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. $\begin{array}{rccc} g: & A^\circ & \longrightarrow & \mathrm{End}(M) \\ & a & \longmapsto & g(a): z \mapsto xa \end{array}$
  $M_3 : g(a \circ b)(x) = x(ba) = (xb)a = g(a)(xb) = g(a) \circ g(b)(x) \ \forall x \in M$

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 $\mathrm{Im}\,\varphi$ is a submodule of N

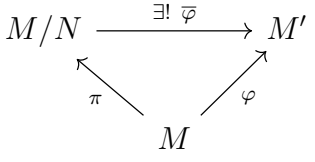
Definition 1.1.4. Let N be a submodule of M. The quotient modules is M/N :

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

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



- 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

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

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

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

$$\sum a_g g + \sum b_g g = \sum (a_g + b_g) g$$

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

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 $(a_1, ..., a_n) = \sum\limits_{i=1}^{n} a_i e_i$ and $\sum\limits_{i=1}^{n} a_i e_i = 0 \iff a_i = 0\ \forall i$

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

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

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

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

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

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

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

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

Define $\varphi : \begin{array}{ccc} A & \longrightarrow & A \times A \\ T & \longmapsto & (T_1, T_2) \end{array}$, 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

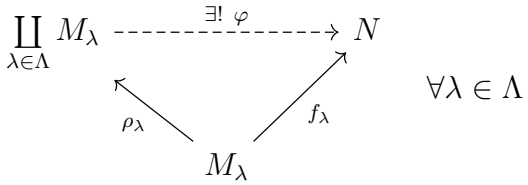
Hence, $A \simeq A^2$

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.



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 :

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

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

$$\begin{array}{ccccc} \rho_\lambda(x_\lambda) \in \coprod_{\lambda\in\Lambda} M_\lambda & \overset{\exists!\ \varphi}{\dashrightarrow} & N \ni f_\lambda(x_\lambda) \\ & \nwarrow^{\rho_\lambda} \quad \nearrow_{f_\lambda} & \\ & x_\lambda \in M_\lambda & \end{array}$$

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

□

Definition 1.2.3 (free module)**.** An A-module F is said to be **free** on a nonempty set S if $\exists$ a mapping $i : S \to F$ 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.

$$\begin{array}{ccc} F & \overset{\exists!\ \varphi}{\dashrightarrow} & M \\ & \nwarrow^{i} \quad \nearrow_{j} & \\ & S & \end{array}$$

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 $f_\lambda : \begin{array}{ccc} M_\lambda & \longrightarrow & M \\ ax_\lambda & \longmapsto & aj(x_\lambda) \end{array}$

By the universal property of direct sum,

$$\begin{array}{ccccc} i(x_\lambda) \in \coprod_{\lambda\in\Lambda} M_\lambda & \overset{\exists!\ \varphi}{\dashrightarrow} & N \ni j(x_\lambda) \\ & \nwarrow^{\rho_\lambda} \quad \nearrow_{f_\lambda} & \\ & M_\lambda & \\ {\scriptstyle i}\ \nwarrow & & \nearrow\ {\scriptstyle j} \\ & x_\lambda \in S & \end{array}$$

Define $i(x_\lambda) = \rho(x_\lambda)$, then $\varphi \circ i = j$ is commute.
(Actually, we can choose $M_\lambda = A$ is also be a possible way.) □

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

Proof: Let $S = \{x_1, ..., x_n\}$. 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 $Q_1 = \begin{pmatrix} Q & O \end{pmatrix}, P_1 = \begin{pmatrix} P \\ O \end{pmatrix} \implies Q_1P_1 = (QP) = I_m$
$\rightsquigarrow 0 = \det Q_1 \det P_1 = \det I_m = 1$ $(\multimap\!\!\!\!\!\times\!\!\!\!\!\multimap)$ □

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

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

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

Proof:

- $|S'| = \infty$: Assume that $|S'| < \infty$, say $S' = \{x'_1, ..., x'_m\} \rightsquigarrow \exists \{x_1, ..., x_n\} \subset S$ 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. $(\multimap\!\!\!\!\!\times\!\!\!\!\!\multimap)$
- $|S| = \infty, |S'| = \infty$. Assume that $|S'| \leq |S|$
  Recall that if $\mathcal{B} = \{T \subseteq S' : |T| < \infty\}$ and $|S'| = \infty$, then $|\mathcal{B}| = |S'|$
  Let $T = \{y'_1, ..., y'_k\} \subseteq S'$ 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, $S_T \subseteq \{y_1, ..., y_n\}$
  - $|S| \leq |S'|$: Let $\mathcal{B} = \{T \subseteq S' : |T| < \infty\}$. Since $|S'| = \infty, |\mathcal{B}| = |S'|$
    Define

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

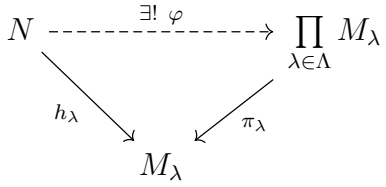
which is well-defined since S' is linearly independent.

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

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

□

Definition 1.2.6 (direct product)**.** Given a family of A-modules $\{M_\lambda : \lambda \in \Lambda\}$, the **direct product** $\prod_{\lambda \in \Lambda} M_\lambda$ is an A-module with projections : $\pi_\lambda : \prod_{\lambda \in \lambda} M_\lambda \to M_\lambda \ \forall \lambda$ 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.



Definition 1.2.7. Define

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

and the operation on it.

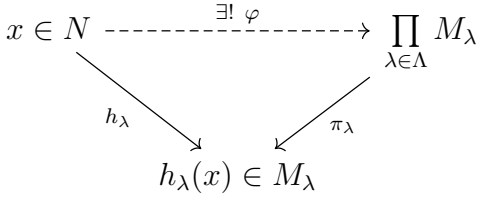
- $(x_\lambda)_{\lambda \in \Lambda} + (y_\lambda)_{\lambda \in \Lambda} = (x_\lambda + y_\lambda)_{\lambda \in \Lambda}$
- $a(x_\lambda)_{\lambda \in \Lambda} = (ax_\lambda)_{\lambda \in \Lambda}$

  So it is a A-module.

- Define the projection π_λ

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

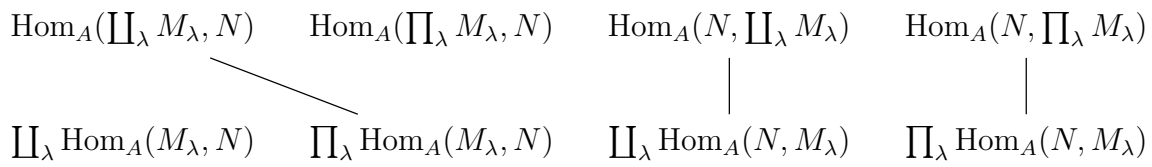
- Given $h_\lambda : N \to M_\lambda$



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.



1.3 Direct limit and inverse limit

1.3.1 Definition

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

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

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

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

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

- $\forall\ i \leq j, \mu_{ij} : M_i \to M_j$ 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 $C := \bigoplus_{i\in I} M_i$ 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

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

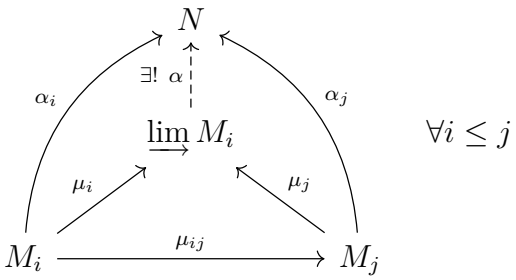
is an A-module. We further consider

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

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.



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 α_k in both side, then

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

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

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

- $\forall\ i \leq j, \pi_{ji} : M_j \to M_i$ 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)**.**

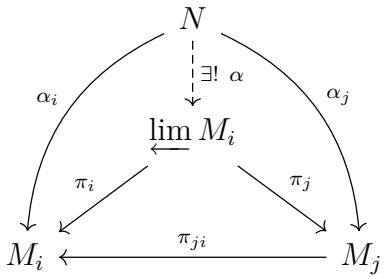
Construction

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

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

Universal property

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



Construction α

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

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

Since $\pi_{ji}(\alpha_j(x)) = \alpha_i(x)\ \forall i \le j \implies (\alpha_i(x))_{i\in I} \in \varprojlim M_i$
And it is clear that $\pi_i \circ \alpha = \alpha_i\ \forall i$

1.3.2 Examples

Ring of p-adic number

Define

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

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 $N(k) \in \mathbb{N}$ s.t. $\forall n \ge N,\ d_p(x_{n+1}, x_n) < p^{-k}$
  Let a_n equal to the k-th term of $x_{N(k)}$, then $(x_n) \to (a_i)_{i\in\mathbb{N}}$. 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 $\begin{matrix} R & \longrightarrow & Ra \\ r & \longmapsto & ra \end{matrix}$, since R is integral domain, $ra = 0 \iff r = 0$. Hence, $Ra \simeq R$.

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

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

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

- Case1. : $\operatorname{Im} \overline{P} = \{0\} \rightsquigarrow N \subseteq \ker P \simeq R^{n-1}$, 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

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

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

□

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

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

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

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 $B_{ij}(a)^{-1} = B_{ij}(-a)$
- $D_i(a) = I_n - e_{ii} + ae_{ii}$ $(a \neq 0)$

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 $\begin{pmatrix} b_{22} & \\ & c_{ij} \end{pmatrix}$ with $b_{22}|c_{33}$.

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

□

Remark 1.4.1. $d_1, d_2, ..., d_r$ 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 of k-th order minors of PA is linear combination of some k-th order minor of A. Hence, $\Delta_k(A)|\Delta_k(PA)$. Similarly, $\Delta_k(A)|\Delta_k(AP)$. If $PAQ = B$, then $\Delta_k(A)|\Delta_k(B)$. In other hand, $P^{-1}BQ^{-1} = A$, then $\Delta_k(B)|\Delta_k(A)$, which means $\Delta_k(A) \simeq \Delta_k(B) = d_1 d_2 \cdots d_k$. Hence, $d_k \simeq A_k(A)/A_{k-1}(A)$ □

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

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

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

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

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

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

$r \in \ker \varphi \iff rw_i = r'd_iw_i \iff r = r'd_i$, thus $\ker \varphi = \langle d_i \rangle$ and $Rw_i/Rd_iw_i \simeq R/\langle d_i \rangle$. 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

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

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

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

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

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

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

where a_i are non-zero 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 $\ell \le k$. By symmetric, $k \le \ell \implies k = \ell$.
  - 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 $a = u p_1^{\alpha_1} \cdots p_\mu^{\alpha_\mu}$, $b_1 = v p_1^{\beta_1} \cdots p_\mu^{\beta_\mu}$. 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 $p \nmid q_1, p | h_1$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\leftarrow)$
    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, $a_i/a_1 \sim b_1/b_1\ \forall i = 2, ..., \ell \implies a_i \simeq b_i$

□

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 $0 \le \alpha_{ik} \le \alpha_{jk}\ \forall i < j$. 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 $k = \dim Z$, 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 $[T]^{\{v_i\}}_{\{v_i\}} = (c_{ij}) \implies T(v_i) = \sum_{j=1}^{n} c_{ji}v_j$ 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. $S := \left\{ f_i := xe_i - \sum_{j=1}^{n} c_{ji}e_j \,\middle|\, i = 1, ..., n \right\}$ forms a basis for $\ker\varphi$ over $k[x]$

Proof:

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

□

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

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

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

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

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

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

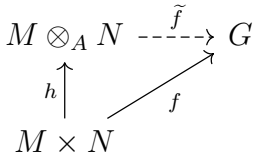
Let $\lambda = \lambda_i, \alpha = \alpha_{ji}, W \simeq k[x]\Big/\langle (x-\lambda)^{\alpha}\rangle$, let $W = k[x]w$ with $\operatorname{ann}(w) = \langle (x-\lambda)^{\alpha}\rangle$. Then $\beta = \{w, (x-\lambda)w, ..., (x-\lambda)^{\alpha-1}w\}$ forms a basis for W over k. Then

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

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



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

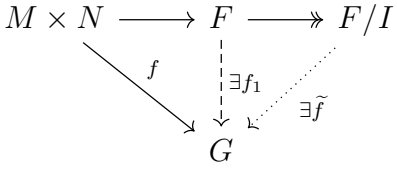
Proof:

- 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

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

  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 :



  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 $\widetilde{f}: F/I\to G$

□

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!
  $(a_1a_2)x\otimes y = a_1(a_2x)\otimes y = a_2x\otimes a_1y = x\otimes a_2a_1y$. 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
  $(a_1a_2)(x\otimes y) = a_1(a_2(x\otimes y)) = a_1(xa_2\otimes y) = xa_2\otimes a_1y = x\otimes a_2a_1y$

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.

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

□

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:

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

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

Conversely,

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

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

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 $x-x'=\sum a_in_i$, then

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

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

Hence, $A/I\otimes_A N\simeq IN/N$. □

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

1.7 Symmetric algebra

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

$T^i(M) := \underbrace{M \otimes \cdots \otimes M}_{i \text{ times}}$ 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 :

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

  Also,

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

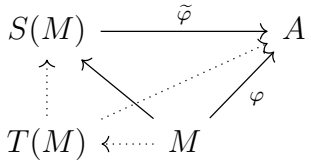
  $\Longrightarrow$ The ring $T(M)$ is called the **tensor algebra** of M and the ring $R = \bigoplus_{k=1}^{\infty} M_i$ satisfy $M_i M_J \subseteq M_{i+j}$ is called **graded ring**.

Definition 1.7.1.

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

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

- $C^k(M) = \langle x_1 \otimes \cdots \otimes x_k - x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(k)} : \forall x_i \in M, \sigma \in S_n \rangle$
  $eg.\ x_1 \otimes x_2 \otimes x_3 - x_3 \otimes x_2 \otimes x_1 = x_1 \otimes (x_2 \otimes x_3 - x_3 \otimes x_2) + (x_1 \otimes x_3 - x_3 \otimes x_1) \otimes x_2$
  $\rightsquigarrow S^k(M) = \langle \overline{x_1} \otimes \cdots \overline{x_k} : x_i \in M \rangle$
- 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.



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

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

□

Property 1.8.2. $R_s \otimes_R M = M_s$

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

Well-defined :

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

$$\Longrightarrow \quad \widetilde{f} : \begin{array}{ccc} R_s \otimes M & \longrightarrow & M_s \\ \frac{a}{t} \otimes x & \longmapsto & \frac{ax}{t} \end{array}$$

- $\widetilde{f}$ 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 $z = \sum_{i=1}^{n} \frac{a_i}{t_i} \otimes x_i \in R_s \otimes M$. 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 $\frac{1}{t} \otimes x \in \ker \widetilde{f} \rightsquigarrow \frac{x}{t} = 0 \rightsquigarrow \exists u \in S,\ ux = 0 \rightsquigarrow \frac{1}{t} \otimes x = \frac{1}{ut} \otimes ux = 0$

□

1.8.2 Localization of prime ideal and maximal ideal

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

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

(1) $M = 0$ (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 $u \in \operatorname{ann}(x) \subseteq m_0$ ($\rightarrow\!\!\!\leftarrow$) □

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 $R = \bigcap_{m\in \operatorname{Max} R} R_m$

Proof: Let $R' = \bigcap_{m\in \operatorname{Max} R} R_m \rightsquigarrow R \subset R' \subset R_m \implies R_m \subseteq R'_m \subseteq (R_m)_m = R_m$. 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)φ is $1-1$ (2)φ_p is $1-1$ $\forall p \in \operatorname{Spec} R$ (3)φ_m is $1-1$ $\forall m \in \operatorname{Max} R$
- TFAE : (1)φ is onto (2)φ_p is onto $\forall p \in \operatorname{Spec} R$ (3)φ_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 $\implies Q = R_S$ (→←)

  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 $\operatorname{Ann}_R(M) = \{a \in R : ax = 0\ \forall x \in M\} \rightsquigarrow M$ 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! $(\subseteq) : \forall a \in \operatorname{Ann}_R(R/I) \rightsquigarrow a(1+I) = I \rightsquigarrow a \in I$ □
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

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

□

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

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

□

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

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

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 $I = \bigcup_{i \in \Lambda} I_i$ 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. $\begin{cases} x^m \in P + \langle a \rangle \\ x^n \in P + \langle b \rangle \end{cases} \implies$
$x^{m+n} \in P + \langle ab \rangle \implies P + \langle ab \rangle \notin S \implies ab \notin P$. □
In particular, $x \notin P \in S$ □

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 $(\rightarrow\!\!\!\!\!\times\!\!\!\!\!\leftarrow)$
- (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. $(\rightarrow\!\!\!\!\!\times\!\!\!\!\!\leftarrow)$. That is $N = N' \in \mathcal{S}$ is f.g..
- (3) $\Rightarrow$ (1) : $M_1 \subseteq M_2 \subseteq \cdots$ in M. Let $N = \bigcup_{i=1}^{\infty} M_i$ which is a submodule of M, say $N = \langle x_1, ..., x_k \rangle_R$ and $x_i \in M_{n_i}$. Let $n = \max_{1 \leq i \leq k} n_i \rightsquigarrow N \subseteq M_n \subseteq N \implies N = M_n$ 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 $\mathbb{Z}, \mathbb{Z}[x], \mathbb{Z}[x, y], ..., k[x_1, ..., x_n]$ 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 $f_3, f_4, ...$ 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. $\langle a_1, ..., a_m\rangle = \langle a_1, ..., a_{m+1}\rangle$, then $a_{m+1} = \sum_{i=1}^{m} r_i a_i$ and

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

□

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

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

Proof:
$(\Rightarrow)$:

- $L_1 \subset L_2 \subset \cdots$ 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 $y \in M_r$
$\implies (x-y) \in \ker g = \operatorname{Im} f \in f(L) \implies x - y \in f(L)\cap M_{r+1} = f(L)\cap M_r \rightsquigarrow$
$x \in M_r$ □

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

Proof: By induction on r. $r = 1$ OK! $r = 2$: Since $0 \to M_1 \to M_1 \oplus M_2 \to M_2$ 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. □

Corollary 1.9.2. A :Noetherian and $M = \langle x_1, ..., x_n\rangle_A$ 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. □

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

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

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

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

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

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

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

Definition 1.9.4 (nilpotent)**.**

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

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)**.**

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

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

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

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

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

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

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

Claim: $P \in \mathrm{Spec}\, R$

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, $\mathrm{ann}(x) \subseteq P \rightsquigarrow M_P \neq 0 \rightsquigarrow P \in \mathrm{Supp}(M)$ 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 $n \implies a^n = 0$
- $\mathrm{Supp}(M) = \mathrm{Spec}\, R$, 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 $\bigcap\limits_{P \in \mathrm{Supp}(M)} P = \bigcap\limits_{P \in \mathrm{Ass}(M)} P$

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

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

pf. $\forall\ p \in \mathrm{Supp}(M),\ \exists 0 \neq x \in M$ 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, $\exists q_p \in \mathrm{Ass}((Rx)_p)$ i.e. $q_p = \mathrm{ann}(\frac{rx}{t})$

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

Conversely, if $a \in \mathrm{ann}(urx) \rightsquigarrow \frac{au}{1} \in q_p$, 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 $\implies \exists M = M_1 \supseteq M_2 \supseteq \cdots \supseteq M_r = 0$ s.t. $M_i/M_{i+1} \simeq R/p_i$ for some $p_i \in \mathrm{Spec}\, R$

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

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

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

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:

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

$$0 \neq (N_2 \cap \cdots \cap N_r)/N \simeq (N_1 + N_2 \cap \cdots \cap N_r)/N_1 \subseteq M/N_1$$

$$\implies \mathrm{Ass}\left((N_2 \cap \cdots \cap N_r)/N\right) = \mathrm{Ass}\left(M/N_1\right) = \{p_1\}$$

Hence,

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

□

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

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

Proof:

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

$$M \xrightarrow[\rho]{} M_q \xrightarrow[f]{} M_q/N_q \quad \text{with} \quad M \xrightarrow{\ \varphi\ } M_q/N_q$$

  $m \in \ker\varphi \iff \frac{m}{1} = \frac{n}{s} \iff usm = un \in N \iff us(m+N) = 0 \iff m + N = 0 \iff m \in N$, 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 $\operatorname{Ass}(M/N_i) = \{p_i\}$. If p_1 is minimal in $\{p_1, ..., p_r\} = \operatorname{Ass}(M/N)$, 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. $\forall p \in \operatorname{Ass}(M)$, $\exists\ N(p) \subset M$ with $\operatorname{Ass}(M/N(p)) = \{p\}$ s.t.

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

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

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

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

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

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

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

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

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

□

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

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

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

□

Corollary 1.10.2. In a Noetherian ring R, $I \subsetneq R \rightsquigarrow I = q_1 \cap \cdots \cap q_r$ 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. □

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 $\overline{x}\overline{y} = \overline{z}^2 \in p^2$, but $\overline{x} \notin p^2, \overline{y}^n \notin p^2\ \forall\ n > 0$

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

1.11 Nakayama's lemma & Artin-Rees lemma

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

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

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, $x_n \in \langle x_1, ..., x_{n-1} \rangle \implies M = \langle x_1, ..., x_{n-1} \rangle$ ($\rightarrow\!\!\leftarrow$) □

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, $M/N = 0 \rightsquigarrow M = N$. □

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, $M = N$. □

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 $\{v_1, ..., v_\ell\}$ is a basis and $w_i = f(v_i)$ $\forall i$

  By Corollary 1.11.2 and commutative ring has IBN, $M/mM = \langle \overline{v}_1, ..., \overline{v}_\ell \rangle_{M/mM}$ 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. $x = \sum_{i=1}^{\ell} a_i v_i$. If $x \in \ker f$ i.e. $0 = f(x) = \sum_{i=1}^{\ell} a_i w_i$. So $a_i = 0$ $\forall i$. Hence, f is $1 - 1$.

- Assume M, N : free. Then $\overline{f}$ 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

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

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

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. □

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. $I^m N_{N_0} = N_{N_0+m}$ □

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, $N = 0$. □

Corollary 1.11.5. (R, m) : Noetherian local, then $\bigcap_{n=0}^{\infty} m^n = 0$
($\forall x \in R, \exists k$ 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 $p(z) = \sum_{k=0}^{r} c_{r-k} \binom{z}{k}$ with $c_i \in \mathbb{Q}$. Note $\binom{z+1}{r} = \binom{z}{r} + \binom{z}{r-1}$ $\rightsquigarrow p(z+1) - p(z) = \sum_{k=0}^{r-1} c_{r-1-k} \binom{z}{k}$ and $\deg(p(z+1) - p(z)) < \deg p(z)$. By induction hypothesis, $c_0, ..., c_{r-1} \in \mathbb{Z}$. $c_r = P(n) - \left(c_0 \binom{n}{r} + \cdots + c_{r-1} \binom{n}{1} \right) \in \mathbb{Z}$ for some $n \gg 1$ □

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. □

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 $(1-t) \not| h(t)$, $h(t) = \sum_{i=0}^{N} a_i t^i$, $a_i \in \mathbb{Z}$. Since

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

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

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

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

□

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

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

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

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

For $\ell > 1$,

$$0 \to m^{\ell-1} M \Big/ m^\ell M \to M \Big/ m^\ell M \to M \Big/ m^{\ell-1} M \to 0$$

$$\begin{aligned} \Longrightarrow \dim_k \left(M \Big/ m^\ell M \right) &= \dim_k \left(m^{\ell-1} M \Big/ m^\ell M \right) + \dim_k \left(M \Big/ m^{\ell-1} M \right) \\ &= \sum_{r=1}^{\ell} \dim_k \left(m^{r-1} M \Big/ m^r M \right) \end{aligned}$$

(2) Let $\langle a_1, ..., a_d \rangle_R = m$. Then $\mathrm{gr}_m(R) = R/m[\overline{a}_1, ..., \overline{a}_d]$, 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 is both Noetherian and **Artinian** (Have DCC)

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

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

We know $\widetilde{C}$: 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. $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$

Similarly, it is also true for Artinian property.

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

1.13 Indecomposable module

In this section, we want 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

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

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

Say $\mathrm{Im}\, f^\infty = \mathrm{Im}\, f^n$ 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 $x \in \operatorname{Im} f^\infty \cap \ker f^\infty$, 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 $\ker f^\infty, \operatorname{Im} f^\infty$ 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. $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$. 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 $h_1^r = 0$) $\rightsquigarrow h_2 \notin I$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$

□

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 $1 = e + (1-e) \implies N = \operatorname{Im} e \oplus \operatorname{Im}(1-e)$ $(\nrightarrow\!\!\!\!\!\leftarrow)$. 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

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

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

  $pf.$ $\ker e_1 = M_2 \oplus \cdots \oplus M_r$ 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 $y \in N_1 \rightsquigarrow x - y \in \ker e_1 \rightsquigarrow x \in N_1 + \ker e_1$ □

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 $\{N_i\}$.

□

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 $\mathcal{S} = \{\underset{\text{finite}}{\cap} m : m \in \operatorname{Max} R\} \neq \varnothing$. 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 $\mathcal{S} = \{J \subseteq R | J m_1^{n_1} \cdots m_\ell^{n_\ell} \neq 0\} \neq \varnothing$ 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, $x m_1^{n_1} \cdots m_\ell^{n_\ell} = x m_1^{n_1+1} \cdots m_\ell^{n_\ell+1} \implies \langle x \rangle \supseteq x m_1 \cdots m_\ell \in \mathcal{S} \rightsquigarrow x m_1 \cdots m_\ell = \langle x \rangle \rightsquigarrow (m_1 \cdots m_\ell)_{\subseteq J_R}(Rx) = Rx$. By Nakayama's lemma, $Rx = 0 \rightsquigarrow x = 0$ ($\lightning$).

(5) R : Artinian, then

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

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

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

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

Chapter 2

Homological algebra

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

2.1 Projective, injective and flat module

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

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

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

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

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

Those property in above please check by yourself.
Notice that it will not from a complete short exact sequence, we see some example.

Example 2.1.1.

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

Definition 2.1.1.

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

Fact 2.1.1.

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

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

  We called $\widetilde{f}$ is a lifting of f.

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

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

  We called $\widetilde{f}$ is an extension of f.

- free $\implies$ projective

$$\begin{array}{ccccc} & & & & F \\ & & \overset{\exists \widetilde{f}}{\swarrow} & & \downarrow f \\ M_2 & \underset{g}{\longrightarrow} & M_3 & \longrightarrow & 0 \end{array}$$

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

- free $\implies$ flat : Say $F \simeq R^n$ where n may not be finite, then $0 \to M_1 \to M_2 \implies 0 \to M_1^{\oplus n} \to M_2^{\oplus n}$ and thus $0 \to R^n \otimes M_1 \to R^n \otimes M_2$.

- S : m.c. in R, $0 \to M_1 \to M_2 \to M_3 \to 0$ exact, then

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

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

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

Goal:

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

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

Theorem 2.1.1 (Baer's criterion)**.** N is injective $\iff$

$$\begin{array}{ccccc} \forall : 0 & \longrightarrow & I & \longrightarrow & R \\ & & {\scriptstyle f}\downarrow & \swarrow_{\exists \widetilde{f}} & \\ & & N & & \end{array}$$

Proof: ($\Rightarrow$) : OK!

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

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

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

Claim: $M^* = M_2$

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

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

Well-defined : $z_1 + r_1 x = z_2 + r_2 x \implies z_1 - z_2 = (r_2 - r_1)x \rightsquigarrow (r_2 - r_1) \in I$

$h(r_2) - h(r_1) = h(r_2 - r_1) = \mu((r_2 - r_1)x) = \mu(z_1 - z_2) = \mu(z_1) - \mu(z_2)$.

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

Property 2.1.1 (key property)**.**

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

  (Over a PID, divisible $\iff$ injective)

Proof:

- $\forall x_0 \in N, r_0 \in R \setminus \{0\}$, define $g : \begin{array}{ccc} Rr_0 & \longrightarrow & N \\ rr_0 & \longmapsto & rx_0 \end{array}$ which is well-defined by ID. By Baer's criterion, $\exists h$ extends g :

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

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

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

□

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

Proof:

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

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

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

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

Claim: N is injective

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

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

Finally, we will check those condition :

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

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

•• $h \in \mathrm{Hom}_R(M_2, N)$

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

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

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

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

□

Now, by $M \hookrightarrow N_0$ we have

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

and get the goal.

□

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

$$M_2 = M_1 \oplus M_3$$

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

Property 2.1.2 (Important property)**.**

(1) TFAE

(a) M is projective

(b) $\forall 0 \to M_1 \to M_2 \to M \to 0$ split

(c) $\exists M'$ s.t. $M \oplus M'$ is free

(2) TFAE

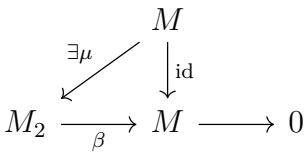
(a) M is injective

(b) $\forall 0 \to M \to M_2 \to M_3 \to 0$ split exact

(3) projective $\implies$ flat

Proof:

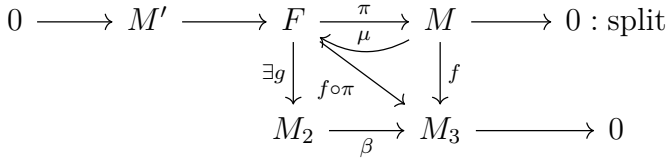
(1) • $(a) \Rightarrow (b)$: Since M is projective



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

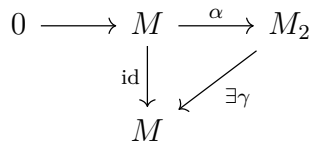
• $(b) \Rightarrow (c)$: $\exists F$: free s.t. $0 \longrightarrow \ker f \xrightarrow{f} M \to 0$. By assumption, $\ker f \oplus M \simeq F$ is free.

• $(c) \Rightarrow (a)$: For all $M_2 \to M_3 \to 0$ with $f : M \to M_3$. Since $M' \oplus M \simeq F$: free



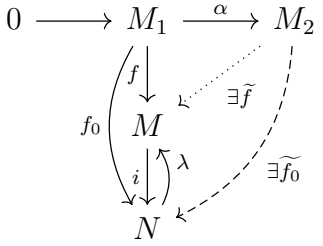
Since the above is split, $\exists \mu : M \to F$ s.t. $\pi \circ \mu = \mathrm{id}_M$. Let $h := g \circ \mu$, then $\beta \circ h = f$

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



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

• $(b) \Rightarrow (a)$: $\exists N$: injective s.t. $M \overset{i}{\hookrightarrow} N$ and consider $0 \to M \to N \to N/M \to 0$ is split, then $\exists \lambda : N \to M$ s.t. $\lambda \circ i = \mathrm{id}_M$. Since N is injective, $\exists \widetilde{f_0}$ extends f_0. Let $\widetilde{f} := \lambda \circ \widetilde{f_0}$, then $\widetilde{f} \circ \alpha = \lambda \circ f_0 = f$ i.e.$\widetilde{f} : M_2 \to M$ is extension of $f : M_1 \to M$.



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

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

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

□

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

□

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

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

Proof: $(\Rightarrow)$: By observation.
$(\Leftarrow)$: We select specific R-module to get the conclusion.

• Let $N = M_3/g(M_2)$ and $i : M_3 \to N$, then $i \circ g = 0 \rightsquigarrow i = 0$ i.e. $M_3 = g(M_2) \rightsquigarrow g$ is onto.

• Let $N = M_3 \rightsquigarrow \mathrm{id}_{M_3} \in \mathrm{Hom}(M_3, N)$ and $0 = \widetilde{f} \circ \widetilde{g}(\mathrm{id}_{M_3}) = g \circ f \rightsquigarrow \mathrm{Im}\, f \subseteq \ker g$

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

□

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

2.2 Homology functor

Definition 2.2.1.

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

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

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

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

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

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

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

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

- A **cochain homomorphism** $\varphi : C^\bullet \to \widetilde{C}^\bullet$:

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

  such that the diagram commutes.

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

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

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

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

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

Now, we want to know want kind of chain homomorphisms are "same".

Definition 2.2.2. (homotopic)

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

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} & \longrightarrow & \cdots \\ & & & \swarrow^{s_n} & \downarrow{\scriptstyle f_n} & \swarrow^{s_{n-1}} & & & \\ \cdots & \longrightarrow & \widetilde{C}_{n+1} & \xrightarrow[\widetilde{d}_{n+1}]{} & \widetilde{C}_n & \xrightarrow[\widetilde{d}_n]{} & \widetilde{C}_{n-1} & \longrightarrow & \cdots \end{array}$$

$$\begin{array}{rccc} \Longrightarrow f_* : & H_n(C_\bullet) & \longrightarrow & H_n(\widetilde{C}_\bullet) \\ & x + \operatorname{Im} d_{n+1} & \longrightarrow & f_n(x) + \operatorname{Im} \widetilde{d}_{n+1} = \left(\widetilde{d}_{n+1}s_n(x) + s_{n-1}d_n(x)\right) + \operatorname{Im} \widetilde{d}_{n+1} = \overline{0} \end{array}$$

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

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

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

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

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & \nearrow & & & \\ 0 & \longrightarrow & \ker \varepsilon & \longrightarrow & F_0 & \to & M & \to & 0 \\ & & \uparrow & \nearrow_{\exists d_1} & & & & & \\ & & F_1 & & & & & & \\ & \nearrow & & & & & & & \\ \ker d_1 & & & & & & & & \end{array}$$

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

Theorem 2.2.1 (Comparison theorem)**.**

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \exists f_2} & & \downarrow{\scriptstyle \exists f_1} & & \downarrow{\scriptstyle \exists f_0} & & \downarrow{\scriptstyle f} & & \\ \cdots & \longrightarrow & C_2 & \xrightarrow[d_2']{} & C_1 & \xrightarrow[d_1']{} & C_0 & \xrightarrow[\varepsilon']{} & N & \longrightarrow & 0 \end{array}$$

: projective resolution

: exact sequence

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

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

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

Claim: $\operatorname{Im}(f_{n-1}d_n) \subseteq \operatorname{Im} d'_n$
pf. Since $\operatorname{Im} d'_n = \ker d'_{n-1}$ and $d'_{n-1}f_{n-1}d_n = f_{n-2}d_{n-1}d_n = 0$. □
By projectivity, there exists $f_n : P_n \to C_n$ such that the diagram commute

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

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

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

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

By projectivity, there exists $s_n : P_n \to C_{n+1}$ s.t. the following diagram commute

$$\begin{array}{ccccc} & & P_n & & \\ & \swarrow_{\exists s_n} & \downarrow{\scriptstyle g_n - f_n - s_{n-1}d_n} & & \\ C_{n+1} & \longrightarrow & \operatorname{Im} d'_{n+1} & \longrightarrow & 0 \end{array}$$

□

Definition 2.2.3. Let $M \in {}_R\mathfrak{M}$ and $\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$ be a projective resolution of M (or simply $P_\bullet \to M \to 0$) $\rightsquigarrow P_M : P_\bullet \to 0$ is chain complex. Then for all $N \in {}_R\mathfrak{M}$,

$$0 \to \operatorname{Hom}(P_0, N) \xrightarrow{\overline{d}_1} \operatorname{Hom}(P_1, N)) \xrightarrow{\overline{d}_2} \operatorname{Hom}(P_2, N) \to \cdots$$

Notice that $\overline{d}_{i+1}\overline{d}_i(f) = f \circ d_i \circ d_{i+1} = 0$, so it form a cochain complex. Define

$$\operatorname{Ext}^n_R(M, N) := H^n(\operatorname{Hom}(P_M, N)) \ \forall n \geq 0$$

$n = 0 : \operatorname{Ext}^0_R(M, N) = \ker \overline{d}_1 / 0 = \ker \overline{d}_1 = \operatorname{Im} \overline{\varepsilon} \simeq \operatorname{Hom}(M, N)$ and

$$0 \to \operatorname{Hom}(M, N) \xrightarrow{\overline{\varepsilon}} \operatorname{Hom}(P_0, N) \xrightarrow{\overline{d}_1} \operatorname{Hom}(P_1, N) \to \cdots : \text{exact}$$

But our definition of Ext is depending on choice of $P_\bullet$. So we see this theorem.

