Algebra II

Minerva

2020-2nd

Contents

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 : $\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, x) & \mapsto & ax \end{array}$ 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 $f : A \to \mathrm{End}(M)$

Property 1.1.1. Two definition of module are equivalent.

Proof:

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

- M1$\rightsquigarrow$ $f(a)(x+y) = a(x+y) = ax + ay = f(a)(x) + f(a)(y) \rightsquigarrow f(a) \in \mathrm{End}(M)$
- 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 $\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a,x) & \longmapsto & f(a)x \end{array}$ and reverse all in $(1 \Rightarrow 2)$ which satisfy 4 law of module. $\square$

Remark 1.1.1. a left A-module = a represention 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 $(A^\circ, \cdot)$ 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. $\begin{array}{cccc} g: & A^\circ & \longrightarrow & \mathrm{End}(M) \\ & a & \longmapsto & g(a) : z \mapsto xa \end{array}$

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

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. $\varphi : M \to N$ 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 $\operatorname{Im} \varphi$ is a submodule of N

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

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

Well defined : $\overline{x_1} = \overline{x_2} \rightsquigarrow x_1 - x_2 \in N \rightsquigarrow ax_1 - ax_2 = a(x_1 - a_2) \in N \rightsquigarrow \overline{ax_1} = \overline{ax_2}$

Theorem 1.1.1. Basic theorems

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

$$\begin{tikzcd} M/N \arrow[rr, "\exists!\ \overline{\varphi}"] & & M' \\ & M \arrow[ul, "\pi"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

- 1st isom.thm. : Given $\varphi : M \to N$, then $M/\ker\varphi \simeq \operatorname{Im}\varphi$
- 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 $N \subseteq N$

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

and $(M/N)/(M'/N) \simeq M/M'$

Definition 1.1.5 (cokernel). $\operatorname{coker}\varphi := N/\ker\varphi$
$\rightsquigarrow \varphi$ is $1-1 \iff \ker\varphi = \{0\}$, φ is onto $\iff \operatorname{coker}\varphi = \{0\}$

1.1.2 Important examples

Homomorphism group

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

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

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

- When A is commutative, $\operatorname{Hom}_A(M,N)$ has an A-module structure:
  - For $a \in A, f \in \operatorname{Hom}_A(M,N)$, define $(af)(x) := f(ax)\ \forall x \in M$
    - $af \in \operatorname{Hom}_A(M,N)$:
      $(af)(x+y) = f(a(x+y)) = f(ax+ay) = f(ax)+f(ay) = (af)(x)+(af)(y)$
      $((a+b))f(x) = f((a+b)x) = f(ax+bx) = f(ax) + f(bx) = (af)(x) + (bf)(x) = (af+bf)(x)$
    - Module law : M1,M2,M4 is obvious.
      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 ${}_AM_B$ is A, B-**bimodule**

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

- Given ${}_AM$, ${}_AM_B$, $\mathrm{Hom}_A(M,N)$ has a right B-module structure. $(fb)(x) = f(x)b$
- Given M_B, ${}_AM_B$, $\mathrm{Hom}_B(M,N)$ 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.
$\forall T \in \mathrm{Hom}_k(V,V) \rightsquigarrow V$ has a $k[x]$-module structure corresponding to T. Define

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

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

representation of group

Let G be a finite group with $|G| = n$, say $G = \{g_1, ..., g_n\}$
Consider $V = \mathbb{R}g_1 \oplus \cdots \oplus \mathbb{R}g_n$ and define

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

then $\begin{array}{rccc} \varphi: & G & \longleftarrow & \mathrm{GL}(V) \\ & g & \longmapsto & \rho_g \end{array}$ 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

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

Example 1.1.2.
- $G = \langle g \rangle$ with $g^3 = e \implies \mathbb{C}[G] = \mathbb{C} \oplus \mathbb{C}g \oplus Cg^2 \simeq \mathbb{C}[x]/\langle x^3 - 1\rangle$
- $\mathbb{Z}$ is $\mathbb{Z}[x]$-module : $\mathbb{Z} \simeq \mathbb{Z}[x]/\langle x \rangle$ is a $\mathbb{Z}[x]$-module and thus $f(x)\cdot n := f(x)\overline{n} = \overline{f(0)n}$

1.2 Free module

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

$$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n)$$
$$a(a_1, ..., a_n) = (aa_1, ..., aa_n)$$

is an A-module. Let $e_i = (0, ..., 1, ..., 0)$ (i-th entry is 1 and others are 0) $\forall i = 1, ..., n$
Then $(a_1, ..., a_n) = \sum_{i=1}^{n} a_i e_i$ 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 $\{x_1, ..., x_n\}$, then $M \simeq A^n$

Proof: Define $\begin{array}{rccc} \varphi: & A^n & \longrightarrow & M \\ & e_i & \longmapsto & x_i \end{array}$ and extend by linearity

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

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 does 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 $\{e_1, e_2, ...\}$

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

Define $\begin{array}{rccc} \varphi: & A & \longrightarrow & A \times A \\ & T & \longmapsto & (T_1, T_2) \end{array}$, 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 $\rho_\lambda : M_\lambda \to \coprod_{\lambda\in\Lambda} M_\lambda\ \forall\lambda \in \Lambda$ s.t. $\forall\ N$ with A-module homo. $f_\lambda : M_\lambda \to N\ \forall\lambda \in \Lambda$, then $\exists!$ A-module homomorphism φ let the diagrams commute.

$$\begin{tikzcd} \coprod_{\lambda\in\Lambda} M_\lambda \arrow[rr, dashed, "\exists!\ \varphi"] & & N \\ & M_\lambda \arrow[ul, "\rho_\lambda"] \arrow[ur, "f_\lambda"'] & \end{tikzcd} \qquad \forall\lambda \in \Lambda$$

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 ρ_λ :

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

- Given $f_\lambda : M_\lambda \to N$

$$\begin{tikzcd} \rho_\lambda(x_\lambda) \in \coprod_{\lambda\in\Lambda} M_\lambda \arrow[rr, dashed, "\exists!\ \varphi"] & & N \ni f_\lambda(x_\lambda) \\ & x_\lambda \in M_\lambda \arrow[ul, "\rho_\lambda"] \arrow[ur, "f_\lambda"'] & \end{tikzcd}$$

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 $i : S \to F$ s.t. giving any mapping $j : S \to M$, where M is an A-module. Then $\exists!$ A-module homomorphism φ let the diagrams commute.

$$\begin{tikzcd} F \arrow[rr, dashed, "\exists!\ \varphi"] & & M \\ & S \arrow[ul, "i"] \arrow[ur, "j"'] & \end{tikzcd}$$

Theorem 1.2.1. Given $S \neq \varnothing$, 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 $j : S \to M$, define $\begin{array}{rccc} f_\lambda : & M_\lambda & \longrightarrow & M \\ & ax_\lambda & \longmapsto & aj(x_\lambda) \end{array}$

By the universal property of direct sum,

$$\begin{tikzcd} i(x_\lambda) \in \coprod_{\lambda\in\Lambda} M_\lambda \arrow[rr, dashed, "\exists!\ \varphi"] & & N \ni j(x_\lambda) \\ & M_\lambda \arrow[ul, "\rho_\lambda"] \arrow[ur, "f_\lambda"'] & \\ & x_\lambda \in S \arrow[uul, bend left, "i"] \arrow[uur, bend right, "j"'] & \end{tikzcd}$$

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. Then we called F has **IBN** (**Invariant basis number**).

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

Claim: $A^n \simeq A^m \iff n = m$

pf. 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 $f_1, ..., f_m$ will have non-trivial linearly relation.

