division ring and M be a free A -module of rank 1. Show that $\text{Hom}_A(M, M) \longleftrightarrow A$.
Is this correspondence a ring homomorphism?

Problem 6.20.3.

- (a) Let $M = N^{\oplus n}$ with N being a simple submodule of M . Let $D' = \text{End}_A(N)$ which is a division ring. Show that

$$\text{End}_A(M) \simeq M_{n \times n}(D') \quad \text{as rings.}$$

- (b) Let $M = N_1^{\oplus m_1} \oplus \cdots \oplus N_r^{\oplus m_r}$ with N_1, \dots, N_r be simple submodules of M and $N_i \not\simeq N_j \forall i \neq j$. Let $D'_i = \text{End}_A(N_i)$, $\forall i = 1, \dots, r$. Show that $\text{End}_A(M)$ is isomorphic to a ring of matrices, of type

$$\begin{pmatrix} I_1 & & O \\ & I_2 & \\ O & & \ddots \\ & & & I_r \end{pmatrix}$$

where $I_i \in M_{m_i \times m_i}(D'_i)$.

Problem 6.20.4.

- (a) Show that every finitely generated semisimple A -module is both Noetherian and Artinian.
- (b) Show that if D is a division ring, then the only two-sided ideals of $M_{n \times n}(D)$ are $\{0\}$ and $M_{n \times n}(D)$.

6.21**Problem 6.21.1.**

- (a) When is an abelian group semisimple (as a \mathbb{Z} -module)?
- (b) Show that a module M is semisimple, if and only if every cyclic submodule of M is semisimple.

Problem 6.21.2.

- (a) Show that the radical of $A/r(A)$ is zero.
- (b) Show that $x \in r(A) \iff 1 - yx$ is invertible for every $y \in A$.
- (c) Show that $r(A)$ is the largest two-sided ideal I such that $1 - x$ is invertible for all $x \in I$.
- (d) Show that if M is a finitely generated A -module such that $r(A)M = M$, then $M = 0$.

Problem 6.21.3. Let R be a semisimple commutative ring. Show that R is a direct product of fields.

Problem 6.21.4. Let R be a finite dimensional commutative algebra over a field k . If R has no nonzero nilpotent element, show that R is semisimple.

6.22

Problem 6.22.1. Show that the only finite dimensional division algebra over an algebraically closed field k is k itself.

Problem 6.22.2. Let E be a finite dimensional vector space over a field k . Let R be a semisimple subalgebra of $\text{End}_k(E)$. Let $a, b \in R$. Assume that

$$\ker b_E \supseteq \ker a_E$$

where a_E, b_E is multiplication by a, b on E , respectively. Show that there exists an element $s \in R$ such that $sa = b$.

Problem 6.22.3. Let E be a finite-dimensional vector space over a field k . Let $A \in \text{End}_k(E)$, we say that A is semisimple if E is a semisimple A -space, or equivalently, let R be the k -algebra generated by A , then E is a semisimple over R . Show that A is semisimple if and only if its minimal polynomial has no factors of multiplicity > 1 over k .

Problem 6.22.4. Let E be a finite-dimensional vector space over a field k , and let S be a commutative set of endomorphisms of E . Let $R = k[S]$. Assume that R is semisimple. Show that every subset of S is semisimple.

6.23

Problem 6.23.1.

- (a) Let $\varphi : G \rightarrow \text{GL}_n(F)$ be a matrix representation. Prove that the map $g \mapsto \det(\varphi(g))$ is a degree 1 representation.
- (b) Prove that the degree 1 representations of G are in bijective correspondence with the degree 1 representations of the abelian group $G/[G, G]$.

Problem 6.23.2.

- (a) Let V be a (possibly infinite dimensional) $F[G]$ -module (G is finite group). Prove that for each $v \in V$, there is an $F[G]$ -submodule containing v of dimension $\leq |G|$.
- (b) Prove that if $|G| > 1$, then every irreducible $F[G]$ -module has dimension $< |G|$.

Problem 6.23.3.

- (a) Exhibit all 1-dimensional complex representations of a finite cyclic group; make sure to decide which are inequivalent (not isomorphic).
- (b) Exhibit all 1-dimensional complex representations of a finite abelian group. Deduce that the number of inequivalent (non-isomorphic) degree 1 complex representations of a finite abelian group equals the order of the group.

Problem 6.23.4.

- (a) Let p be a prime, let P be a p -group and let F be a field of characteristic p . Prove that the only irreducible representation of P over F is the trivial representation.
- (b) Let p be a prime, let P be a nontrivial p -group and let F be a field of characteristic p . Prove that the regular representation is not completely reducible.
- (c) Let p be a prime, let P be a nontrivial p -group and let F be a field of characteristic p . Prove that the regular representation is indecomposable.