Theorem 2.2.2 (Independency of the choice of projective resolution)**.**

Proof:

(1) Consider two projective resolution of M and $\widetilde{M}$ and $F : M \to \widetilde{M}$. By comparison theorem, there exists $f = \{f_i\}$

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \exists f_1} & & \downarrow{\scriptstyle \exists f_0} & & \downarrow{\scriptstyle F} & & \\ \cdots & \longrightarrow & \widetilde{P}_1 & \xrightarrow[\widetilde{d}_1]{} & \widetilde{P}_0 & \xrightarrow[\varepsilon']{} & \widetilde{M} & \longrightarrow & 0 \end{array}$$

Take Hom functor on whole diagram, we get

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_R(P_0, N) & \xrightarrow{\overline{d}_1} & \mathrm{Hom}_R(P_1, N) & \longrightarrow & \cdots \\ & & \uparrow{\scriptstyle \overline{f}_0} & & \uparrow{\scriptstyle \overline{f}_1} & & \\ 0 & \longrightarrow & \mathrm{Hom}_R(\widetilde{P}_0, N) & \xrightarrow{\overline{\widetilde{d}_1}} & \mathrm{Hom}_R(\widetilde{P}_1, N) & \longrightarrow & \cdots \end{array}$$

Then $\overline{f}^* : \mathrm{Ext}^\bullet_R(\widetilde{M}, N) \to \mathrm{Ext}^\bullet_R(M, N)$. For another $g = \{g_i\}$, f and g are homotopic i.e. $\exists\{s_i\}$ s.t. $g_n - f_n = s_{n-1}d_n + \widetilde{d}_{n+1}s_n \rightsquigarrow \overline{g}_n - \overline{f}_n = \overline{s}_{n-1}\overline{d}_n + \overline{\widetilde{d}_{n+1}}\overline{s}_n \rightsquigarrow \overline{f}^* = \overline{g}^*$

(2) Let $\widetilde{M} = M$ and $f = \mathrm{id}$

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 & & \\ & & \downarrow{\scriptstyle \exists g_0} & & \downarrow{\scriptstyle \mathrm{id}} & & & & \\ & \overset{\mathrm{id}}{\swarrow} & P'_0 & \longrightarrow & M & \longrightarrow & 0 & & \\ & & \downarrow{\scriptstyle \exists f_0} & & \downarrow{\scriptstyle \mathrm{id}} & & & & \\ \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 & & \end{array}$$

$\rightsquigarrow \{f_i \circ g_i\}$ and $\{\mathrm{id}_i\}$ are homotopic, so $\overline{g}^* \circ \overline{f}^* = (\mathrm{id})^* = \mathrm{id}$. By symmetry, $\overline{f}^* \circ \overline{g} = \mathrm{id} \rightsquigarrow \overline{f}^*_i : H^i(\mathrm{Hom}(P_\bullet, N)) \xrightarrow{\sim} H^i(\mathrm{Hom}(\widetilde{P}_\bullet, N))$

□

Theorem 2.2.3 (Long exact sequence for Ext)**.** If $0 \to L \to M \to K \to 0$ is exact for R-module, then

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}(K, N) & \longrightarrow & \mathrm{Hom}(M, N) & \longrightarrow & \mathrm{Hom}(L, N) \\ & \searrow & & & & & \\ & & \mathrm{Ext}^1(K, N) & \longrightarrow & \mathrm{Ext}^1(M, N) & \longrightarrow & \mathrm{Ext}^1(L, N) \\ & & & \searrow & & & \\ & & \mathrm{Ext}^2(K, N) & \longrightarrow & \mathrm{Ext}^2(M, N) & \longrightarrow & \cdots \end{array}$$

We will use Horseshoe lemma and snake lemma in below, which will put the statement in Homework 13.

Proof: We choose $P_\bullet \to L$: proj. resol. of L and $\widetilde{P}_\bullet \to K$: proj. resol. of K. By the Horseshoe lemma, $\exists \overline{P}_\bullet \to M \to 0$: proj. resol of M s.t.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_\bullet & \longrightarrow & \overline{P}_\bullet & \longrightarrow & \widetilde{P}_\bullet & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & K & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Notice that $\widetilde{P}_i$ is projective, $0 \to P_i \to \overline{P}_i \to \widetilde{P}_i \to 0$ is split, then $\overline{P}_i \simeq P_i \oplus \widetilde{P}_i$ and thus $\mathrm{Hom}(\overline{P}, N) \simeq \mathrm{Hom}(P_i, N) \oplus \mathrm{Hom}(\widetilde{P}_i, N)$, then we have a exact sequence :

$$0 \to \mathrm{Hom}(\widetilde{P}_i, N) \to \mathrm{Hom}(\overline{P}_i, N) \to \mathrm{Hom}(P_i, N) \to 0$$

and thus

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(\widetilde{P}_1, N) & \longrightarrow & \mathrm{Hom}(\overline{P}_1, N) & \longrightarrow & \mathrm{Hom}(P_1, N) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathrm{Hom}(\widetilde{P}_0, N) & \longrightarrow & \mathrm{Hom}(\overline{P}_0, N) & \longrightarrow & \mathrm{Hom}(P_0, N) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Fact: $0 \to A^\bullet \xrightarrow{\alpha^\bullet} B^\bullet \xrightarrow{\beta^\bullet} C^\bullet \to 0$ exact, then

$$0 \to H^0(A^\bullet) \to H^0(B^\bullet) \to H^0(C^\bullet) \to H^1(A^\bullet) \to H^1(B^\bullet) \to H^1(C^\bullet) \to \cdots$$

pf. Since $\mathrm{Im}\, a_i = \ker a_{i+1} \subseteq A^i$ and by snake lemma we have

$$\begin{array}{ccccccc}
 & & \ker a_i & \longrightarrow & \ker b_i & \longrightarrow & \ker c_i \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & A^{i-1} & \longrightarrow & B^{i-1} & \longrightarrow & C^{i-1} \longrightarrow 0 \\
 & & \downarrow{\scriptstyle a_i} & & \downarrow{\scriptstyle b_i} & & \downarrow{\scriptstyle c_i} \\
0 & \longrightarrow & \ker a_{i+1} & \longrightarrow & \ker b_i & \longrightarrow & \ker c_{i+1} \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & H^i(A^\bullet) & \longrightarrow & H^i(B^\bullet) & \longrightarrow & H^i(C^\bullet)
\end{array}$$

By some discuss, we can get $0 \to \ker a_i/\operatorname{Im} a_{i-1} \to \ker b_i/\operatorname{Im} b_{i-1} \to \ker c_i/\operatorname{Im} c_{i-1}$. Now, we only need to prove that if $\lambda : \ker c_i \to H^i(A^\bullet)$ in the above diagram, then $\operatorname{Im} c_{i-1} \subseteq \ker \lambda$ and thus we can use factor theorem s.t. $\ker c_i/\operatorname{Im} c_{i-1} \to H^i(A^\bullet)$.

$\ker \lambda = \beta_{i-1}(\ker b_i) = \beta_{i-1}b_{i-1}(B^{i-1}) = \operatorname{Im} c_{i-1}\beta_{i-2}(B^{i-1}) = \operatorname{Im} c_{i-1}(C^{i-1}) = \operatorname{Im} c_{i-1}$

□

2.3 Ext and Tor (I)

For simplicity, R is commutative. But we still can discuss it when R is not commutative for somewhere.
Observation: Given $M, N \in \mathfrak{M}_R$, there are two ways to define $\operatorname{Ext}^n(M, N)$.

- Find any proj. resol. $P_\bullet \xrightarrow{\alpha} M \to 0$ and let $P_M : P_\bullet \to 0$ (complex). We define

$$\operatorname{Ext}^n_{proj}(M, N) = H^n(\operatorname{Hom}(P_M, N))$$

  and

$$0 \xrightarrow{\overline{d}_0} \operatorname{Hom}(P_0, N) \xrightarrow{\overline{d}_1} \operatorname{Hom}(P_1, N) \to \cdots$$

  So $\ker \overline{d}_1/\operatorname{Im} \overline{d}_0 = \ker \overline{d}_1 = \operatorname{Im} \overline{\alpha} = \operatorname{Hom}(M, N)$ which is well define.

- Find any injective resol. $0 \to N \xrightarrow{\beta} I^\bullet$ and let $I_N : 0 \to I^\bullet$ (complex). We define

$$\operatorname{Ext}^n_{inj}(M, N) = H^n(\operatorname{Hom}(M, I_N)) \rightsquigarrow \operatorname{Ext}^0_{inj}(M, N) = \operatorname{Hom}(M, N)$$

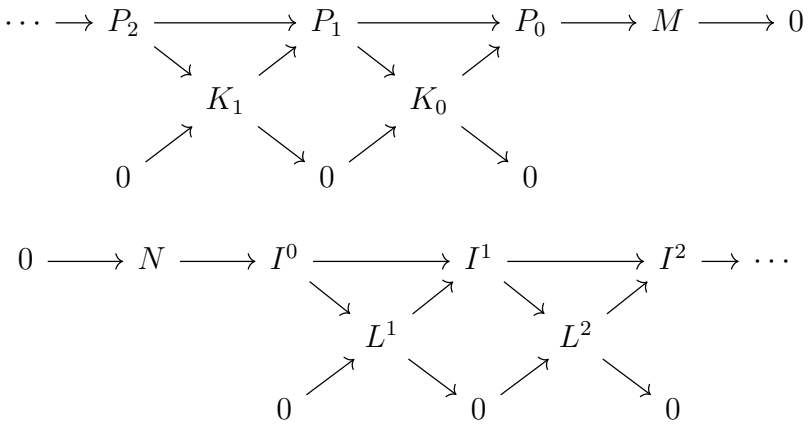
Theorem 2.3.1 (Equivalence of two definitions)**.**

Proof:

- **Observation:** M : proj. $\implies 0 \to M \xrightarrow{\text{id}} M \to 0 \rightsquigarrow \cdots \to 0 \to M \to 0$ (complex), so $\operatorname{Ext}^n_{proj}(M, N) = 0 \ \forall n > 0$

  N : inj. $\implies \operatorname{Ext}^n_{inj}(M, N) = 0 \ \forall n > 0$

- Recall the construction of projective resolution and injective resolution :



For $0 \to K_0 \to P_0 \to M \to 0$ and $0 \to N \to I^0 \to L^1 \to 0$, by long exact of Ext, we have

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathrm{Hom}(M,N) & \to & \mathrm{Hom}(M,I^0) & \xrightarrow{\varphi} & \mathrm{Hom}(M,L^1) & \to & \mathrm{Ext}^1_{inj}(M,N) \to \mathrm{Ext}^1_{inj}(M,I^0) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathrm{Hom}(P_0,N) & \to & \mathrm{Hom}(P_0,I^0) & \xrightarrow{\sigma} & \mathrm{Hom}(P_0,L^1) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \to & \mathrm{Hom}(K_0,N) & \to & \mathrm{Hom}(K_0,I^0) & \xrightarrow{\tau} & \mathrm{Hom}(K_0,L^1) & \to & \mathrm{Ext}^1_{inj}(K_0,N) \to \mathrm{Ext}^1_{inj}(K_0,I^0) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathrm{Ext}^1_{proj}(M,N) & & 0 & & \mathrm{Ext}^1_{proj}(M,L^1) & & \\
 & & \downarrow & & & & \downarrow & & \\
 & & \mathrm{Ext}^1_{proj}(P_0,N) & & & & \mathrm{Ext}^1_{proj}(P_0,L^1) & &
\end{array}$$

where blue modules are 0 by above observation and red are 0 by the property of projective and injective. So

$$\begin{aligned}
\mathrm{Ext}^1_{proj}(M,N) &= \operatorname{coker}\alpha & \mathrm{Ext}^1_{inj}(M,N) &= \operatorname{coker}\varphi \\
\mathrm{Ext}^1_{proj}(M,L') &= \operatorname{coker}\gamma & \mathrm{Ext}^1_{inj}(K_0,N) &= \operatorname{coker}\tau
\end{aligned}$$

Apply snake lemma for (α,β,γ),

$$\mathrm{Hom}(M,I^0) \xrightarrow{\varphi} \mathrm{Hom}(M,L^1) \to \operatorname{coker}\alpha \to 0$$

and thus $\operatorname{coker}\alpha \simeq \operatorname{coker}\varphi$ i.e. $\mathrm{Ext}^1_{proj}(P_0,N) \simeq \mathrm{Ext}^1_{inj}(M,N)$.

Also, $\operatorname{Im}\gamma = \gamma(\mathrm{Hom}(P_0,L^1)) = \gamma(\sigma(\mathrm{Hom}(P_0,I^0))) = \tau(\beta(\mathrm{Hom}(P_0,I^0))) = \operatorname{Im}\tau \rightsquigarrow \operatorname{coker}\gamma = \operatorname{coker}\tau \rightsquigarrow \mathrm{Ext}^1_{proj}(M,L^1) = \mathrm{Ext}^1_{inj}(K_0,N)$.

Similarly using on $0 \to K_j \to P_j \to K_{j-1} \to 0$ and $0 \to L^i \to I^i \to L^{i+1} \to 0$, we can get

$$\mathrm{Ext}^1(K_{j-1},L^{i+1}) \simeq \mathrm{Ext}^1(K_j,L^i) \quad (K_{-1} := M, L^0 := N)$$

(Notice that we had proved two definition of Ext^1 are equivalent)

Observe that $0 \to L^{n-1} \to I^{n-1} \xrightarrow{\overline{d}_n} I^n \xrightarrow{\overline{d}_{n+1}} I^{n+1} \to \cdots$ is inj. resol. of L^{n-1}

$$\implies \mathrm{Ext}^1(M,L^{n-1}) \simeq \ker\overline{d}_{n+1}/\ker\overline{d}_n \simeq \mathrm{Ext}^n_{inj}(M,N)$$

Similarly, by $\cdots \to P_n \to P_{n-1} \to K_{n-2}$, $\mathrm{Ext}^n_{proj}(M,N) \simeq \mathrm{Ext}^1_{proj}(K_{n-2},N)$. Hence,

$$\begin{aligned}
\mathrm{Ext}^n_{inj}(M,N) &\simeq \mathrm{Ext}^1(M,L^{n-1}) \simeq \mathrm{Ext}^1(K_0,L^{n-2}) \\
&\simeq \cdots \simeq \mathrm{Ext}^1(K_{n-2},L^0) \simeq \mathrm{Ext}^n_{proj}(M,N) \ \forall n \geq 2
\end{aligned}$$

□

Definition 2.3.1. Let $P_\bullet \to M \to 0$ be a projective resol. and $N \in \mathfrak{M}_R$. Define

$$\mathrm{Tor}_n(M,N) = H_n(P_M \otimes N)\ \forall n \geq 0 \quad (\mathrm{Tor}_0(M,N) \simeq M \otimes_R N)$$

Fact 2.3.1. $\mathrm{Tor}_n(U,N) = 0\ \forall n > 0, \forall N \in \mathfrak{M}_R$

Proof: Let F, F' be free s.t. $0 \to \ker\varepsilon \to F \xrightarrow{\varepsilon} U$ and $0 \to \ker\varepsilon' \to F' \xrightarrow{\varepsilon'} N$, apply snake lemma on (α, β, γ),

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & \ker\varepsilon \otimes \ker\varepsilon' & \longrightarrow & F \otimes \ker\varepsilon' & \longrightarrow & U \otimes \ker\varepsilon' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 & \longrightarrow & \ker\varepsilon \otimes F' & \longrightarrow & F \otimes F' & \longrightarrow & U \otimes F' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\varepsilon'} & & \\
 & & \ker\varepsilon \otimes N & \longrightarrow & F \otimes N & \xrightarrow{\varepsilon} & U \otimes N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

$$0 = \ker\gamma \to \mathrm{coker}\,\alpha \to \mathrm{coker}\,\beta \to \mathrm{coker}\,\gamma \to 0$$

and $\mathrm{coker}\,\alpha = \ker\varepsilon \otimes N, \mathrm{coker}\,\beta = F \otimes N, \mathrm{coker}\,\gamma = U \otimes N$. But

$$\mathrm{Tor}_1(U,N) \to \ker\varepsilon \otimes N \to F \otimes N \to U \otimes N \to 0 \implies \mathrm{Tor}_1(U,N) = 0$$

We induct $\mathrm{Tor}_n(U,N) = 0\ \forall n > 0$ on n. If $n = 1$: OK!. If $n > 1$, notice that $\mathrm{Tor}_n(F,N) = 0\ \forall n > 0$ since F is projective. By long exact sequence for Tor (Homework 14),

$$0 = \mathrm{Tor}_n(F,N) \to \mathrm{Tor}_n(U,N) \to \mathrm{Tor}_{n-1}(\ker\varepsilon, N) \to \mathrm{Tor}_{n-1}(F,N) = 0$$

So $\mathrm{Tor}_n(U,N) = \mathrm{Tor}_{n-1}(\ker\varepsilon, N)$. For all $0 \to M' \to M \to M'' \to 0$,

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
\mathrm{Tor}_1(U,M') & \longrightarrow & \ker\varepsilon \otimes M' & \longrightarrow & F \otimes M' & \longrightarrow & U \otimes M' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\mathrm{Tor}_1(U,M) & \longrightarrow & \ker\varepsilon \otimes M & \longrightarrow & F \otimes M & \longrightarrow & U \otimes M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\varepsilon'} & & \\
\mathrm{Tor}_1(U,M'') & \longrightarrow & \ker\varepsilon \otimes M'' & \longrightarrow & F \otimes M'' & \xrightarrow{\varepsilon} & U \otimes M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Red zeros by flat and blue zeros by $\mathrm{Tor}_1(\text{flat}, N) = 0$. By nine lemma,

$$0 \to \ker\varepsilon \otimes N' \to \ker\varepsilon \otimes N \to \ker\varepsilon \otimes N'' \to 0$$

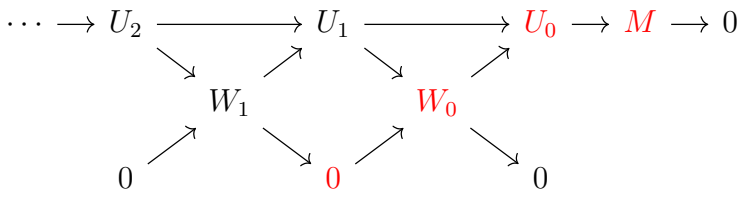
i.e. $\ker\varepsilon$ is flat. By induction hypothesis, $\mathrm{Tor}_{n-1}(\ker\varepsilon, N) = 0 \implies \mathrm{Tor}_n(U, N) = 0$. □

Property 2.3.1 (Tor for flat resolutions)**.** Let $U_\bullet \to M \to 0$ be a flat resolution of M. Then

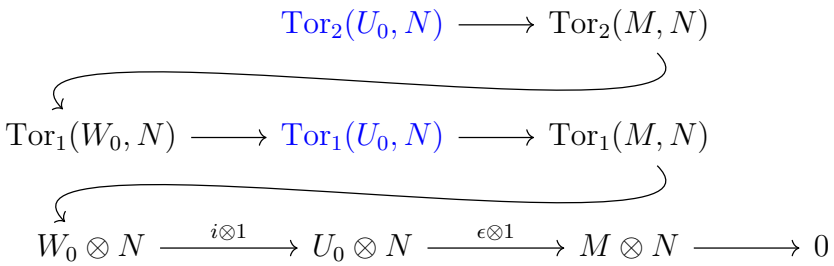
$$\mathrm{Tor}_n(M, N) \simeq H_n(U_M \otimes N)\ \forall n > 0$$

Proof:

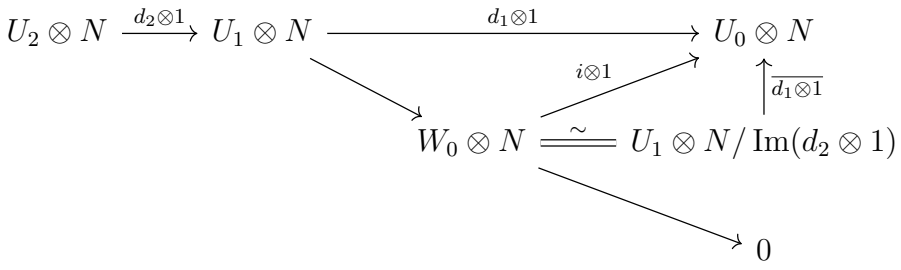
- $n = 0$: $\because U_1 \otimes N \xrightarrow{\bar{d}_1} U_0 \otimes N \to M \otimes N \to 0$ exact $\rightsquigarrow U_1 \otimes N \xrightarrow{\bar{d}_1} U_0 \otimes N \to 0$ complex $\therefore H_0(U_M \otimes N) = U_0 \otimes N / \operatorname{Im}\bar{d}_1 \simeq M \otimes N = \mathrm{Tor}_0(M, N)$
- $n = 1$: Let $W_i = \ker d_i$ and consider



By long exact sequence for Tor on $0 \to W_0 \to U_0 \to M \to 0$,



where the blue one is 0 by U_0 is flat. So $\mathrm{Tor}_2(M, N) \simeq \mathrm{Tor}_1(W_0, N)$ and $\mathrm{Tor}_1(M, N) \simeq \ker(i \otimes 1)$. In the other hand,



Thus,

$$\mathrm{Tor}_1(M, N) \simeq \ker(i \otimes 1) = \ker\overline{d_1 \otimes 1} = \ker(d_1 \otimes 1)/\operatorname{Im}(d_2 \otimes 1) = H_1(U_M \otimes N)$$

- $n > 1$: $\mathrm{Tor}_2(M,N) \simeq \mathrm{Tor}_1(W_0,N) = H_1(U_{W_0} \otimes N) = H_2(U_M \otimes N)$. In general, $\mathrm{Tor}_n(M,N) \simeq \mathrm{Tor}_{n-1}(W_0,N) \simeq H_{n-1}(U_{W_0} \otimes N) \simeq H_n(U_M \otimes N)$ by induction hypothesis.

□

Example 2.3.1. For any abelian group G, determine $\mathrm{Tor}_n(\mathbb{Q}/\mathbb{Z}, G)$:

- Consider the flat resolution : $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$(Recall that R_S is R flat module). Let $0 \xrightarrow{\overline{d}_2} \mathbb{Z} \otimes_{\mathbb{Z}} G \xrightarrow{\overline{d}_1} \mathbb{Q} \otimes_{\mathbb{Z}} G \to 0$ is a complex. Then $\mathrm{Tor}_1(\mathbb{Q}/\mathbb{Z}, G) = \ker \overline{d}_1 / \operatorname{Im} \overline{d}_2 = \ker \overline{d}_1$. Since $\mathbb{Q} \otimes_{\mathbb{Z}} G \simeq G_{\mathbb{Z}\setminus\{0\}}$ and $\mathbb{Z} \otimes_{\mathbb{Z}} G \simeq G$,

  $$g \in \ker \overline{d}_1 \iff \frac{g}{1} = 0 \text{ in } G_{\mathbb{Z}\setminus\{0\}} \iff \exists m \in \mathbb{Z}\setminus\{0\} \text{ s.t. } mg = 0 \iff g \in \mathrm{Tor}(G)$$

  So $\mathrm{Tor}_1(\mathbb{Q}/\mathbb{Z}, G) = \mathrm{Tor}(G)$
- Since $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \rightsquigarrow \cdots \to 0 \to 0 \to \mathbb{Z}\otimes G \to \mathbb{Q}\otimes G \to \mathbb{Q}/\mathbb{Z}\otimes G \to 0$ is a complex and thus $\mathrm{Tor}_n(\mathbb{Q}/\mathbb{Z}, G) = 0\ \forall n \geq 2$.

Proposition 2.3.1. TFAE

(1) M is flat

(2) $\mathrm{Tor}_1(M, R/I) = 0\ \forall I \subseteq R$

(3) $\forall 0 \to I \to R \implies 0 \to M \otimes I \to M \otimes R$ exact

(4) $M^* := \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is an injective R-module

Proof:

- (2) $\iff$ (3) : For $0 \to I \to R \to R/I \to 0$, by long exact sequence for Tor,

  $$0 = \mathrm{Tor}_1(R, M) \to \mathrm{Tor}_1(R/I, M) \to I \otimes M \xrightarrow{f} R \otimes M \to R/I \otimes M \to 0$$

  By Homework 14, we will prove that if R is commute, then $\mathrm{Tor}_n(M,N) = \mathrm{Tor}_n(N,M)$. So (2) $\iff$ f injective $\iff$ (3)
- (1) $\iff$ (4) : $\forall 0 \to N' \to N$: exact, by Homework 12, we have

  $$\mathrm{Hom}_R(N, M^*) \simeq \mathrm{Hom}_{\mathbb{Z}}(M \otimes N, \mathbb{Q}/\mathbb{Z}) = (M \otimes N)^*$$

  $$\mathrm{Hom}_R(N', M^*) \simeq \mathrm{Hom}_{\mathbb{Z}}(M \otimes N', \mathbb{Q}/\mathbb{Z}) = (M \otimes N')^*$$

  Fact:

  - $A^* = 0 \iff A = 0$
    pf. ($\Leftarrow$) : OK! ($\Rightarrow$) : If $\exists 0 \neq a \in A$, let $f : \langle a \rangle_{\mathbb{Z}} \to \mathbb{Q}/\mathbb{Z}$ by $a \mapsto o(a)^{-1} + \mathbb{Z}$ or $a \mapsto 1 + \mathbb{Z}$ (if $o(a) = \infty$). Since $\mathbb{Q}/\mathbb{Z}$ is injective and $0 \to \langle a \rangle \to A$, there exists $\widetilde{f} : A \to \mathbb{Q}/\mathbb{Z}$ is $\mathbb{Z}$-module homomorphism i.e. $A^* \neq 0$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\leftarrow$)

- $0 \to B \xrightarrow{f} C \iff C^* \xrightarrow{f^*} B^* \to 0$
  $pf.\ 0 \to \ker f \to B \xrightarrow{f} C \to 0 \rightsquigarrow C^* \xrightarrow{f^*} B^* \to (\ker f)^* \to 0$ by $\mathbb{Q}/\mathbb{Z}$ is injective.
  So $\ker f = 0 \iff \operatorname{coker} f^* \simeq (\ker f)^* = 0$

Hence,

$$\begin{aligned} & M^* \text{ is injective} \\ \iff & (M \otimes N)^* \to (M \otimes N')^* \to 0 \text{ exact } \forall 0 \to N' \to N \\ \iff & 0 \to M \otimes N' \to M \otimes N \text{ exact } \forall 0 \to N' \to N \iff M \text{ is flat} \end{aligned}$$

- $(4) \iff (3) : M^*$ is injective $\xleftarrow{bear's\ criterion} (M \otimes R)^* \to (M \otimes I)^* \to 0\ \forall I \subseteq R \iff 0 \to M \otimes I \to M \otimes R\ \forall I \subseteq R$

□

2.4 Ext and Tor (II) and an important application

2.4.1 group-module

Definition 2.4.1. Let M be an abelian group and G be a group. We say

$$G \curvearrowright M \iff \exists \text{ a group homo. } (G, \cdot) \to (\operatorname{Aut}(M), \circ)$$

and extend to a ring homo.

$$\mathbb{Z}[G] \to (\operatorname{Aut}(M), +, \circ) \implies M : \text{left } \mathbb{Z}[G]\text{-module}$$

- $H^n(G, M) := \operatorname{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M)$, here $G \curvearrowright \mathbb{Z}$ trivially i.e. $\forall g \in G, \forall n \in \mathbb{Z}$, $gn = n$
- $H_n(G, M) := \operatorname{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M) \simeq \operatorname{Tor}_n^{\mathbb{Z}[G]}(M, \mathbb{Z})$

But M is only left $\mathbb{Z}[G]$-module, we need to give M the right $\mathbb{Z}[G]$-module structure. We will complete the definition in remark.

Remark 2.4.1. Since G is may not abelian, $\mathbb{Z}[G]$ may not be commutative ring. But $\mathbb{Z}[G]$ is a group ring have some good structure, we can define the right $\mathbb{Z}[G]$-module structure on M. Define

$$\begin{array}{rccc} \rho : & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z}[G] \\ & g & \longmapsto & g^{-1} \end{array}$$

Then ρ is additive homo. and $\rho(ab) = \rho(b)\rho(a)$ (we called it **antiautomorphism**) or say $\rho : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]^o$ is an isomorphism. By

$$\mathbb{Z}[G]^o \xrightarrow{\rho^{-1}} \mathbb{Z}[G] \to \operatorname{Aut}(M)$$

gives M a right $\mathbb{Z}[G]$-module structure, denote M^r.
Similarly. For given N be a left $\mathbb{Z}[G]$ module,

$$\mathbb{Z}[G] \xrightarrow{\rho} \mathbb{Z}[G]^o \to \operatorname{Aut}(M)$$

gives N a left $\mathbb{Z}[G]$-module structure, denote N^ℓ and $\forall x \in N^\ell, a \in \mathbb{Z}[G], a \cdot x := x\rho(a)$
So we can extend the definition of Tor.

- Two left $\mathbb{Z}[G]$-module M, N. Define $M \otimes_{\mathbb{Z}[G]} N := M^r \otimes_{\mathbb{Z}[G]} N$. Then

$$\mathrm{Tor}_n^{\mathbb{Z}[G]}(M,N) := \mathrm{Tor}_n^{\mathbb{Z}[G]}(M^r,N),\ \mathrm{Tor}_n^{\mathbb{Z}[G]}(N,M) := \mathrm{Tor}_n^{\mathbb{Z}[G]}(N^r,M)$$

- $\mathrm{Tor}_n^{\mathbb{Z}[G]}(M,N) \simeq \mathrm{Tor}_n^{\mathbb{Z}[G]}(N,M)$:
  - P is a projective right $\mathbb{Z}[G]$-module $\iff$ P^ℓ is a projective left $\mathbb{Z}[G]$-module :
    - $\rho(a\cdot b) = \rho(b\rho(a)) = \rho^2(a)\cdot\rho(b) = a\rho(b)$. So $\mathbb{Z}[G] \overset{\rho}{\simeq} \mathbb{Z}[G]$ as left $\mathbb{Z}[G]$ module.
    - $(\mathbb{Z}[G]^{\oplus n})^\ell \simeq \mathbb{Z}[G]^{\oplus n}$.

$$\begin{aligned} & p \text{ is projective} \iff \exists p' \text{ s.t. } p\otimes p' = \mathbb{Z}[G]^{\oplus n} \\ \iff & p^\ell \oplus (p')^\ell \simeq (p\oplus p')^{\oplus n} \simeq \left(\mathbb{Z}[G]^{\oplus n}\right)^\ell \simeq \mathbb{Z}[G]^{\oplus n} \\ \iff & p^\ell \text{ is projective} \end{aligned}$$

  - $P_\bullet \to M^r$: right projective resolution $\iff$ $P_\bullet^\ell \to (M^r)^\ell = M$: left projective resolution of M.

2.4.2 resolution of $\mathbb{Z}$

- **The bar resolution of $\mathbb{Z}$:** $B[G] : \cdots \to B_n \xrightarrow{d_n} B_{n-1} \to \cdots \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$
  - $B_0 = \mathbb{Z}[G][\ ]$ and $\varepsilon : [\ ] \mapsto 1$ i.e. $\varepsilon(\sum \lambda_g g) = \sum \lambda_g$, where $[\ ]$ just a generator for convenient symbol in later.
  - $B_n = \bigoplus_{x_i\in G} \mathbb{Z}[G][x_1|x_2|\cdots|x_n]$ and define

$$d_n : [x_1|x_2|\cdots|x_n] \longmapsto x_1[x_2|\cdots|x_n] + \sum_{i=1}^{n-1}(-1)^i[x_1|\cdots|x_ix_{i+1}|\cdots|x_n] + (-1)^n[x_1|\cdots|x_{n-1}]$$

    For example,
    - $d_1[x] = x[\ ] - [\ ]$
    - $d_2[x|y] = x[y] - [xy] + [x]$
    - $d_3[x|y|z] = x[y|z] - [xy|z] + [x|yz] - [x|y]$
  - It is clear that B_i are free, but it not easy to check that $B[G]$ is projective resolution. We will using another resolution to prove it.