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

Definition 1.2.4 (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 $S' = \{x'_1, ..., x'_m\} \rightsquigarrow \exists \{x_1, ..., x_n\} \subset S$ s.t. $S' \subseteq \langle x_1, ..., x_n\rangle_A \rightsquigarrow F = \langle S'\rangle_A \subseteq \langle x_1, ..., x_n\rangle_A \subseteq F \rightsquigarrow F = \langle x_1, ..., x_n\rangle$. Since $|S| = \infty, \exists x \in S \setminus \{x_1, ..., x_n\} \rightsquigarrow x \in \langle x_1, ..., x_n\rangle_A$, but $x, x_1, ..., x_n$ are linearly independent. $(\rightarrow\leftarrow)$
- $|S| = \infty, |S'| = \infty$. Assume that $|S'| \le |S|$

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

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

  - $|S_T| < \infty : \langle T\rangle_A \subseteq \langle y_1, ..., y_n\rangle_A$ for some $\{y_1, ..., y_n\} \subset S$
    $\rightsquigarrow S_T \subseteq \langle T\rangle_A \subseteq \langle y_1, ..., y_n\rangle_A$. By linear independence of S, $S_T \subseteq \{y_1, ..., y_n\}$
  - $|S| \le |S'|$: Let $\mathcal{B} = \{T \subseteq S' : |T| < \infty\}$. Since $|S'| = \infty, |\mathcal{B}| = |S'|$
    Define

$$\begin{array}{rccc} f: & S & \longrightarrow & \mathcal{B} \\ & \sum_{i=1}^{k} a_i y'_i = y & \longmapsto & \{y'_1, ..., y'_k\} \end{array}$$

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

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

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

$\square$

Definition 1.2.5 (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 : $\pi_\lambda : \prod_{\lambda\in\lambda} M_\lambda \to M_\lambda \ \forall\lambda$ s.t. for any A-module N with $h_\lambda : N \to M_\lambda \ \forall\lambda$, then $\exists!$ A-module homomorphism φ let the diagram commute.

$$\begin{tikzcd}
N \arrow[rr, dashed, "\exists!\ \varphi"] \arrow[dr, "h_\lambda"'] & & \prod_{\lambda\in\Lambda} M_\lambda \arrow[dl, "\pi_\lambda"] \\
& M_\lambda &
\end{tikzcd}$$

Definition 1.2.6. 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

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

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

$$\begin{tikzcd}
x \in N \arrow[rr, dashed, "\exists!\ \varphi"] \arrow[dr, "h_\lambda"'] & & \prod_{\lambda\in\Lambda} M_\lambda \arrow[dl, "\pi_\lambda"] \\
& h_\lambda(x) \in M_\lambda &
\end{tikzcd}$$

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.

$$\begin{tikzcd}
\mathrm{Hom}_A(\coprod_\lambda M_\lambda, N) \arrow[dr, dash] & \mathrm{Hom}_A(\prod_\lambda M_\lambda, N) & \mathrm{Hom}_A(N, \coprod_\lambda M_\lambda) \arrow[d, dash] & \mathrm{Hom}_A(N, \prod_\lambda M_\lambda) \arrow[d, dash] \\
\coprod_\lambda \mathrm{Hom}_A(M_\lambda, N) & \prod_\lambda \mathrm{Hom}_A(M_\lambda, N) & \coprod_\lambda \mathrm{Hom}_A(N, M_\lambda) & \prod_\lambda \mathrm{Hom}_A(N, M_\lambda)
\end{tikzcd}$$

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

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

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

Definition 1.3.4 (direct limits).

Construction:

Let $C := \bigoplus\limits_{i \in I} M_i$ 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

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

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

Universal Property

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

$$\begin{tikzcd}
 & N & \\
 & \varinjlim M_i \arrow[u, dashed, "\exists !\ \alpha"] & \\
M_i \arrow[uur, bend left, "\alpha_i"] \arrow[ur, "\mu_i"] \arrow[rr, "\mu_{ij}"] & & M_j \arrow[uul, bend right, "\alpha_j"'] \arrow[ul, "\mu_j"']
\end{tikzcd} \qquad \forall i \leq j$$

Construction of α

Define $\alpha : \varinjlim M_i \to N$ 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 μ_k in both side, then

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

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

- $\forall\ i \leq j, \pi_{ji} : M_j \to M_i$ 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 $\pi_i : \varprojlim M_i \to M_i$, then $\pi_i = \pi_{ji} \circ \pi_i \ \forall i \leq j$

Universal property

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

$$\begin{tikzcd}
& N \arrow[d, dashed, "\exists!\ \alpha"] \arrow[ddl, bend right, "\alpha_i"'] \arrow[ddr, bend left, "\alpha_j"] & \\
& \varprojlim M_i \arrow[dl, "\pi_i"'] \arrow[dr, "\pi_j"] & \\
M_i & & M_j \arrow[ll, "\pi_{ji}"']
\end{tikzcd}$$

Construction α

Define $\alpha : N \to \varprojlim M_i$ 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

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

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 $a_n = \overline{a} \in \mathbb{Z}/p^n\mathbb{Z}$

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

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

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

  - $d_p(a, b) = 0 \iff a_n = b_n\ \forall n \iff a = b$
  - $d_p(a, b) = d_p(b, a)$
  - $d_p(a, c) \le \max\{d_p(a, b), d_p(b, c)\}$
- **Claim:** $\mathbb{Z}_p$ is a complection 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.

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

  Notice that

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

  So we can rewrite the condition :

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

  Choose $\varepsilon = p^{-k}$, then exists $N \in \mathbb{N}$ s.t. $\forall n \ge N,\ d_p(x_{n+1}, x_n)$
  Let a_n equal to the k-th term of x_N, then $(x_n) \to (a_i)_{i\in\mathbb{N}}$. 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 $C(U) := \{f : U \to Y \text{ is continuous}\}$
$I := \{U \underset{\text{open}}{\subseteq} X : x \in U\}$ with $U \le V \iff V \subseteq U$
Construct a direct system over $I : \forall u \le v$

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

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 $\begin{array}{ccc} R & \longrightarrow & Ra \\ r & \longmapsto & ra \end{array}$, since R is integral domain, $ra = 0 \iff r0$. Hence, $Ra \simeq R$.

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

$$P : \begin{array}{ccc} R^n & \longrightarrow & R \\ (x_1, ..., x_n) & \longmapsto & x_1 \end{array}$$

and $\overline{P} : N \to R$ is the restriction on N.

- Case1. : $\operatorname{Im} \overline{P} = \{0\} \rightsquigarrow N \subseteq \ker P_1 \simeq R^{n-1}$, by induction hypothesis, N is free of rank $\leq n-1$
- Case2. : $\operatorname{Im} \overline{P} \neq \{0\}$ is a ideal in R, write $\operatorname{Im} \overline{P} = \langle a \rangle$ and $\overline{P}(x) = a$ for some $x \in N$

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

  - $\ker \overline{P} \cap Rx = \langle 0 \rangle : 0 = \overline{P}(rx) = r\overline{P}(x) = ra \in R \implies r = 0 \implies rx = 0$
  - $N = \ker \overline{P} + Rx : \forall y \in N,\ \overline{P}(y) = ra = \overline{P}(rx) \implies \overline{P}(y - rx) = 0 \implies y - rx \in \ker \overline{P} \implies y \in \ker \overline{P} + Rx$

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

  $$\begin{cases} \ker \overline{P} \subseteq \ker P \subseteq R^n \rightsquigarrow \ker \overline{P} \text{ is free of rank} \leq n-1 \\ rx = 0 \iff 0 = \overline{P}(rx) = ra \in R \rightsquigarrow r = 0 \rightsquigarrow Rx \simeq R \text{ is free of rank1} \end{cases}$$

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

□

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

$$\begin{tikzcd} 0 \arrow[r] & \ker f \arrow[r] & R^n \arrow[r, "f", "e_i \mapsto f_i"'] & M \arrow[r] & 0 \\ & R^m \arrow[u, "\wr"] \arrow[ur, "T"'] & & & \end{tikzcd}$$

$M \simeq R^n / \ker f$ and $\begin{pmatrix} f_1 & f_2 & \cdots & f_m \end{pmatrix} = \begin{pmatrix} e_1 & e_2 & \cdots & e_n \end{pmatrix} A$ for some $A \in M_{n\times m}(R)$.

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

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

with $d_i | d_{i+1}$

Before we prove the theorem, we give some notations.

Notation 1.4.1.

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

Proof: Define the length $\ell(a)$ of non-unit a to be r if $a = p_1p_2\cdots p_r$, p_i : prime (Since PID $\Longrightarrow$ 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 $\begin{cases} a_{11}|a_{1k} & \forall k = 2, ..., m \\ a_{11}|a_{k1} & \forall k = 2, ..., n \end{cases}$:

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

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

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 $a_{11}|b_{k\ell}$, 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 $\begin{pmatrix} b_{22} & \\ & \boldsymbol{c_{ij}} \end{pmatrix}$ with $b_{22}|c_{33}$.