- **The homogeneous resolution of $\mathbb{Z}$:** $P(G) : \cdots \to P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon'} \mathbb{Z} \to 0$
  - $P_n = \bigoplus_{x_i\in G} \mathbb{Z}(x_0,...,x_n)$ and $G \curvearrowright P_n$ by

$$x(x_0,...,x_n) = (xx_0,...,xx_n)$$

    So $P_n = \bigoplus_{x_i\in G} \mathbb{Z}[G](1,x_1,...,x_n)$

- $\varepsilon' : (x_0) \mapsto 1 \rightsquigarrow \varepsilon' = \varepsilon$, since $P_0 \simeq P[G](1)$
- $\partial_n : (x_0, ..., x_n) \longmapsto \sum_{i=0}^{n} (-1)^i (x_0, ..., \hat{x}_i, ..., x_n)$
- $P(G) \simeq B(G)$: Consider

$$\begin{array}{ccccccccccccc} \longrightarrow & P_{n+1} & \xrightarrow{\partial_{n+1}} & P_n & \xrightarrow{\partial_n} & P_{n-1} & \xrightarrow{\partial_{n-1}} & \cdots & \longrightarrow & P_0 & \longrightarrow & \mathbb{Z} & \longrightarrow 0 \\ & \downarrow{\scriptstyle \tau_{n+1}} & & \downarrow{\scriptstyle \tau_n} & & \downarrow{\scriptstyle \tau_{n-1}} & & & & \downarrow{\scriptstyle \tau_0} & & \downarrow{\scriptstyle \mathrm{id}} & \\ \longrightarrow & B_{n+1} & \xrightarrow[d_{n+1}]{} & B_n & \xrightarrow[d_n]{} & B_{n-1} & \longrightarrow & \cdots & \xrightarrow[d_{n-1}]{} & B_0 & \longrightarrow & \mathbb{Z} & \longrightarrow 0 \end{array}$$

  and define $\tau_n : (x_0, ..., x_n) \longmapsto x_0[x_0^{-1}x_1|x_1^{-1}x_2|...|x_{n-1}^{-1}x_n]$, then we can check that τ_n is $\mathbb{Z}$-module homomorphism and $\tau_{n-1} \circ \partial_n = d_n \circ \tau_n$.
  So $\tau_n^{-1} : [x_1|\cdots|x_n] \longmapsto (1, x_1, x_1x_2, ..., x_1x_2\cdots x_n)$ and $\tau_n \circ \tau_n^{-1} = \mathrm{id}_{B_n}, \tau_n^{-1} \circ \tau_n = \mathrm{id}_{P_n}$.
- $P(G)$ is exact : Define $s_{-1} : \mathbb{Z} \to P_0$ by $1 \longmapsto (1)$ and

$$\begin{array}{rccc} s_n : & P_n & \longrightarrow & P_{n+1} \\ & (x_0, ..., x_n) & \longmapsto & (1, x_0, ..., x_n) \end{array}$$

  are $\mathbb{Z}$-module homomorphism. Notice that $1_{P_n} = s_{n-1} \circ \partial_n + \partial_{n+1} \circ s_n$, which means $\mathrm{id} : P(G) \to P(G)$ and $0 : P(G) \to P(G)$ are homotopic $\rightsquigarrow H_n(P(G)) = 0 \ \forall n \rightsquigarrow P(G)$ is exact.
- So $P(G), B(G)$ are free resolution of $\mathbb{Z}$.

- **Normalized bar resolution of $\mathbb{Z}$:** $B^\bullet(G) : \cdots \to B_2^* \xrightarrow{d_2^*} B_1^* \xrightarrow{d_1^*} B_0^* \xrightarrow{\varepsilon} \mathbb{Z} \to 0$
  - Let $U_n = \bigoplus_{\substack{x_i \in G \\ \exists x_i = 1}} \mathbb{Z}[G][x_1|\cdots|x_n]$, then $B_n^* := B_n/U_n \simeq \bigoplus_{1 \neq x_i \in G} \mathbb{Z}[G][x_1|\cdots|x_n]$ and $B_0^* = B_0$.
  - Define $[x_1|\cdots|x_n]^* := [x_1|\cdots|x_n] + U_n \in B_n^*$
  - Construct $d_n^* : [x_1|\cdots|x_n] + U_n \longmapsto d_n([x_1|\cdots|x_n]) + U_{n-1}$, since $d_n(U_n) \subseteq U_{n-1}$ by Homework 15.
  - $B^*(G)$ is exact : Define $t_n := \tau_{n+1} \circ s_n \circ \tau_n^{-1}$ i.e.

$$\begin{array}{rccc} t_n : & B_n & \longrightarrow & B_{n+1} \\ & x[x_1|\cdots|x_n] & \longmapsto & [x|x_1|\cdots|x_n] \end{array}$$

    By $t_n(U_n) \subseteq U_{n+1}$, we can define $t_n^* : B_n^* \longrightarrow B_{n+1}^*$ by $x[x_1|\cdots|x_n]^* \longmapsto [x|x_1|\cdots|x_n]^*$. Notice that $1_{B_n^*} = d_{n+1}^* t_n^* + t_{n-1}^* d_n^* \rightsquigarrow B^*(G)$ is exact.

2.4.3 Augmentation ideal

The first part of resolution (ε) is essential to calculate H^1.

Definition 2.4.2. Define **augmentation ideal**

$$IG := \ker \varepsilon = \{\sum \lambda_g g \in \mathbb{Z}[G] : \sum \lambda_g = 0\}$$

is two-side ideal of $\mathbb{Z}[G]$, and say ε is the **augmentation map**.

- $\mathbb{Z}[G]/IG \simeq \mathbb{Z}$ as $\mathbb{Z}[G]$-module isomorphism, since $\mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$.
- $IG = \langle g-1 : g \in G\rangle_{\mathbb{Z}} : \sum \lambda_g g \in \ker \varepsilon \iff \sum \lambda_g = 0 \iff \sum \lambda_g g = \sum \lambda_g (g-1)$
- IG is $\mathbb{Z}$-free : If $\sum\limits_{g\neq 1} r_g(g-1) = 0 \rightsquigarrow \sum\limits_{g\neq 1} r_g g - \left(\sum\limits_{g\neq 1} r_g\right)\cdot 1 = 0 \rightsquigarrow r_g = 0 \ \forall g \in G.$
- For given $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$, say $f : 1 \mapsto x$, then x is G-invariant. So $H^0(G,M) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \simeq M^G = \{x \in M : gx = x \ \forall g \in G\} = \{x \in M : \ IGx = 0\}$ is $\mathbb{Z}[G]/IG$-module and $G \curvearrowright M^G$ trivially.
- $H_0(G,M) = Z \otimes_{\mathbb{Z}[G]} M \simeq \mathbb{Z}[G]/IG \otimes_{\mathbb{Z}[G]} M \simeq M/IGM =: M_G$ is the largest quotient of M, which G acts trivially.

  $pf.$ $N \subseteq M$, $G \curvearrowright M/N$ trivially $\iff gx + N = x + N \ \forall g \in G, x \in M \iff (g-1)x \in N \ \forall h \in G, \forall x \in M \iff (IG)M \subseteq N$

  - $H^0(G,\mathbb{Z}) = \mathbb{Z}^G = \mathbb{Z}, \ H_0(G,\mathbb{Z}) = \mathbb{Z}_G = \mathbb{Z}$
  - $H^0(G,\mathbb{Z}[G]) = \mathbb{Z}[G]^G = \begin{cases} \mathbb{Z} & ,\text{if } |G| < \infty \\ 0 & ,\text{if } |G| = \infty \end{cases}$

    $pf.$ $\forall g' \in G, \ g'(\sum \lambda_g g) = \sum(\lambda_g g) \rightsquigarrow \lambda_g = \lambda_{g'g} \rightsquigarrow$ all λ_g are the same, say λ.

    If $|G| \leq \infty$, then $\sum\limits_{g\in G} \lambda_g g = \lambda \sum\limits_{g\in G} g \rightsquigarrow \mathbb{Z}[G]^G = \left\langle \sum\limits_{g\in G} g \right\rangle_{\mathbb{Z}} \simeq \mathbb{Z}.$

    If $|G| = \infty \rightsquigarrow \lambda = 0$ i.e. $\mathbb{Z}[G]^G = 0$
  - $H_0(G,\mathbb{Z}[G]) = \mathbb{Z}[G]_G \simeq \mathbb{Z}[G]/IG\mathbb{Z}[G] = \mathbb{Z}[G]/IG \simeq \mathbb{Z}$
  - $H_1(G,\mathbb{Z}[G]) = 0$, since $\mathbb{Z}[G] \simeq \bigoplus\limits_{g\in G} \mathbb{Z}g$ is free and thus flat.
  - $H_1(G,\mathbb{Z}) : 0 \to IG \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, then

$$\begin{array}{ccccccc} & & & & H_1(G,\mathbb{Z}[G]) & \longrightarrow & H_1(G,\mathbb{Z}) \\ & & & \curvearrowright & & & \\ \mathbb{Z}\otimes_{\mathbb{Z}[G]} IG & \xrightarrow{g} & \mathbb{Z}\otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] & \xrightarrow{f} & \mathbb{Z}\otimes_{\mathbb{Z}[G]} \mathbb{Z} & \longrightarrow & 0 \end{array}$$

    where the blue one is 0.

    $f : n \otimes \sum \lambda_g g \longmapsto n \otimes \sum \lambda_g = n \otimes (\sum \lambda_g g)\cdot 1 = (\sum \lambda_g g)\cdot n \otimes 1$ and $n \otimes \lambda_g g = (\sum \lambda_g g)\cdot n \otimes 1$, so f is id and thus $g = 0$, so $H_1(G,\mathbb{Z}) \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} IG \simeq \mathbb{Z}[G]/IG \otimes_{\mathbb{Z}[G]} IG \simeq IG/(IG)^2$.

    Claim: $G/[G,G] \simeq IG/(IG)^2$, where $[G,G]$ is commutator of G.

    proof: Define $\varphi : \begin{array}{ccc} G & \longrightarrow & IG/(IG)^2 \\ g & \longmapsto & (g-1)+(IG)^2 \end{array}$

- Homo : $\varphi(g_1g_2) = \overline{g_1g_2 - 1} = \overline{(g_1-1)(g_2-1)} + \overline{g_1 - 1} + \overline{g_2 - 1} = \varphi(g_1) + \varphi(g_2)$
- $\because$ $IG/(IG)^2$ is abelian as addition $\therefore$ $[G,G] \leq \ker\varphi \rightsquigarrow \overline{\varphi} : G/[G,G] \longrightarrow IG/(IG)^2$
- Define $\begin{array}{rccc} \psi : & IG & \longrightarrow & G/[G,G] \\ & g-1 & \longmapsto & g[G,G] \end{array}$
  Subclaim: $(IG)^2 \subseteq \ker\psi (\rightsquigarrow \overline{\psi} : IG/(IG)^2 \longrightarrow G/[G,G])$
  subproof: $u = (\sum m_i(x_i-1))(\sum n_j(y_j-1)) = \sum m_in_j(x_i-1)(y_j-1) = \sum m_in_j(x_iy_j - 1 + x_i - 1 + y_j - 1) \rightsquigarrow \psi(u) = \prod (x_iy_jx_i^{-1}y_j^{-1})^{m_in_j}[G,G] = 0$
- Finally, $\overline{\varphi}\circ\overline{\psi}, \overline{\psi}\circ\overline{\varphi}$ are identity, so $G/[G,G] \simeq IG/(IG)^2$

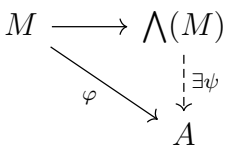
2.5 Koszul complex

When we calculate the Ext or Tor, it is necessary to find a good resolution which is easier to realize the structure and calculate the homology, cohomology.

2.5.1 Wedge product and Koszul complex

Assume R : **commutative with char**$R \neq 2$ **and** $M \in \mathfrak{M}_R$
Goal: To construct a free resolution of R/I.

Definition 2.5.1. Recall that $T^k(M) = M\otimes\cdots\otimes M$ (k times), $T(M) = \bigoplus_{k=0}^{\infty} T^k(M)$

- $A(M) = \langle x\otimes x : x \in M\rangle_{T(M)} \rightsquigarrow A^k(M) := A(M) \cap T^k(M)$ is the submodule of $T^k(M)$ generated by all $x_1\otimes\cdots\otimes x_k$ with $x_i = x_j$ for some distinct i, j.
- $\bigwedge(M) = T(M)/A(M) = \bigoplus_{k=0}^{\infty} \bigwedge^k(M)$
  $\bigwedge^k(M) = T^k(M)/A^k(M) = \langle \overline{x_1\otimes\cdots\otimes x_k} : x_i \in M\rangle$
  denote $\overline{x_1\otimes\cdots\otimes x_k} = x_1\wedge\cdots\wedge x_k$. Notice that $(x_1+x_2)\wedge(x_1+x_2)$ and thus
  $$x_1\wedge x_1 + w_1\wedge x_2 + w_2\wedge x_1 + w_2\wedge x_2 = 0 \implies x_1\wedge x_2 = -x_2\wedge x_1$$
  which is satisfy concept of notation of differential form.
- $f : M\times\cdots\times M \to L$ is an **alternating** k-mutilinear map if $f(x_1,...,x_m) = 0$ $\forall x_i \in M$ with $x_i = x_j$ for distinct i, j.
- Universal property : If A is an R-algebra with $a^2 = 0$ $\forall a \in A$, and $\varphi : M \to A$ is a R-module homomorphism. Then there exists a unique R-algebra homomorphism ψ such that
  

  commute.

Goal: Let $f : M \to R$ be an R-module homomorphism, consider

$$\begin{array}{ccc} M^n & \longrightarrow & \bigwedge^{n-1} M \\ (x_1, ..., x_n) & \longmapsto & \sum_{i=1}^{n} (-1)^{i+1} f(x_i) x_1 \wedge \cdots \wedge \widetilde{x_i} \wedge \cdots \wedge x_n \end{array}$$

which is an alternating. By universal property,

$$\begin{array}{rccc} \exists d_f : & \bigwedge^n M & \longrightarrow & \bigwedge^{n-1} M \\ & x_1 \wedge \cdots \wedge x_n & \longmapsto & \sum_{i=1}^{n} (-1)^{i+1} f(x_i) x_1 \wedge \cdots \wedge \widetilde{x_i} \wedge \cdots \wedge x_n \end{array}$$

By Homework 16, $d_f \circ d_f = 0$. Then we get a **Koszul complex** :

$$K_\bullet(f) : \cdots \longrightarrow \bigwedge^n M \xrightarrow{d_f} \bigwedge^{n-1} M \xrightarrow{d_f} \cdots \xrightarrow{d_f} \bigwedge^2 M \xrightarrow{d_f} \bigwedge M \xrightarrow{f} R \to 0$$

where $f \circ d_f : x \wedge y \mapsto f(x)y - f(y)x \mapsto f(x)f(y) - f(y)f(x) = 0$, so $K_\bullet(f)$ is a complex. Note : $d_f : \bigwedge M \to \bigwedge M$ is graded R-algebra of deg -1.

Definition 2.5.2. Let $(C_\bullet, d), (C'_\bullet, d')$ be two chain complexes of R-modules, then

$$(C_\bullet \otimes C'_\bullet)_n := \bigoplus_{i=0}^{n} (C_i \otimes_R C'_{n-i})$$

and

$$\begin{array}{rccc} d \otimes d' : & (C_\bullet \otimes C'_\bullet)_n & \longrightarrow & (C_\bullet \otimes C'_\bullet)_{n-1} \\ & \sum_{i=0}^{n} x_i \otimes y_{n-i} & \longmapsto & \sum_{i=0}^{n} dx_i \otimes y_{n-i} + (-1)^i x_i \otimes d' y_{n-i} \end{array}$$

$\rightsquigarrow (d \otimes d') \circ (d \otimes d') = 0$

- Let $M_1, M_2 \in \mathfrak{M}_R$, $f_1 \in \mathrm{Hom}_R(M_1, R)$, $f_2 \in \mathrm{Hom}_R(M_2, R)$. Define $f = f_1 + f_2 : M_1 \oplus M_2 \to R$ with $(x, y) \mapsto f_1(x) + f_2(y)$. Then

  $$K_\bullet(f_1) \otimes K_\bullet(f_2) \simeq K_\bullet(f)$$

  and

  $$\bigoplus_{i=0}^{n} \left(\bigwedge^i M_1 \otimes \bigwedge^{n-i} M_2 \right) \simeq \bigwedge^n (M_1 \oplus M_2)$$

  Actually, $(\bigwedge^i M_1) \wedge (\bigwedge^{n-i} M_2) \simeq \bigwedge^i M_1 \otimes \bigwedge^{n-i} M_2$, since M_1, M_2 haven't common non-zero element. And

  $$(d_{f_1} \otimes d_{f_2})(x \otimes y) = d_{f_1}(x) \otimes y + (-1)^{\deg x} x \otimes d_{f_2}(y)$$

  We will check in Homework 16 that $d_{f_1} \otimes d_{f_2} = d_f$ under the above isomorphism.

- Let $M = Re_1 \oplus \cdots \oplus Re_n$ be free R-module and $\underline{x} = x_1, \cdots, x_n$ with $x_i \in R \ \forall i = 1, ..., n$. We associate $(M, \underline{x})$ with $f : M \to R$, $e_i \mapsto x_i$. Let

  $$\begin{array}{rccc} f_i : & Re_i & \longrightarrow & R \\ & e_i & \longmapsto & x_i \end{array}$$

Then $K_\bullet(f) \simeq K_\bullet(f_1) \otimes \cdots \otimes K_\bullet(f_n)$. Consider the Koszul complex for $(\cdot x_i)$

$$\begin{array}{rccccl} K_\bullet(x_i) : 0 \longrightarrow & R & \xrightarrow{\cdot x_i} & R & \longrightarrow 0 \\ & r & \longmapsto & rx_i & \end{array}$$

Then $K_\bullet(\underline{x}) \simeq K_\bullet(x_1) \otimes \cdots \otimes K_\bullet(x_n)$.

Therefore we see a Koszul complex of a free module can be decomposed into n lines.

Property 2.5.1. Let $x \in R$ and $(C_\bullet, \partial)$ be a chain complex of R-modules. Then $\exists$ two chain maps ρ, π s.t.

$$0 \to C_\bullet \xrightarrow{\rho} C_\bullet \otimes K_\bullet(x) \xrightarrow{\pi} C_\bullet(-1) \to 0$$

is exact, where $(C_\bullet(-1))_n = C_{n-1}$

Proof: Since $K_\bullet : 0 \to \underset{1}{R} \underset{\mapsto}{\to} \underset{x}{R}$, $(C_\bullet \otimes K_\bullet(x))_n = (C_n \otimes R) \oplus (C_{n-1} \otimes R)$

$$\begin{array}{rccc} d_n : & (C_n \otimes R) \oplus (C_{n-1} \otimes R) & \longrightarrow & (C_{n-1} \otimes R) \oplus (C_{n-2} \otimes R) \\ & (z_1 \otimes r_1, z_2 \otimes r_2) & \longmapsto & (\partial z_1 \otimes r_1 + (-1)^{n-1} z_2 \otimes r_2 x, \partial z_2 \otimes r_2) \end{array}$$

Under isomorphism $C_n \otimes_R R \simeq C_n$, we get

$$\begin{array}{rccc} d_n : & C_n \oplus C_{n-1} & \longrightarrow & C_{n-1} \oplus C_{n-2} \\ & \begin{pmatrix} r_1 z_1 \\ r_2 z_2 \end{pmatrix} & \longmapsto & \begin{pmatrix} \partial & (-1)^{n-1} x \\ 0 & \partial \end{pmatrix} \begin{pmatrix} r_1 z_1 \\ r_2 z_2 \end{pmatrix} \end{array}$$

Let $\rho_n : C_n \longrightarrow C_n \oplus C_{n-1}$ be inclusion and $\pi_n : C_n \oplus C_{n-1} \longrightarrow C_{n-1}$ be projection. Then

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_n & \xrightarrow{\rho_n} & C_n \oplus C_{n-1} & \xrightarrow{\pi_n} & C_{n-1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle \partial_{n-1}} & & \\ 0 & \longrightarrow & C_{n-1} & \xrightarrow{\rho_{n-1}} & C_{n-1} \oplus C_{n-2} & \xrightarrow{\pi_{n-1}} & C_{n-2} & \longrightarrow & 0 \end{array}$$

is commute. □

Corollary 2.5.1. This induces a long exact sequence :

$$\cdots \to H_n(C_\bullet) \xrightarrow{\rho_*} H_n(C_\bullet \otimes K_\bullet(x)) \xrightarrow{\pi_*} H_n(C_\bullet(-1)) \xrightarrow{(-1)^{n-1}x} H_{n-1}(C_\bullet) \to \cdots$$

For the map $\pm x$: Given $z \in C_{n-1}$ with $\partial(z) = 0$

$$z \xrightarrow{\pi^{-1}} (0, z) \xrightarrow{d} ((-1)^{n-1} xz, 0) \xrightarrow{\rho^{-1}} (-1)^{n-1} xz$$

Definition 2.5.3. x is $C_\bullet$-regular if x is not a zero divisor of C_n $\forall n$ and $C_n / xC_n \neq 0$ $\forall n$.

Property 2.5.2. If x is $C_\bullet$-regular, then $H_n(C_\bullet \otimes K_\bullet(x)) \simeq H_n(C_\bullet / xC_\bullet)$ $\forall n \geq 0$.

Proof: Let

$$\begin{array}{ccc} \phi_n : C_n \oplus C_{n-1} & \longrightarrow & C_n/xC_n \\ (z_1, z_2) & \longmapsto & \overline{z_1} \end{array}$$

Then

$$\begin{array}{ccc} C_n \oplus C_{n-1} & \longrightarrow & C_n/xC_n \\ {\scriptstyle d_n}\downarrow & & \downarrow{\scriptstyle \overline{\partial_n}} \\ C_{n-1} \oplus C_{n-2} & \longrightarrow & C_{n-1}/xC_{n-1} \end{array}$$

will commute $\rightsquigarrow \{\phi_n\}$ is a chain map. Therefore there induce the homomorphism

$$H_n(C_\bullet \otimes K_\bullet(x)) \xrightarrow{\phi_*} H_n(C_\bullet/xC_\bullet) \ \forall n \geq 0$$

- ϕ_* is onto : Given $\overline{z} \in \ker \overline{\partial_n}$ i.e. $\partial(z) \in xC_{n-1}$, say $\partial z = xz'$, where $z' \in C_{n-1}$

  $$d(z, (-1)^n z') = (\partial z + (-1)^{n-1}(-1)^n xz', (-1)^n \partial z') = (0, (-1)^n \partial z')$$

  Since $0 = \partial\partial z = x\partial z' \implies \partial z' = 0$ (x is not zero divisor) $\rightsquigarrow (z, (-1)^n z') \in \ker d$ and $\phi(z, (-1)^n z') = \overline{z}$

- ϕ_* is $1-1$: Let $(z, z') \in \ker d_n$ with $\phi_n(z, z') = \overline{z} \in \operatorname{Im} \overline{\partial_{n+1}} \subseteq C_n/xC_n$, say $\overline{z} = \overline{\partial z''}$ with $z'' \in C_{n+1} \rightsquigarrow z - \partial z'' = xz'''$ for $z''' \in C_n$.

  On the other hand, $0 = d_n(z, z') = (\partial z + (-1)^{n-1} xz, \partial z') \rightsquigarrow \partial z = (-1)^n xz', \partial z' = 0$. Consider $d_{n+1}(z'', (-1)^n z''') = (\partial z'' + xz''', (-1)^n \partial z''') = (z, (-1)^n \partial z''')$.

  $\because z - \partial z'' = xz''' \therefore \partial z = x\partial z'''$ and $\partial z = (-1)^n xz' \implies (-1)^n z' = \partial z'''$, since x is not zero divisor. So $(z, z') = d_{n+1}(z'', (-1)^n z''') \in \operatorname{Im} d_{n+1}$

□

2.5.2 R-regular sequence

Definition 2.5.4. $\{a_1, ..., a_n\} \subset R$ is called an **R-regular sequence** if

- $\langle a_1, ..., a_n \rangle_R \neq R$
- For $i = 0, ..., n-1$, a_{i+1} is not a zero divisor of $R/\langle a_1, ..., a_i \rangle$

Note : Second condition is different to the linearly independent and depends on the order of a_i. For example, $R = k[x, y, z]$, where k is a field. Then $x, y(1-x), z(1-x)$ is regular but $y(1-x), z(1-x), x$ is not.

Theorem 2.5.1. If $\underline{x} = x_1, ..., x_n$ is a R-regular sequence, then $K_\bullet(x)$ is a free resolution of $R/\langle x_1, ..., x_n \rangle$.

Proof: By induction on n : $n = 1 : 0 \to R \xrightarrow{x} R \to R/xR \to 0$. For $n > 1$, we assume that $\underline{x}' = x_1, ..., x_{n-1}$ and

$$K_\bullet(\underline{x}') \to R/\langle x_1, ..., x_{n-1} \rangle \to 0 : \text{exact}$$

i.e. $H_i(K_\bullet(\underline{x}')) = 0\ \forall i > 0$. We have $K_\bullet(\underline{x}) = K_\bullet(\underline{x}') \otimes K_\bullet(x_n)$ and $\forall i > 1$

$$\cdots \to H_i(K_\bullet(\underline{x}')) \to H_i(K_\bullet(\underline{x})) \to H_i(K_\bullet(\underline{x}')(-1)) \xrightarrow{(-1)^{i-1}x_i} H_{i-1}(K_\bullet(\underline{x}')) \to \cdots$$

By induction hypothesis, $H_i(K_\bullet(\underline{x}')) = 0$ and $H_i(K_\bullet(\underline{x}')(-1)) = H_{i-1}(K_\bullet(\underline{x}')) = 0$, so $H_i(K_\bullet(\underline{x})) = 0\ \forall i > 1$. For $i = 1$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_1(K_\bullet(\underline{x})) & \longrightarrow & H_0(K_\bullet(\underline{x}')) & \xrightarrow[1-1]{x_1} & H_0(K_\bullet(\underline{x}')) \\ & & & & \| \wr & & \| \wr \\ & & & & R/\langle x_1, ..., x_{n-1}\rangle & & R/\langle x_1, ..., x_{n-1}\rangle \end{array}$$

Hence, $H_1(K_\bullet(\underline{x})) = 0$. □

2.6 Extensions of abelian groups

Definition 2.6.1. Let $M \lhd E$ and $G \simeq E/M$. We call E an extension of M by G and denoted by $1 \to M \to E \to G \to 1$.

Note: We will using addition for some times and we will replace 1 by 0.
Goal: When M and G are given, try to obtain all extensions of M by G, where we assume M : abelian, G : arbitrary.

Definition 2.6.2. ℓ is called a **lifting** of p if $\ell(1) = 1$ and

$$1 \longrightarrow M \longrightarrow E \underset{\ell}{\overset{p}{\rightleftarrows}} G \longrightarrow 1$$

such that $p \circ \ell = \mathrm{id}_G$. Note : $G \simeq E/M$, $p \circ \ell(\overline{x}) = xM = \ell(\overline{x})M$ and a lifting is an assignment of representative for cosets of M.

Property 2.6.1. For a lifting ℓ,

$$\begin{array}{rccc} \exists\theta : & G & \longrightarrow & \mathrm{Aut}(M) \\ & \overline{x} & \longmapsto & \theta_{\overline{x}} : a \mapsto \ell(\overline{x})a\ell(\overline{x})^{-1} \end{array}$$

is a group homo. ($\rightsquigarrow G \curvearrowright M$) and θ is independent of the choice of ℓ.

Proof:

- For another ℓ', $\because \ell'(\overline{x})M = xM = \ell(\overline{x})M \therefore \ell'(\overline{x}) = \ell(\overline{x})b$ for some $b \in M$. $\forall a \in M$

$$\ell'(\overline{x})a\ell'(\overline{x})^{-1} = \ell(\overline{x})bab^{-1}\ell(\overline{x})^{-1} = \ell(\overline{x})bb^{-1}a\ell(\overline{x})^{-1}$$

- $\theta_{\overline{xy}}(a) = \ell(\overline{xy})a\ell(\overline{xy})^{-1}$, $\theta_{\overline{x}} \circ \theta_{\overline{y}}(a) = \ell(\overline{x})\ell(\overline{y})a\ell(\overline{y})^{-1}\ell(\overline{x})^{-1}$.
  $p(\ell(\overline{xy})) = p(\ell(\overline{x}))p(\ell(\overline{y})) = xy \therefore \ell(\overline{x})\ell(y)$ is a lifting of $\overline{xy}$ so $\ell_{\overline{xy}} = \theta_{\overline{x}} \circ \theta_{\overline{y}}$.

□

Definition 2.6.3. $1 \to M \to E \to G \to 1$ splits if $\exists$ a lifting $\ell : G \to E$ is a group homomorphism.

Definition 2.6.4. $1 \to M \to E \to G \to 1$ is splits $\iff$ $\exists$ a subgroup $K \leq E$ s.t. $K \simeq G$ and $K \cap M = \{1\}, KM = E \rightsquigarrow \varphi : G \to \mathrm{Aut}(M),\ E \simeq M \rtimes_\varphi K$.

Proof: $(\Rightarrow)$: Let $K = \mathrm{Im}\,\ell$ which is a subgroup of E since ℓ is a group homomorphism.

- $\ell : G \twoheadrightarrow K$. If $\ell(\overline{x}) = \ell(\overline{y}) \rightsquigarrow p(\ell(\overline{x})) = p(\ell(\overline{y})) \rightsquigarrow \overline{x} = \overline{y}$ so $\ell : G \simeq K$
- $E = KM : \forall x \in E, \ell(p(x)) = y \in K \rightsquigarrow p\ell(p(x)) = p(y) \rightsquigarrow y^{-1}x \in \ker p = M$
- $K \cap M = \{1\} : a = \ell(\overline{x}) \in K \cap M \rightsquigarrow 1 = p(a) = p(\ell(\overline{x})) = x \rightsquigarrow a = \ell(\overline{1}) = 1$

  $(\Leftarrow)$:
- $p|_K : K \to G$ is a isomorphism :
  - Onto : $p(K) = p(KM) = p(E) = G$
  - 1-1 : $\ker(p|_K) = M \cap K = \{1\}$
- $\ell := (p|_K)^{-1}$ is a lifting and also is a group homomorphism.

□

Observation: Given $1 \to M \to E \to G \to 1$ for $\overline{x}, \overline{y} \in G$,

$$p(\ell(\overline{xy})) = xy,\ p(\ell(x)\ell(y)) = xy$$

Then $M\ell(\overline{x})\ell(\overline{y}) = M\ell(\overline{xy}) \rightsquigarrow \exists f(x,y) \in M$ s.t. $\ell(\overline{x})\ell(\overline{y}) = f(\overline{x},\overline{y})\ell(\overline{xy})$. Then $f : G \times G \to M$ is called the **obstruction of** ℓ being a group homomorphism.

Property 2.6.2.

- $\forall \overline{x}, \overline{y} \in G,\ f(\overline{x},\overline{1}) = f(\overline{1},\overline{y}) = 1$
  $pf.\ \ell(\overline{1})\ell(\overline{y}) = f(1,\overline{y})\ell(\overline{y}) \rightsquigarrow \ell(\overline{1},\overline{y}) = 1$
- (**Cocycle identity**) By associativity, $\forall \overline{x}, \overline{y}, \overline{z} \in G$
  $(\ell(\overline{x})\ell(\overline{y}))\ell(\overline{z}) = f(\overline{x},\overline{y})\ell(\overline{xy})\ell(z) = f(\overline{x},\overline{y})f(\overline{xy},\overline{z})\ell(\overline{xyz})$
  $\ell(\overline{x})(\ell(\overline{y})\ell(\overline{z})) = \ell(\overline{x})f(\overline{x},\overline{y})\ell(\overline{xy}) = \ell(\overline{x})f(\overline{y},\overline{z})\ell(\overline{x})^{-1}\ell(\overline{x})\ell(\overline{yz}) = \theta_{\overline{x}}(f(\overline{y},\overline{z}))f(\overline{x},\overline{yz})\ell(\overline{xyz})$.
  Hence,
  $$f(\overline{x},\overline{y})f(\overline{xy},\overline{z}) = \theta_{\overline{x}}(f(\overline{y},\overline{z}))f(\overline{x},\overline{yz})$$
  and the additive version
  $$f(\overline{x},\overline{y}) + f(\overline{xy},\overline{z}) = \overline{x}\cdot f(\overline{y},\overline{z}) + f(\overline{x},\overline{yz})$$
  where $\cdot$ is a kind of group action $(G \curvearrowright M)$.

The function $f : G \times G \to M$ satisfy above property is called a **factor set w.r.t.** ℓ.

Theorem 2.6.1. Let $\sigma : \underset{x}{G} \underset{\mapsto}{\to} \underset{\sigma_x}{\operatorname{Aut} M}$ be a group homomorphism and $f : G \times G \to M$ satisfy two condition in Property 2.6.2. Then $\exists 1 \to M \to E \to G \to 1$ and $\ell : G \to E$ be a lifting s.t. $\theta = \sigma$ and f is corresponding factor set w.r.t. ℓ.

Proof:

- Define $E(M, G, f, \sigma) =: E := M \times G$ equipped with the operation

$$(a, x)(b, y) = (a\sigma_x(b)f(x, y), xy) \quad (\text{Note:} f = 1 \rightsquigarrow E = M \rtimes_\varphi G)$$

  - associativity :

$$((a, x)(b, y))(c, z) = (a\sigma_x(b)f(x, y), xy)(c, z) = (a\sigma_x(b)f(x, y)\sigma_{xy}(c)f(xy, z), xyz)$$

$$\begin{aligned}(a, x)((b, y)(c, z)) &= (a, x)(b\sigma_y(c)f(y, z), yz) = (a\sigma_x(b\sigma_y(c)f(y, z))f(x, yz), xyz) \\ &= (a\sigma_x(b)\sigma_{xy}(c)\sigma_x(f(y, z))f(x, yz), xyz)\end{aligned}$$

  - identity : $(1, 1)$
  - $(a, x)^{-1} : (a, x)(\sigma_{x^{-1}}(a^{-1}f(x, x^{-1})^{-1}), x^{-1}) = (a\sigma_x(\sigma_{x^{-1}}(a^{-1}f(x, x^{-1})^{-1}))f(x, x^{-1}), 1) = (1, 1)$
  - $p : \begin{array}{ccc} E & \longrightarrow & G \\ (a, x) & \longmapsto & x \end{array}$ is a group homomorphism.
  - $i : \begin{array}{ccc} M & \longrightarrow & E \\ a & \longmapsto & (a, 1) \end{array}$ is a group homomorphism.