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

$\square$

Remark 1.4.1. $d_1, d_2, ..., d_r$ 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

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

and $\det(PA)$ 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, $d_k \simeq A_k(A)/A_{k-1}(A)$ $\square$

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

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

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

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

and

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

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

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

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

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

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

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

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

$$\begin{array}{rccccc} \varphi: & R & \to & Rw_i & \to & Rw_i/Rd_i w_i \\ & r & \mapsto & rw_i & \mapsto & \overline{rw_i} \end{array}$$

$r \in \ker\varphi \iff rw_i = r' d_i w_i \iff r = r' d_i$, thus $\ker\varphi = \langle d_i \rangle$ and $Rw_i/Rd_i w_i \simeq R/\langle d_i \rangle$. 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 $d_1, d_2, ..., d_k$ are units and $d_{k+1}, ..., d_m$ are not units, rewrite $d_{k+1} = a_1, ..., d_m = a_\ell$. 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 $z \longleftrightarrow \overline{1} \in R/\langle a_1 \rangle$, then $a_1 z \longleftrightarrow a_1 \overline{1} = \overline{a_1} = \overline{0} \in R/\langle a_1 \rangle$, 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

- $\mathrm{ann}(z) := \{r \in R : rz = 0\}$ is a left ideal of R is called **annihilate** of z.
- z is called a **torsion element** if $\mathrm{ann} \neq \langle 0 \rangle$
- $\mathrm{Tor}(M) = \{\text{torsion elements of } M\}$
  - R is integral domain$\rightsquigarrow$ $\mathrm{Tor}(M)$ 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 $\mathrm{Tor}(M) = M$
- M is torsion free if $\mathrm{Tor}(M) = \langle 0 \rangle$

(If M is finite generated over a PID, then $M = \mathrm{Tor}(M) \oplus R^s$ and $M/\mathrm{Tor}(M) \simeq R^s$ 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 proved 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 $\operatorname{ann}(u) = \langle d\rangle$ and $d = pq$
  - $N^{(1)}(p) \simeq F$:
    - $N^{(1)}(p) = \langle q\rangle/\langle d\rangle$:
      Since $r \in N^{(1)}(p) \rightsquigarrow rp = \overline{0}$ 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

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

      $r \in \ker f \iff rq = r'd \iff r = r'p$. Thus, $\ker f = \langle p\rangle$
  - $pN = p \cdot R/\langle d\rangle \simeq (\langle p\rangle + \langle d\rangle)/\langle d\rangle \simeq \langle \gcd(p,d)\rangle/\langle d\rangle \simeq \langle p\rangle/\langle d\rangle \simeq Rp/Rpq \simeq R/\langle q\rangle$ (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
  - $N^{(1)}(p) \simeq \bigoplus_{i=1}^{\ell} (R/\langle d_i\rangle)^{(1)}(p) \simeq F^\ell$
  - $$N/pN \simeq \left(\bigoplus_{i=1}^{\ell} R\Big/\langle d_i\rangle\right)\Bigg/\left(\bigoplus_{i=1}^{\ell} \langle p\rangle\Big/\langle d_i\rangle\right) \simeq F^\ell$$

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

$$M \simeq R\Big/\langle a_1\rangle \oplus \cdots \oplus R\Big/\langle a_\ell\rangle \oplus R^s \tag{*}$$

where a_i are non-zerp and non-unit. Also, s is unique (which is called **rank** of M) and $a_1, ..., a_\ell$ (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 $a_i|a_{i+1}, b_i|b_{i+1}$

- $M/\operatorname{Tor}(M) \simeq R^s \simeq R^t \implies s = t$
- $\operatorname{Tor}(M) \simeq R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_\ell\rangle \simeq R/\langle b_1\rangle \oplus \cdots \oplus R/\langle b_k\rangle$
  - If $\operatorname{Tor}(M) \ni x \longleftrightarrow x_1^{\in R/\langle a_1\rangle} + \cdots + x_\ell$, then $x \in \operatorname{Tor}(M)^{(1)}(p) \iff px_i = 0\ \forall i$ $\iff px_i \in \langle a_i\rangle \iff px_i = r_i a_i \rightsquigarrow p|r_i a_i \rightsquigarrow \begin{cases} p|r_i \rightsquigarrow a_i|x_i \rightsquigarrow x_i = 0 \text{ in } R\langle a_i\rangle \\ p|a_i \end{cases}$
    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 og elements b_j, so $\ell \leq k$. By symmetric, $k \leq \ell \implies k = \ell$.
  - Moreover, we get that $\begin{cases} p|a_1 \rightsquigarrow p|b_1 \\ p|b_1 \rightsquigarrow p|a_1 \end{cases} \rightsquigarrow a_1, b_1$ share the same prime divisor $p_1, ..., p_\mu$. 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

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

    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, $\alpha_i = \beta_i \rightsquigarrow a_1 \sim b_1$

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

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

$\square$

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,

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

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 $T \in \mathrm{Hom}_k(V, V)$. 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 $= \dim Z$, then $\{v, xv, ..., x^{k-1}v\}$ form a basis for $Z \implies x^k v + a_{k-1}x^{k-1}v + \cdots a_1 xv + v = 0$ for some $a_i \in k$. Hence, $v \in \mathrm{Tor}(V)$ □

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

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

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

Proof:

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

□

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

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

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

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

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

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

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

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

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

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

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: $\det P \det A \det Q = d_1(x)d_2(x)\cdots d_r(x)$. 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 $\det A = ch_T(x) = d_1(x)d_2(x)\cdots d_r(x)$. $\begin{cases} d_i(x)v_i = 0 \\ d_i | d_r \end{cases} \rightsquigarrow d_r(x)v_i = 0$ $\forall i = 1, ..., r$ 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 $m_T | d_r$. Consider $(1, 1, ..., 1) \leftrightarrow v$. Since $m_T(x)v = 0 \implies m_T(x)1 = 0$ in $R/\langle d_r \rangle \implies d_r | m_T$. Hence, $d_r = m_T$

Jordan canonical form of T

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

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

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

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

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 $f : M \times N \to G$ 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 $h : M \times N \to M \otimes N$ s.t. $\forall$ abelian group G and $\forall A$-biadditive function $f : M \times N \to G, \exists! \mathbb{Z}$-module homo. $\widetilde{f}$ let the diagram commute

$$\begin{tikzcd} M \otimes_A N \arrow[r, dashed, "\widetilde{f}"] & G \\ M \times N \arrow[u, "h"] \arrow[ur, "f"'] & \end{tikzcd}$$

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

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

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

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

$$\begin{tikzcd} M \times N \arrow[r] \arrow[dr, "f"'] & F \arrow[r, two heads] \arrow[d, dashed, "\exists f_1"] & F/I \arrow[dl, dotted, "\exists \widetilde{f}"] \\ & G & \end{tikzcd}$$

By universal property of free module, $\exists!$ module homomorphism $f_1 : F \to G$ 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 $\widetilde{f} : F/I \to G$

$\square$

Remark 1.6.1.

- This yields

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

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

  $(a_1 a_2)x \otimes y = a_1(a_2 x) \otimes y = a_2 x \otimes a_1 y = x \otimes a_2 a_1 y$. We need A 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 $\begin{array}{rccc} \rho_b : & M & \longrightarrow & M \\ & x & \longmapsto & bx \end{array}$ is a right A-module homo.
$\rho_b(xa) = b(xa) = (bx)a = \rho_b(x)a$ and

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

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

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

$\square$

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

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

is a group homomorphism.

Proof: We only need to proof that

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

is an A-biadditive. Which is trivial. □

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

Then we have

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

Corollary 1.6.2. Let $f : A \to B$ 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.

- $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$ ($\because q \otimes \overline{a} = \frac{q}{n} \cdot n \otimes \overline{a} = \frac{q}{n} \otimes n\overline{a} = \frac{q}{n} \otimes 0 = 0$)
- $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\gcd(m, n)\mathbb{Z}$ (let $d = \gcd(m, n)$)
  - $\overline{a} \otimes \overline{b} = ab(\overline{1} \otimes \overline{1}) \rightsquigarrow \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \otimes \overline{1} \rangle_{\mathbb{Z}}$
  - $m(\overline{1} \otimes \overline{1}) = \overline{0} \otimes \overline{1} = 0, n(\overline{1} \otimes \overline{1}) = \overline{1} \otimes \overline{0} = 0 \rightsquigarrow o(\overline{1} \otimes \overline{1})|d$
  - $\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/d\mathbb{Z} \\ (\overline{a}, \overline{b}) & \longmapsto & \overline{ab} \end{array}$ is $\mathbb{Z}$-bilinear $\rightsquigarrow \exists! \mathbb{Z}$-module homo.

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

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

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

Proof:

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

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

Conversely,

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

$$\Longrightarrow \begin{array}{ccc} M \otimes_A N & \xrightarrow{homo.} & (M \oplus M') \otimes N \\ x \otimes y & \longmapsto & (x,0) \otimes y \end{array}$$

Similarly,

$$\Longrightarrow \begin{array}{ccc} M' \otimes_A N & \xrightarrow{homo.} & (M \oplus M') \otimes N \\ x' \otimes y & \longmapsto & (0,x') \otimes y \end{array}$$

By universal property of direct sum,

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

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 $\begin{array}{ccc} A/I \times N & \longrightarrow & N/IN \\ (\overline{a}, \overline{x}) & \longmapsto & \overline{ax} \end{array}$ is A-biadditive

$$f: \begin{array}{ccc} A/I \otimes N & \longrightarrow & N/IN \\ \overline{a} \otimes x & \longmapsto & \overline{ax} \end{array}$$

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

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

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

- $g \circ f(\overline{a} \otimes x) = g(\overline{ax}) = \overline{1} \otimes ax = \overline{a} \otimes x$
- $f \circ g(\overline{x}) = f(\overline{1} \otimes x) = \overline{x}$

Note: $A \otimes_A N \simeq N$ □

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

$T^i(M) := \underbrace{M \otimes \cdots \otimes M}_{i \text{ times}}$ is a R-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 $\varphi : M \to A$ is an R-module homo., then $\exists! \widetilde{\varphi} : T(M) \longrightarrow A$ is an R-alg. homo.:

  Define
$$\begin{array}{rccc} f_k : & M \times \cdots \times M & \longrightarrow & A \\ & (x_1, ..., x_k) & \longmapsto & \varphi(x_1)\varphi(x_2)\cdots\varphi(x_k) \end{array}$$
  is a R-multilinaer$\rightsquigarrow \exists!\ \widetilde{f_k} : M \otimes \cdots \otimes M \longrightarrow A$ is R-module homo.

  By universal property of direct sum :

$$\begin{tikzcd} \exists!\ \varphi :\ T(M) \arrow[rr, "R\text{-module homo.}"] & & A \\ & T^k(M) \arrow[ul, "\rho_k"] \arrow[ur, "f_k"'] & \end{tikzcd}$$

  Also,

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

$\Longrightarrow$ The ring $T(M)$ is called the **tensot 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 $T(M)$

- $S(M) = T(M)\big/C(M)$ is called **symmetric algebraic** and

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

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

$$\begin{tikzcd}
S(M) \arrow[rr, "\widetilde{\varphi}"] & & A \\
T(M) \arrow[u, dotted] \arrow[urr, dotted] & M \arrow[l, dotted] \arrow[ul] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

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

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

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

- $\sim$ is an equivalence relation
- $\dfrac{x}{t}$ = the equivalence class of (x,t)
- M_s is an R_s-module $\left(\dfrac{a}{s} \cdot \dfrac{x}{t} = \dfrac{ax}{st}\right)$
- $f : M \to N$ is an R-module homo. $\rightsquigarrow \begin{array}{cccc} f_s : & M_s & \to & N_s \\ & \frac{x}{t} & \mapsto & \frac{f(x)}{t} \end{array}$

  Well-defined :

$$\frac{x_1}{t_1} = \frac{x_2}{t_2} \rightsquigarrow \exists u \in S,\ ut_2x_1 = ut_1x_2 \rightsquigarrow ut_2 f(x_1) = ut_1 f(x_2) \rightsquigarrow \frac{f(x_1)}{t_1} = \frac{f(x_2)}{t_2}$$

Property 1.8.1. If $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} L \longrightarrow 0$ is exact for R-modules, then $0 \longrightarrow M_s \xrightarrow{f_s} N_s \xrightarrow{g_s} L_s \longrightarrow 0$ 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. $g(y) = z \rightsquigarrow g_s(\frac{y}{t}) = \frac{z}{t}$
- $\operatorname{Im} f_s \subseteq \ker g_s : g_s(f_s(\frac{x}{t})) = \frac{g(f(x))}{t} = \frac{0}{t} = 0$
- $\ker g_s \subseteq \operatorname{Im} f_s : g_s(\frac{y}{t}) = 0 \rightsquigarrow \exists u \in S,\ ug(y) = 0 \rightsquigarrow uy = f(x) \rightsquigarrow \frac{y}{t} = \frac{f(x)}{ut} \in \operatorname{Im} f_s$

$\square$

Property 1.8.2. $R_s \otimes_R M = M_s$

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

Well-defined :

$$\frac{a_1}{t_1} = \frac{a_2}{t_2} \rightsquigarrow \exists u \in S \text{ s.t. } u(t_1a_2 - t_2a_1) = 0 \rightsquigarrow u(t_1a_2 - t_2a_1)x = 0 \rightsquigarrow \frac{a_1x}{t_1} = \frac{a_2x}{t_2}$$

$$\Longrightarrow \begin{array}{rccc} \widetilde{f}: & R_s \otimes M & \longrightarrow & M_s \\ & (\frac{a}{t}, x) & \longmapsto & \frac{ax}{t} \end{array}$$

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

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

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

$\square$

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

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

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

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

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

(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 $\forall m \in \operatorname{Max} R,\ R \subset R_m \subset K$ and $R = \bigcap\limits_{m \in \operatorname{Max} R} R_m$

Proof: Let $R' = \bigcap\limits_{m \in \operatorname{Max} R} R_m \rightsquigarrow R \subset R' \subset R_m \implies R_m \subseteq R'_m \subseteq (R_m)_m = R_m$. So $R_m = R'_m\ \forall m \in \operatorname{Max} R \rightsquigarrow R = R'$ □

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

- TFAE : $(1)\varphi$ is $1-1$ $(2)\varphi_p$ is $1-1$ $\forall p \in \operatorname{Spec} R$ $(3)\varphi_m$ is $1-1$ $\forall m \in \operatorname{Max} R$
- TFAE : $(1)\varphi$ is onto $(2)\varphi_p$ is onto $\forall p \in \operatorname{Spec} R$ $(3)\varphi_m$ is onto $\forall m \in \operatorname{Max} R$

  $(1) \Rightarrow (2) : M \to N \to 0 \rightsquigarrow M_p \to N_p \to 0$

  $(2) \Rightarrow (3)$: OK!

  $(3) \Rightarrow (1) : M \xrightarrow{\varphi} N \longrightarrow \operatorname{coker} \varphi \longrightarrow 0 \implies M_m \xrightarrow{\varphi_m} N_m \longrightarrow (\operatorname{coker} \varphi)_m \longrightarrow 0 \implies (\operatorname{coker} \varphi)_m = 0 \implies \varphi$ is onto.

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

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

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 $\dfrac{a}{t} \cdot \dfrac{b}{s} \in P_S \rightsquigarrow \dfrac{ab}{ts} = \dfrac{c}{v},\ c \in P \rightsquigarrow \exists u \in S,\ uvab = utsc \in P$, since $c \in P$. Since $uv \in S$ and $S \cap P = \varnothing \rightsquigarrow ab \in P \rightsquigarrow a \in P$ 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. $(\subseteq)$: $\frac{a}{1} \in P_s \rightsquigarrow \frac{a}{1} = \frac{b}{t},\ b \in P \rightsquigarrow \exists u \in S,\ uta = ub \in P \rightsquigarrow a \in P$

□

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

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

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

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

Proof: Let $M = \langle x_1, ..., x_n \rangle_R$. By induction on n.
$n = 1 : M = Rx_1 \simeq R/\operatorname{ann}(x_1)$.
Claim: $\operatorname{Ann}_R(R/I) = I$
pf. $(\supseteq)$: OK! $(\subseteq) : \forall a \in \operatorname{Ann}_R(R/I) \rightsquigarrow a(1+I) = I \rightsquigarrow a \in I$ $\square$
So

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

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

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

$\square$

Definition 1.8.4. N, L are submodules of M.
Define $(N : L) := \{x \in R : xL \subseteq N\} = \operatorname{Ann}_R\left((L+N)\big/N\right)$

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

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

$\square$

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. $\sqrt{\langle 0 \rangle} = \bigcap\limits_{P \in \operatorname{Spec} R} P$

Proof: $(\subseteq) : x^n = 0 \in P\ \forall P \in \operatorname{Spec} R \implies x \in P\ \forall p \in \operatorname{Spec} R$
$(\supseteq)$: If $x \notin \sqrt{\langle 0 \rangle}$ i.e. $x^n \neq 0\ \forall n > 0$, then consider

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

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 $I = \bigcup\limits_{i \in \Lambda} I_i$ is a ideal and $x^n \neq I\ \forall n > 0 \rightsquigarrow I$ is a least upper bound for T. By Zorn's lemma, S has a maximal element. Say P.
Claim: $P \in \operatorname{Spec} R$
pf. For $a, b \notin P$. $\langle a \rangle + P, \langle b \rangle + P \supsetneq P$, so $\exists m, n > 0$ s.t. $\begin{cases} x^m \in P + \langle a \rangle \\ x^n \in P + \langle b \rangle \end{cases} \implies$
$x^{m+n} \in P + \langle ab \rangle \implies P + \langle ab \rangle \notin S \implies ab \notin P$. $\square$
In particular, $x \notin P \in S$ $\square$

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

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

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

□

1.9 Noetherian modules

Definition 1.9.1. An (left) A-module M is said to be **Noetherian** if every ascending chain of submodule $M_i : M_1 \subseteq M_2 \subseteq M_2 \subseteq \cdots$ becomes stationary i.e. $\exists n \in N$ s.t. $M_n = M_{n+1} = \cdots$
(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. $M_2 \subsetneq M_3 \rightsquigarrow M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots$ will stationary $(\rightarrow\leftarrow)$
- (2) $\Rightarrow$ (3) : For $N \leq M$, consider $\mathcal{S} = \{\text{all f.g. submodules of } N\} \neq \varnothing$, 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) : $M_1 \subseteq M_2 \subseteq \cdots$ in M. Let $N = \bigcup\limits_{i=1}^{\infty} M_i$ which is a submodule of M, say $N = \langle x_1, ..., x_k \rangle_R$ and $x_i \in M_{n_i}$. Let $n = \max\limits_{1 \leq i \leq k} n_i \rightsquigarrow N \subseteq M_n \subseteq N \implies N = M_n$ and $M_n = M_{n+1} = \cdots$

□

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 $Z, Z[x], \mathbb{Z}[x, y], ..., k[x_1, ..., x_n]$ 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 $f_3, f_4, \ldots$ and let $\deg f_i = n_i$, the leading coefficient is $a_i \rightsquigarrow n_1 \leq n_2 \leq \cdots$.