    $(a, 1)(b, 1) = (a\sigma_1(b)f(1, 1), 1) = (ab, 1)$

- $\ker p = \operatorname{Im} i$
- Let $\ell : \begin{array}{ccc} G & \longrightarrow & E \\ x & \longmapsto & (1, x) \end{array}$ be a lifting. For $a \in M, x \in G$,

$$\begin{aligned}\theta_x(a) &= \ell(x)(a, 1)\ell(x)^{-1} = (1, x)(a, 1)(\sigma_{x^{-1}}(f(x, x^{-1})^{-1}), x^{-1}) \\ &= (\sigma_x(a)f(x, 1), x)(\sigma_{x^{-1}}(f(x, x^{-1})^{-1}), x^{-1}) \\ &= (\sigma_x(a)\sigma_x(\sigma_{x^{-1}}(f(x, x^{-1})^{-1})f(x, x^{-1}), 1) = (\sigma_x(a), 1)\end{aligned}$$

- $\ell(x)\ell(y)\ell(xy)^{-1} = f(x, y)$

$$\begin{aligned}\ell(x)\ell(y)\ell(xy)^{-1} &= (1, x)(1, y)(\sigma_{(xy)^{-1}}(f(xy, (xy)^{-1})^{-1}), (xy)^{-1}) \\ &= (f(x, y), xy)(\sigma_{(xy)^{-1}}(f(xy, (xy)^{-1})^{-1}), (xy)^{-1}) \\ &= (f(x, y)\sigma_{xy}(\sigma_{(xy)^{-1}}(f(xy, (xy)^{-1})^{-1}))f(xy, (xy)^{-1}), 1) \\ &= (f(x, y), 1)\end{aligned}$$

□

Observation: Let $1 \to M \to E \xrightarrow{p} G \to 1$ and $\ell : G \to E$ be a lifting, then θ is independent of ℓ and f depends on ℓ. Since $E = \bigsqcup_{x \in G} M\ell(\overline{x})$, construct

$$\begin{array}{rccc} \varphi : & E & \longrightarrow & E(M, G, f, \theta) \\ & a\ell(\overline{x}) & \longmapsto & (a, \overline{x}) \end{array}$$

Then

$$\varphi((a\ell(\overline{x}))(b\ell(\overline{y}))) = \varphi(a\theta_{\overline{x}}(b)f(\overline{x}, \overline{y})\ell(\overline{xy})) = (a\theta_{\overline{x}}(b)f(\overline{x}, \overline{y}), \overline{xy})$$
$$\varphi(a\ell(\overline{x}))\varphi(b\ell(y)) = (a, \overline{x})(b, \overline{y}) = (a\theta_{\overline{x}}(b)f(\overline{x}, \overline{y}), \overline{xy})$$

So φ is group homomorphism and it clear that is isomorphism.

Definition 2.6.5. Two extensions are **equivalent** if $\exists \varphi$ s.t.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & {\scriptstyle 1_M}\downarrow & & {\scriptstyle \wr}\downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 1 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Theorem 2.6.2.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & {\scriptstyle 1_M}\downarrow & & {\scriptstyle \wr}\downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 1 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

are equivalent $\iff$ They associate the same action $\theta : G \to \mathrm{Aut}(M)$ and $\exists$ liftings $\begin{cases} \ell : G \to E \\ \ell' : G \to E' \end{cases}$ s.t. $\exists h : G \to M$ with $h(1) = 1$ and

$$f'(\overline{x}, \overline{y})f(\overline{x}, \overline{y})^{-1} = \theta_{\overline{x}}(h(\overline{y}))h(\overline{xy})^{-1}h(\overline{x})$$

Proof: $(\Rightarrow)$: Choose a lifting $\ell : G \to E$ and $\ell' = \varphi \circ \ell$

- $\forall a \in M$,

$$\begin{aligned} \ell'(\overline{x})a\ell'(\overline{x})^{-1} &= \varphi(\ell(\overline{x}))a(\varphi \circ \ell(\overline{x}))^{-1} = \varphi(\ell(\overline{x}))\varphi(a)\varphi(\ell^{-1}(\overline{x})) \\ &= \varphi(\underbrace{\ell(\overline{x})a\ell^{-1}(\overline{x})}_{\in M}) = \ell(\overline{x})a\ell^{-1}(\overline{x}) \end{aligned}$$

-

$$\begin{aligned} f'(\overline{x}, \overline{y})f(\overline{x}, \overline{y})^{-1} &= \ell'(\overline{x})\ell'(\overline{y})\ell'(\overline{xy})f(\overline{x}, \overline{y})^{-1} \\ &= \varphi(\ell(\overline{x}))\varphi\ell(\overline{y})\varphi(\ell(\overline{xy}^{-1})f(\overline{x}, \overline{y})^{-1} \\ &= \varphi(\underbrace{f(\overline{x}, \overline{y})}_{\in M})f(\overline{x}, \overline{y})^{-1} = 1 \end{aligned}$$

Let $h = 1$ and get the result.

- By observation

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \wr\varphi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & M & \longrightarrow & E(M,G,f,\theta) & \longrightarrow & G & \longrightarrow & 1 \end{array} \qquad \begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \wr\varphi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & M & \longrightarrow & E(M,G,f',\theta) & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

  Define

$$\begin{array}{rccc} \overline{\varphi}: & E(M,G,f',\theta) & \longrightarrow & E(M,G,f,\theta) \\ & (a,\overline{x}) & \longmapsto & (ah(\overline{x}),\overline{x}) \end{array}$$

  - $\overline{\varphi}$ is a group homomorphism :

$$\overline{\varphi}((a,\overline{x})(b,\overline{y})) = \varphi(a\theta_{\overline{x}}(b)f'(\overline{x},\overline{y}),\overline{xy}) = (a\theta_{\overline{x}}(b)f'(\overline{x},\overline{y})h(\overline{xy}),\overline{xy})$$

$$\overline{\varphi}(a,\overline{x})\overline{\varphi}(b,\overline{y}) = (ah(\overline{x}),x)(bh(\overline{y}),\overline{y}) = (ah(\overline{x})\theta_x(bh(\overline{y}))f(\overline{x},\overline{y}),\overline{xy})$$

    Since M is abelian and $f'(\overline{x},\overline{y})f(\overline{x},\overline{y})^{-1} = \theta_{\overline{x}}(h(\overline{y}))h(\overline{xy})^{-1}h(\overline{x})$, we have $\overline{\varphi}$ is homomorphism.
  - $1-1 : (ah(\overline{x}),\overline{x}) = (1,1) \rightsquigarrow \overline{x} = 1 \rightsquigarrow a = 1$
  - Onto : $E(M,G,f',\theta) = \bigcup_{x\in G} M\ell'(\overline{x}) \rightsquigarrow \overline{\varphi}(E(M,G,f',\theta)) = \bigcup_{x\in G} Mh(\overline{x})\ell(\overline{x}) = \bigcup_{x\in G} M\ell(\overline{x}) = E(M,G,f,\theta)$

□

Definition 2.6.6.

- $e(G,M) :=$ equivalence classes of extensions of M by G
- $Z^2(G,M) :=$ the abelian group of all factor sets $f : G\times G \to M$ satisfies $f(\overline{x},\overline{1}) = f(\overline{1},\overline{y}) = 1$ and cocycle identity.
- $B^2(G,M) :=$ the abelian group of all functions $f : G\times G \to M$ such that $\exists h : G \to M$ with $h(1) = 1$ and

$$f(x,y) = \sigma_x(h(y))h(xy)^{-1}h(x)$$

Then by Homework 17, $B^2(G,M) \le Z^2(G,M)$ and thus

$$Z^2(G,M)\Big/B^2(G,M) \simeq e(G,M)$$

2.7 $H^2(G,M)$ and $H^1(G,M)$

Recall:The normalized bar resolution of $\mathbb{Z}$:

$$\cdots \to B_3^* \xrightarrow{d_3^*} B_2^* \xrightarrow{d_2^*} B_1^* \xrightarrow{d_1^*} B_0^* \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

$$\rightsquigarrow 0 \to \mathrm{Hom}(B_0^*,M) \xrightarrow{\overline{d_1^*}} \mathrm{Hom}(B_1^*,M) \xrightarrow{\overline{d_2^*}} \mathrm{Hom}(B_2^*,M) \xrightarrow{\overline{d_3^*}} \mathrm{Hom}(B_3^*,M) \to \cdots$$

Observation: As we fix $G \overset{\sigma}{\curvearrowright} M$

- $f \in \ker \overline{d_3^*}$
  - $f : B_2/U_2 \to M \rightsquigarrow f([x|1]) = f([1|y]) = 0$
  - $f \circ d_3 = 0 \rightsquigarrow 0 = f \circ d_3([x|y|z]) = f(x[y|z] - [xy|z] + [x|yz] - [x|y]) = xf([y|z]) - f([xy|z]) + f([x|yz]) - f(x|y)$

  Consider the corresponding $f([x|y]) \longleftrightarrow f(x,y)$, then f is satisfy the condition of factor set. Hence, $\ker \overline{d_3^*} = Z^2(G,M)$.

- $g \in \operatorname{Im} \overline{d_2^*} \rightsquigarrow g = h \circ d_2^*$
  - $g([x|y]) = h \circ d_2([x|y]) = h(x[y] - [xy] + [x]) = xh([y]) - h([xy]) + h([x])$
  - $h : B_1/U_1 \to M \rightsquigarrow h([1]) = 1$

  Hence, $\operatorname{Im} \overline{d_2^*} = B^2(G,M)$

- Hence, $H^2(G,M) \simeq Z^2(G,M) \Big/ B^2(G,M) \simeq e(G,M)$

$$\begin{array}{ccc} Z^2(G,M)/B^2(G,M) & \longleftrightarrow & e(G,M) \\ \overline{f} & \longmapsto & [1 \to M \to E(M,G,f,\sigma) \to G \to 1] \\ \overline{f} & \longleftarrow\!\shortmid & [\ 1 \longrightarrow M \longrightarrow E \underset{\ell \rightsquigarrow f}{\longrightarrow} G \longrightarrow 1\ ] \\ \overline{0} & \longleftrightarrow & [1 \to M \to M \rtimes_\sigma G \to G \to 1] \end{array}$$

- $f \in \ker \overline{d_2^*}$
  - $f : B/U_1 \to M \rightsquigarrow f(1) = 0$
  - $f \circ d_2 = 0 \rightsquigarrow 0 = f \circ d_2([x|y]) = f(x[y] - [xy] + [x]) \rightsquigarrow f([xy]) = xf([y]) + f([x])$

  i.e. $f : G \to M$ satisfies

  (1) $f(1) = 0$

  (2) $f(xy) = xf(y) + f(x) = xf(y) + f(x)y$, where $M \curvearrowleft G$ trivially.

  and called f is a **derivation** and denote $\operatorname{Der}(G,M)$ is a group of all derivation $f : G \to M$.

- $g \in \operatorname{Im} \overline{d_1^*}$
  - $g = h \circ d_1 \rightsquigarrow h([\,]) = a_0 \in M$
  - $g[x] = h \circ d_1([x]) = h(x[\,] - [\,]) = xa_0 - a_0$

  and called g is a **principle derivation** and denote $\operatorname{PDer}(G,M)$ is a group of all principle derivation $f : G \to M$.

- $H^1(G,M) \simeq \operatorname{Der}(G,M) \Big/ \operatorname{PDer}(G,M)$

Definition 2.7.1.

- $\varphi \in \mathrm{Aut}(E)$ is **stabilizes** $1 \to M \to E \to G \to 1$ if

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

  commute.

- $\mathrm{Stab}_E(G,M) = \{\text{stabilizing automorphism}\} \leq \mathrm{Aut}(E)$

Theorem 2.7.1. Let $1 \to M \to E \xrightarrow{p} G \to 1$ and $\ell : G \to E$ be a lifting. Then $\forall \varphi \in \mathrm{Stab}_E(G,M)$, $\exists d : G \to M$ s.t. $\varphi(a\ell(x)) = ad(x)\ell(x)$ $\forall a \in M, x \in G$ and d is independent of the choice of ℓ and $d(xy) = xd(y) + d(x)$ $\forall x, y \in G$.
Conversely, such d defines an $\varphi \in \mathrm{Stab}_E(G,M)$.

Proof:

- By diagram chasing,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \xrightarrow{a\mapsto a} & E & \xrightarrow{\ell(x)\mapsto x} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 1 & \longrightarrow & M & \xrightarrow[a\mapsto a]{} & E & \xrightarrow[\varphi(\ell(x))\mapsto x]{} & G & \longrightarrow & 1 \end{array}$$

  we have $\varphi(a) = a$ $\forall a \in M$, $M\ell(x) = M\varphi(\ell(x)) \rightsquigarrow \varphi(\ell(x)) = d(x)\ell(x)$ for some $d(x) \in M$. Hence, $\varphi(a\ell(x)) = ad(x)\ell(x)$.

- For another $\ell' : G \to E$, say $\ell'(x) = g(x)\ell(x)$ for some $g(x) \in M$. Then

$$\begin{aligned} d'(x) = \varphi(\ell'(x))\ell'(x)^{-1} &= \varphi(g(x)\ell(x))(g(x)\ell(x))^{-1} \\ &= g(x)d(x)\ell(x)\ell^{-1}(x)g(x)^{-1} = d(x) \end{aligned}$$

  Since $g(x), d(x), g(x)^{-1} \in M$ and M is abelian.

- Check $d : G \to M$ is derivation :

$$\begin{aligned} d(xy) &= \varphi(\ell(xy))\ell(xy)^{-1} = \varphi(f(x,y)^{-1}\ell(x)\ell(y))(f(x,y)^{-1}\ell(x)\ell(y))^{-1} \\ &= f(x,y)^{-1}d(x)\ell(x)d(y)\ell(y)\ell(y)^{-1}\ell(x)^{-1}f(x,y) \\ &= f(x,y)^{-1}d(x)(x \cdot d(y))f(x,y) = d(x)(x \cdot d(y)) \end{aligned}$$

  In additive version : $d(xy) = d(x) + xd(y)$

- Conversely, define $\varphi(a\ell(x)) = ad(x)\ell(x)$ $\forall a \in M, x \in G$ and well define by $E = \bigcup_{x \in G} M\ell(x)$.

  - In additive version, $d(1) = 1 \cdot d(1) + d(1) \rightsquigarrow d(1) = 0$, in multiplicative version, $d(1) = 1$.

- $\forall a \in M,\ \varphi(a) = \varphi(a\ell(1)) = ad(1)\ell(1) = a$
- $p(\varphi(a\ell(x))) = p(ad(x)\ell(x)) = p(a\ell(x))$
- Check $\varphi \in \mathrm{Aut}(E)$:

$$\begin{aligned}\varphi((a\ell(x))(b\ell(y))) &= \varphi(a(x\cdot b)f(x,y)\ell(xy)) = a(x\cdot b)f(x,y)d(xy)\ell(xy)\\ \varphi(a\ell(x))\varphi(b\ell(y)) &= (ad(x)\ell(x))(bd(y)\ell(y)) = ad(x)(x\cdot bd(y))f(x,y)\ell(xy)\\ &= ad(x)(x\cdot b)(x\cdot d(y))f(x,y)\ell(xy)\end{aligned}$$

By $d(xy) = xd(y)+d(x)$ and M is abelian, $\varphi((a\ell(x))(b\ell(y))) = \varphi(a\ell(x))\varphi(b\ell(y))$

Hence, $\varphi \in \mathrm{Stab}_E(G, M)$.

□

Definition 2.7.2.

$$\mathrm{Inn}_E(G,M) = \left\{\varphi \in \mathrm{Stab}_E(G,M) \middle| \varphi : \begin{array}{ccc} E & \longrightarrow & E \\ z & \longmapsto & a_0 z a_0^{-1} \end{array} \text{ for some } a_0 \in M\right\}$$

Remark 2.7.1. Let $\varphi \in \mathrm{Inn}_E(G,M)$, say $\varphi(z) = a_0 z a_0^{-1}$ with $a_0 \in M$

$$\varphi(\ell(x)) = d(x)\ell(x) \rightsquigarrow d(x) = a_0\ell(x)a_0^{-1}\ell(x)^{-1} = a_0(x\cdot(a_0^{-1}))$$

In additive version : $d(x) = a_0 - xa_0$

Theorem 2.7.2. $H^1(G,M) \simeq \mathrm{Stab}_E(G,M)\Big/\mathrm{Inn}_E(G,M)$ (Similar to Theorem 2.7.1)

Theorem 2.7.3. Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K) \rightsquigarrow G \curvearrowright L^\times$. Then $H^1(G, L^\times) = 0$

Proof: Let $d : G \to L^\times$ be a derivation i.e. $d(\sigma\tau) = (\sigma d(\tau))d(\sigma)$
Claim: $\exists b \in L^\times$ s.t. $d(\sigma) = b(\sigma(b))^{-1}$ ($\rightsquigarrow d$ is principle)
pf. By linear independent of automorphism $\exists c \in L^\times$ s.t.

$$b = \sum_{\tau\in G} d(\tau)\tau(c) \neq 0 \rightsquigarrow b \in L^\times$$

$$\forall\sigma \in G,\ \sigma(b) = \sum_{\tau\in G}\sigma(d(\tau))(\sigma(\tau(c))) = \sum_{\tau\in G} d(\sigma\tau)d(\sigma)^{-1}((\sigma\tau)(c)) = d(\sigma)^{-1}b$$

□

2.8 Applications

G : **a finite group,** M : **abelian,** $G \curvearrowright M$

Definition 2.8.1. The norm map define by

$$\mathrm{N} : \begin{array}{ccc} M & \longrightarrow & M \\ a & \longmapsto & N(a) = \sum_{x\in G} x\cdot a \end{array}$$

Observation:

$$\forall y \in G \begin{cases} y\,\mathrm{N}(a) = \sum_{x\in G}(yx)a = \mathrm{N}(a) \rightsquigarrow \mathrm{Im}\,\mathrm{N} \subseteq M^G \\ (y-1)\cdot a \in IGM \text{ and } \mathrm{N}((y-1)a) = \mathrm{N}(ya) - \mathrm{N}(a) = 0 \rightsquigarrow IGM \subseteq \ker \mathrm{N} \end{cases}$$

- Let $M = \mathbb{Z}[G]$, recall $\mathbb{Z}[G]^G = \mathbb{Z}\cdot\left(\sum_{x\in G} x\right)$ and denote $N = \sum_{x\in G} x \in \mathbb{Z}[G]$
  - $\mathrm{Im}\,\mathrm{N} = \mathbb{Z}[G]^G = \mathbb{Z}N$:
    $(\supseteq) : \forall a \in \mathbb{Z}[G]^G = \mathbb{Z}N$, say $a = nN = \sum_{x\in G} nx = \sum_{x\in G} n(x\cdot 1_G) = \sum_{x\in G} x(n\cdot 1_G) = \mathrm{N}(n\cdot 1_G) \in \mathrm{Im}\,\mathrm{N}$
  - $IGM = \ker \mathrm{N}$:
    $(\supseteq) : 0 = \mathrm{N}(\sum_{x\in G} n_x x) = \sum_{x\in G} n_x\,\mathrm{N}(x) = \left(\sum_{x\in G} n_x\right) N \rightsquigarrow \sum_{x\in G} n_x = 0$ i.e. $\sum_{x\in G} n_x x \in IGM$.

  Hence, $0 \to IG \xrightarrow{i} \mathbb{Z}[G] \xrightarrow{\mathrm{N}} \mathbb{Z}N \to 0$
- $G = C_n = \langle\sigma\rangle$ with $o(\sigma) = n \rightsquigarrow N = 1 + \sigma + \cdots + \sigma^{n-1}$ and $(\sigma-1)N = \sigma^n - 1 = 0 \rightsquigarrow \mathrm{Im}\,\mathrm{N} \subseteq \ker(\sigma-1)$.

Property 2.8.1. $0 \to \mathbb{Z}\cdot N \xrightarrow{i} \mathbb{Z}[C_n] \xrightarrow{\sigma-1} IC_n \to 0$ is exact.

Proof:

- $(\sigma-1)N = 0 \rightsquigarrow \mathrm{Im}\,i \subseteq \ker(\sigma-1)$
- $a \in \ker(\sigma-1) \rightsquigarrow (\sigma-1)a = 0 \rightsquigarrow \sigma(a) = a \rightsquigarrow \sigma^i(a) = a\ \forall i = 0,...,n-1$ i.e $a \in \mathbb{Z}[C_n]^{C_n} = \mathbb{Z}N$
- $IC_n = \langle\sigma^i - 1 : i = 1,...,n-1\rangle_{\mathbb{Z}[C_n]}$ and $\sigma^i - 1 = (\sigma-1)(\sigma^{i-1}+\cdots+1) \in \mathrm{Im}(\sigma-1)$.

□

Now, we get two exact sequence, combine them we have

- a periodic $\mathbb{Z}[C_n]$-free resolution of $\mathbb{Z}$

$$\cdots \longrightarrow \mathbb{Z}[C_n] \xrightarrow{\sigma-1} \mathbb{Z}[C_n] \xrightarrow{\mathrm{N}} \mathbb{Z}[C_n] \xrightarrow{\sigma-1} \mathbb{Z}[C_n] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

$$\begin{array}{ccccccccccc} & & & \nearrow_{\sigma-1} & & \nearrow_{\mathrm{N}} & & \nearrow_{\sigma-1} & & & \\ & & IC_n & & \mathbb{Z}\cdot N & & IC_n & & & & \\ & \nearrow & & \searrow & & \nearrow & & \searrow & & & \\ 0 & & & & 0 & & & & 0 & & 0 \end{array}$$

- Let $C_n \curvearrowright M$, take $\cdot \otimes_{\mathbb{Z}[C_n]} M$ functor on above resolution,

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & \mathbb{Z}[C_n]\otimes M & \xrightarrow{(\sigma-1)_*} & \mathbb{Z}[C_n]\otimes M & \xrightarrow{\mathrm{N}_*} & \mathbb{Z}[C_n]\otimes M & \xrightarrow{(\sigma-1)_*} & \mathbb{Z}[C_n]\otimes M & \longrightarrow & 0 \\ & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\ & & M & \xrightarrow{\sigma-1} & M & \xrightarrow{\mathrm{N}} & M & \xrightarrow{\sigma-1} & M & & \end{array}$$

So we get the red exact sequence with natural maps and thus

$H_0(C_n, M) \simeq \mathbb{Z} \otimes_{\mathbb{Z}[C_n]} M \simeq \mathbb{Z}[G]/IC_n \otimes_{\mathbb{Z}[C_n]} M \simeq M/IC_nM =: M_{C_n}$

$H_1(C_n, M) \simeq \ker(\sigma - 1)/\operatorname{Im} \mathrm{N} \simeq M^{C_n}/NM \simeq H_{\text{odd}}(C_n, M)$

$H_2(C_n, M) \simeq \ker \mathrm{N} / \operatorname{Im}(\sigma - 1) \simeq \ker \mathrm{N} /(\sigma - 1)M \simeq H_{\text{even}}(C_n, M)$

- Let $C_n \curvearrowright M$, take $\mathrm{Hom}_{\mathbb{Z}[c_n]}(\cdot, M)$ functor on above resolution,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[c_n]}(\mathbb{Z}[C_n], M) & \xrightarrow{(\sigma-1)^*} & \mathrm{Hom}_{\mathbb{Z}[c_n]}(\mathbb{Z}[C_n], M) & \xrightarrow{\mathrm{N}^*} & \mathrm{Hom}_{\mathbb{Z}[c_n]}(\mathbb{Z}[C_n], M) & \xrightarrow{(\sigma-1)^*} & \cdots \\ & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\ & & M & \xrightarrow{\sigma-1} & M & \xrightarrow{\mathrm{N}} & M & & \end{array}$$

For $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[C_n], M)$, $(\sigma - 1)^*(f) : 1 \mapsto f(\sigma - 1) = (\sigma - 1)f(1)$. So we get the red exact sequence with natural maps and thus

$H^0(C_n, M) = M^{C_n}$

$H^1(C_n, M) = \ker \mathrm{N} / \operatorname{Im}(\sigma - 1) = \ker \mathrm{N} /(\sigma - 1)M \simeq H^{\text{odd}}(C_n, M).$

$H^2(C_n, M) = \ker(\sigma - 1)/ \operatorname{Im} \mathrm{N} = M^{C_n}/NM \simeq H^{\text{even}}(C_n, M)$

Theorem 2.8.1 (Hilbert theorem 90)**.** Let L/K be a cyclic extension with $G = \mathrm{Gal}(L/K) = \langle \sigma \rangle$ and $\sigma^n = 1$. Then

$$N(x) = 1 \iff \exists y \in L^\times \text{ s.t. } x = \sigma y/y$$

Proof: By Theorem 2.7.3 $0 = H^1(C_m, L^\times) = \ker N/ \operatorname{Im}(\sigma - 1) \rightsquigarrow \ker N = \operatorname{Im}(\sigma - 1)$. Then $N(x) = 1 \iff \exists y \in L^\times$ s.t. $x = \sigma y/y$ for some $y \in L^\times$. □

Recall : $\operatorname{Im} \mathrm{N} \subseteq M^G$, $IGM \subseteq \ker \mathrm{N}$, we have

$$\begin{array}{ccccccccc} & & & & M & & & & \\ & & & & \downarrow{\scriptstyle \pi} & \searrow^{\mathrm{N}} & & & \\ 0 & \longrightarrow & \ker \mathrm{N} /IGM & \xrightarrow{i} & M/IGM & \xrightarrow{\overline{\mathrm{N}}} & M^G & \xrightarrow{\pi} & M^G/NM \longrightarrow 0 \\ & & & & \downarrow\wr & & \downarrow\wr & & \\ & & & & H_0(G, M) & \xrightarrow[\mathrm{N}]{} & H^0(G, M) & & \end{array}$$

The blue one is by factor theorem and we get red exact sequence

$$0 \to \ker \mathrm{N} /IGM \to H_0(G, M) \xrightarrow{\mathrm{N}} H^0(G, M) \to M^G/NM \to 0$$

Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be exact in $\mathfrak{M}_{\mathbb{Z}[G]}$, then apply general snake lemma on $(\mathrm{N}, \mathrm{N}, \mathrm{N})$

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & H^1(G, M_3) & \longrightarrow & H_0(G, M_1) & \longrightarrow & H_0(G, M_2) & \longrightarrow & H_0(G, M_3) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \\ & & 0 & \longrightarrow & H^0(G, M_1) & \longrightarrow & H^0(G, M_2) & \longrightarrow & H^0(G, M_3) & \longrightarrow & H^1(G, M_1) \longrightarrow \cdots \end{array}$$

We get

$$\cdots \longrightarrow H_1(G,M_3) \longrightarrow {}^{\ker_{M_1} \mathrm{N}}\!\Big/_{IG\cdot M_1} \longrightarrow {}^{\ker_{M_2} \mathrm{N}}\!\Big/_{IG\cdot M_2} \longrightarrow {}^{\ker_{M_3} \mathrm{N}}\!\Big/_{IG\cdot M_3}$$

pt

$$\longrightarrow {}^{M_1^G}\!\Big/_{NM_1} \longrightarrow {}^{M_2^G}\!\Big/_{NM_2} \longrightarrow {}^{M_3^G}\!\Big/_{NM_3} \longrightarrow H^1(G,M_1) \longrightarrow \cdots$$

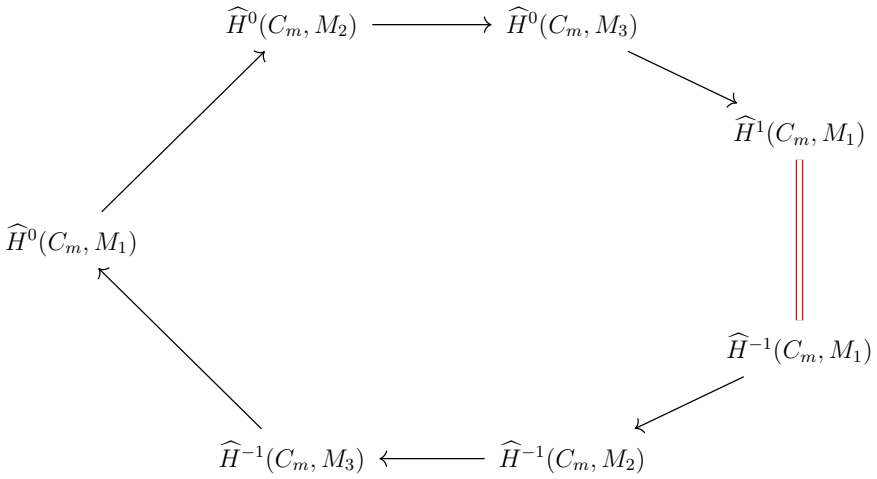
Define **Tate cohomology group** by

$$\widehat{H}^n(G,M) = \begin{cases} H^n(G,M) & , \text{if } n \geq 1 \\ \operatorname{coker} \mathrm{N} = {}^{M^G}\!\Big/_{NM} & , \text{if } n = 0 \\ \ker \mathrm{N} = {}^{\ker_M \mathrm{N}}\!\Big/_{IG\cdot M} & , \text{if } n = -1 \\ H_{-(n+1)}(G,M) & , \text{if } n \leq -2 \end{cases}$$

Then $\forall -\infty < n < \infty$,

$$\cdots \to \widehat{H}^n(G,M_1) \to \widehat{H}^n(G,M_2) \to \widehat{H}^n(G,M_3) \to \widehat{H}^{n+1}(G,M_1) \to \cdots$$

Example 2.8.1. $G \simeq C_n$



For red isomorphism :

$$\widehat{H}^{-1}(C_m,M_1) \simeq {}^{\ker_{M_1} N}\!\Big/_{IC_n\cdot M_1} = {}^{\ker_{M_1} N}\!\Big/_{(\sigma-1)\cdot M_1} \simeq \widehat{H}^1(C_m,M_1)$$

Example 2.8.2. $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{1,a,b,c\},\ M = \mathbb{Z}/2\mathbb{Z}$
Since $\mathrm{Aut}(M) = \{\mathrm{id}\} \implies G \curvearrowright M$ trivially i.e. $ax = x\ \forall a \in G, x \in M$.
Calculate $H^2(G,M)$:
$\mathrm{Hom}_{\mathbb{Z}[G]}(B_2^*, M) = \mathrm{Func}((G\setminus\{1\})^2, M) \rightsquigarrow \# = 2^9$.
If $f \in Z^2(G,M)$, then f must satisfy cocycle identity i.e.

$$f(x,y) + f(xy,z) = xf(y,z) + f(x,yz)\ \forall x \in G\setminus\{1\}.$$

Then

$$f(x,y) + f(xy,z) + f(y,z) + f(x,yz) = 0$$

$x = y : f(x,x) + f(\underset{=1}{x^2}, z) + f(x,z) + f(x,xz) = 0 \rightsquigarrow f(x,a) + f(x,b) + f(x,c) = 0.$
If we fix $f(a,a) = \alpha, f(a,b) = \beta, f(b,a) = \delta, f(b,b) = \varepsilon$. Then other value can be uniquely decided. So $|Z^2(G,M)| \leq 2^4$.
Now, if $f \in B^2(G,M)$, then $\exists h : G \to M$ s.t. $f(x,y) = h(y) - h(xy) + h(x)\ \forall x, y \in G$.
$x = y : f(x,x) = h(x) + h(x^2) + h(x) = 0$
$x \neq y : f(x,y) = h(a) + h(b) + h(c) \rightsquigarrow |B^2(G,M)| = 2$ and thus $|H^2(G,M)| \leq 8$.
In this case, $E \simeq (\mathbb{Z}/2\mathbb{Z})^3, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_4, Q_8$.

- $E \simeq (\mathbb{Z}/2\mathbb{Z})^3$, then $1 \to M \to E \to G \to 1$ splits $\rightsquigarrow f = 0 \in H^2(G,M)$
- $E \simeq \underset{=\langle x \rangle}{\mathbb{Z}/4\mathbb{Z}} \times \underset{=\langle y \rangle}{\mathbb{Z}/2\mathbb{Z}}, M = \langle x^2 \rangle$: Then we have

  $$Mx = \{x, x^3\},\ Mxy = \{xy, x^3y\},\ My = \{y, x^2y\}$$

  with order $4, 4, 2$ respectively. One of $\ell(a), \ell(b), \ell(c)$ has order 2 and others are 4. So we have 3 inequivalent extensions.
- $E \simeq D_4 = \langle x, y : x^4 = y^2 = e, yx = x^{-1}y \rangle,\ M = \langle x^2 \rangle$: Then we have

  $$Mx = \{x, x^3\},\ My = \langle y, x^2y \rangle,\ Mxy = \{xy, x^3y\}$$

  with order $4, 2, 2$ respectively. One of $\ell(a), \ell(b), \ell(c)$ has order 4 and others are 2. So we have 3 inequivalent extensions.
- $E \simeq Q_8,\ M = \langle 1, -1 \rangle$: Then we have

  $$Mi = \langle \pm i \rangle,\ Mj = \langle \pm j \rangle,\ Mk = \langle \pm k \rangle$$

  with order 4. So we have 1 inequivalment extensions.

So $|H^2(G,M)|$ is exactly 8.
Calculate $H^1(G,M) \simeq \mathrm{Der}(G,M) \Big/ \mathrm{PDer}(G,M)$:
If $d \in \mathrm{Der}(G,M) : d(xy) = xd(y) + d(x)y = d(x) + d(y)$ which is group homomorphism.
If $d \in \mathrm{PDer}(G,M) : d(x) = xv - v = v - v = 0$
So $H^1(G,M) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \rightsquigarrow |H^1((G,M)| = 4$

Chapter 3

Representation theory

3.1 Semisimple modules

In this section, A may not be commute and M be a left A-module.

3.1.1 Semisimple modules

Definition 3.1.1. Let A be a ring and M be a left A-module

- M is **simple** if $M \neq 0$ and it has no nontrivial proper submodule.
- M is **semisimple** if $M = \bigoplus_{i \in \Lambda} M_i$ with M_i : simple submodules of M $\forall i$

Lemma 3.1.1 (Schur's lemma)**.** Let M, N be two simple A-modules. Then $\forall 0 \neq f \in \mathrm{Hom}_A(M, N)$, f is an isomorphism, In particular, M : simple $\implies \mathrm{End}_A(M)$ is a division ring. Sometimes we will denote $\mathrm{End}_A(M)$ by $A'(M)$ or A'.

Proof: $\because \ker f \leq M$ and $\mathrm{Im}\, f \leq N$ $\therefore \ker f = 0$ or M and $\mathrm{Im}\, f = 0$ or N. If $\ker f = M$ or $\mathrm{Im}\, f = 0$, then $f = 0$ $(\rightarrow\!\!\!\!\leftarrow)$. So $\ker f = 0$, $\mathrm{Im}\, f = N \rightsquigarrow f$ is isomorphism. □

Property 3.1.1. TFAE

(1) M is semisimple

(2) $\forall\ 0 \neq N \subseteq M$, $\exists N' \leq M$ s.t. $M = N \oplus N'$

(3) $M = \sum_{i \in J} M_i$ with M_i : simple in M.