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

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

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

$\square$

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

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:
$(\Rightarrow)$:

- $L_1 \subset L_2 \subset \cdots$ in $L \rightsquigarrow f(L_1) \subset f(L_2) \subset \cdots$ in $M \rightsquigarrow f(L_n) = f(L_{n+1}) = \cdots$
  Since f is $1-1$, $L_n = L_{n+1} = \cdots$
- $N_1 \subset N_2 \subset \cdots$ in $N \simeq M/L$, by 3rd isom. thm., we have $N_i \longleftrightarrow M_i/L$ and $M_1 \subset M_2 \subset \cdots$ in $M \rightsquigarrow M_n = M_{n+1} = \cdots$ and thus $N_n = N_{n+1} = \cdots$

$(\Leftarrow)$:
$M_1 \subset M_2 \subset \cdots$ in M, then

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

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 $y \in M_r$ $\implies (x-y) \in \ker g = \operatorname{Im} f \in f(L) \implies x - y \in f(L) \cap M_{r+1} = f(L) \cap M_r \rightsquigarrow x \in M_r$ $\square$

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

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

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

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

Proof: Consider

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

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

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

Observation: R : commutative and M : R-module, $\forall 0 \neq x \in M \implies \operatorname{ann}(x) \subsetneq R$
If P is a maximal element in $\{\operatorname{ann}(x) : x \in M\}$, say $P = \operatorname{ann}(z) \implies P \in \operatorname{Spec} R$

pf. $p \subsetneq R$. If $ab \in P$ and $a \notin P$, then $abz = 0, az \neq 0 \implies b \in \operatorname{ann}(az) \supseteq \operatorname{ann}(z) \implies \operatorname{ann}(az) = \operatorname{ann}(z) \implies b \in P$.

Definition 1.9.3 (**Associated prime**)**.**

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

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

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

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

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, $a^n \in \operatorname{Ann}(M)$ i.e. $a \in \sqrt{\operatorname{Ann}(M)}$
- $a \in R$ 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, $a^{n(x)} \in \operatorname{ann}(x)$ $\forall x \in M$ i.e. $a \in \bigcap\limits_{x \in M} \sqrt{\operatorname{ann}(x)}$

Fact 1.9.2. M is f.g. R-module $\rightsquigarrow$ "local nilpotent $\implies$ nilpotent"

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

Definition 1.9.5 (Support)**.**

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

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

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

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

Property 1.9.3. a is locally nilpotent on $M \iff a \in \bigcap\limits_{P \in \operatorname{Supp}(M)} P$

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

$(\Leftarrow)$: 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. $\{1, a, a^2, ...\}_{:=S} \cap \operatorname{ann}(x) = \varnothing$. Let $\mathcal{S} = \{\operatorname{ann}(x) \subseteq I \subseteq R : I \cap S = \varnothing\} \neq \varnothing$, since $\operatorname{ann}(x) \in \mathcal{S}$. By Zorn's lemma, $\exists$ a max element $P \in \mathcal{S}$.

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

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

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

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

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

and by Property 1.8.4 we will get the result.

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

Proof: $(\subseteq)$: By Fact 1.9.3

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

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

By Homework 7, R is Noetherian $\implies R_p$ is Noetherian $\forall p \subsetneq R$

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

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

Let $u = u_1 \cdots u_m \notin p \rightsquigarrow a_i u r x = 0\ \forall\ i = 1, ..., r \rightsquigarrow q \subseteq \operatorname{ann}(urx)$

Conversely, if $a \in \operatorname{ann}(urx) \rightsquigarrow \frac{au}{1} \in q_p$, 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 $wsu \notin q$ ☐

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

Proof: Let $\mathcal{S} := \{N \subseteq M | N$ satisfies condition in above$\} \neq \varnothing$, since $\exists\, p \in \operatorname{Ass}(M) \rightsquigarrow Rx \simeq R/p \in \mathcal{S}$. 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 $\implies \exists\ q \in \operatorname{Ass}(M/N)$ and say $q = \operatorname{ann}(y+N)$ i.e. $R\overline{y} = (Ry+N)/N \simeq R/q \rightsquigarrow N \subsetneq Ry+N \in \mathcal{S}(\rightarrow\leftarrow)$ ☐

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

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

is a R-module homomorphism.

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

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

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

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

Proof: $(\Rightarrow)$: If $a \in P \rightsquigarrow a_M$ is locally nilpotent. If $a \notin P \rightsquigarrow a_M$ is injective.

$$(\Leftarrow) : R = \left(R \setminus \bigcup_{p\in \mathrm{Ass}(M)} p\right) \bigcup \left(\bigcap_{p\in \mathrm{Ass}(M)} p\right) \rightsquigarrow |\mathrm{Ass}(M)| = 1$$ ☐

Definition 1.10.3.

- An ideal q of R is **primary** if $q \subsetneq R$ and
$$xy \in q, x \notin q \implies y^n \in q \text{ for some } n > 0$$
($\iff R/q \neq 0$ and the zero divisors in R/q 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 $\mathrm{Ass}(M/N) = \{p\}$

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

Proof:

- If $xy \in \sqrt{q}, x \notin \sqrt{q} \implies x^n y^n \in q,\ (x^n)^m \neq q$ 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 $\mathrm{Ass}(R/q) = \{\sqrt{\langle \overline{0} \rangle}\} = \{\sqrt{q}\}$) ☐

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 $M/N_1 \cap N_2 \hookrightarrow M/N_1 \otimes M/N_2$, by Homework 7.,

$$\varnothing \neq \mathrm{Ass}\left(M/N_1 \cap N_2\right) \subset \mathrm{Ass}\left(M/N_1 \otimes M/N_2\right) \subset \mathrm{Ass}\left(M/N_1\right) \cup \mathrm{Ass}\left(M/N_2\right) = \{p\}$$

Hence, $\mathrm{Ass}\left(M/N_1 \cap N_2\right) = \{p\}$. ☐

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 $\mathrm{Ass}(M/N_i) = \{p_i\}$, then $\mathrm{Ass}(M/N) = \{p_1, ..., p_r\}$

Proof:

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

$$0 \neq (N_2 \cap \cdots \cap N_r)/N \simeq (N_1 + N_2 \cap \cdots \cap N_r)/N_1 \subseteq M/N_1$$
$$\implies \mathrm{Ass}\left((N_2 \cap \cdots \cap N_r)\big/N\right) = \mathrm{Ass}\left(M/N_1\right) = \{p_1\}$$

Hence,
$$\{p_1\} = \mathrm{Ass}\left((N_2 \cap \cdots \cap N_r)\big/N\right) \subseteq \mathrm{Ass}(M/N)$$

□

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

- $p \nsubseteq q \implies M_q = N_q$
- $p \subseteq q \implies \rho^{-1}(N_q) = N$ (sometimes we will denote $\rho^{-1}(N_q) = M \cap N_q$)

Proof:

- $M_q/N_q \simeq (M/N)_q$ and thus $\mathrm{Ass}(M_q/N_q) = \mathrm{Ass}(M/N) \cap \{q \supseteq P \in \mathrm{Spec}\, R\} = \varnothing$. Hence, $M_q = N_q$.
- $\because$ $\mathrm{Ass}(M/N) = \{p\}$ 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.

$$\begin{tikzcd} M \arrow[r, "\rho"'] \arrow[rr, bend left, "\varphi"] & M_q \arrow[r, "f"'] & M_q/N_q \end{tikzcd} \quad \text{with}$$

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

  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 $\mathrm{Ass}(M/N_i) = \{p_i\}$. If p_1 is minimal in $\{p_1, ..., p_r\} = \mathrm{Ass}(M/N)$, 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. $\forall p \in \mathrm{Ass}(M)$, $\exists\ N(p) \subset M$ with $\mathrm{Ass}(M/N(p)) = \{p\}$ s.t.