Proof: Before proof TFAE, we see the key lemma.

Key lemma: If $M = \sum_{i \in J} M_i$ with M_i : simple, then $\exists I \subseteq J$ s.t. $M = \bigoplus_{i \in I} M_i$

pf. Let $\mathcal{S} = \{I' \subseteq J : \sum_{i \in I'} M_i \text{ is direct}\} \neq \varnothing$ and $\{I_i\}_{i \in \Lambda}$ be a chain in $\mathcal{S}$.

Consider $I' = \bigcup_{i \in \Lambda} I_i$ which is lies in $\mathcal{S}$, since if $x \in M_k \cap \left(\bigoplus_{j \in I \setminus \{k\}} M_j \right) \rightsquigarrow x \in$

$M_k \cap \bigoplus_{j\in J'} M_j$ for some finite subsets J' of $I \setminus k$ and $\{k\} \cup J' \subseteq I_i$ for some $i \rightsquigarrow x = 0$.
By Zorn's lemma, $\exists$ a maximal I in $\mathcal{S}$. We claim that $M = \bigoplus_{i\in I} M_i$. For $j \in J \setminus I$, consider $M_j \cap \left(\bigoplus_{i\in I} M_i\right) \leq M_j$. By M_j is simple, $M_j \cap \left(\bigoplus_{i\in I} M_i\right) = 0$ or M_j. For former, $I \subseteq \{j\} \cup I \in \mathcal{S}$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$. For latter, $M_j \subseteq \bigoplus_{i\in I} M_i$. □

Back to origin problem.

- (3) $\Rightarrow$ (1) : By key lemma.
- (1) $\Rightarrow$ (2) : Let $M = \bigoplus_{i\in J} M_i$. Consider

$$\mathcal{S} = \left\{ I' \subseteq J \middle| N + \left(\bigoplus_{i\in I'} M_i\right) \text{ is direct} \right\}.$$

  By Zorn's lemma, $\exists$ a maximal element $I \in \mathcal{S}$. We claim that $M = N \oplus \left(\bigoplus_{i\in I} M_i\right)$.
  $\forall j \in J \setminus I$, $M_j \subseteq$ RHS (by similar reason in above).

- (2) $\Rightarrow$ (3) : First, we prove if M satisfy the assumption, then M contain a simple submodule : Let $0 \neq x \in M$ and $\varphi : A \to Ax \rightsquigarrow \ker\varphi$ is a proper left ideal of A. By Zorn's lemma, $\exists$ a left maximal ideal $\mathfrak{m}$ in A s.t. $\ker\varphi \subseteq \mathfrak{m} \rightsquigarrow \mathfrak{m}x$ is a maximal proper submodule of $Ax \subseteq M$. By assumption, $M = \mathfrak{m}x \oplus M' \rightsquigarrow Ax = \mathfrak{m}x \oplus (M' \cap Ax)$.

  Claim : $M' \cap Ax$ is a simple submodule of M.

  - $\mathfrak{m}x \subsetneq Ax \rightsquigarrow M' \cap Ax \neq 0$
  - If $M' \cap Ax$ has a nontrivial proper submodule N, then $\mathfrak{m}x \subsetneq \mathfrak{m}x \oplus N \subsetneq Ax$

  Let $M_0 = \sum_{M_i\subseteq M}^{\text{simple}} M_i$. If $M \neq M_0$, then $M = M_0 \oplus M_0'$ with $M_0' \neq 0$. Notice that M_0' also satisfy the assumption, so $\exists$ a simple submodule $N \leq M_0'$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$.

□

Theorem 3.1.1. If $M \simeq M_1^{\oplus n_1} \oplus \cdots \oplus M_r^{\oplus n_r} \simeq N_1^{\oplus m_1} \oplus \cdots \oplus N_s^{\oplus m_s}$ with N_i, M_j : simple and $M_i \neq M_j, N_i \neq N_j$ $\forall i \neq j$. Then $r = s$ and $M_i \simeq N_i$ $\forall i$ after rearrangement of indices and $n_i = m_i$.

Proof: Let $f_{ij} : M_i \xhookrightarrow{\rho_i} M \xrightarrow{\pi_j} N_j$. By Schur's lemma, $\forall i$, $f_{ij} = 0$ or isomorphism. For fixed i, if $\forall j$, $f_{ij} = 0 \rightsquigarrow \rho_i : M_i \to M$ is zero map $\forall i \rightsquigarrow M_i = 0$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$. So $\exists!$ j s.t. f_{ij} is isom. and thus $M_i \simeq N_j$ (otherwise $N_{j_1} \simeq M_i \simeq N_{j_2}$ for distinct j_1, j_2.). Thus $r \leq s$. By symmetry, $r = s$. Finally, $M_i^{\oplus n_i} \simeq N_i^{\oplus m_i} \rightsquigarrow n_i = m_i$. □

3.1.2 Matrix form of simple and semisimple modules

Observation:

- $M = N^{\oplus n}$ with N : simple. Let $\varphi \in \mathrm{Hom}_A(M, M)$ and $\rho_i : N \hookrightarrow M, \pi_i : M \to N$ be inclusion from i-th N to M and projection form M to i-th N.

  Define $\varphi_{ij} = \pi_i \circ \varphi \circ \rho_j : N \to N$, then $\varphi_{ij} \in \mathrm{End}_A(N) =: D'$ and for $x = (x_1, ..., x_n) \in M$ with $x_i \in N \ \forall i$

$$\begin{aligned}\varphi(x) &= \varphi\left(\sum_{j=1}^{n} \rho_j(x_j)\right) = \sum_{j=1}^{n} \varphi(\rho_j(x_j)) \\ &= \left(\pi_1\left(\sum_{j=1}^{n} \varphi \circ \rho_j(x_j)\right), \cdots, \pi_n\left(\sum_{j=1}^{n} \varphi \circ \rho_j(x_j)\right)\right)\end{aligned}$$

$$\implies \varphi(x) = \begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n} \\ \varphi_{21} & \ddots & & \cdots \\ \vdots & & & \\ \varphi_{n1} & \varphi_{n2} & \cdots & \varphi_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

  Hence, $\varphi \longleftrightarrow (\varphi_{ij}) \in M_{n\times n}(D')$ and we leave the checking

$$\mathrm{End}_A(M) \simeq M_{n\times n}(D') \text{ as a ring}$$

  in Homework 20.

- $M = N_1^{\oplus m_1} \oplus \cdots \oplus N_r^{\oplus m_r}$: For all $\varphi \in \mathrm{End}_A(M)$, we have the corresponding

$$\varphi \longleftrightarrow \begin{pmatrix} \left(\varphi|_{N_1^{\oplus m_1}}\right) & & & \\ & \left(\varphi|_{N_2^{\oplus m_2}}\right) & & \\ & & \ddots & \\ & & & \left(\varphi|_{N_r^{\oplus m_r}}\right) \end{pmatrix}$$

  where $\left(\varphi|_{N_i^{\oplus m_i}}\right) \in M_{m_i\times m_i}(D_i')$ and $D_i' = \mathrm{End}_A(N_i)$. Notice that others blocks are all zero, for example $(m_1+1, 1)$-entry is $\pi_{m_1+1} \circ \varphi \circ \rho_1 : N_1 \to N_2$ which is not isomorphism and thus is zero map. This give us

$$\mathrm{End}_A(M) \simeq M_{m_1\times m_1}(D_1') \oplus \cdots \oplus M_{m_r\times m_r}(D_r') \text{ as a ring}$$

  which leave it at Homework 20.

- Let M be a semisimple A-module and $A' = \mathrm{End}_A(M)$, consider

$$\begin{array}{ccc} A' \times M & \longrightarrow & M \\ (\varphi, x) & \longmapsto & \varphi(x) \end{array}$$

  So M is an A'-module i.e. M is a module over a division ring.

  Now, consider $\forall a \in A$,

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

- f_a is not always A-homomorphism, since in general the equality will not hold. It need A is commutative.

$$f_a(bx) = (ab)x \neq (ba)x = bf_a(x)$$

- However, f_a is A'-homomorphism

$$f_a(\varphi(x)) = a\varphi(x) = \varphi(ax) = \varphi(f_a(x))$$

So $f_a \in \mathrm{End}_{A'}(M)$ and denote $\mathrm{End}_{A'}(M)$ by A''. This give as a ring homomorphism $A \to A''$, but it will not always a ring isomorphism.

Theorem 3.1.2 (Jacobson theorem)**.** If $M = N_1^{\oplus m_1} \oplus \cdots \oplus N_r^{\oplus m_r}$ with N_i : simple and let $A' = \mathrm{End}_A(M)$. Then

(1) If $f \in A'' = \mathrm{End}_{A'}(M)$ and $x_1, ..., x_n \in M$, then $\exists a \in A$ s.t. $f(x_i) = f_a(x_i)\ \forall i$

(2) If $M = \langle x_1, ..., x_n \rangle_{A'}$, then $\begin{array}{ccc} A & \longrightarrow & A'' \\ a & \longmapsto & f_a \end{array}$

Proof:

(1) First, we prove the cases $n = 1$: Write $M = Ax \oplus M'$, since M is semisimple. Let $\pi : M \to Ax$ be the projection $\rightsquigarrow \pi \in A'$. By $f \in \mathrm{End}_{A'}(M)$, we have

$$f(x) = f(\pi(x)) = \pi(f(x)) \in Ax \rightsquigarrow \exists\ a \in A \text{ s.t. } f(x) = ax$$

For $n > 1$: It's the most trick part, consider

$$\begin{array}{rccc} f^{\oplus n}: & M^{\oplus n} & \longrightarrow & M^{\oplus n} \\ & (y_1, ..., y_n) & \longmapsto & (f(y_1), ..., f(y_n)) \end{array}$$

Then we can write as the matrix version :

$$\begin{pmatrix} f & & \\ & \ddots & \\ & & f \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Notice that we always can write $\mathrm{End}_A(M^{\oplus n})$ as $M_n(A')$.

Claim: $f^{\oplus n} \in \mathrm{End}_{\mathrm{End}_A(M^{\oplus n})}(M^{\oplus n})$

pf. Write it as matrix version. For all $\varphi \in \mathrm{End}_A(M^{\oplus n})$, we can write it as $(\varphi_{ij}) \in M_n(A')$. Then we have

$$(\delta_{ij}f)(\varphi_{ij}) = (f\varphi_{ij}) = (\varphi_{ij}f) = (\varphi_{ij})(\delta_{ij}f).$$

The red equality is from $f \in \mathrm{End}_{A'}(M)$. □

Apply the cases $n = 1$ on $f^{\oplus n}$, let $\overline{x} = (x_1, ..., x_n)$, there $\exists a \in A$ s.t. $f^{\oplus n}(\overline{x}) = a\overline{x}$ i.e. $f(x_i) = ax_i\ \forall i = 1, ..., n$.

(2) Apply (1), $\forall f \in A''\ \exists a \in A$ s.t. $f(x_i) = f_a(x_i)\ \forall i \rightsquigarrow f = f_a$.

□

Theorem 3.1.3 (Wedderburn's theorem)**.** Let M be a simple **faithful** (def : $\mathrm{Ann}(M) = 0$) module over A. Let $D = \mathrm{End}_A(M)$ and M be finite dimensional n over D. Then $A \simeq M_n(D^\circ)$.

Proof: Let $M = \langle x_1, ..., x_n \rangle_D$, by Jacobson theorem,

$$\begin{array}{ccccc} A & \twoheadrightarrow & \mathrm{End}_D(M) & \simeq M_n(\mathrm{End}_D(D)) \simeq M_n(D^\circ) \\ a & \mapsto & f_a & \end{array}$$

Now, if $f_a = f_b$ for some $a, b \in A$, then $ax = bx \ \forall x \in M \rightsquigarrow (a-b) \in \mathrm{Ann}_A(M) \rightsquigarrow a = b$. Hence, $A \simeq M_n(D^\circ)$ □

3.2 Semisimple rings

3.2.1 Semisimple rings

Definition 3.2.1. A ring R is semisimple if $R \neq 0$ and it is semisimple as a left R-module. (or denoted by ${}_RR$)

Property 3.2.1. R is semisimple $\iff \forall M \in {}_R\mathfrak{M}$, M is semisimple.

Proof: ($\Leftarrow$) : OK!

($\Rightarrow$) : R is semisimple $\rightsquigarrow$ any free R-module is semisimple. Since any R-module is a quotient of free R-module and thus it is semisimple. □

Property 3.2.2. Any semisimple ring R is a finite direct sum of minimal left ideals and every simple R-module is isomorphic to one of them. In particular, it is left Artinian and Noetherian.

Proof:

- Let $R = \bigoplus_{i \in \Lambda} I_i$ with I_i : minimal left ideal of $R \ \forall i$,

  $\because 1 \in R \therefore 1 = x_1 + \cdots + x_n$ with $x_k \in I_{i_k} \ \forall k \rightsquigarrow R \subseteq \bigoplus_{k=1}^{n} I_{i_k}$ and thus $R = \bigoplus_{k=1}^{n} I_k$

- Let M be a simple R-module and $0 \neq x \in M \rightsquigarrow M = Rx$. Consider

  $$\varphi : \begin{array}{ccc} R & \longrightarrow & M \\ r & \longmapsto & rx \end{array} \text{ and } \varphi|_{I_{i_k}} : I_{i_k} \longrightarrow M$$

  Then $\varphi|_{I_{i_k}} = 0$ or isomorphism. Since $\varphi \neq 0 \rightsquigarrow \exists k$ s.t. $\varphi|_{I_{i_k}} \neq 0 \rightsquigarrow \varphi|_{I_{i_k}} : I_{i_k} \xrightarrow{\sim} M$

- Let $J_r = \bigoplus_{k=1}^{r} I_k \rightsquigarrow R = J_n \supseteq J_{n-1} \supseteq \cdots \supseteq J_1 \supseteq J_0 = 0$ and $J_k/J_{k-1} \simeq I_k$: simple. So R has a finite composition series $\rightsquigarrow R$ is Artinian and Noetherian.

□

Theorem 3.2.1 (Artin-Wedderburn theorem)**.** A semisimple ring R is a finite direct product of matrix rings over division rings.

Proof: Let $R = I_1 \oplus \cdots \oplus I_n$ with I_i : minimal left ideal of R. Rewrite R as $I_{i_1}^{\oplus s_1} \oplus \cdots \oplus I_{i_t}^{\oplus s_t}$ with $I_{i_p} \not\simeq I_{i_q}$ for distinct p, q. Let $D_j = \mathrm{End}_R(I_{i_j})$, then

$$\mathrm{End}_R({}_RR) \simeq M_{s_1 \times s_1}(D_1) \oplus \cdots \oplus M_{s_t \times s_t}(D_t) \text{ as rings}$$

- Define $f_a : R \to R$ by $1 \mapsto a \rightsquigarrow f_a : r \mapsto ra$. Then $f_a \circ f_b(r) = f_a(rb) = r(ba) \rightsquigarrow \mathrm{End}_R({}_RR) \simeq R^\circ$ and thus

$$R \simeq (R^\circ)^\circ \simeq \bigoplus_{i=1}^{t} (M_{s_i}(D_i))^\circ$$

- $\forall i$ define $\begin{array}{rccc} \psi : & (M_n(D_i))^\circ & \longrightarrow & M_n(D_i^\circ) \\ & A = (a_{ij}) & \longmapsto & A^t = (a'_{ij}) \end{array}$, where $a'_{ij} = a_{ji}$ (In below, we use $\cdot$ represent the opposite multiplication). Then

$$\begin{aligned} \psi(A \cdot B) = \psi(BA) = (BA)^t &= \left(\sum_{k=1}^{n} b_{ik} \cdot a_{kj} \right)^t = \left(\sum_{k=1}^{n} b_{jk} \cdot a_{ki} \right) \\ &= \left(\sum_{k=1}^{n} a_{ki} b_{jk} \right) = \left(\sum_{k=1}^{n} a'_{ik} b'_{kj} \right) = A^t B^t = \psi(A)\psi(B) \end{aligned}$$

  Combine with D_i : division $\rightsquigarrow D_i^\circ$: division, we have

$$R \simeq \bigoplus_{i=1}^{t} M_{s_i}(D_i^\circ)$$

  i.e. R is a finite direct sum of matrix rings over division rings and we will discuss the relation between direct sum and direct product.

□

3.2.2 Product of ring

Before we move forward, We check something about product, so that we can use them freely after.
Observation:

- $R \simeq R_1 \times \cdots \times R_n$ with R_i : ring $\forall i$. Let $I_i \longleftrightarrow (0, ..., 0, R_i, 0, ..., 0)$.
  - I_i is two-sided ideal with $I_i \simeq R_i$ as rings.
  - $I_i I_j = 0$ for all $i \neq j$
  - $R = \sum_{i=1}^{n} I_i = \bigoplus_{i=1}^{n} I_i$ (Note : I_i is a ring but not a subring of R if $n \geq 2$)

- Conversely, if $\exists\{I_i\}_{i\in\Lambda}$ s.t. $\begin{cases} I_i: \text{ two-sided ideal } \forall i \text{ and } R=\sum_{i\in\Lambda} I_i \\ I_iI_j=0 \text{ for all } i\neq j \end{cases}$, then
  - $|\Lambda|=n<\infty$
  - I_i is a ring R_i s.t. $R\simeq R_1\times\cdots\times R_n$

  proof:

  - Let $1=\sum_{i\in\Lambda} e_i$ with $e_i=0$ for almost all i.
    For $x\in I_i$, $x=x\cdot 1=xe_i$. If $e_j=0 \rightsquigarrow I_j=0$ and thus $|\Lambda|=n<\infty$.
  - I_i : two-sided ideal $\rightsquigarrow$ $\begin{cases} I_i \text{ is closed under ``}+,\cdot\text{''} \\ xe_i=e_i\forall x\in I_i \rightsquigarrow e_i \text{ is identity for } I_i \end{cases}$
    $\rightsquigarrow I_i$ is a ring R_i.
  - $R=\sum_{i=1}^n I_i$ is direct : If $x\in I_i\cap\left(\sum_{j\neq i} I_j\right) \rightsquigarrow x=e_ix=0$
  - $R\simeq R_1\times\cdots\times R_n$: Given $x=\sum_{i=1}^n x_i, y=\sum_{i=1}^n y_i \rightsquigarrow xy=\sum_{i=1}^n x_iy_i$, sine $x_iy_j=0$ for $i\neq j$.

- If $R=R_1\times\cdots\times R_n$, then a simple left R-module M is a simple left R_i-module for some i.

  proof:

  - $\sum_{i=1}^n R_iM=\left(\sum_{i=1}^n R_i\right)M=RM=M\neq 0 \rightsquigarrow R_iM\neq 0$ for some i.
    Since $R_iR_j=0$ for $i\neq j$, $R_iM=RR_iM \rightsquigarrow R_iM$ is a left R-submodule of M $\rightsquigarrow R_iM=M \rightsquigarrow R_jM=R_jR_iM=0\ \forall j\neq i$.
  - Let e_j be the identity of R_j $\forall j=1,...,n \rightsquigarrow 1=\sum_{j=1}^n e_j \rightsquigarrow \forall x\in M,\ x=1\cdot x=\sum_{j=1}^n e_jx=e_ix \rightsquigarrow M$ is an R_i-module.
  - M is R_i-simple : If N is an R_i-submodule of M, then $RN=\left(\sum_{j=1}^n R_j\right)N=R_iN=N \rightsquigarrow N$ is an R-submodule of $M \rightsquigarrow N=0$ or M.

- Conversely, M is a simple R_i-module, then by $R_jM=R_jR_iM=0\ \forall j\neq i$, M is a R-module. If N is a R-submodule of M, then $R_iN=\left(\sum_{j=1}^n R_j\right)N=RN\subseteq N$ i.e. N is an R_i-submodule of $M \rightsquigarrow N=0$ or M.

From now on, the concept of direct sum and direct product has a correspondence and we will feel free using those.

3.2.3 Radical

In this subsection, we try to transfer useful properties in commutative algebra to non-commutative algebra. For example : basis property of Jacobson radical and Nakayama's lemma. We leave it in Homework 21 and we will use it unreservedly.

Definition 3.2.2. Let A be a ring. The **(Jacobson) radical** of A, denoted by $r(A)$ is the intersection of all max left ideals of A. (Note : the existence of max left ideals is by Zorn's lemma, which may not assume A is commutative)

Property 3.2.3. $r(A) = \bigcap_{M\text{: simple}} \operatorname{Ann}(M)$ is a two-sided ideal.

Proof:

- RHS $= \bigcap_{M\text{: simple}} \bigcap_{x\in M\setminus\{0\}} \operatorname{ann}(x)$. For $x \in M \setminus \{0\}$, $\operatorname{ann}(x) \neq A \rightsquigarrow \exists$ a max left ideal $\mathfrak{m}$ s.t. $\operatorname{ann}(x) \subseteq \mathfrak{m}$ (By Zorn's lemma).
  $\because M = Ax \simeq A/\operatorname{ann}(x) \supsetneq \mathfrak{m}/\operatorname{ann}(x) \implies \mathfrak{m}/\operatorname{ann}(x) = 0$ i.e. $\mathfrak{m} = \operatorname{ann}(x) \implies r(A) \subseteq \bigcap_{M\text{: simple}} \operatorname{Ann}(M)$
- Let $\mathfrak{m}$ be a maximal left ideal of A, then $A/\mathfrak{m}$ is simple A-module and $\mathfrak{m} = \operatorname{ann}(\overline{1})$ with $\overline{1} \in A/\mathfrak{m} \implies$ RHS $\subseteq r(A)$.

□

Definition 3.2.3. Given a ring A and I is a ideal of A. Then

- I is **nil ideal** if $\forall a \in I, a^n = 0$ for some $n \in \mathbb{N}$ depend on a.
- I is **nilpotent ideal** if $\exists n \in \mathbb{N}$ s.t. $I^n = 0$.

Property 3.2.4. Any nil ideal I is contained in $r(A)$.

Proof: $\forall a \in I\ \forall y \in A$, $ya \in I$, say $(ya)^n = 0$, then

$$(1 - ya)^{-1} = 1 + ya + \cdots + (ya)^{n-1}$$

i.e. $\forall y \in A$, $1 - ya$ is unit in $A \rightsquigarrow a \in r(A)$. □

Property 3.2.5. Let R be a left Artinian. Then $r(R)$ is the largest nilpotent ideal in R.

Proof: $r(R) \subseteq r(R)^2 \subseteq \cdots \rightsquigarrow r(R)^m = r(R)^{m+1} = \cdots =: I \rightsquigarrow I^2 = I$.

Assume that $I \neq 0$. Let $\mathcal{S} = \{J \subseteq R : IJ \neq 0\} \neq \varnothing$, since $I \in \mathcal{S}$. Since R is Artinian, $\exists J_0$ is minimal element in $\mathcal{S}$ i.e. $IJ_0 \neq 0$. Pick $a \in J_0$ s.t. $Ia \neq 0 \rightsquigarrow I(Ra) \neq 0$ and $Ra \subseteq J_0 \rightsquigarrow J_0 = Ra$ is f.g. And $0 \neq IJ_0 = I(IJ_0) \rightsquigarrow J_0 \supseteq IJ_0 \in \mathcal{S} \implies IJ_0 = J_0$. By Nakayama's lemma, $J_0 = 0$ ($\rightarrow\!\!\!\!\!\!\leftarrow$).

So $I = 0 \implies r(R)^m = 0$ i.e. $r(R)$ is nilpotent ideal. Finally, $\forall J$: left nilpotent ideal $\implies J$ is nil ideal. By Property 3.2.4, $J \subseteq r(R)$. □

Property 3.2.6. R : left Artinian $\rightsquigarrow r(R) = \bigcap_{i=1}^{n} m_i$ with m_i : maximal left ideal.

Proof: Let $\mathcal{S} = \{\text{finite intersection of maximal left ideals}\} \neq \varnothing$ by Zorn's lemma. Since R is Artinian $\rightsquigarrow \bigcap_{i=1}^{n} m_i$ is minimal in $\mathcal{S}$. Then for all m : maximal left ideal of A, $m \cap \left(\bigcap_{i=1}^{n} m_i\right) = \bigcap_{i=1}^{n} m_i \rightsquigarrow r(R) = \bigcap_{i=1}^{n} m_i$. □

Theorem 3.2.2. TFAE

(1) R is semisimple.

(2) R is Artinian and $r(R) = 0$.

Proof:

- (1) $\Rightarrow$ (2) : By Property 3.2.2, R is Artinian. Let $R = \bigoplus_{i=1}^{n} I_i \implies 0 = \mathrm{Ann}_R(R) = \bigcap_{i=1}^{n} \mathrm{Ann}_R(I_i) = r(R)$, since every simple R-module will isomorphic to I_k for some k.
- (2) $\Rightarrow$ (1) : Since R is left Artinian, $r(R) = \bigcap_{i=1}^{n} m_i$ for some m_i : maximal left ideal. By Chinese remainder theorem,

$$R \simeq R\Big/r(R) \simeq R\Big/\bigcap_{i=1}^{n} m_i \simeq R/m_1 \times \cdots \times R/m_n$$

So R is semisimple.

□

3.3 Simple rings

3.3.1 Simple rings and Artin-Wedderburn theorem

Definition 3.3.1. R is **simple** if R is semisimple and has no two-sided ideals other than 0 and R.

Property 3.3.1 (key property)**.** Let R be a semisimple ring. Then R is simple $\iff$ all simple R-module are isomorphic.

Proof:

- ($\Rightarrow$) : Recall $R = \bigoplus_{i=1}^{n} I_i$, I_i : minimal left ideal of R. If M is a simple R-module, then $M \simeq I_j$ for some j. Pick a minimal left ideal of R, say I. For $0 \neq a \in I$,

$Ra = I$ by minimality of I. The two-sided RaR is nonzero, so $RaR = R$. That is $R = \sum_{b \in R} Rab$.

Claim: $Rab = 0$ or $Rab \simeq Ra = I$.

pf. Consider $\rho_b : \begin{array}{ccc} R & \longrightarrow & R \\ r & \longmapsto & rb \end{array} \rightsquigarrow \rho_b(r'r) = (r'r)b = r'(rb) = r'\rho_b(r) \rightsquigarrow \rho_b \in \mathrm{End}_R({}_RR)$. It is clear that $Rab = \rho_b(Ra) \simeq Ra/\ker \rho_b|_{Ra}$.

Since Ra is minimal, $\ker \rho_b|_{Ra} = 0$ or $Ra \rightsquigarrow Rab \simeq Ra$ or 0 □

By Claim, if $Rab \neq 0$, then Rab is a minimal left ideal. So $R = \bigoplus_{i=1}^{n} Rab_i$ and $Rab_i \simeq I$. By recall, every simple R-module will isomorphic to I.

- ($\Leftarrow$) : By assumption, $R \simeq I^{\oplus n}$ with I : minimal left ideal. So $R^\circ \simeq \mathrm{End}_R({}_RR) \simeq M_n(D)$, where $D = \mathrm{End}_R(I)$. Since I is simple, D is a division ring. So $R \simeq M_n(D^\circ)$ and D° also is a division ring. By Homework 20, the only two-sided ideals of matrix ring over division ring are 0 and itself. Hence, R is simple.

□

Theorem 3.3.1 (Artin-Wedderburn theorem)**.** R is simple $\iff$ $R \simeq M_n(D)$ with D : division ring.

Proof:

- ($\Rightarrow$) : By the proof of key property $R \simeq M_n(D)$, where $D = (\mathrm{End}_R(I))^\circ$
- ($\Leftarrow$) : First, we study "$M_n(D)$".
  - •• $\exists$ a composition series ($\rightsquigarrow$ Artinian) : Let $e_{ij} \in M_n(R)$ s.t. only (i,j)-entry is 1, and others are 0. Observe that

$$M_n(D) = M_n(D)e_{11} \oplus \cdots \oplus M_n(D)e_{nn}$$

Claim: $M_n(D)e_{ii}$ is a minimal left ideal of $M_n(D)$

pf. Let $0 \neq I \subseteq M_n(D)e_{ii}$ and $0 \neq \sum_{j=1}^{n} a_j e_{ji} \in I$, say $a_k \neq 0$, then

$$I \ni a_k^{-1} e_{ik} \sum_{j=1}^{n} a_j e_{ji} = \sum_{j=1}^{n} a_k^{-1} a_j e_{ik} e_{ji} = e_{ii} \implies I = M_n(D)e_{ii}$$

□

Let $C_j = \bigoplus_{i=1}^{j} M_n(D)e_{ii} \rightsquigarrow C_j/C_{j-1} \simeq M_n(D)e_{jj}$: simple. So

$$M_n(D) = C_n \supset C_{n-1} \supset \cdots \supset C_1 \supset C_0 = 0 \text{ is a composition series}$$

Hence, $\ell(M_n(D)) = n$.

- $\because$ radical is the intersection of all maximal left ideal $\therefore r(M_n(D)) \subsetneq M_n(D)$.
  $\because M_n(D)$ has no two-sided ideal other than 0 and $M_n(D)$ and radical is two-sided ideal $\therefore r(M_n(D)) = 0$.

Hence, $M_n(D)$ is semisimple. Finally, the only two-sided ideal of $M_n(D)$ are 0 and $M_n(D)$, so $M_n(D)$ is simple.

□

Example 3.3.1. M is simple faithful A-module. Then $D = \mathrm{End}_A(M)$ is division ring and $M \in {}_D\mathfrak{M}$. If $\dim_D M = n$, by Wedderburn's theorem, $A \simeq M_n(D^\circ)$. So $A \simeq M_n(D^\circ)$ is a simple ring.
Conversely, If M is simple A-module and A is simple, then M is faithful A-module. pf. If $0 \neq a \in \mathrm{Ann}(M)$, then $A = AaA$ and $M = AM = AaAM = AaM = 0$ $(\rightarrow\!\!\!\!\leftarrow)$.

3.3.2 Matrix rings

Theorem 3.3.2. If $R = M_n(D)$ with D : division ring and N is the unique simple R-module, then $D \simeq (\mathrm{End}_R(N))^\circ$. Which means D is unique determined by R.

Proof: We can choose $N = M_n(D)e_{11}$. For $a \in D$, define

$$\begin{array}{rccc} \rho_a : & N & \longrightarrow & N \\ & U & \longmapsto & U(ae_{11}) \end{array}$$

- $\rho_a \in \mathrm{End}_R(N) : \ \forall\, V \in M_n(D), U \in M_n(D)e_{11},$

$$\rho_a(VU) = (VU)(ae_{11}) = V(U(ae_{11})) = V\rho_a(U)$$

- Now, we have the correspondence between D and $\mathrm{End}_R(N)$. Based on previous experience, we found that this correspondence is anti-homomorphism. So we define

$$\begin{array}{rccc} \varphi : & D^\circ & \longrightarrow & \mathrm{End}_R(N) \\ & a & \longmapsto & \rho_a \end{array}$$

  - φ is a ring homo : $\varphi(a \cdot b) = \varphi(ba) = \rho_{ba}$

$$\rho_{ba}(U) = U((ba)e_{11}) = (Ube_{11})(ae_{11}) = \rho_a(Ube_{11}) = \rho_a\rho_b(U)$$

  - φ is $1-1$: $\rho_a(U) = 0 \rightsquigarrow U(ae_{11}) = 0\ \forall U$. If $a \neq 0$, then $U = a^{-1}e_{11} \in N$ and $U(ae_{11}) = e_{11} \neq 0$ $(\rightarrow\!\!\!\!\leftarrow)$.
  - φ is onto : For $f \in \mathrm{End}_R(N)$. Let $f(e_{11}) = \sum_{i=1}^{n} a_i e_{i1}$. Since f is R-linear,

$$f(e_{11}) = f(e_{11}^2) = e_{11}f(e_{11}) = e_{11}\left(\sum_{i=1}^{n} a_i e_{i1}\right) = a_1 e_{11} = \rho_{a_1}(e_{11})$$

    Then $(f - \rho_{a_1})$ has nontrivial kernel i.e. $(f - \rho_{a_1})$ is not an isomorphism. Since N is simple module, by Schur's lemma, $f - \rho_{a_1} = 0$ i.e. $f = \rho_{a_1}$.

Hence, $\varphi : D^\circ \xrightarrow{\sim} \mathrm{End}_R(N) \rightsquigarrow D \simeq (\mathrm{End}_R(N))^\circ$.

□

Corollary 3.3.1. If $M_{n_1}(D_1) \simeq M_{n_2}(D_2)$, where $n_i \in \mathbb{N}$ and D_i : division ring $\forall i$. Then $n_1 = n_2$, $D_1 \simeq D_2$.

Proof:

- Since $M_{n_1}(D_1)$ and $M_{n_2}(D_2)$ have the same length, so $n_1 = n_2$.
- Let $R \simeq M_{n_1}(D_1) \simeq M_{n_2}(D_2)$. By Theorem 3.3.2, $D_1 \simeq \mathrm{End}_R(N)^\circ$, $D_2 \simeq \mathrm{End}_R(N)^\circ$, where N is unique simple R-module. So $D_1 \simeq D_2$.

□

Observation: Now, we want to given a division ring D, is there a relation between ${}_D\mathfrak{M}$ and ${}_{M_n(D)}\mathfrak{M}$. Obviously, we can have the correspondence with the constraint of n.

- $M \in {}_D\mathfrak{M}$ and $\dim_D M = n \rightsquigarrow \mathrm{End}_D(M) \simeq M_n(D)$. Since $M \in {}_{\mathrm{End}_D(M)}\mathfrak{M} \rightsquigarrow M \in {}_{M_n(D)}\mathfrak{M}$.

  Claim: M is simple $M_n(D)$-module.

  $pf.$ $\forall v \in M$, we can extend $\{v\}$ to a basis $\{v, v_2, ..., v_n\}$ for M over D. Since $\forall w \in M$, $\exists \varphi \in M_n(D)$ s.t. $\varphi(v) = w$. That is M cannot have any $M_n(D)$-invariant subspace other than 0 and M.

- $N \in {}_{M_n(D)}\mathfrak{M}$
  - $M_n(D)$ is simple $\rightsquigarrow$ N is semisimple over $M_n(D)$
  - Define
    $$\begin{array}{ccc} D & \hookrightarrow & M_n(D) \\ a & \mapsto & aI_n \end{array} \text{ as rings}$$
    So we can regard D as a subring of $M_n(D)$ and thus $N \in {}_D\mathfrak{M}$.
  - Let S be the unique simple $M_n(D)$-module. ($S \simeq M_n(D)e_{11}$ and $\dim_D S = n$) Since N is semisimple over $M_n(D)$, we can write $M = \bigoplus_{i\in\Lambda} S$. In particular, if $N = \bigoplus_{i=1}^{n} S$, then $\dim_D N = mn$.
  - Hence, if $M, N \in {}_{M_n(D)}\mathfrak{M}$ and $\dim_D M = \dim_D N$, then $M \simeq N$ in ${}_{M_n(D)}\mathfrak{M}$, since $n \dim_D(M) = \dim_{M_n(D)} M$.

3.3.3 Simple Algebra over a algebraically closed field

In this subsection, we require more algebra structure to our ring.

Theorem 3.3.3 (Burnside's theorem)**.** Let $k = \overline{k}$ and $\dim_k V = n$. If R is a subalgebra of $\mathrm{End}_k(V)$ and V is simple over R, then $R = \mathrm{End}_k(V)(\simeq M_n(k))$.

Proof:

- $V \in {}_R\mathfrak{M} : R \subseteq \mathrm{End}_k(V) \curvearrowright V \implies R \curvearrowright V$

- V : simple/$R \rightsquigarrow R' = \mathrm{End}_R(V)$ is a division ring.
- Since R contains identity which can be regard as the identity in k, so $k \subset R$. Then $R' = \mathrm{End}_R(V) \subseteq \mathrm{End}_k(V)$ as k-subspaces.
- $\forall\ 0 \neq \alpha \in R'$, since R' is division $\rightsquigarrow k(\alpha)$ is a field and $k(\alpha) \subseteq R' \subseteq \mathrm{End}_k(V)$ as k-module and notice that $\dim_k \mathrm{End}_k(V) = n^2 < \infty \rightsquigarrow k(\alpha)/k$ is finite extension i.e. α algebraic over $k \rightsquigarrow \alpha \in k$, since $\overline{k} = k$. So $R' = k$
- Let $V = \langle v_1, ..., , v_n\rangle_k = \langle v_1, ..., v_n\rangle_{R'}$. By Jacobson theorem, $R \twoheadrightarrow R'' = \mathrm{End}_{R'}(V) = \mathrm{End}_k(V)$. Hence, $R = \mathrm{End}_k(V)$.

□

Corollary 3.3.2. Let R be a simple algebra over algebraically closed field k and $\dim_k R < \infty$. Then $R \simeq M_n(k)$.

Proof:

- Since R is simple ring, let S be the unique minimal left ideal of R and $D = \mathrm{End}_R(S)$ be the corresponding division ring. Then $R \simeq S^{\otimes n} \rightsquigarrow R \simeq M_n(D^\circ)$.
- Since S is an ideal of R, $RS \subseteq S \rightsquigarrow kS \subseteq S$ i.e. S is a k-subspace of R. Then $\dim_k R < \infty \implies \dim_k S < \infty$, say $\dim_k S = m$.
- **Claim:** R can be regarded as a subalgebra of $\mathrm{End}_k(S)$

  pf. Define

$$\begin{array}{rccc} \varphi: & R & \longrightarrow & \mathrm{End}_k(S) \\ & a & \longmapsto & \begin{pmatrix} T_a: & S & \to & S \\ & x & \mapsto & ax \end{pmatrix} \end{array}$$

  - $T_a \in \mathrm{End}_k(S) : \forall r \in k,\ T_a(rx) = a(rx) = (ar)x = (ra)x = rT_a(x)$. For red equality is by R is k-algebra.
  - $T_a \circ T_b(x) = T_a(bx) = a(bx) = (ab)x = T_{ab}(x) \rightsquigarrow \varphi$ is a k-algebra homo.

  $\because R$: simple and S : simple/$R \therefore S$: faithful/$R \rightsquigarrow \varphi : R \hookrightarrow \mathrm{End}_k(S)$. □
- By Burnside's theorem, $R \simeq \mathrm{End}_k(S) \simeq M_m(k)$. Since D°, k is division ring and $M_n(D^\circ) \simeq M_m(k)$, we have $n = m$ and $D^\circ \simeq k$. Hence, $R \simeq M_n(k)$.

□

Finally, given R : semisimple algebra over a algebraically closed field k. By Artin-Wedderburn theorem,

$$R \simeq M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

Let $R_i \subseteq R$ be the two-sided ideal such that $R_i \longleftrightarrow M_{n_i}(D_i)$, then $M_{n_i}(D_i)$ is simple algebra over k. By Corollary 3.3.2, $R_i \simeq M_{n_i}(k)$. That is

$$R \simeq M_{n_1}(k) \times \cdots \times M_{n_r}(k)$$

Remark 3.3.1.

- R is right-semisimple if R° is left-semisimple. Since we have the correspondent of right ideals of R and left ideals of R°, so this definition is reasonable.
- R is semisimple $\iff R \simeq \prod_{i=1}^{r} M_{n_i}(D_i) \iff R^\circ \iff \prod_{i=1}^{r} M_{n_i}(D_i^\circ) \simeq R^\circ$ is semisimple. Hence, left semisimple $\iff$ right semisimple.

3.4 Representations and Semisimplicity

Let G be a finite group and F be a field. If V is a vector space over F, then $\mathrm{GL}(V)$ is the group of nonsingular linear transformations : $V \to V$.

3.4.1 Definition-example

Definition 3.4.1. A group homomorphism $\rho : \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(V) \\ s & \longmapsto & \rho_s = \rho(s) \end{array}$ is called a linear representation of G.

- ρ is called **faithful** if it is injective.
- V is called a **representation space** of G and $\dim V$ is called the degree of ρ.
- $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(V)$ are **isomorphic** if $\exists$ a F-linear isomorphism $\tau : V \to V'$ s.t.

$$\tau \circ \rho_s = \rho'_s \circ \tau \ \forall s \in G \ \text{ i.e. } \begin{array}{ccc} V & \xrightarrow{\rho_s} & V \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ V & \xrightarrow[\rho'_s]{} & V \end{array} \text{ commute}$$

- For a subspace $W \subset V$, W is **invariant** under G if $\forall s \in G$, $\rho_s(W) \subseteq W$. Then

$$\rho|_W : G \longrightarrow \mathrm{GL}(W) \text{ is a } \textbf{subrepresentation} \text{ of } \rho$$

- ρ is **irreducible** if ρ has no proper nontrivial subrepresentation.

As we do in group extension, given a group G acts on a module M. Since M is a abelian group i.e. a $\mathbb{Z}$-module, we can given M a $\mathbb{Z}[G]$-module structure. Now, we want to similar way on V, recall : $F[G] = \{\sum_{g\in G} \alpha_g g | \alpha_g \in F\}$ and see the key property in below.

Property 3.4.1 (key properties)**.**

- $\{V : \text{an } F[G]\text{-module}\} \longleftrightarrow \{\rho : G \to \mathrm{GL}(V)\}$
- $\{W \subset V : \text{an } F[G]\text{-submodule}\} \longleftrightarrow \{W \subseteq V : \text{a } G\text{-invariant subspace}\}$

- V is a simple $F[G]$-module $\iff$ ρ is an irreducible representation
- ρ, ρ' are isomorphism $\iff$ $V \simeq V'$ as $F[G]$-modules.

Example 3.4.1.

- (**Regular representation**) $V = F[G] = \bigoplus_{g\in G} Fg$, define

$$\begin{array}{rccc} \rho^{\mathrm{reg}}: & G & \longrightarrow & \mathrm{GL}(V) \\ & s & \longmapsto & \rho_s^{\mathrm{reg}}: \sum_{g\in G} \alpha_g g \mapsto \sum_{g\in G} \alpha_g (sg) \end{array}$$

  Notice that $\{sg : g \in G\} = \{g : g \in G\}$, so ρ_s^{reg} can be regard as exchange the coefficient of the basis $\{g : g \in G\}$ i.e. $[\rho_s^{\mathrm{reg}}]_G$ is a matrix with every column, row has exactly one entry is 1 and others are 0.

- (**Permutation representation**) Let $V = \bigoplus_{i=1}^{n} Fe_i$ and consider

$$\begin{array}{rccc} \rho: & S_n & \longrightarrow & \mathrm{GL}(V) \\ & \sigma & \longmapsto & \rho_\sigma: \sum_{i=1}^{n} \alpha_i e_i \mapsto \sum_{i=1}^{n} \alpha e_{\sigma(i)} \end{array}$$

  For example : $G = S_3$, then $\dim_F V = 3$. Let $\sigma = (1\ 2)$, then $\rho_\sigma : \begin{cases} e_1 \mapsto e_2 \\ e_2 \mapsto e_1 \\ e_3 \mapsto e_3 \end{cases}$

  Note : By Cayley theorem, $G \hookrightarrow S_n$ for some n. Restrict ρ on G, then we get a linear representation $\rho|_G : G \longrightarrow \mathrm{GL}(V)$. Actually, $\rho|_G$ is isomorphic to regular representation of G.

- Unfortunately, those two representation are all not the irreducible when $n \geq 2$, the reason in below :

  - For the permutation representation :

    $N = \{\alpha_1 e_1 + \cdots + \alpha_n e_n : \alpha_1 = \alpha_2 = \cdots = \alpha_n\}$ is an S_n-invariant subspace

    which is called the **trace submodule** of V over $F[S_n]$ and $\dim_F N = 1$.

    $I = \{\alpha_1 e_1 + \cdots + \alpha_n e_n : \alpha_1 + \cdots + \alpha_n = 0\}$ is also S_n-invariant

    which is called the **augmentation submodule** of V over $F[S_n]$ and $\dim_F I = n - 1$.

  - For the regular representation : Let $n = |G|$

    $N = \{\alpha_1 g_1 + \cdots + \alpha_n g_n : \alpha_1 = \alpha_2 = \cdots = \alpha_n\}$ is an G-invariant subspace

    which is called the **trace ideal** of $F[G]$ and $\dim_F N = 1$.

    $I = \{\alpha_1 g_1 + \cdots + \alpha_n g_n : \alpha_1 + \cdots + \alpha_n = 0\}$ is also G-invariant

    which is called the **augmentation ideal** of $F[G]$ and $\dim_F I = n - 1$.
    And both N, I are two-sided ideals of $F[G]$.

Now, we know how to divide the representation to some smaller subrepresentation. So we may ask how to piece some representation together into larger representation. We introduce two operations on representation : Given $\rho_1 : G \to \mathrm{GL}(V_1)$, $\rho_2 : G \to \mathrm{GL}(V_2)$ with $\dim_F V_1 = n, \dim_F V_2 = m$ and $\beta_1 = \{v_1, ..., v_n\}, \beta_2 = \{w_1, ..., w_m\}$ be the basis for V_1, V_2 respectively. Construct

- (Direct sum)
$$\begin{array}{rccc} \rho_1 \oplus \rho_2 : & G & \longrightarrow & \mathrm{GL}(V_1 \oplus V_2) \\ & s & \longmapsto & (\rho_1 \oplus \rho_2)_s = ((\rho_1)_s, (\rho_2)_s) \end{array}$$
Then the degree of $\rho_1 \oplus \rho_2$ is $\dim_F(V_1 \oplus V_2) = m + n$ and $[(\rho_1 \oplus \rho_2)_s]_{\beta_1 \cup \beta_2}$ is form
$$\begin{pmatrix} [(\rho_1)_s]_{\beta_1} & O \\ O & [(\rho_2)_s]_{\beta_2} \end{pmatrix}$$
- (Tensor product)
$$\begin{array}{rccc} \rho_1 \otimes \rho_2 : & G & \longrightarrow & \mathrm{GL}(V_1 \otimes_F V_2) \\ & s & \longmapsto & (\rho_1 \otimes \rho_2)_s = (\rho_1)_s \otimes (\rho_2)_s : v \otimes w \mapsto (\rho_1)_s(v) \otimes (\rho_2)_s(w) \end{array}$$
Then the degree of $\rho_1 \otimes \rho_2$ is $\dim_F(V_1 \oplus V_2) = mn$, since $\{v_i \otimes w_j\}$ form a basis.

3.4.2 Complete reducibility

Theorem 3.4.1 (Maschke's theorem)**.** Assume $\mathrm{char}F \nmid |G|$. Let $\rho : G \to \mathrm{GL}(V)$ and W be a subrepresentation of G in V. Then $\exists W' \subset V$ s.t. W' is G-invariant and $W \oplus W' = V$ as $F[G]$-modules.

Proof: First, pick arbitrary W_1 s.t. $V = W \oplus W_1$ and let $\pi : V \to W$ be the projection. Notice that W_1 may not be G-invariant, so π may not be a $F[G]$-module homomorphism. To get a $F[G]$-module homomorphism, we have the common method : take average. Under this ideal, define
$$\pi' = \frac{1}{|G|} \sum_{s \in G} \rho_s^{-1} \circ \pi \circ \rho_s : V \longrightarrow W$$
Since W is G-invariant, $\pi'(V) \subseteq W$. Notice that W is G-invariant, so $\forall w \in W$, $\rho_s(w) \in W \rightsquigarrow \pi \circ \rho_s(w) = \rho_s(w) \rightsquigarrow \rho_s^{-1} \circ \pi \circ \rho_s(w) = w$. Then $\sum_{s \in G} \rho_s^{-1} \circ \pi \circ \rho_s(w) = |G| \cdot w$. So the assumption of $\mathrm{char}F \nmid |G|$ is necessary, otherwise it will be the zero map (before divide $|G|$). Hence, $\pi'(w) = w \implies \pi'(V) = W$.
Claim: π' is an $F[G]$-module epimorphism.
pf. We need to prove "$\rho_s \circ \pi' = \pi' \circ \rho_s \ \forall s \in G$". For all $v \in V$
$$\begin{aligned} \pi'(\rho_s(v)) &= \frac{1}{|G|} \sum_{t \in G} \rho_t^{-1} \circ \pi \circ \rho_t \circ \rho_s(v) \\ &= \frac{1}{|G|} \sum_{t \in G} \rho_s \circ \rho_s^{-1} \circ \rho_t^{-1} \circ \pi \circ \rho_t \circ \rho_s(v) \\ &= \frac{\rho_s}{|G|} \sum_{t \in G} \rho_{ts}^{-1} \circ \pi \circ \rho_{ts}(v) = \rho_s \circ \pi'(v) \end{aligned}$$

□

By Claim, $W' := \ker \pi'$ is an $F[G]$-submodule of V i.e. W is G-invariant. Since V is a F-vector space, $0 \to W' \to V \to W \to 0$ splits i.e. thus $V = W \oplus W'$. □

Theorem 3.4.2. Assume $\mathrm{char}F \nmid |G|$. Every representation of G of finite degree is a direct sum of irreducible representations.

Proof: Let $\rho : G \to \mathrm{GL}(V)$ with $\dim_F V = n$. We need to prove that V is semisimple over $F[G]$. By induction on $\dim V$, if V is simple, then done! Otherwise, $\exists$ a nontrivial proper $F[G]$-submodule W of V. By Maschke's theorem, $\exists W'$ which is also an $F[G]$-submodule s.t. $V = W \oplus W'$ as $F[G]$-modules. By induction hypothesis, W, W' are direct sums of simple $F[G]$-submodules, hence so is V. □

3.4.3 Application for semisimplicity

Observation: G : finite group; F : field with $\mathrm{char}F \nmid |G|$.

- We can interpret the regular representation of G as

  "$F[G]$ is a left module over itself"

- By Maschke's theorem, $F[G]$ can be decomposed into a direct sum of simple $F[G]$-modules $\rightsquigarrow F[G]$ is a semisimple algebra/F.

- $\mathbb{C}[G]$ is a semisimple algebra/$\mathbb{C}$, then by Corollary of Burnside theorem,

  $$\mathbb{C}[G] \simeq M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

  By this isomorphism, we have

  - $\mathbb{C}[G]$ has exactly r distinct isomorphic types of simple modules.
  - $|G| = \sum_{i=1}^{r} n_i^2$ by comparing the dim /$\mathbb{C}$ on both sides.
  - $\dim_{\mathbb{C}} Z(\mathbb{C}[G]) = r$, since $Z(M_{n_i}(\mathbb{C})) = \mathbb{C} \cdot I_{n_i}$.

Property 3.4.2. $r = \#$ of conjugacy classes of G.

Proof: Let $K_1, ..., K_\ell$ be distinct conjugacy classes of G. Set

$$x_i = \sum_{g \in K_i} g \in \mathbb{C}[G]$$

Then x_i, x_j have no common terms for $i \neq j \rightsquigarrow x_i$'s are linearly indep./$\mathbb{C}$. Also, $\forall g \in G$, $g x_i g^{-1} = g \rightsquigarrow x_i \in Z(\mathbb{C}[G])$. Conversely, $\forall x \in \mathbb{Z}(\mathbb{C}[G])$, say $x = \sum_{g \in G} \alpha_g g$.

$$\because \forall h \in G,\ h^{-1} x h = x \rightsquigarrow \sum_{g \in G} \alpha_g h^{-1} g h = \sum_{g \in G} \alpha_g g \text{ in } \mathbb{C}[G] \rightsquigarrow \alpha_{hgh^{-1}} = \alpha_g\ \forall h \in G$$

$$\therefore x = \sum_{i=1}^{\ell} \alpha_i x_i \rightsquigarrow Z(\mathbb{C}[G]) = \langle x_1, ..., x_\ell \rangle_{\mathbb{C}}$$

Hence, $r = \dim_{\mathbb{C}} Z(\mathbb{C}[G]) = \ell$. □

In above, since we choose a algebraically closed field so we have Burnside theorem. In general, By Artin-Wedderburn theorem, we only have

$$F[G] \simeq M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

with division ring D_i. Then we have

- Let I_{n_i} be the identity in $M_{n_i}(D_i)$, and let $z_i \longrightarrow (0, ..., 0, I_{n_i}, 0, ..., 0)$ under the isomorphism. Then
  - $z_i^2 = z_i$, $z_i z_j = 0$ for all $i \neq j$
  - $\sum_{i=1}^{r} z_i = 1$
  - $z_i F[G] \simeq M_{n_i}(D_i)$
  - $z_i \in Z(F[G])$

  Here $z_1, ..., z_r$ are called the **primitive central idempotents** of $F[G]$.
- M : simple $F[G]$-module $\rightsquigarrow$ M : simple $M_{n_i}(D_i)$-module for some i. So M can be uniquely determined $(M_{n_i}(D_i)e_{11})$. Now, we give a method to find i :

  $M = 1 \cdot M = (z_1 + \cdots + z_r)M = z_1M + \cdots + z_rM$. Actually, it will be direct, since if $y \in z_1M \cap (z_2M + \cdots + z_rM)$, say $y = z_1x = z_2x_2 + \cdots z_rx_r$, then $y = z_1x = z_1^2x = z_1(z_2x_2 + \cdots + z_rx_r) = 0$. Since M is simple, $M = z_iM$ for some i.

Example 3.4.2. Find all irreducible representations of $G = S_3$:
Conjugacy classes : $\{e\}, \{(1\ 2), (1\ 3), (2\ 3)\}$, $\{(1\ 2\ 3), (1\ 3\ 2)\}$.
Notice that $|G| = 6 = 1^2 + 1^2 + 2^2$ is unique solution for $|G| = \sum_{i=1}^{3} n_i^2$. So

$$\mathbb{C}[S_3] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$$

ρ : irreducible representation $\longleftrightarrow$ S : simple/$\mathbb{C}[S_3]$ $\rightsquigarrow$ S : simple/$\mathbb{C}$ or simple/$\mathbb{C}$ or simple/$M_2(\mathbb{C})$. So there have three different irreducible representation.
Recall the permutation representation of S_3, then $V = \langle e_1, e_2, e_3 \rangle_{\mathbb{C}}$ have two non-trivial proper submodule.

- $\rho_1 \longleftrightarrow$ trace submodule $W_1 = \{\alpha e_1 + \alpha e_2 + \alpha e_3 : \alpha \in \mathbb{C}\}$ of V. So $\rho_1 : \sigma \mapsto \mathrm{id}$ is trivial representation.
- Let $W_2 = \{\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3\}$ be the augmentation submodule of V. It's clear that W_2 is simple over $\mathbb{C}[S_3]$ and $V = W_1 \oplus W_2$.

  $\rho_2 \longleftrightarrow W_2$
- For last one, we have

$$\begin{array}{rccc} \rho_3 : & S_3 & \longrightarrow & \mathbb{C}^* \simeq \mathrm{GL}(\mathbb{C}) \\ & \text{even} & \longmapsto & 1 \\ & \text{odd} & \longmapsto & -1 \end{array}$$

As you see, if we only using the technology in this section, it is not enough to clearly understand all irreducible representation. We will introduce more powerful technology in later sections.

3.5 Character theory

Let G be a finite group and V be a vector space/F with $\dim_F V = n$. Fix a basis $\alpha = \{e_1, ..., e_n\}$ for V over F.

3.5.1 Basis property

Definition 3.5.1. Let $\rho : G \to \mathrm{GL}(V)$ be a representation

- Let $\phi : \mathrm{GL}(V) \simeq \mathrm{GL}_n(F)$ via α, define $R = \phi \circ \rho : G \to \mathrm{GL}_n(F)$ by $s \mapsto R_s = [\rho_s]_\alpha$
- The **character** χ_ρ of ρ is the map $\chi_\rho : \begin{array}{ccc} G & \longrightarrow & F \\ s & \longmapsto & \mathrm{tr}(R_s) \end{array}$
- The **degree** of χ_ρ is defined to be the degree of ρ i.e. $\dim V$.
- χ_ρ is called an **irreducible** character if ρ is irreducible.
- The **trace function** related to ρ on $F[G]$ is unique extension of χ_ρ by F-linearity, which is still denoted by χ_ρ.

Remark 3.5.1.

- χ_ρ is independent of the choice of α :
  Let β be another basis for V, then $R_s = [\rho_s]_\alpha$, $R'_s = [\rho_s]_\beta$. Notice that
  $$R'_s = [\rho_s]_\beta = [\mathrm{id}]^\beta_\alpha [\rho_s]_\alpha [\mathrm{id}]^\alpha_\beta = Q^{-1} R_s Q$$
  $$\implies \mathrm{tr}\, R'_s = \mathrm{tr}((Q^{-1}R_s)Q) = \mathrm{tr}(Q(Q^{-1}R_s)) = \mathrm{tr}\, R_s$$
- $\rho \simeq \rho' \implies \chi_\rho = \chi_{\rho'}$:
  Let $\tau : V \xrightarrow{\sim} V'$ s.t. $\tau \circ \rho_s = \rho'_s \circ \tau$ for all $s \in G$
  $$\begin{array}{ccc} V & \xrightarrow{\rho_s} & V \\ {\scriptstyle\tau}\downarrow\wr & & \wr\downarrow{\scriptstyle\tau} \\ V' & \xrightarrow[\rho_s]{} & V' \end{array}$$
  Let $\alpha' = \tau(\alpha)$ is a basis for V'. Then
  $$\mathrm{tr}\, R_S = \mathrm{tr}[\rho_s]_\alpha = \mathrm{tr}\left([\tau^{-1}]^\alpha_{\alpha'}[\rho'_s]_{\alpha'}[\tau]^{\alpha'}_\alpha\right) = \mathrm{tr}\left([\rho'_s]_{\alpha'}[\tau]^{\alpha'}_\alpha[\tau^{-1}]^\alpha_{\alpha'}\right) = \mathrm{tr}[\rho'_s]_{\alpha'} = \mathrm{tr}\, R'_s$$

Property 3.5.1.

- $\chi_\rho(e) = \deg \rho = n$:
  $\rho(e) = \mathrm{id}$ and $\mathrm{tr}\, I_n = n$
- χ_ρ is a **class function** i.e. it is constant on each conjugacy class in G :
  $\chi_\rho(tst^{-1}) = \mathrm{tr}\, R_{tst^{-1}} = \mathrm{tr}\, R_t R_s R_t^{-1} = \mathrm{tr}\, R_s = \chi_\rho(s)\ \forall s, t \in G$.

- If $F = \mathbb{C}$, then $\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}$:

  If the eigenvalue of R_s are $\lambda_1, ..., \lambda_n \neq 0$, then the eigenvalue of $R_{s^{-1}} = (R_s)^{-1}$ are $\lambda^{-1}, ..., \lambda_n^{-1}$. Since

  $$\det(\lambda I - A) = \det((\lambda A^{-1} - I)A) = \det(\lambda I)\det(A^{-1} - \lambda^{-1} I)\det A$$

  and $\det A, \lambda \neq 0$.

  $\because |G| < \infty \therefore s^m = e \rightsquigarrow R_s^m = I_n \rightsquigarrow |\lambda_i| = 1 \rightsquigarrow \lambda_i^{-1} = \overline{\lambda_i}$. Thus,

  $$\chi_\rho(s^{-1}) = \operatorname{tr} R_{s^{-1}} = \overline{\lambda_1} + \cdots + \overline{\lambda_i} = \overline{\operatorname{tr} R_s} = \overline{\chi_\rho(s)}$$

- $\chi_{\rho\oplus\rho'} = \chi_\rho + \chi_{\rho'}$: Since

  $$\chi_{\rho\oplus\rho'} \longleftrightarrow R_s = \begin{pmatrix} A_s & O \\ O & B_s \end{pmatrix}$$

  where $A_s \longleftrightarrow \rho_s$, $B_s \longleftrightarrow \rho'_s$. Hence, $\operatorname{tr} R_s = \operatorname{tr} A_s + \operatorname{tr} B_s$.

- $\chi_{\rho\otimes\rho'} = \chi_\rho \cdot \chi_{\rho'}$: Let $\{e_i\}, \{e'_i\}$ be a basis for V, V' respectively. Then $\{e_i \otimes e'_j\}$ is a basis for $V \otimes V'$. If

  $$\begin{cases} \rho_s(e_j) = \sum_{i=1}^{n} r_{ij} e_i \\ \rho'_s(e'_j) = \sum_{i=1}^{n'} r'_{ij} e'_i \end{cases} \implies \begin{cases} R_s = (r_{ij}) \in M_n(F) \\ R'_s = (r'_{ij}) \in M_{n'}(F) \end{cases}$$

  So

  $$\rho_s \otimes \rho'_s(e_p \otimes e'_q) = \rho_s(e_p) \otimes \rho'_s(e'_q) = \left(\sum_{i=1}^{n} r_{ip} e_i\right) \otimes \left(\sum_{j=1}^{n'} r_{jq} e'_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n'} r_{ip} r'_{jq} (e_i \otimes e'_j)$$

  $$\implies \chi_{\rho\otimes\rho'}(s) = \sum_{p=1}^{n}\sum_{q=1}^{n'} r_{pp} r'_{qq} = \left(\sum_{p=1}^{n} r_{pp}\right)\left(\sum_{q=1}^{n'} r_{qq}\right) = \chi_\rho(s) \cdot \chi_{\rho'}(s)$$

3.5.2 Space of class functions and Orthogonality

In last subsection, given a representation ρ we can induce a character χ_ρ and we know that is a class function. Now, given a class function, we want to find a representation ρ which character is that class function.

Definition 3.5.2. Let $F = \mathbb{C}$

- $X(G) :=$ the vector space of all complex valued class functions on G.

  Assume that $K_1, ..., K_r$ are distinct conjugacy classes in G. Define $f_i(K_j) = \delta_{ij} \rightsquigarrow \{f_1, ..., f_r\}$ forms a basis for $X(G)$ over $\mathbb{C}$

  - $\forall f \in X(G)$, say $f(K_i) = a_i \rightsquigarrow f = \sum_{i=1}^{r} a_i f_i$

- If $\sum_{i=1}^{r} a_i f_i = 0$. For $s_j \in K_j$, $0 = \sum_{i=1}^{r} a_i f_i(s_j) = a_j \ \forall j$.

So $\dim_{\mathbb{C}} X(G) = r$.

- $\forall \varphi, \psi \in X(G)$, $\langle \varphi, \psi \rangle := \frac{1}{|G|} \sum_{s \in G} \varphi(s)\overline{\psi(s)}$. We check that $\langle \cdot, \cdot \rangle$ is a positive definite Hermitian form on $X(G)$.

  - $\langle a\varphi_1 + \varphi_2, \psi \rangle = \frac{1}{|G|} \sum_{s \in G} (a\varphi_1(s) + \varphi_2(s))\overline{\psi(s)} = a\langle \varphi_1, \psi \rangle + \langle \varphi_2, \psi \rangle$
  - $\langle \psi, \varphi \rangle = \frac{1}{|G|} \sum_{s \in G} \psi(s)\overline{\varphi(s)} = \overline{\frac{1}{|G|} \sum_{s \in G} \varphi(s)\overline{\psi(s)}} = \overline{\langle \varphi, \psi \rangle}$
  - $\langle \varphi, \varphi \rangle = \frac{1}{|G|} \sum_{s \in G} \varphi(s)\overline{\varphi(s)} > 0$ if $\varphi \neq 0$

  So we can define norm on $X(G)$.

Now, recall that

$$\begin{array}{ccc} \mathbb{C}[G] & \xrightarrow{\sim} & M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}) \\ z_i & \longleftrightarrow & (0, ..., 0, I_{n_i}, 0, ..., 0) \end{array}$$

where z_i is primitive central idempotent and we will have $z_1, ..., z_r$ are $\mathbb{C}$-linearly independent. There are r non-isomorphic irreducible representations of G, say $\rho_1, ..., \rho_r$, where

$$\rho_i \longleftrightarrow \text{the simple module } V_i / M_{n_i}(\mathbb{C})$$

Then $V_i \simeq M_{n_i}(\mathbb{C})e_{11} \rightsquigarrow \dim V_i = n_i$ and ρ_i induce a character $\chi_{\rho_i} =: \chi_i$. Notice that r also is the number of conjugacy class of G, and we found that $\{\chi_1, ..., \chi_r\}$ will forms a basis for $X(G)$ and will prove it below.

First, recall that we can extend a character by linearity from G to $\mathbb{C}[G]$. $\forall z = \sum_{s \in G} \alpha_s s \in \mathbb{C}[G]$ and a representation ρ

$$\chi_\rho(z) = \sum_{s \in G} \alpha_s \chi_\rho(s) = \sum_{s \in G} \alpha_s \operatorname{tr}(R_s) = \operatorname{tr}\left(\sum_{s \in G} \alpha_s R_s \right)$$

So z can be regard as a linear transformation on V and $\chi_\rho(z)$ is its trace. Now,

$$\rho_i : G \longrightarrow \mathrm{GL}(M_{n_i}(\mathbb{C})e_i)$$

and $z_1, ..., z_r \in \mathbb{C}[G]$. Since z_i acts as the identity on $M_{n_i}(\mathbb{C})e_{11}$ and z_j acts as zero on $M_{n_i}(\mathbb{C})e_{11}$ for $j \neq i$, $\chi_i(z_i) = \operatorname{tr} \mathrm{id}_{V_i} = n_i$ and $\chi_j(z_i) = 0$ for $j \neq i$. Hence, $\chi_1, ..., \chi_r$ are linearly independent over $\mathbb{C}$ and notice that $\dim \chi(G) = r$, so $\{\chi_1, ..., \chi_r\}$ forms a basis of $X(G)$ over $\mathbb{C}$.

Property 3.5.2.

$$z_i = \frac{\chi_i(1)}{|G|} \sum_{s \in G} \chi_i(s^{-1}) s \ \forall i = 1, ..., r$$

Proof: Write $z = z_i = \sum_{s\in G} \alpha_s s$. Via the regular representation, we have

$$\mathbb{C}[G] \simeq M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

Notice that $\mathbb{C}[G] \longleftrightarrow \rho^{\text{reg}}$ and $M_{n_1}(\mathbb{C}) = M_{n_1}(\mathbb{C})e_{11} \oplus \cdots \oplus M_{n_1}(\mathbb{C})e_{n_1 n_1} \longleftrightarrow \rho_1^{\oplus n_1}$, so

$$\rho^{\text{reg}} \simeq \rho_1^{\oplus n_1} \oplus \cdots \oplus \rho_r^{\oplus n_r} \implies \chi^{\text{reg}} = \sum_{j=1}^{r} n_j \chi_j = \sum_{j=1}^{r} \chi_j(1)\chi_j$$

Observation: $\rho_e = I_{|G|} \rightsquigarrow \chi^{\text{reg}}(1) = |G|$. For $s \neq e$, $\rho_s(t) = st$, so every entries on diagonal of $R^{\text{reg}}(s)$ are $0 \rightsquigarrow \chi^{\text{reg}}(s) = 0$. Then

$$|G| = \chi^{\text{reg}}(1) = \sum_{j=1}^{r} \chi_j(1)\chi_j(1) = \sum_{j=1}^{r} n_j^2$$

which had learned it before. Now, for $t \in G$, $z = \sum_{s\in G} \alpha_s s \implies zt^{-1} = \sum_{e\neq s\in G} \alpha_{st} s + \alpha_t e$. Take χ^{reg} both side, then

$$0 + \alpha_t |G| = \chi^{\text{reg}}(zt^{-1}) = \sum_{j=1}^{r} \chi_j(1)\chi_j(zt^{-1})$$

Now, $zt^{-1} \in \mathbb{C}[G]$, we need to see zt^{-1} as the linear transformation on V. First, $\rho_j(t^{-1}) \in \text{GL}(V_j)$ and $z = z_i \longleftrightarrow \begin{cases} \text{id}_{V_i} & \text{, for } j = i \\ 0_{V_j} & \text{, for } j \neq i \end{cases}$

$$\implies zt^{-1} = \begin{cases} t^{-1} & \text{on } V_i \\ 0 & \text{on } V_j \text{ for } j \neq i \end{cases} \implies \alpha_t |G| = \chi_i(1)\chi_i(t^{-1})$$

Hence, $z_i = \dfrac{\chi_i(1)}{|G|} \sum_{t\in G} \chi_i(t^{-1})t$. □

Theorem 3.5.1. The set of all of all irreducible characters of G over $\mathbb{C}$ forms an orthonormal basis for the $\mathbb{C}$-space $X(G)$ i.e.

$$\langle \chi_i, \chi_j \rangle = \delta_{ij}$$

Proof: Notice that $z_i z_j = \delta_{ij} z_i$. By Property 3.5.2

$$\begin{aligned} \frac{\delta_{ij}\chi_i(1)}{|G|} \sum_{u\in G} \chi_j(u^{-1})u = \delta_{ij} z_i = z_i z_j &= \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{s\in G}\sum_{t\in G} \chi_i(t^{-1})\chi_j(s^{-1})st \\ &= \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{u\in G} \left(\sum_{s\in G} \chi_i(su^{-1})\chi_j(s^{-1}) \right) u \end{aligned}$$

Consider the coefficient of u in both side, we have

$$\delta_{ij}\chi_j(u^{-1}) = \frac{\chi_j(1)}{|G|} \sum_{s\in G} \chi_i(su^{-1})\chi_j(s^{-1}) = \frac{\chi_j(1)}{|G|} \sum_{s\in G} \chi_i(su^{-1})\overline{\chi_j(s)}$$

Take $u = e$, then $\delta_{ij}\chi_j(1) = \dfrac{\chi_j(1)}{|G|} \sum_{s\in G} \chi_i(s)\overline{\chi_j(s)} = \chi_j(1)\langle \chi_i, \chi_j \rangle \implies \langle \chi_i, \chi_j \rangle = \delta_{ij}$. □

3.5.3 Basic application

Corollary 3.5.1. $\rho \simeq \rho' \iff \chi_\rho = \chi_{\rho'}$

Proof: ($\Rightarrow$) : Done!