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

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

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

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

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

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

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

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

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

$\square$

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

Proof: We have $|\mathrm{Ass}(M/N)| < \infty$, say $\mathrm{Ass}(M/N) = \{p_1, ..., p_r\}$ and $p_i \longleftrightarrow N(p_i) = N_i/N$, then $\langle \overline{0} \rangle = \bigcap\limits_{i=1}^{r} N_i/N \implies N = \bigcap\limits_{i=1}^{r} N_i$

$$\mathrm{Ass}\left({}^{M}\!/\!{}_{N_i}\right) = \mathrm{Ass}\left({}^{M/N}\!\Big/\!{}_{N_i/N}\right) = \{p_i\} \rightsquigarrow N_i : p_i\text{-primary}$$

$\square$

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 $\{p_1, ..., p_r\}$ 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 $p_1 = \langle x\rangle \in \operatorname{Spec} R, p_2 = \langle x, y\rangle \in \operatorname{Max} R$, 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 $\operatorname{Spec}(R/q) = \{m/q\}$ and $\mathfrak{N}_{R/q} = m/q$. So $R/q \backslash m/q = \{\text{units}\} \implies$ all zero divisors are nilpotent. $\square$

Remark 1.10.2.

- A prime-power is not necessarily primary :

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

- A max-power is primary : Say $q = m^n$, $m \supseteq \bigcap\limits_{m^n \subseteq p} p = \sqrt{m^n} \supseteq m \implies m = \sqrt{m^n} = \sqrt{q}$. 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. $\operatorname{Ass}(M) = \{p\} \implies \operatorname{Ann}(M)$ is p-primary

Proof: $\forall a \in R$, a_M is injective ($\leftrightarrow a \notin p$) or nilpotent ($\leftrightarrow a \in p$). So $\operatorname{Ann}(M) \subseteq p$. If $ab \in \operatorname{Ann}(M) \subseteq p$. If $a \in p \rightsquigarrow a^n M = 0 \rightsquigarrow a^n \in \operatorname{Ann}(M)$. If $a \notin p \rightsquigarrow b \in p$ and by symmetric, $a^n \in \operatorname{Ann}(M)$. Hence, $\operatorname{Ann}(M)$ 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 $J_R := \bigcap\limits_{m \in \operatorname{Max} R} m$

Property 1.11.1.

- $I \subsetneq R \implies \langle I, J_R\rangle \subsetneq R$:

  $pf.$ $\exists m \in \max R$ 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 $M = \langle x_1, ..., x_n\rangle$, where n is the smallest integer s.t. M is generated by n elements. And $x_n \in M = IM$, say $x_n = a_1x_1 + \cdots + a_nx_n$ with $a_i \in I$, then $(1 - a_n)x_n = a_1x_1 + \cdots + a_{n-1}x_{n-1}$. Since $1 - a_n$ is unit, $x_n \in \langle x_1, ..., x_{n-1}\rangle \implies M = \langle x_1, ..., x_{n-1}\rangle$ ($\rightarrow\leftarrow$) $\square$

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 $M/mM = \langle \overline{x}_1, ..., \overline{x}_n\rangle_{R/m}$, where $\{\overline{x}_1, ..., \overline{x}_n\}$ is a basis, then $M = \langle x_1, ..., x_n\rangle_R$

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

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

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

  pf. $N/mN = \operatorname{Im}\overline{f} = (f(M) + mN)/mN \implies N = mN + f(M) \rightsquigarrow N = f(M)$ i.e. f is onto.

- Assume M, N : free, then $\overline{f}$ is $1-1 \implies f$ is $1-1$:

  pf. Let $M = \langle v_1, ..., v_\ell\rangle_R$ with $\{v_1, ..., x_\ell\}$ is a basis and $w_i = f(v_i)\ \forall i$

  By Corollary 1.11.2 and commutative ring has IBN, $M/mM = \langle \overline{v}_1, ..., \overline{v}_\ell\rangle_{M/mM}$ and $\operatorname{Im}\overline{f} = \langle \overline{w}_1, ..., \overline{w}_\ell\rangle_{N/mN} \subseteq N/mN$. Since $\overline{f}$ is $1-1$, $\dim \operatorname{Im}\overline{f} = \ell \rightsquigarrow \{\overline{w}_1, ..., \overline{w}_\ell\}$ is a basis for $\operatorname{Im}\overline{f}$.

  We can extend $\{\overline{w}_1, ..., \overline{w}_\ell\}$ to a basis $\{\overline{w}_1, ..., \overline{w}_\ell, \overline{w}_{\ell+1}, ..., \overline{w}_k\}$ for N/mN. By Corollary 1.11.2, $\{w_1, ..., w_k\}$ is a free basis for N.

  Now $\forall x \in M, \exists! a_i$ s.t. $x = \sum\limits_{i=1}^{\ell} a_iv_i$. If $x \in \ker f$ i.e. $0 = f(x) = \sum\limits_{i=1}^{\ell} a_iw_i$. So $a_i = 0\ \forall i$. Hence, f is $1-1$.

- Assume M, N : free. Then $\overline{f}$ 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 a 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. $\{M_i\}, \{M_i'\}$: stable I-filtration of $M \implies \exists d \in \mathbb{N}$ 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 : Noetherian $\iff R_0$: Noetherian and $R = R_0[a_1, ..., a_n]$ with $a_i \in R$

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

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

Claim: $R_k \subseteq R_0[a_1, ..., a_n]\ \forall\ k \geq 0$ and thus $R = R_0[a_0, ..., a_n]$
pf. By induction on k : $k = 0 \rightsquigarrow R_0 \subseteq R_0[a_1, ..., a_n]$.

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 $r_i \in R_{k-d_i} \subseteq R_0[a_0, ..., a_n]$ (by induction hypothesis). Hence, $x \in R_0[a_0, ..., a_n]$ □

Theorem 1.11.2 (General form of Artin-Rees lemma)**.** R : Noetherian, $I \subseteq R$, M : f.g. R-module with a stable I-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.

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

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

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

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

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

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

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 $U_m = \langle f_1, ..., f_p \rangle_R$) and thus L_m is f.g. S-module since $L_m = \langle f_1, ..., f_p \rangle_S$. Also, $L_m \subseteq L_{m+1} \subseteq \cdots$ and $\bigcup_{m=0}^{\infty} L_m = \widetilde{M}$. Since S is Noetherian, there exists N s.t. $L_N = L_{N+1} = L_{N+2} = \cdots$ and thus $\widetilde{M}$ is Noetherian and thus f.g. S-module. In fact, we have

$$\begin{aligned} \widetilde{M} \text{ is f.g. } S\text{-module} &\iff \widetilde{M} = L_{N_0} \text{for some } N_0 \in \mathbb{N} \\ &\iff I^m M_{N_0} = M_{m+M_0} \quad \forall m \geq 0 \\ &\iff \{M_i\} \text{is } I\text{-stable} \end{aligned}$$

$\because \widetilde{N} := \bigoplus_{n=0}^{\infty} N_n t^n$ 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. $I^m N_{N_0} = N_{N_0+m}$ $\square$

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

$$I^2 M \cap N = \langle x^2 \rangle \cap \langle x \rangle = \langle x^2 \rangle, \; I^2(M \cap N) = \langle x^2 \rangle \langle x \rangle = \langle x^3 \rangle$$

$$I^n (M^2 \cap N) = \langle x^n \rangle \langle x^2 \rangle = \langle x^{n+2} \rangle, I^{n+2} M \cap N = \langle x^{n+2} \rangle \cap \langle x \rangle = \langle x^{n+2} \rangle$$

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 $N \cap I^n M = N \; \forall n \geq 0$

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

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

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

1.12 Hilbert polynomial

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

Definition 1.12.1.

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

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

  For given $\varphi : \mathfrak{M}_{R_0}^{<\infty} \to \mathbb{Z}$ 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 $\exists c_0, c_1, ..., c_r \in \mathbb{Z}$ s.t.

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

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

Property 1.12.2. If $f : \mathbb{Z} \to \mathbb{Z}$ 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 $\widetilde{p}(z) = \sum_{k=0}^{r} c_{r-k}\binom{z}{k+1}$. Then $\widetilde{p}(z+1) - \widetilde{p}(z) = Q(z) \rightsquigarrow \widetilde{p}(n+1) - f(n+1) = \widetilde{p}(n) - \widetilde{f}(n)\ \forall n \gg 0 \rightsquigarrow \widetilde{p}(n) - f(n)$ is a constant $c_{r+1} \in \mathbb{Z}\ \forall n \gg 0$. Then $f(n) = \widetilde{p}(n) - c_{r+1}$ is numerical polynomial. $\square$

Theorem 1.12.1 (Hilbert-Serre)**.**

(1) $P_\varphi(M,t) = \dfrac{f(t)}{\prod_{i=1}^{n}(1-t^{d_i})}$ for some $f(t) \in \mathbb{Z}[t]$

(2) If $d_i = 1\ \forall i = 1 \sim n$, $P_\varphi(M,t) = \dfrac{h(t)}{(1-t)^d}$ for $(1-t) \not| h(t)$, 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 $n : n = 0 \rightsquigarrow R = R_0 \rightsquigarrow M$: f.g. R_0-module $\rightsquigarrow M_n = 0\ \forall n \gg 0$. Then $P_\varphi(M,t) \in \mathbb{Z}[t]$ OK!

Now, let $n > 0$. Consider

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

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

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

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

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

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

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

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

(2) By (1), write $P_\varphi(M,t) = h(t)/(1-t)^d$ with $(1-t) \nmid h(t)$, $h(t) = \sum\limits_{i=0}^{N} a_i t^i$, $a_i \in \mathbb{Z}$. 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
$$\varphi(M_n) = \sum_{i=0}^{N} a_i \binom{d+n-i-1}{d-1} = \left(\sum_{i=0}^{N} a_i\right) t^{d-1} + \cdots$$
and $\sum\limits_{i=0}^{N} a_i = h(1) \neq 0 \rightsquigarrow$ it is a polynomial with degree $d-1$

$\square$

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

(1) $\dim_k \left(M \big/ m^\ell M\right) < \infty$

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

Proof:

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

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

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

For $\ell > 1$,
$$0 \to m^{\ell-1}M \big/ m^\ell M \to M \big/ m^\ell M \to M \big/ m^{\ell-1} M \to 0$$
$$\begin{aligned} \implies \dim_k \left(M \big/ m^\ell M\right) &= \dim_k \left(m^{\ell-1}M \big/ m^\ell M\right) + \dim_k \left(M \big/ m^{\ell-1} M\right) \\ &= \sum_{r=1}^{\ell} \dim_k \left(m^{r-1}M \big/ m^r M\right) \end{aligned}$$

(2) Let $\langle a_1, \ldots, a_d \rangle_R = m$. Then $\mathrm{gr}_m(R) = R/m[\overline{a}_1, \ldots, \overline{a}_d]$, where $\overline{a}_i \in m/m^2$. By Hilbert-Serre, $\exists!$ $p(z) \in \mathbb{Q}[z]$ of deg $\leq d-1$ s.t.
$$p(n) = \dim_k \left(m^n M \big/ m^{n+1} M\right) \ \forall n \gg 0$$
Thus, $\dim_k \left(M \big/ m^{n+1} M\right) - \dim_k \left(M \big/ m^n M\right) = \dim_k \left(m^n N \big/ m^{n+1} M\right) = p(n)$ $\forall n \gg 0$. By Property 1.12.2, $\exists g(z) \in \mathbb{Q}[z]$ with deg $\leq d$ s.t.
$$g(n) = \dim_k \left(M \big/ m^n M\right) \ \forall n \gg 0$$

□

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 expect 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 Schreir refinement theorem)

Proposition 1.12.1. TFAE

(1) M has a composition series

(2) M us 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 $\widetilde{C}$: a refinement of C s.t. $\widetilde{C}$ is a composition series $\rightsquigarrow \ell(\widetilde{C}) = n = \ell(C) \rightsquigarrow C = \widetilde{C}$, 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. $M = M_0 \subsetneq M_1 \subsetneq \cdots$. Since M is Artinian, $\exists n$ s.t. $M_n = 0$ □

1.13 Indecomposable module

In this section, we want 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 $f \in \mathrm{End}_A(M)$, then

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

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

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

Lemma 1.13.1 (Fitting lemma)**.**

(1) $M = \operatorname{Im} f^\infty \oplus \ker f^\infty$

(2) $f|_{\operatorname{Im} f^\infty}$ is an automorphism

(3) $f|_{\ker f^\infty}$ is nilpotent

Proof:

(1) • If $x \in \operatorname{Im} f^\infty \cap \ker f^\infty = \{0\}$, say $f^n(z) = x$ and $0 = f^n(x) = f^{2n}(z)$
$\implies z \in \ker f^{2n} = \ker f^n \rightsquigarrow x = 0$

• $\forall x \in M$, $f^n(x) \in \operatorname{Im} f^n = \operatorname{Im} f^{2n} \implies f^n(x) = f^n(y)$ for some $y \in \operatorname{Im} f^n$
$\implies x - y \in \ker f^n \rightsquigarrow x \in \ker f^n + \operatorname{Im} f^n = \ker f^\infty + \operatorname{Im} f^\infty$

(2) $f|_{\operatorname{Im} f^\infty} : \operatorname{Im} f^\infty \to \operatorname{Im} f^\infty$ is surjective. If $f^n(x) \in \ker f|_{\operatorname{Im} f^\infty}$, then $f^{n+1}(x) = 0 \rightsquigarrow x \in \ker f^{n+1} = \ker f^n \rightsquigarrow f^n(x) = 0$

(3) $f|_{\ker f^\infty} : \ker f^\infty \to \ker f^\infty$, $f^n(x) = 0\ \forall x \in \ker f^\infty \rightsquigarrow f^n = 0$

□

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) $\forall f \in \operatorname{End}(M)$, f is either an auto. or a nilpotent.

(2) $\operatorname{End}(M)$ 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 M_1, M_2 is 0. The former is auto, the latter is nilpotent.

(2) Let $I = \operatorname{End}(M) \setminus \{\text{unit}\}$. For $f \in I$, f is nilpotent i.e. $M = \ker f^\infty$.

• $\forall g \in \operatorname{End}(M)$. Notice that $\operatorname{Im} f^n = 0 \iff \ker f^n = M$.

•• If $\ker f = M \rightsquigarrow (gf)(x) = 0\ \forall x \in M \rightsquigarrow gf$ is not $1-1 \rightsquigarrow gf \in I$
If $\ker f^{n-1} \subsetneq \ker f^n = M \rightsquigarrow \operatorname{Im} f^{n-1} \neq 0 \exists f^{n-1}(x) \neq 0$, then $gf(f^{n-1}(x)) = 0 \rightsquigarrow gf \in I$

•• $fg(M) \subseteq f(M) \neq M$, otherwise $f(M) = M \rightsquigarrow \operatorname{Im} f = M$. By Fitting lemma, $\ker f^\infty = 0 \implies f$ is an anto. $(\to\leftarrow)$. 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 $h_2^{-1} = 1 + h_1 + h_1^2 + \cdots + h_1^{r-1}$ (if $h_1^r = 0$)$\rightsquigarrow h_2 \notin I$ $(\to\leftarrow)$

□

Property 1.13.2. Let M, N be A-modules and N indecomposable. If $f : M \to N$ and $g : N \to M$ 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 $1 = e + (1-e) \implies N = \operatorname{Im} e \oplus \operatorname{Im}(1-e)$ $(\rightarrow\leftarrow)$. 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! $\cdots$

  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 $M_1' = M_2 \oplus M_2'$. $\cdots$.

  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 $e_i : M \to M_i$, $p_j : M \to N_j$. 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

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

  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 $g_1|_{M_1} : M_1 \to N_1, f_1|_{N_1} : N_1 \to M_1$ 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: $M = N_1 \oplus (M_2 \oplus \cdots M_r)$

  $pf.$ $\ker e_1 = M_2 \oplus \cdots \oplus M_r$ 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 $M_i \simeq N_i$ $\forall i = 2, ..., r$ 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 $\operatorname{Max} R = \operatorname{Spec} R$

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

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

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

(4) If R is Artinian and $\operatorname{Max} R = \{m_1, ..., m_\ell\}$, then $\exists n_1, ..., n_\ell \in \mathbb{N}$ 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 $\mathcal{S} = \{J \subseteq R | Jm_1^{n_1} \cdots m_\ell^{n_\ell}\} \neq \varnothing$ 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, $xm_1^{n_1} \cdots m_\ell^{n_\ell} = xm_1^{n_1+1} \cdots m_\ell^{n_\ell+1} \implies xm_1 \cdots \langle x\rangle \supseteq m_\ell \in$ $\mathcal{S} \rightsquigarrow xm_1 \cdots m_\ell = \langle x\rangle \rightsquigarrow (m_1 \cdots m_\ell)_{\subseteq J_R}(Rx) = Rx$. By Nakayama's lemma, $Rx = 0 \rightsquigarrow x = 0$ $(\rightarrow\leftarrow)$.