($\Leftarrow$) : If $\begin{cases} \rho \simeq \rho_1^{\oplus \ell_1} \oplus \cdots \oplus \rho_r^{\oplus \ell_r} \rightsquigarrow \chi_\rho = \ell_1\chi_1 + \cdots + \ell_r\chi_r \\ \rho' \simeq \rho_1^{\oplus \ell'_1} \oplus \cdots \oplus \rho_r^{\oplus \ell'_r} \rightsquigarrow \chi_{\rho'} = \ell'_1\chi_1 + \cdots + \ell'_r\chi_r \end{cases}$. By $\chi_\rho = \chi_{\rho'}$

$$\ell_i = \langle \chi_\rho, \chi_i \rangle = \langle \chi_{\rho'}, \chi_i \rangle = \ell'_i$$

So $\rho \simeq \rho'$. □

Fact 3.5.1. $\theta \in X(G)$, then $\theta = \chi_\rho$ for some $\rho : G \to \mathrm{GL}(V) \iff \theta = \sum_{i=1}^{r} \alpha_i \chi_i$ with $\alpha_i \in \mathbb{Z}_{\geq 0}$

Proof: ($\Rightarrow$) : $\rho \simeq \rho_1^{\oplus \ell_1} \oplus \cdots \oplus \rho_r^{\oplus \ell_r} \implies \theta = \chi_\rho = \sum_{i=1}^{r} \ell_i \chi_i$.

($\Leftarrow$) : Let $\rho' = \rho_1^{\oplus \alpha_1} \oplus \cdots \oplus \rho_r^{\oplus \alpha_r} \rightsquigarrow \theta = \chi_{\rho'}$. □

Fact 3.5.2. $\|\chi_\rho\| = 1 \iff \rho$ is irreducible. Here, $\|\theta\| := \sqrt{\langle \theta, \theta \rangle}$ for all $\theta \in X(G)$.

Proof: Let $\rho \simeq \rho_1^{\oplus \ell_1} \oplus \cdots \oplus \rho_r^{\oplus \ell_r} \rightsquigarrow \chi_\rho = \sum_{i=1}^{r} \ell_i \chi_i \rightsquigarrow \|\chi_\rho\|^2 = \sum_{i=1}^{r} \ell_i^2$

($\Rightarrow$) : $1 = \sum_{i=1}^{n} \ell_i^2 \rightsquigarrow \ell_i = 1$ for some i and others are $0 \rightsquigarrow \rho \simeq \rho_i$ is irr.

($\Leftarrow$) : $\rho \simeq \rho_i \rightsquigarrow \chi_\rho = \chi_i \rightsquigarrow \|\chi_\rho\|^2 = \langle \chi_i, \chi_i \rangle = 1$. □

By check those condition we had not explained clearly in Example 3.4.2

Example 3.5.1. $G \simeq S_3$, $V = \langle e_1, e_2, e_3 \rangle_{\mathbb{C}}$. Let $\rho : G \to \mathrm{GL}(V)$ be the permutation representation.

$$\rho_1 \longleftrightarrow N = \{\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 : \alpha_1 = \alpha_2 = \alpha_3 \text{ in } \mathbb{C}\} = \langle e_1, e_2, e_3 \rangle_{\mathbb{C}}$$

$\forall \sigma \in S_3$, $\sigma(e_1 + e_2 + e_3) = e_1 + e_2 + e_3$, so ρ_1 is trivial and we say χ_1 is **principal character**.

$$\rho_2 \longleftrightarrow I = \{\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 : \alpha_1 + \alpha_2 + \alpha_3 = 0 \text{ in } \mathbb{C}\} = \langle e_1 - e_2, e_2 - e_3 \rangle_{\mathbb{C}}$$

We check that ρ_2 is irreducible by checking norm. Since χ_{ρ_2} is class function, we only need to confirm the linear transformation corresponding to $e, (12), (123)$.

$$e_1 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad (12) \longmapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \qquad (123) \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

So $\chi_2(e) = 2$, $\chi(\text{two cycle}) = 0$, $\chi_2(\text{three cycle}) = -1$ and thus

$$\langle \chi_2, \chi_2 \rangle = \frac{1}{6}\left(2^2 + 3 \cdot 0^2 + 2 \cdot (-1)^2\right) = 1$$

So ρ_2 is indeed irreducible. Now, we check that $\rho_1, \rho_3 : \text{even} \mapsto 1, \text{odd} \mapsto (-1)$ are not isomorphic. Since $\chi_3(12) = -1$ but $\chi_1(12) = 1$. By Corollary 3.5.1, $\rho_1 \not\simeq \rho_3$. Now, we know that we can accurately write a representation as direct sum of some irreducible representation. We give a example : Let $\rho = \rho_2 \otimes \rho_2$, then $\chi_\rho = \chi_2 \cdot \chi_2$ i.e.

$$\chi_\rho(e) = 4 \qquad \chi_\rho(\text{two cycle}) = 0 \qquad \chi_\rho(\text{three cycle}) = 1$$

Then,

$$\begin{aligned}\langle \chi_\rho, \chi_1 \rangle =& \frac{1}{6}\left(4 \times 1 + 3(0 \times 1) + 2(1 \times 1)\right) = 1\\ \langle \chi_\rho, \chi_2 \rangle =& \frac{1}{6}\left(4 \times 2 + 3(0 \times 0) + 2(1 \times (-1))\right) = 1\\ \langle \chi_\rho, \chi_3 \rangle =& \frac{1}{6}\left(4 \times 1 + 3(0 \times (-1)) + 2(1 \times 1)\right) = 1\end{aligned}$$

and thus $\rho \simeq \rho_1 \oplus \rho_2 \oplus \rho_3$.

3.6 Divisibility and Burnside's theorem

3.6.1 Divisibility

Goal: Show that $\chi_i(1) \big| |G| \ \forall i = 1, ..., r$

Lemma 3.6.1 (Schur's lemma)**.** Let $T : V_1 \to V_2$ be a $\mathbb{C}[G]$-module homomorphism with V_1, V_2 : simple.

- If $V_1 \simeq V_2 \simeq V \rightsquigarrow T = \lambda I_V$ for some $\lambda \in \mathbb{C}$
- If $V_1 \not\simeq V_2 \rightsquigarrow T = 0$

Proof: By Schur's lemma in previous section, $T = 0$ or T is isomorphism (i.e $V_1 \simeq V_2$). If $V_1 \not\simeq V_2 \rightsquigarrow T = 0$. If $V_1 \simeq V_2$, regard V as $\mathbb{C}$-module homomorphism and $\lambda \in \mathbb{C}$ be the eigenvalue of T, say $Tv = \lambda v$ for some $0 \neq v \in V$. Then $v \in \ker(T - \lambda I_V) \neq 0 \implies \ker(T - \lambda I_V) = V$ i.e. $T = \lambda I_V$. □

Definition 3.6.1. Let $\alpha \in \mathbb{C}$. TFAE

- α is a root of a monic polynomial in $\mathbb{Z}[x]$
- α is algebraic over $\mathbb{Q}$ and $m_{\alpha,\mathbb{Q}} \in \mathbb{Z}[x]$
- $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module

Here, we call α is an **algebraic integer** in $\mathbb{C}$.
(Note: (1) ⇒ (2) by Gauss lemma)

Lemma 3.6.2. Let S be f.g. abelian subgroup of $\mathbb{C}$ and $x \in \mathbb{C}$. If $xS \subseteq S$, then x is an algebraic integer.

Proof: Say $S = \langle s_1, ..., s_n \rangle_{\mathbb{Z}}$, $xs_i = \sum_{j=1}^{n} a_{ij} s_j$ with $a_{ij} \in \mathbb{Z}$. Let $A = (a_{ij})$ and $\mathbf{s} = (s_1, ..., s_n)^t \neq 0$, then $(xI - A)\mathbf{s} = 0 \implies \det(xI - A) = 0$. □

Property 3.6.1. The set of all algebraic integers forms a subring of $\mathbb{C}$.

Proof: If α, β is a root of monic polynomial with degree m, n respectively. Let $S = \langle \alpha^i \beta^j : 0 \leq i \leq m, 0 \leq j \leq n \rangle_{\mathbb{Z}}$, then $\alpha S, \beta S \subset S$ and thus $(\alpha \pm \beta)S \subseteq S, \alpha\beta S \subseteq S$. By Lemma 3.6.2, $\alpha \pm \beta$, $\alpha\beta$ is algebraic integer. □

Lemma 3.6.3 (key lemma)**.** Let $K_1, ..., K_r$ be the distinct conjugacy classes of G.

(1) $\sum_{s \in K_j} \rho_i(s) = \dfrac{|K_j| \chi_i(t)}{\chi_i(1)} I_{n_i}$ for any $t \in K_j$.

(2) $\lambda_i(K_j) = \dfrac{|K_j| \chi_i(t)}{\chi_i(1)}$ with $t \in K_j$ is an algebraic integer $\forall i, j$.

Proof:

(1) LHS $T : V_i \to V_i$ is a $\mathbb{C}$-module homomorphism. In order to be able to use Schur lemma, we need to prove that is a $\mathbb{C}[G]$-module homomorphism. Since

$$\rho_i(u) T \rho_i(u)^{-1} = \sum_{s \in K_j} \rho_i(usu^{-1}) = T \ \forall u \in G$$

$\implies$ T is a $\mathbb{C}[G]$-module homomorphism.

By Schur lemma, say $T = \lambda I_{n_i}$ for some $\lambda \in \mathbb{C}$, then

$$\mathrm{tr}(T) = |K_j| \chi_i(t) \ \forall t \in K_j$$

In other hand, $\mathrm{tr}(T) = \lambda n_i = \lambda \chi_i(1)$. Hence,

$$\lambda = \frac{|K_j| \chi_i(t)}{\chi_i(1)} \ \forall t \in K_j$$

(2) For $u \in K_\ell$, define $n_{i,j,\ell} = \left| \{(s_i, s'_j) \in K_i \times K_j | s_i s'_j = u\} \right|$, which is indep. of choice of u since $(xs_i x^{-1})(xs_j x^{-1}) = xux^{-1}$.

Claim: $\lambda_t(K_i)\lambda_t(K_j) = \sum_{\ell=1}^{r} n_{i,j,\ell} \lambda_t(K_\ell) \ \forall i, j, t$.

pf.

$$\lambda_t(K_i) I_{n_t} \lambda_t(K_j) I_{n_t} = \left(\sum_{s \in K_i} \rho_t(s) \right) \left(\sum_{s' \in K_j} \rho_t(s') \right) = \sum_{\substack{s \in K_i \\ s' \in K_j}} \rho_t(ss')$$

$$= \sum_{\ell=1}^{r} \sum_{u \in K_\ell} n_{i,j,\ell} \rho_t(u) = \sum_{\ell=1}^{r} n_{i,j,\ell} \lambda_t(K_\ell) I_{n_t}$$

□

Hence, $\mathbb{Z}[\lambda_t(K_1), ..., \lambda_t(K_r)] = \langle 1, \lambda_t(K_1), ..., \lambda_t(K_r)\rangle_{\mathbb{Z}} = S$. Since $\mathbb{Z}$ is a PID and $\mathbb{Z}[\lambda_t(K_i)]$ is a submodule of S which is f.g. $\mathbb{Z}$-module $\implies \mathbb{Z}[\lambda_t(K_i)]$ is also f.g. over $\mathbb{Z} \implies \lambda_t(K_i)$ is an alg. integer.

□

Theorem 3.6.1. $\chi_i(1)\big||G|$ $\forall i = 1, ..., r$.

Proof:

$$\begin{aligned}\mathbb{Q} \ni \frac{|G|}{\chi_i(1)} &= \frac{|G|}{\chi_i(1)}\langle\chi_i, \chi_i\rangle = \frac{|G|}{\chi_i(1)} \cdot \frac{1}{|G|}\sum_{s\in G}\chi_i(s)\overline{\chi_i(s)} \\ &= \frac{1}{\chi_i(1)}\sum_{j=1}^{r}|K_j|\chi_i(t_j)\overline{\chi_i(t_j)} \text{ for some } t_j \in K_j \\ &= \sum_{j=1}^{r}\lambda_i(K_j)\overline{\chi_i(t_j)} = \sum_{j=1}^{r}\lambda_i(K_j)\chi_i(t_j^{-1})\end{aligned}$$

Note : In general, $\chi(s)$ is an algebraic integer since it is a sum of roots of 1 and each root of 1 is an algebraic integer. Hence, $\frac{|G|}{\chi_i(1)}$ is an alg. integer $\implies \frac{|G|}{\chi_i(1)} \in \mathbb{Z}$. □

3.6.2 Burnside's theorem

First, we see the statement of Burnside's theorem :

Theorem 3.6.2 (Burnside's theorem)**.** Let p, q be prime integers. If $|G| = p^a q^b$ with $a, b \in \mathbb{Z} \geq 0$, then G is solvable.

From the proof of Burnside's theorem, we can see another processing method provided by group representation. Before proving this theorem, we see some lemma will be used. (Or you can read this sub-section backwards)
Recall :

- $T \in \mathrm{Hom}_{\mathbb{C}}(V, V)$, $\langle\cdot,\cdot\rangle$: positive definite Hermitian form. TFAE
  - $T^*T = TT^* = 1$
  - $\langle Tx, Ty\rangle = \langle x, y\rangle$ $\forall x, y \in V$
- T is normal $\iff$ T is unitarily equivalent to a diagonal matrix.

Theorem 3.6.3. $\rho : G \to \mathrm{GL}(V)$, $\dim V = n \rightsquigarrow \exists$ a matrix representation $R : G \to \mathfrak{U}_n$ (all unitary matrix)

Proof: Given any positive definite Hermitian form $[\cdot,\cdot]$ on V. Define

$$\langle v, w\rangle = \frac{1}{|G|}\sum_{s\in G}[\rho_s(v), \rho_s(w)]$$

Then $\langle\rho_t(v), \rho_t(w)\rangle = \langle v, w\rangle$ $\forall t \in G, v, w \in V$. Hence, ρ_t is unitary. □

Lemma 3.6.4. Let G be a finite group and K be a conjugacy class in G. If ρ is an irr. representation of G with $\gcd(|K|, \chi_\rho(1)) = 1$, then $\forall s \in K$, either $\chi_p(s) = 0$ or ρ_s is a scalar matrix.

Proof:

- $\gcd(|K|, \chi_\rho(1)) = 1 \implies \exists a, b \in \mathbb{Z}$ s.t. $a|K| + b\chi_\rho(1) = 1$. For $s \in K$

$$\frac{\chi_\rho(s)}{\chi_\rho(1)} = a \underbrace{\frac{|K|\chi_\rho(s)}{\chi_\rho(1)}}_{=\lambda_\rho(K)} + b\chi_\rho(s) \text{ is algebraic integer}$$

  Let $\alpha = \frac{\chi_\rho(s)}{\chi_\rho(1)}$ and $f(x) = m_{\alpha,\mathbb{Q}} \in \mathbb{Z}[x]$. And let L be the splitting field of $f(x)$ over $\mathbb{Q}$.

- Since $\mathrm{char}\mathbb{Q} = 0$ and $m_{\alpha,\mathbb{Q}}$ is irreducible, $\mathrm{Gal}(L/F)$ is transitive. For each root β of $f(x)$, $\exists \sigma \in \mathrm{Gal}(L/\mathbb{Q})$ s.t. $\sigma(\alpha) = \beta$.

$$\because \alpha = \frac{\chi_\rho(s)}{\chi_\rho(1)} = \frac{\xi_1 + \cdots + \xi_{\chi_\rho(1)}}{\chi_\rho(1)} \text{ with } \xi_i : |G| \text{ th root of unity}$$

$$\therefore \beta = \sigma(\alpha) = \frac{1}{\chi_\rho(1)} \Big(\sigma(\xi_1) + \cdots + \sigma(\xi_{\chi_\rho(1)})\Big)$$

  Notice that $(\sigma(\xi_1))^{|G|} = \sigma(\xi_1^{|G|}) = \sigma(1) = 1$, then

$$|\beta| = \frac{1}{|\chi_\rho(1)|} \Big|\sigma(\xi_1) + \cdots + \sigma(\xi_{\chi_\rho(1)})\Big| \leq \frac{1 + \cdots + 1}{\chi_\rho(1)} = 1$$

- Hence, let $\beta_1 = \alpha, \beta_2, ..., \beta_k$ be roots of $f(x)$.

$$\implies |f(0)| = \left|\prod_{i=1}^{k} \beta_i\right| \leq \prod_{i=1}^{k} |\beta_i| \leq 1 \text{ and notice that } f(0) \in \mathbb{Z}$$

  - If $f(0) = 0 \rightsquigarrow \exists \beta_j = 0$, say $\alpha = \sigma(\beta_j) = 0 \rightsquigarrow \chi_\rho(s) = 0$
  - If $f(0) = \pm 1 \rightsquigarrow |\beta_i| = 1 \ \forall i$. In particular $|\alpha| = 1 \implies |\chi_\rho(s)| = \chi_\rho(1) := n$. If $\zeta_i \neq \zeta_j$, then

$$|\chi_\rho(s)| = |\xi_1 + \cdots + \xi_n| \leq |\xi_i + \xi_j| + (n-2) < 2 + (n-2) \ (\rightarrow\!\!\!\leftarrow)$$

    Hence, ρ_s has a diagonal matrix representation with diagonal entries are all same i.e. scalar matrix.

□

Lemma 3.6.5. Assume that $K \neq \{e\}$ is conjuacy class of $s \in G$. If $|K| = p^c$, then G is not a non-abelian simple group.

Proof: Assume not, say G is a non-abelian simple group.

- $c = 0$: Say $K = \{s \neq e\} \rightsquigarrow s \in Z(G)$ and $\{e\} \neq Z(G) \trianglelefteq G$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$
- $c > 0$: $\chi^{\text{reg}} = \sum_{i=1}^{r} \chi_i(1)\chi_i$. Let $e \neq s \in K$ and ρ_1 : trivial, then

$$0 = \chi^{\text{reg}}(s) = 1 + \sum_{i=2}^{r} n_i \chi_i(s)$$

  - If $p | n_i$ for all i s.t. $\chi_i(s) \neq 0$, then

$$\frac{-1}{p} = \sum_{i=2}^{r} \frac{n_i}{p} \chi_i(s) \text{ is algebraic integer } (\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$$

  - $p \nmid n_j$ for some j with $\chi_j(s) \neq 0$: Since G is simple, $\rho_j : G \hookrightarrow \mathrm{GL}(V_j) \simeq \mathrm{GL}_{n_j}(\mathbb{C})$. Notice that ρ_j is irr. and $\gcd(p, \chi_j(1)) = 1$. By Lemma 3.6.4, since $\chi_j(s) \neq 0 \implies \rho_j(s)$ is a scalar matrix. Since $\rho_j(s)$ commutes with all $\rho_j(s') \in \rho_j(G)$ $\therefore$ $\rho_j(s) \in Z(\rho_j(G))$ and thus $e \neq s \in Z(G)$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$.

□

Proof: (Burnside's theorem) We have known that if $|G|$ is a p-group, then G is solvable. So here, we assume $p \neq q$ and $a > 0, b > 0$. Let G be a counter example of minimal order.

- If G has a proper nontrivial normal subgroup N, then N, G/N are solvable by minimality, which implies that G is solvable $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$. So we may assume that G is a non-abelian simple group.
- Let $P \in \mathrm{Syl}_p(G) \rightsquigarrow \exists e \neq s \in Z(P)$. $\because P \leq C_G(s)$ and $|K_s| = [G : C_G(s)] = |G|/|C_G(s)|$ $\therefore$ $|K_s| = q^d$ for some $d \geq 0$. By lemma 3.6.5, G is not a non-abelian simple group. $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$

Hence, every group at most two prime divisors of order is solvable. □

3.7 Examples

3.7.1 Examples (Dihedral group and S_5)

- $G = S_3$: By previous example, there exists actually 3 irreducible character :

classes	1	(12)	(123)
size	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

with $\deg\chi_1 = \deg\chi_2 = 1$ and $\deg\chi_3 = 2$. Let $\chi_4 = \chi_3 \otimes \chi_3 \rightsquigarrow \rho_4 = \rho_1 \oplus \rho_2 \oplus \rho_3$. Let $\rho_5 = \rho_3 \otimes \rho_4$, then

classes	1	(12)	(123)
χ_5	8	0	-1

$$\langle\chi_5, \chi_1\rangle = \frac{1}{6}(8\cdot 1 + 0 + 2\cdot(-1)\cdot 1) = 1$$
$$\langle\chi_5, \chi_2\rangle = \frac{1}{6}(8\cdot 1 + 0 + 2\cdot(-1)\cdot 1) = 1$$
$$\langle\chi_5, \chi_3\rangle = \frac{1}{6}(8\cdot 2 + 0 + 2\cdot(-1)\cdot(-1)) = 3$$

Hence, $\rho_5 = \rho_1 \oplus \rho_2 \oplus \rho_3^{\oplus 3}$.

Now, we want to find all irreducible representation of Dihedral group.

- $G = D_{2n} = \langle x, y | x^n = 1, y^2 = 1, yxy^{-1} = x^{-1}\rangle$ with n : even :
  - irr. rep. of degree 1 : By Homework 23, we have the correspondence between degree 1 representation of G and degree 1 representation of $G/[G,G]$. Let $H = \langle x^2\rangle \rightsquigarrow |H| = \frac{n}{2}$ and $H \trianglelefteq D_{2n}$ (since $yx^2y^{-1} = x^{-2}$) $\rightsquigarrow |D_{2n}/H| = 4 \rightsquigarrow D_{2n}/H$ is abelian $\rightsquigarrow [D_{2n}, D_{2n}] \leq H$. $\because x^{-2} = yxy^{-1}x^{-1}$ $\therefore H = [D_{2n}, D_{2n}]$.
    $D_{2n}\Big/[D_{2n}, D_{2n}] = \langle\overline{x}, \overline{y}\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so there as 4 rep. of degree 1

classes	$\{e\}$	$\{\overline{x}\}$	$\{\overline{y}\}$	$\{\overline{xy}\}$
size	1	1	1	1
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

  - irr. rep. of degree 2 : For all $1 \leq k \leq n-1$, define

$$\begin{aligned} R_k : \quad x &\longmapsto \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix} \\ y &\longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \Longrightarrow \quad x^\ell &\longmapsto \begin{pmatrix} \cos\frac{2\pi k\ell}{n} & -\sin\frac{2\pi k\ell}{n} \\ \sin\frac{2\pi k\ell}{n} & \cos\frac{2\pi k\ell}{n} \end{pmatrix} \\ x^\ell y &\longmapsto \begin{pmatrix} -\sin\frac{2\pi k\ell}{n} & \cos\frac{2\pi k\ell}{n} \\ \cos\frac{2\pi k\ell}{n} & \sin\frac{2\pi k\ell}{n} \end{pmatrix} \end{aligned}$$

    Notice that for $k = \frac{n}{2}$, $x : e_1 + e_2 \mapsto -(e_1+e_2)$ and $y : e_1+e_2 \mapsto (e_1+e_2) \implies \mathbb{C}^2$ has nontrivial proper G-invariant which means R_k is not irreducible. Notice that

$$\begin{cases} \chi_{R_k}(x^\ell y) = 0 \\ \chi_{R_k}(x^\ell) = 2\cos\frac{2\pi k\ell}{n} \end{cases} \rightsquigarrow \begin{cases} \chi_{R_k} = \chi_{R_{n-k}} \ \forall k = 1, ..., \frac{n}{2} - 1 \\ \implies \chi_{R_1}, ..., \chi_{R_{\frac{n}{2}-1}} \text{ are distinct irr. character. of deg 2} \end{cases}$$

- Since $2n = 4\cdot 1^2 + (\frac{n}{2}-1)\cdot 2^2 \implies \chi_1, ..., \chi_4, \chi_{R_1}, ..., \chi_{R_{\frac{n}{2}-1}}$ are all irr. character.

- $G = D_{2n}$ with n is odd :
  - Let $|H| = \langle x \rangle \rightsquigarrow |H| = n$ and $|D_{2n}/H| = 2 \implies [D_{2n}, D_{2n}] \leq H$. Since $\gcd(n, 2) = 1$, $H = \langle x^2 \rangle$ and thus $x^{-2} = yxy^{-1}x^{-1} \in [D_{2n}, D_{2n}]$.
    Then $D_{2n}\Big/[D_{2n}, D_{2n}] = \langle \overline{y} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. There are two rep. of degree $1 : x \mapsto 1$, $y \mapsto \pm 1$.
  - For $1 \leq k \leq n-1$, define

$$R_k : \begin{array}{ccc} x & \longmapsto & \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix} \\ y & \longmapsto & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array}$$

    We can check that $\chi_{R_k} = \chi_{R_{n-k}}$ for $k = 1, ..., \frac{n-1}{2} \rightsquigarrow \chi_{R_1}, ..., \chi_{R_{\frac{n-1}{2}}}$ are distinct.
    Notice that $2n = 2\cdot 1^2 + \frac{n-1}{2}\cdot 2^2 \implies R_1, ..., R_{\frac{n-1}{2}}$ are all irr. rep. of deg 2 and does exists irr. rep. of deg ≥ 3.

Now, we want to find all irreducible representation of Dihedral group.

- $G = S_5$: $[S_5, S_5] = A_5$ since $S_5/A_5 \simeq \mathbb{Z}/2\mathbb{Z} \implies [S_5, S_5] \leq A_5$ and $(abc) = (acb)^2 = (ab)(ac)(ab)^{-1}(ac)^{-1} \in [S_5, S_5]$. Then there are two irr. rep. of deg 1, which are trivial rep. and "sign" function.

conjugacy class	$\{e\}$	$\{(12)\}$	$\{(123)\}$	$\{(1234)\}$	$\{(12345)\}$	$\{(12)(34)\}$	$\{(12)(345)\}$
size	1	10	20	30	24	15	20

  Hence, $\exists 7$ irr. rep. of S_5.

- Permutation representation : $V = \langle e_1, ..., e_5 \rangle_{\mathbb{C}} = \mathbb{C}(e_1 + \cdots + e_5) \oplus W =: N \oplus W$.
  Let $\rho : S_5 \to \mathrm{GL}_5(V)$ be permutation representation. Then consider $[\rho_s]_{\{e_1,...,e_5\}}$ we have

	{e}	{(12)}	{(123)}	{(1234)}	{(12345)}	{(12)(34)}	{(12)(345)}
χ_ρ	5	3	2	1	0	1	0

  and denoted by $\chi_\rho = (5, 3, 2, 1, 0, 1, 0)$. Let $\chi^W := \chi_{\rho|_W}$. Since $V = N \oplus W \implies \chi_\rho = \chi^N + \chi^W$. Combine with $\chi^N = (1, ..., 1)$, we have $\chi^W = (4, 2, 1, 0, -1, 0, -1)$. Then

$$\langle \chi^W, \chi^W \rangle = \frac{1}{120}\left(1\cdot 4^2 + 10\cdot 2^2 + 20\cdot 1^2 + 30\cdot 0^2 + 24\cdot(-1)^2 + 15\cdot 0^2 + 20\cdot(-1)^2\right) = 1$$

  i.e. ρ^W is irreducible.

- Now, we have

$$\chi_1 = (1,1,1,1,1,1,1) : \deg 1 \longleftrightarrow \text{trivial}$$
$$\chi_2 = (1,-1,1,-1,1,1,-1) : \deg 1 \longleftrightarrow \text{sign function}$$
$$\chi_3 = (4,2,1,0,-1,0,-1) : \deg 4$$

  By homework 24, tensor of degree 1 and a irreducible rep. is also a irreducible. So $\chi_4 := \chi_2\chi_3 = (4,-2,1,0,-1,0,1)$: is irr. with deg 4.

- Now, we need to introduce new method to find irreducible representation.

  Let $V = \{e_1, ..., e_n\}_{\mathbb{C}}$. Define

$$\theta : \begin{array}{ccc} V \otimes V & \longrightarrow & V \otimes V \\ e_i \otimes e_j & \longmapsto & e_j \otimes e_i \end{array} \implies \theta(x \otimes y) = y \otimes x$$

  Define

$$\textbf{Symmetric power} : \mathrm{Sym}^2(V) := \{z \in V \otimes V : \theta(z) = z\} \subseteq V \otimes V$$
$$\textbf{Alternating power} : \mathrm{Alt}^2(V) := \{z \in V \otimes V : \theta(z) = -z\} \subseteq V \otimes V$$

  Then $V \otimes V = \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$, since

$$v \otimes w = \underbrace{\frac{1}{2}(v \otimes w + w \otimes v)}_{\in \mathrm{Sym}^2(V)} + \underbrace{\frac{1}{2}(v \otimes w - w \otimes v)}_{\in \mathrm{Alt}^2(V)}$$

  and $\dim_{\mathbb{C}} \mathrm{Sym}^2(V) = \dfrac{n(n+1)}{2}$, $\dim_{\mathbb{C}} \mathrm{Alt}^2(V) = \dfrac{(n-1)n}{2}$.

  - Given $\rho : G \to \mathrm{GL}(V)$, define $\widetilde{\rho} = \rho \otimes \rho : G \to \mathrm{GL}(V \otimes V)$

    $\mathrm{Sym}^2(V)$ is G-invariant : If $z = \sum_{i=1}^{m} a_i(v_i \otimes w_i)$ with $\theta(z) = z$. Then

$$\widetilde{\rho}(z) = \sum_{i=1}^{m} a_i(\rho_i(v_i) \otimes \rho(w_i)) \implies \theta(\widetilde{\rho}(z)) = \sum_{i=1}^{m} a_i(\rho(w_i) \otimes \rho(v_i))$$
$$= \widetilde{\rho}(\sum_{i=1}^{m} a_i(w_i \otimes v_i)) = \widetilde{\rho}(\theta(z)) = \widetilde{\rho}(z) \implies \widetilde{\rho}(z) \in \mathrm{Sym}^2(V)$$

    $\mathrm{Alt}^2(V)$ is G-invariant : Similarly.

  - Given ρ_s, choose suitable basis β s.t. $[\rho_s]_\beta = \mathrm{diag}(\xi_1, ..., \xi_n)$. Then $\rho_s \otimes \rho_s(v_i \otimes v_j) = \xi_i\xi_j(v_i \otimes v_j)$. Choose the basis $v_i \otimes v_j$ with $i \le j$ for $\mathrm{Sym}^2(V)$, then

$$\chi^{\mathrm{sym}}(s) = \sum_{i \le j} \xi_i\xi_j = \frac{1}{2}\left(\left(\sum_i \xi_i\right)^2 + \sum_i \xi_i^2\right) = \frac{1}{2}(\chi_\rho(s)^2 + \chi_\rho(s^2))$$

$$\implies \chi^{\mathrm{alt}}(s) = \chi_{\widetilde{\rho}}(s) - \chi^{\mathrm{sym}}(s) = \chi_\rho(s)^2 - \frac{1}{2}(\chi_\rho(s)^2 + \chi_\rho(s^2)) = \frac{1}{2}(\chi_\rho(s)^2 - \chi_\rho(s^2))$$

- Now, back to find the irreducible representation of S_5.

  $\chi_3 \rightsquigarrow \rho : G \to \mathrm{GL}(V)$ with $\dim V = 4$. Then $\widetilde{\rho} = \rho \otimes \rho : G \to \mathrm{GL}(V \otimes V)$. Then

  $$\chi^{\mathrm{sym}} = \frac{1}{2}(\chi_\rho(s)^2 + \chi_\rho(s^2)) = (10, 4, 1, 0, 0, 2, 1) \implies \langle \chi^{\mathrm{sym}}, \chi^{\mathrm{sym}} \rangle = 3$$

  $$\chi^{\mathrm{alt}} = (6, 0, 0, 0, 1, -2, 0) \implies \langle \chi^{\mathrm{alt}}, \chi^{\mathrm{alt}} \rangle = 1$$

  Let $\chi_5 = \chi^{\mathrm{alt}}$ is irreducible representation. Now, we see if there exists new irr. representation in χ^{sym}.

  $$\langle \chi^{\mathrm{sym}}, \chi_1 \rangle = 1,\ \langle \chi^{\mathrm{sym}}, \chi_2 \rangle = 0,\ \langle \chi^{\mathrm{sym}}, \chi_3 \rangle = 1,\ \langle \chi^{\mathrm{sym}}, \chi_4 \rangle = 0,\ \langle \chi^{\mathrm{sym}}, \chi_5 \rangle = 0$$

  Then $\chi^{\mathrm{sym}} = \chi_1 + \chi_3 + \chi_?$ for some $\chi_?$ with deg 5.

- Since $120 = 2 \cdot 1^2 + 2 \cdot 4^2 + 6^2 + a^2 + b^2$ for some $a, b \in \mathbb{N}$. Then $(a, b) = (5, 5), (7, 1)$. But $7 \nmid 120$. So $\chi_?$ has a high probability is what we want.

  Let $\chi_6 - \chi^{\mathrm{sym}} - \chi_1 - \chi_3 = (5, 1, -1, -1, 0, 1, 1) \rightsquigarrow \langle \chi_6, \chi_6 \rangle = 1$ i.e. χ_6 is irreducible.