(5) R : Artinian, then

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

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

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

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

Chapter 2

Homework

2.1

Problem 2.1.1. Let A be a ring and M be a left A-module.

(a) For any left ideal I of A, define

$$IM = \left\{ \sum_{\text{finite}} a_i x_i \,\middle|\, a_i \in I, x_i \in M \right\}$$

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 2.1.2. 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 2.1.3.

(a) Show that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/\gcd(m,n)\mathbb{Z}$

(b) Let A be a commutative ring and M be an A-module. Show that $\operatorname{Hom}_A(A, M) \simeq M$ as left A-modules.

(c) Let A be a commutative ring. Show that $\operatorname{Hom}_A(A, A) \simeq A$ as a ring.

2.2

Problem 2.2.1. Construct a ring A such that for all $m, n \in \mathbb{N}$, $A^n \simeq A^m$

Problem 2.2.2. If A is a division ring, then A has IBN.

Problem 2.2.3. 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 $f : B \to A$ is a ring epimorphism and A is a division ring, then B has IBN.

Problem 2.2.4. Let $\{M_i\}$ be a directed family of modules over a ring. For any module N show that

$$\varprojlim \mathrm{Hom}(H, M_i) = \mathrm{Hom}(N, \varprojlim M_i)$$

2.3

Problem 2.3.1. Let G be an abelian group and

$$\begin{aligned} G = \langle x, y, z, u, v |\ & x - 7y + 14z - 21u = 5x - 7y - 2z + 10u - 15v \\ =& 3x - 3y - 2z + 6u - 9v = x - y + 2z - 3v = 0\rangle \end{aligned}$$

Please write G as a direct sum of cyclic groups.

Problem 2.3.2. 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 2.3.3. 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 $v_1, ..., v_m$ be a maximal set of such elements, and let A_0 be the subgroup of A contained in the R-space generated by $v_1, ..., v_{m-1}$. By induction, one may assume that any element of A_0 is a linear integral combination of $v_1, ..., v_{m-1}$. Let S be the subset of elements $v \in A$ of the form $v = a_1 v_1 + \cdots + a_m v_m$ with real cofficients a_i satisfying

$$\begin{cases} 0 \leq a_i < 1 & \text{if } i = 1, ..., m-1 \\ 0 \leq a_m \leq 1 \end{cases}$$

If v'_m is an element of S with the smallest $a_m \neq 0$, show that $\{v_1, ..., v_{m-1}, v'_m\}$ 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 2.3.4. Let M be a finitely generated abelian group. By a **seminorm** on M we mean a real-value function $v \to |v|$ 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 means 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 $v_1, ..., v_r \in M$ be linearly independent over $\mathbb{Z}$ mod M_0. Prove that there exists a basis $\{w_1, .., w_r\}$ 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 $M_1 = \langle v_1, ..., v_r \rangle$. 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 $n_{j,1}, ..., n_{j,j-1}$ satisfying

$$n_{j,1}v_1 + \cdots + n_{j,j}v_j = dw_j \text{ for some } w_j \in M$$

Without loss of generality we may assume $0 \leq n_{j,k} \leq d-1$. Then the elements $w_1, ..., w_r$ form the disired basis.)

2.4

Problem 2.4.1.

(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 2.4.2. 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 $\operatorname{ann}(z_i) = \langle d_i \rangle \neq R$ and $d_i | d_{i+1}$ for all $i = 1, ..., r-1$, then the ring $(\operatorname{Hom}_R(M, M), +, \circ)$ is isomorphism 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 $\operatorname{diag}\{d_1, ..., d_r\}C = B \operatorname{diag}\{d_1, ..., d_r\}$ and I is the ideal of matrices of the form $\operatorname{diag}\{d_1, ..., d_r\}Q, Q \in M_{r\times r}(R)$.

Problem 2.4.3. Let $A \in M_{n\times n}(k)$ with k being a field. Assume that $d_1(x), ..., d_r(x)$ are the non-unit monic invariant factors of $(xI_n - A)$ with $\deg d_i(x) = n_i > 0$. Show that

$$\dim_k\{B \in M_{n\times n}(k) : BA = AB\} = \sum_{j=1}^{r} (2r - 2j + 1)n_j$$

2.5

Problem 2.5.1.

(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 2.5.2. 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 2.5.3. 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 2.5.4. Let R be a commutative ring.

(a) Let F be a free R-module of rank n. Show that

$$S(F) \simeq R[x_1, ..., x_n]$$

(b) Let $F = F_1 \oplus F_2$ be a direct sum on finite free R-modules. Show that

$$S^n(F) \simeq \bigoplus_{p+q=n} S^p(F_1) \otimes S^q(F_2)$$

2.6

Problem 2.6.1. 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 2.6.2. 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 2.6.3 (Prime avoidance lemma)**.** Let R be a commutative ring. Show that

(a) If $P_1, ..., P_n \in \operatorname{Spec} R$ 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 $I_1, ..., I_n$ are ideals of R and $P \in \operatorname{Spec} R$ containing $\bigcap_{i=1}^{n} I_i$, then there exists an I_k such that $P \supseteq I_k$.

Problem 2.6.4. 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, $\sqrt{I + J} = \sqrt{\left(\sqrt{I} + \sqrt{J}\right)}$

(d) $\sqrt{I} = \bigcap_{I \subseteq P \in \operatorname{Spec} R} P$

2.7

Problem 2.7.1. Show that of A is a (left) Noetherian ring, then the formal power series ring $A[[x]]$ is (left) Noetherian.

Problem 2.7.2. Let R be a commutative Noetherain 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

$$\operatorname{Ass}_R(M_S) = \operatorname{Ass}_R(M) \cap \{P \in \operatorname{Spec} R : P \cap S = \varnothing\}$$

Problem 2.7.3. Let R be a commutative ring. Show that if $0 \to M_1 \to M_2 \to M_3 \to 0$ is an exact sequence of R-modules, then

$$\operatorname{Ass}(M_1) \subset \operatorname{Ass}(M_2) \subset \operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_3)$$

Problem 2.7.4. Let R be a commutative Noetherian ring and M be a finitely generated R-module. Show that $\operatorname{Ass}(M)$ is a finite set.

2.8

Problem 2.8.1. 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 2.8.2.

(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 2.8.3. 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 2.8.4.

(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 $\mathfrak{q}_1, ..., \mathfrak{q}_i$ 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 $S^{-1}\mathfrak{a}$.

2.9

Problem 2.9.1. Let R be a commutative ring and I be an ideal of R.

(a) Show that $\operatorname{gr}_I(R) := \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$ has a graded ring structure.

(b) Show that if M is an R-module, then $\operatorname{gr}_I(M) := \bigoplus_{n=0}^{\infty} I^n M/I^{n+1}M$ has a graded $\operatorname{gr}_I(R)$-module structure.

Problem 2.9.2. Let $\varphi : S_I(R) \to \operatorname{gr}_I(R)$ 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 $S_I(R)/IS_I(R) \simeq \operatorname{gr}_I(R)$.

Problem 2.9.3. Show that $\operatorname{gr}_I(M) \simeq S_I(R)M/IS_I(R)M$
(Here, $S_I(R)M = M \oplus IMt \oplus I^2Mt^2 \oplus \cdots$)

Problem 2.9.4. Show that if R is Noetherian and M is a finitely generated R-module, then $\operatorname{gr}_I(M)$ is a finitely generated $\operatorname{gr}_I(R)$-module.

2.10

Problem 2.10.1. 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 $i = 1, 2, ...$ and

$$\ell(R/Q^n) = \sum_{i=0}^{n-1} \ell(Q^i/Q^{i+1})$$

(3) Show that there exists $\chi_Q^B(t) \in \mathbb{Q}[t]$ 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 2.10.1.

- We call χ_Q^R is the **characteristic polynomial** of R relative to Q.
- $d(R) := \deg \chi_Q^R$.

2.11

Problem 2.11.1. Let A, B be local rings with maximal ideals $\mathfrak{m}_A, \mathfrak{m}_B$, respectively. Let $f : A \to B$ 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) $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ is an isomorphism

(2) $\mathfrak{m}_A \to \mathfrak{m}_B/\mathfrak{m}_B^2$ is surjective

(3) B is a finite A-module, via f.

Prove that f is surjective.

Problem 2.11.2. 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 2.11.3. Let R be a commutative ring. Show that R is Artinian if and only if R is Noetherian and $\operatorname{Spec} R = \operatorname{Max} R$.

Problem 2.11.4. Let $(R, \mathfrak{m})$ be an Artinian local ring. Show that TFAE :

(1) R is a PID

(2) $\mathfrak{m}$ is principal

(3) $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \le 1$