  Now we only have one missing, we can consider χ^{reg} subtract suitable character :

  $$5\chi_7 = \chi^{\mathrm{reg}} - \chi_1 - \chi_2 - 4\chi_3 - 4\chi_4 - 6\chi_5 - 5\chi_6$$

  or using χ_6 multiply a irreducible character of degree 1 :

  $$\chi_7 = \chi_2\chi_6 = (5, -1, -1, 1, 0, 1, -1)$$

3.7.2 Product of groups

$\rho : G \to \mathrm{GL}(V)$, $\rho' : G' \to \mathrm{GL}(V')$. Define

$$\begin{array}{rccc} \rho \otimes \rho' : & G \times G' & \longrightarrow & \mathrm{GL}(V \otimes V') \\ & (s, s') & \longmapsto & \rho_s \otimes \rho'_s \end{array}$$

- group homo : $\rho \otimes \rho'((s, s')(t, t')) = \rho \otimes \rho'(st, s't') = \rho_{st} \otimes \rho'_{s't'} = (\rho_s\rho_t) \otimes (\rho'_{s'}\rho'_{t'}) = (\rho_s \otimes \rho'_{s'}) \circ (\rho_t \otimes \rho'_{t'})$
- $\chi_{\rho\otimes\rho'} = \chi_\rho \odot \chi'_{\rho'} : (s, s') \mapsto \chi_\rho(s)\chi_{\rho'}(s')$
- ρ, ρ' : irr. $\implies$ $\rho \otimes \rho'$: irr. :

  $\because \rho, \rho'$ are irr. $\therefore \dfrac{1}{|G|}\displaystyle\sum_{s\in G} |\chi_\rho(s)|^2 = 1,\ \dfrac{1}{|G'|}\sum_{s'\in G'} |\chi_{\rho'}(s')|^2 = 1$

  Thus,

  $$1 = \frac{1}{|G||G'|}\left(\sum_{s\in G} |\chi_\rho(s)|^2\right)\left(\sum_{s'\in G'} |\chi_{\rho'(s')}|^2\right) = \frac{1}{|G \times G'|}\sum_{(s,s')\in G\times G'} |\chi_\rho(s)\chi_{\rho'}(s')|$$

  $$\implies \langle \chi_{\rho\otimes\rho'}, \chi_{\rho\otimes\rho'} \rangle = 1$$

- Each irr. rep. of $G \times G'$ is isom. to some $\rho \otimes \rho'$:

  pf. Let $\{\rho_1, ..., \rho_r\}, \{\rho'_1, ..., \rho'_{r'}\}$ be the set of all irr. rep. of G, G' respectively. Write $\chi_i = \chi_{\rho_i}$ and $\chi'_j = \chi_{\rho'_j}$.

  Claim: Let $\mathfrak{D} = \langle \chi_i \odot \chi_j : i = 1, ..., r, j = 1, ..., r' \rangle_{\mathbb{C}}$. Then $\mathfrak{D} = X(G \times G')$

  pf. Let $f \in \mathfrak{D}^{\perp}$. By def,

$$\frac{1}{|G \times G'|} \sum_{(s,s') \in G \times G'} f(s, s') \overline{\chi_i(s) \chi'_j(s')} = 0 \ \forall i, j$$

  Rewrite as

$$\frac{1}{|G'|} \sum_{s' \in G'} \left(\frac{1}{|G|} \sum_{s \in G} f(s, s') \overline{\chi_i(s)} \right) \overline{\chi'_j(s')} = 0 \ \forall i, j$$

  Then

$$\left\langle \frac{1}{|G|} \sum_{s \in G} f(s, \cdot) \overline{\chi_i(s)}, \chi'_j \right\rangle = 0 \ \forall i, j$$

$\implies \frac{1}{|G|} \sum_{s \in G} f(s, \cdot) \overline{\chi_i(s)} \in \langle \chi'_1, ..., \chi'_{r'} \rangle_{\mathbb{C}}^{\perp} = 0$ in $X(G')$. Again,

$$\frac{1}{|G|} \sum_{s \in G} f(s, s') \overline{\chi_i(s)} = 0 \ \forall i, \forall s' \implies f(\cdot, s') \in \langle \chi_1, ..., \chi_r \rangle_{\mathbb{C}}^{\perp} = 0 \text{ in } X(G) \ \forall s'$$

  Hence, $f(s, s') = 0 \ \forall s \in G, s' \in G'$.

Example 3.7.1. $G = D_8 \times S_5$:

- We're calculate irreducible representation of D_8 quickly again.

	e	y	x	x^2	xy
χ_1	1	1	1	1	1
χ_2	1	-1	-1	1	1
χ_3	1	-1	1	1	-1
χ_4	1	1	-1	1	-1

  By $8 = 4 \cdot 1^2 + 2^2 \implies \chi^{\text{reg}} = \chi_1 + \chi_2 + \chi_3 + \chi_4 + 2\chi_5$. Hence,

$$\chi_5 = (2, 0, 0, -2, 0)$$

- S_5 :

	$\{e\}$	$\{(12)\}$	$\{(123)\}$	$\{(1234)\}$	$\{(12345)\}$	$\{(12)(34)\}$	$\{(123)(45)\}$
χ'_1	1	1	1	1	1	1	1
χ'_2	1	-1	1	-1	1	1	-1
χ'_3	4	2	1	0	-1	0	-1
χ'_4	4	-2	1	0	-1	0	1
χ'_5	6	0	0	0	1	-2	0
χ'_6	5	1	-1	-1	0	1	1
χ'_7	5	-1	-1	1	0	1	-1

- $\chi_i\chi'_j = (\cdot, ..., \cdot)$ has 35 entry.

  eg. Given a order for conjugacy classes, we have

$$\chi_2\chi'_3 = (4, 2, 1, 0, -1, 0, -1, -4, -2, -1, 0, 1, 0, 1, -4, -2, -1, 0, 1, 0, 1, \cdots)$$

3.8 Induced representations (I)

3.8.1 Definition and properties

Ques : How to obtain a representation of G from the representation of its subgroups?
Observation : It may not be possible to extend a representation of H to a representation ρ of G in such a way that $\rho|_H = \varphi$. For example :

$$\begin{array}{rccc} \varphi: & A_3 & \longrightarrow & \mathbb{C}^\times \\ & 1 & \longmapsto & 1 \\ & (123) & \longmapsto & \omega \\ & (132) & \longmapsto & \omega^2 \end{array}$$

But every degree 1 representation of S_3 obtain $A_3 = [S_3, S_3]$ in its kernel i.e. φ cannot be extended to S_3.

Definition 3.8.1. Let $H \leq G$ and V be a $\mathbb{C}[H]$-module via $\varphi : H \to \mathrm{GL}(V)$. The $\mathbb{C}[G]$-module $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ is called the **induced module**, denoted by $\mathrm{Ind}_H^G(V)$. $\rho : G \to \mathrm{GL}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V)$ is called the **induced representation** and χ_ρ is called the **induced character**, denoted by $\mathrm{Ind}_H^G(\chi_\varphi)$.

Property 3.8.1 (basic)**.** Let $H \leq G$ and $\{a_1H, ..., a_mH\}$ be the set of distinct left cosets of H in G. Let $\varphi : H \to \mathrm{GL}(V)$ with $\dim V = n$ and $W = \mathbb{C}[G] \otimes_{\mathbb{C}[G]} V$. Then $\dim_{\mathbb{C}} W = mn$ and $\exists$ a basis $\{e_i\}$ for W s.t. $\forall s \in G$

$$[\rho_s]_{e_i} = \begin{pmatrix} [\varphi_{a_1^{-1}sa_1}]_{n\times n} & \cdots & [\varphi_{a_1^{-1}sa_m}]_{n\times n} \\ \vdots & & \vdots \\ [\varphi_{a_m^{-1}sa_1}]_{n\times n} & \cdots & [\varphi_{a_m^{-1}sa_m}]_{n\times n} \end{pmatrix}$$

Here, $\varphi_{a_i^{-1}sa_j} := 0$ whenever $a_i^{-1}sa_j \notin H$.

Proof:

- First, as a $\mathbb{C}$-vector space,

  $\mathbb{C}[G] = \mathbb{C}\cdot a_1H \oplus \cdots \oplus \mathbb{C}\cdot a_mH = a_1\mathbb{C}[H] \oplus \cdots \oplus a_m\mathbb{C}[H]$: free right $\mathbb{C}[H]$-module

$$\implies W = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V \simeq \bigoplus_{i=1}^{m} a_i\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V = \bigoplus_{i=1}^{m} a_i \otimes_{\mathbb{C}[H]} V$$

  since $a_iz \otimes v = a_i \otimes zv \ \forall z \in \mathbb{C}[H]$ and $\mathbb{C}[H]V = V$.

  Since $\mathbb{C}[G]$ is $\mathbb{C}[G], \mathbb{C}[H]$-bimodule and V is left $\mathbb{C}[H]$-module $\rightsquigarrow \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ is $\mathbb{C}[G]$-module with action : $g(z \otimes v) = (gz) \otimes v$.

- So if $\{v_1, ..., v_n\}$ be a basis for V over $\mathbb{C}$, then $\{a_i \otimes v_j : 1 \le i \le m, 1 \le j \le n\}$ is a basis for W over $\mathbb{C} \implies \dim_{\mathbb{C}} W = mn$. We give the order by $a_i \otimes v_j = e_{n(i-1)+j}$.
- Now, we want to calculate $[\rho_s]_{e_i}$. $\forall s \in G$, by $sa_i \in G = \bigcup_{k=1}^{m} a_k H$, say $sa_i = a_k h$ for some $k \in \{1, ..., m\}, h \in H$. Then $\forall j$

  $\rho_s(a_i \otimes v_j) = sa_i \otimes v_j = (a_k h) \otimes v_j = a_k \otimes (hv_j) = a_k \otimes \varphi_h(v_j) = a_k \otimes \varphi_{a_k^{-1} s a_i}(v_j)$

  Hence, (i,k)-block in $[\rho_s]_{e_i}$ is $[\varphi_{a_k^{-1} s a_i}]_{\{v_i\}}$ and (i,k')-block in $[\rho_s]_{e_i}$ is O for all $k' \ne k$.

□

Corollary 3.8.1. By Property 3.8.1, we can directly get

$$\mathrm{Ind}_H^G(\chi_\varphi)(s) = \sum_{i=1}^{m} \chi_\varphi(a_i^{-1} s a_i)$$

where $\chi_\varphi(a_i^{-1} s a_i) = 0$ if $a_i^{-1} s a_i \notin H$. Notice that this formula is depend on the representation of left cosets. After some adjustments, we have
Reciprocity formula :

$$\mathrm{Ind}_H^G(\chi)\varphi)(s) = \frac{1}{|H|} \sum_{a \in G} \chi_\varphi(a^{-1} s a)$$

where $\chi_\varphi(a^{-1} s a) = 0$ if $a^{-1} s a \notin H$.

Proof: $\because G = \bigcup_{i=1}^{m} a_i H \ \therefore \forall a \in a_i H$, say $a = a_i h$, $a^{-1} s a = h^{-1}(a_i^{-1} s a_i) h$ i.e. $a^{-1} s a$ and $a_i^{-1} s a_i$ are conjugate. Since χ_φ is class function, $\chi_\varphi(a^{-1} s a) = \chi_\varphi(a_i^{-1} s a_i)$. □

Corollary 3.8.2. If s is not conjugate to some elements of H in G, then $\mathrm{Ind}_H^G(\chi_\varphi)(s) = 0$. In particular, if $H \lhd G$, then $\mathrm{Ind}_H^G(\chi_\varphi)\big|_{G \setminus H} = 0$.

Example 3.8.1. $G = D_{12} = \langle x, y | x^6 = 1, y^2 = 1, yxy = x^{-1} \rangle$, $H = \langle 1, x^3, y, x^3 y \rangle \simeq V_4$. $[G : H] = 3 \rightsquigarrow G = 1 \cdot H \cup xH \cup x^2 H =: a_1 H \cup a_2 H \cup a_3 H$. Consider

$$\begin{array}{rccc} \varphi: & H & \longrightarrow & \mathrm{GL}_2(\mathbb{C}) \\ & x^3 & \longmapsto & \begin{pmatrix} -1 & \\ & 1 \end{pmatrix} = A \\ & y & \longmapsto & \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} = B \\ & x^3 y & \longmapsto & \begin{pmatrix} -1 & \\ & -1 \end{pmatrix} = C \end{array}$$

Then $\dim_{\mathbb{C}} W = 6$ with basis $\begin{cases} e_1 = 1 \otimes v_1 & e_3 = x \otimes v_1 & e_5 = x^2 \otimes v_1 \\ e_2 = 1 \otimes v_2 & e_4 = x \otimes v_2 & e_6 = x^2 \otimes v_2 \end{cases}$

$$\begin{aligned} \rho_x(1 \otimes v_i) &= x \cdot 1 \otimes v_i = x \otimes v_i & \rho_y(1 \otimes v_i) &= y \cdot 1 \otimes v_i = 1 \otimes y v_i \\ \rho_x(x \otimes v_i) &= x \cdot x \otimes v_i = x^2 \otimes v_i & \rho_y(x \otimes v_i) &= y \cdot x \otimes v_i = x^5 y \otimes v_i = x^2 \otimes x^3 y v_i \\ \rho_x(x^2 \otimes v_i) &= x \cdot x^2 \otimes v_i = 1 \otimes x^3 v_i & \rho_y(x^2 \otimes v_i) &= y x^2 \cdot 1 \otimes v_i = x \otimes x^3 y v_i \end{aligned}$$

$$\Longrightarrow [\rho_x] = \begin{pmatrix} O & O & A \\ I_2 & O & O \\ O & I_2 & O \end{pmatrix} \text{ and } [\rho_y] = \begin{pmatrix} B & O & O \\ O & O & C \\ O & C & O \end{pmatrix}$$

Or we can using Property 3.8.1 help us to calculate the block in $[\rho_x], [\rho_y]$.
$a_i = x^{i-1} \rightsquigarrow a_i^{-1} x a_j = x^{j-i+1}$, $a_i^{-1} y a_j = x^{2-i-j} y$. Then

$a_i^{-1}xa_j$			
	x	x^2	x^3
	1	x	x^2
	x^3	1	x

$$\Longrightarrow [\rho_x] = \begin{pmatrix} \varphi_x & \varphi_{x^2} & \varphi_{x^3} \\ \varphi_1 & \varphi_x & \varphi_{x^2} \\ \varphi_{x^3} & \varphi_1 & \varphi_x \end{pmatrix} = \begin{pmatrix} O & O & A \\ I_2 & O & O \\ O & I_2 & O \end{pmatrix}$$

Property 3.8.2 (important)**.**

(1) Regard Ind_H^G as a operator form $X(H)$ to $X(G)$. By Reciprocity formula,

$$\mathrm{Ind}_H^G(\chi_\varphi + \chi_{\varphi'})(s) = \frac{1}{|H|} \sum_{a \in G} (\chi_\varphi + \chi_{\varphi'})(a^{-1}sa) = \left(\mathrm{Ind}_H^G(\chi_\varphi) + \mathrm{Ind}_H^G(\chi_{\varphi'})\right)(s)$$

i.e. Ind_H^G is linear.

(2) If $\begin{cases} H \leq K \leq G \\ \varphi : H \to \mathrm{GL}(V) \end{cases}$. By $\mathbb{C}[G] \otimes_{\mathbb{C}[K]} \left(\mathbb{C}[K] \otimes_{\mathbb{C}[H]} V\right) \simeq \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$, we have

$$\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(\chi_\varphi)) = \mathrm{Ind}_H^G(\chi_\varphi)$$

(3) (**Frobenius reciprocity**) If $g \in X(H)$, $f \in X(G)$, then

$$\langle g, \mathrm{Res}\, f \rangle_H = \langle \mathrm{Ind}\, g, f \rangle_G$$

where $\mathrm{Res}\, f := f|_H$ and $(\mathrm{Ind}\, g)(s) = \dfrac{1}{|H|} \displaystyle\sum_{\substack{a \in G \\ a^{-1}sa \in H}} g(a^{-1}sa)$.

$$\begin{cases} \mathrm{Res}: & X(G) \longrightarrow X(H) \\ \mathrm{Ind}: & X(H) \longrightarrow X(G) \end{cases} \Longrightarrow \text{ Res and Ind are adjoints of each other.}$$

Proof: Recall that $X(G) = \langle \chi_{\rho_1}, ..., \chi_{\rho_r} \rangle_{\mathbb{C}}$ and $X(H) = \langle \chi_{\rho'_1}, ..., \chi_{\rho'_\ell} \rangle_{\mathbb{C}}$, where $\{\chi_{\rho_i}\}$ and $\{\chi_{\rho'_i}\}$ are all irreducible representation of G and H respectively. Together with (1), we may assume that $\begin{cases} f = \chi_\rho \text{ with } \varphi : G \to \mathrm{GL}(W) : \text{irr.} \\ g = \chi_\varphi \text{ with } \varphi : H \to \mathrm{GL}(V) : \text{irr.} \end{cases}$. Now, we see a important claim first :

Claim : If $\begin{cases} \rho : G \to \mathrm{GL}(W) \\ \rho' : G \to \mathrm{GL}(W') \end{cases}$, then $\langle \chi_\rho, \chi_{\rho'} \rangle = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(W, W') =: \langle W, W' \rangle_G$

pf. Write

$$\begin{array}{ccc} \rho \simeq \rho_1^{\oplus m_1} \oplus \cdots \oplus \rho_r^{\oplus m_r} & & \rho' \simeq \rho_1^{\oplus m'_1} \oplus \cdots \oplus \rho_r^{\oplus m'_r} \\ \rightsquigarrow \quad W \simeq W_1^{\oplus m_1} \oplus \cdots \oplus W_r^{\oplus m_r} & \text{and} & \rightsquigarrow \quad W' \simeq W_1^{\oplus m'_1} \oplus \cdots \oplus W_r^{\oplus m'_r} \\ \rightsquigarrow \quad \chi_\rho \simeq m_1\chi_1 + \cdots + m_r\chi_r & & \rightsquigarrow \quad \chi_{\rho'} \simeq m'_1\chi_1 + \cdots + m'_r\chi_r \end{array}$$

Then $\langle \chi_\rho, \chi'_\rho \rangle = \sum_{i,j} m_i m'_j \langle \chi_i, \chi_j \rangle = \sum_{i=1}^{r} m_i m'_i$ and

$$\mathrm{Hom}_{\mathbb{C}[G]}(W, W') \simeq \bigoplus_{i,j} \left(\mathrm{Hom}_{\mathbb{C}[G]}(W_i, W_j)\right)^{\oplus m_i m'_j}$$

By Schur's lemma, we have

$$\mathrm{Hom}_{\mathbb{C}[G]}(W_i, W_j) = \begin{cases} 0 & , \text{if } i \neq j \\ \{\lambda I | \lambda \in \mathbb{C}\} \simeq \mathbb{C} & , \text{if } i = j \end{cases}$$

Hence, $\dim \mathrm{Hom}_{\mathbb{C}[G]}(W, W') = \dim_{\mathbb{C}} \bigoplus_{i=1}^{r} \mathbb{C}^{\oplus m_i m'_i} = \sum_{i=1}^{r} m_i m'_i = \langle \chi_\rho, \chi_{\rho'} \rangle$ □

By claim,

$$\begin{aligned} \langle \mathrm{Ind}\, \chi_\varphi, \chi_\rho \rangle &= \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V, W) \\ &= \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[H]} \left(V, \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], W)\right) \\ &= \dim \mathrm{Hom}_{\mathbb{C}[H]}(V, W) = \langle \chi_\varphi, \mathrm{Res}\, \chi_\rho \rangle \end{aligned}$$

□

Corollary 3.8.3. The number of times that V occurs in $\mathrm{Res}_H(W)$ = the number of times that W occurs in $\mathrm{Ind}_H^G(V)$.

Proof:

$\mathrm{RHS} = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V, W) = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[H]} \left(V, \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], W)\right) = \mathrm{LHS}$

□

3.8.2 Mackey's irreducibility criterion

Motivation: Given a irreducible representation φ of H, but the induced representation of φ of G may not be irreducible. So we want to study about induced and restricted representation. One of idea is consider the restricted representation of induced representation ρ of φ, most of times $\rho \neq \varphi$, so that we are curious what has changed in these operations. In this subsection, we study the induced from H to G and restricted from G to K. In particular, we choose $K = H$ and get the result.

Recall. Let $K, H \leq G$. Define the (K, H) **double cosets** of G are KaH, $a \in G$.

- We can find a subset $S := K \backslash G / H \subseteq G$ s.t. $\{KaH : a \in S\}$ is the set of distinct (K, H) double cosets of G and $G = \bigcup_{a \in S} KaH$.
- $|KaH| = |H|[K : K \cap a^{-1}Ha] = |K|[H : H \cap a^{-1}Ka]$:
  $b, b' \in aH$, say $b = ah$, $b' = ah'$ with $h, h' \in H$

  $$Kb = Kb' \iff b'b^{-1} \in K \iff (ah')h^{-1}a^{-1} \in K \iff h'h^{-1} \in a^{-1}Ka$$

  In KaH, there are $[H : H \cap a^{-1}Ka]$ distinct cosets Kah, so it is done!

Definition 3.8.2. $H_a = aHa^{-1} \cap K \leq K \rightsquigarrow \forall s \in H_a \subseteq K \implies s \in aHa^{-1} \rightsquigarrow a^{-1}sa \in H$ can apply the representation for H.

Property 3.8.3. Let $\varphi : H \to \mathrm{GL}(V)$ and induced module $W = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$. $\forall a \in S$, define

$$\begin{array}{rccc} \varphi_a : & H_a & \longrightarrow & \mathrm{GL}(V_a) \\ & s & \longmapsto & \varphi(a^{-1}sa) \end{array}$$

where $V_a = V$ is $\mathbb{C}[H_a]$-module. Then

$$\mathrm{Res}_K \mathrm{Ind}_H^G(V) \simeq \bigoplus_{a \in S} \mathrm{Ind}_{H_a}^K(V_a)$$

Definition 3.8.3.

- $W = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V = \bigoplus_{a \in S} \underbrace{\mathbb{C}[KaH] \otimes_{\mathbb{C}[H]} V}_{:= W(a)}$, where $W(a)$ is $\mathbb{C}[K]$-module.
- **Claim:** $W(a) \simeq \mathrm{Ind}_{H_a}^K(V_a)$
  - $a \otimes_{\mathbb{C}[H]} V$ is a $\mathbb{C}[H_a]$-module : $\forall s \in H_a$, say $s = aha^{-1} \in K$

    $$s(a \otimes V) = (aha^{-1})a \otimes V = a \otimes hV \subseteq a \otimes V$$

  - $V_a \simeq a \otimes_{\mathbb{C}[H]} V$ as $\mathbb{C}[H_a]$-modules : Define

    $$\begin{array}{ccc} V_a & \longrightarrow & a \otimes V \\ v & \longmapsto & a \otimes v \end{array}$$

    $\forall s \in H_a$, say $s = aha^{-1}$, $s \cdot v = \varphi(h)(v) \mapsto a \otimes \varphi(h)(v) = a \otimes h \cdot v = s(a \otimes v)$.
- $W(a) = \mathbb{C}[KaH] \otimes_{\mathbb{C}[H]} V = \mathbb{C}[K]a \otimes_{\mathbb{C}[H]} V \simeq \mathbb{C}[K] \otimes_{\mathbb{C}[H_a]} (a \otimes_{\mathbb{C}[H]} V) \simeq \mathbb{C}[K] \otimes_{\mathbb{C}[H_a]} V_a = \mathrm{Ind}_{H_a}^K(V_a)$

Theorem 3.8.1 (Mackey's criterion)**.** Consider the case of $K = H$. Define $H_a = aHa^{-1} \cap H$, $\varphi : H \to \mathrm{GL}(V)$, $\begin{array}{ccc} \varphi_a : & H_a & \longrightarrow & \mathrm{GL}(V) \\ & aha^{-1} & \longmapsto & \varphi(h) \end{array}$. Then $W = \mathrm{Ind}_H^G(V)$ is irreducible $\iff$

(1) φ is irreducible

(2) $\forall a \in G \setminus H$, φ_a and $\mathrm{Res}_{H_a}(\varphi)$ are disjoint (have not same irreducible part) i.e. $\langle \chi_a, \chi_{\mathrm{Res}_{H_a}(\varphi)} \rangle = 0$.

Proof: First, we calculate the norm of $\mathrm{Ind}_H^G(\chi_\varphi)$:

$$\begin{aligned} &\langle \mathrm{Ind}_H^G(\chi_\varphi), \mathrm{Ind}_H^G(\chi_\varphi) \rangle = \langle W, W \rangle_G = \langle \mathrm{Ind}_H^G(V), W \rangle_G \\ =&\langle V, \mathrm{Res}_H W \rangle_W = \sum_{a \in S} \langle V, \mathrm{Ind}_{H_a}^H V_a \rangle_H = \sum_{a \in S} \langle \mathrm{Res}_{H_a} V, V_a \rangle_{H_a} \end{aligned}$$

Notice that $a = e : \langle \mathrm{Res}_{H_a} V, V_a\rangle_{H_a} = \langle V, V\rangle_H > 0$ and $\langle \mathrm{Res}_{H_a} V, V_a\rangle_{H_a} = \dim_{\mathbb{C}}(\cdots) \in \mathbb{Z}_{\geq 0}$. Hence, W is irr. $\iff \langle W, W\rangle_G = 1 \iff \langle V, V\rangle_H = 1$ and $\langle \mathrm{Res}_{H_a} V, V_a\rangle_{H_a} = 0\ \forall e \neq a \in S$ i.e. φ is irreducible and $\forall e \neq a \in S\ \langle \chi_a, \chi_{\mathrm{Res}_{H_a}(\varphi)}\rangle = 0$.
Now, we claim that $\forall e \neq a \in S \iff \forall b \in G \setminus H$ (for condition (2)). For all $b \in G \setminus H$, $b \in G = \bigcup_{a \in S} HaH$ with $a \neq e \rightsquigarrow HaH = HbH$. Let $S' = (S - \{a\}) + \{b\}$ and apply the theorem for S'. □

Corollary 3.8.4. $H \lhd G$, $\varphi : H \to \mathrm{GL}(V)$, $\rho : G \to \mathrm{GL}(W)$ with $W = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$. Then

$$\rho \text{ is irr.} \iff \begin{cases} \varphi \text{ is irr.} \\ \varphi \not\simeq \varphi_a\ \forall a \notin H. \end{cases}$$

Proof: $H \lhd G \rightsquigarrow \forall a \in G$, $H_a = (aHa^{-1}) \cap H = H \rightsquigarrow \mathrm{Res}_{H_a} V = V$. So $\forall a \in H$,

$$\langle V, V_a\rangle_H = 0 \iff \varphi \not\simeq \varphi_a$$

This corollary tell us that

$$\varphi : \begin{array}{ccc} H & \longmapsto & \mathrm{GL}(V) \\ s & \longmapsto & \varphi(s) \end{array} \not\simeq \varphi_a : \begin{array}{ccc} H_a = H & \longmapsto & \mathrm{GL}(V) \\ s & \longmapsto & \varphi(a^{-1}sa) \end{array} \forall a \notin H$$

□

Application. Construct an irr. rep. of $\mathrm{SL}_2(\mathbb{F}_p)$ of degree $p+1$:
Let $h : \mathbb{F}_p^\times \to \mathbb{C}^\times$ with $h^2 \neq 1$ and $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in \mathbb{F}_p \right\} \subseteq \mathrm{SL}_2(\mathbb{F}_p)$. If

$$\varphi : \begin{array}{ccc} H & \longmapsto & \mathbb{C}^\times \\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} & \longmapsto & h(a) \end{array}$$

then $\mathrm{Ind}_H^{\mathrm{SL}_2(\mathbb{F}_p)}(\varphi)$ is irr. of degree $(p+1)$.

Proof: Let $G = \mathrm{SL}_2(\mathbb{F}_p)$ and $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \middle| c = 0 \right\}$. Let $z \in \mathbb{F}_p^\times$ s.t. $h(z)^2 \neq 1$.
Since $|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$, $|\mathrm{SL}_2(\mathbb{F}_p)| = (p^2-1)p$, $|H| = (p-1)p \rightsquigarrow [\mathrm{SL}_2(\mathbb{F}_p) : H] = p+1$. Hence, $\dim \mathrm{Ind}_H^{\mathrm{SL}_2(\mathbb{F}_p)} = \dim \mathbb{C} \cdot [\mathrm{SL}_2(\mathbb{F}_p) : H] = p+1$.
Now, we want to apply Mackey's criterion. for $A \in G \setminus H$. If $\langle \varphi_A, \varphi|_{H_A}\rangle \neq 0$, since φ_A, $\varphi|_{H_A}$ are degree 1 $\implies \varphi_A \simeq \varphi|_{H_A} \implies \chi_{\varphi_A} = \chi_{\varphi|_{H_A}}$. Say $A = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}$ with $c_0 \neq 0 \rightsquigarrow A^{-1} = \begin{pmatrix} d_0 & -b_0 \\ -c_0 & a_0 \end{pmatrix}$. If $A \begin{pmatrix} z & b \\ 0 & d \end{pmatrix} A^{-1} \in AHA^{-1} \cap H$, then $d = z^{-1}$ and

$$A \begin{pmatrix} z & b \\ 0 & d \end{pmatrix} A^{-1} = \begin{pmatrix} a_0 d_0 z - a_0 c_0 b - b_0 c_0 d & \bullet \\ c_0 d_0 z - c_0^2 b - c_0 d_0 d & \bullet \end{pmatrix} \in H \implies d_0 z = c_0 b + d_0 d$$

Then

$$\varphi_A \left(A \begin{pmatrix} z & b \\ 0 & d \end{pmatrix} A^{-1} \right) = \varphi \left(\begin{pmatrix} z & b \\ 0 & d \end{pmatrix} \right) = h(z)$$

and

$$\varphi|_{H_A}\left(A\begin{pmatrix}z & b\\ 0 & d\end{pmatrix}A^{-1}\right) = h(a_0d_0z - c_0(a_0b+b_0d)) = h(a_0(c_0b+d_0d) - c_0(a_0b+b_0d)) = h(d)$$

Hence, $h(z) = h(d) = h(z^{-1}) = h(z)^{-1} \implies 1 = h(z)^2 = h(z^2)$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$). By Mackey's criterion, $\mathrm{Ind}_H^{\mathrm{SL}_2(\mathbb{F}_p)}(\varphi)$ is irr. of degree $(p+1)$. □

3.9 Induced representations (II)

Goal : Find all irreducible representations of $G = A \rtimes H$ with A : abelian.

Fact 3.9.1. $X = \mathrm{Hom}_{\mathrm{gp}}(A, \mathbb{C}^\times)$ is the group of irreducible representation of A.

Proof: $\because$ A is abelian $\therefore$ $\forall a \in A$, $\{a\}$ is a conjugacy class of $A \rightsquigarrow |A|$ = number of conjugacy classed $\rightsquigarrow |A| = 1^2 + \cdots + 1^2 \rightsquigarrow$ each irr. rep. of A is of degree 1 i.e. $\varphi : A \to \mathbb{C}^\times \simeq \mathrm{GL}_1(\mathbb{C})$. (Notice that $\chi_\varphi = \varphi$ can be regard as a irr. rep.)
Conversely, $\forall \varphi \in \mathrm{Hom}_{\mathrm{gp}}(A, \mathbb{C}^\times)$, φ is an irr. rep. of deg 1. □

Observation : $\forall s \in G = AH$, say $s = bh$, then χ_s is define on $A_s = sAs^{-1} \cap A = A$ since $A \lhd G$. Then

$$\chi_s(a) = \chi(s^{-1}as) = \chi(h^{-1}\underbrace{b^{-1}ab}_{=a}h^{-1}) = \chi_h(a)$$

So we define a action

$$\begin{array}{ccc} H \times X & \longrightarrow & X \\ (h, \chi) & \longmapsto & \chi_h \end{array}$$

with $\{H\chi_1, ..., H\chi_\ell\}$ be the set of distinct orbits in X under H. We know that

$$|H\chi_i| = [H : H_i] \text{ where } H_i := \mathrm{Stab}_H \chi_i = \{h \in H | h\chi_i = \chi_i\}$$

- So H_i is act trivially on χ_i and thus we can extend χ_i to $G_i := AH_i$ by $\widetilde{\chi}_i(ah) = \chi_i(a)$ for all $a \in A$ and $h \in H_i$. Then

$$\begin{aligned}\widetilde{\chi}_i((ah)(ah')) &= \widetilde{\chi}_i(a(ha'h^{-1})(hh')) = \chi_i(a(ha'h^{-1})) = \chi_i(a)\chi_i(ha'h^{-1}) \\ &= \chi_i(a)\chi_i(ha'h^{-1}) = \chi_i(a)(\chi_i)_{h^{-1}}(a') = \chi_i(a)\chi_i(a') = \widetilde{\chi}_i(ah)\widetilde{\chi}_i(a'h')\end{aligned}$$

  $\rightsquigarrow \widetilde{\chi}_i$ is a degree 1 irr. rep. of G_i.

- Now, we take care of the part of H : Let $\rho_i : H_i \to \mathrm{GL}(V_i)$ with $\dim V_i = n_i$ be an irreducible representation. Define

$$\begin{array}{rccc} \widetilde{\rho}: & G_i & \longrightarrow & \mathrm{GL}(V_i) \\ & ah & \longmapsto & \rho(h) \end{array}$$

  $$\implies \widetilde{\rho}((ah)(a'h')) = \widetilde{\rho}(a(ha'h^{-1})(hh')) = \rho(hh') = \rho(h)\rho(h') = \widetilde{\rho}(ah)\widetilde{\rho}(a'h')$$

  $\rightsquigarrow \widetilde{\rho}$ is representation of G_i.

Fact 3.9.2. $\widetilde{\rho}$ is also irr.

Proof: If $\widetilde{\rho}$ is reducible, say $\exists 0 \neq W_i \subsetneq V_i$ s.t. W_I is G_i invariant. By definition of $\widetilde{\rho}$, W_i is H_i-invariant $\rightsquigarrow$ ρ is reducible $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$. □

- Define $\theta_{i,\rho} := \mathrm{Ind}_{G_i}^{G}(\widetilde{\chi}_i \otimes \widetilde{\rho})$

  - $\begin{cases} \widetilde{\chi}_i \text{ is of deg 1} \\ \widetilde{\rho} \text{ is irr.} \end{cases} \implies \widetilde{\chi}_i \otimes \widetilde{\rho}$ is irr.

  - $\theta_{i,\rho}$ is an irr. rep. of G :
    By Mackey's criterion, we need "$\forall s \in G \setminus G_i$, $(\widetilde{\chi}_i \otimes \widetilde{\rho})_s$ and $(\widetilde{\chi}_i \otimes \widetilde{\rho})|_{(G_i)_s}$ are disjoint." Notice that $(G_i)_s = (sG_is^{-1}) \cap G_i \supseteq A$.
    Claim : The restriction of these two rep. to rep. to A are disjoint.
    $\forall a \in A$,

$$(\widetilde{\chi}_i \otimes \chi_{\widetilde{\rho}})_s|_A(a) = \widetilde{\chi_i}(s^{-1}as)\chi_{\widetilde{\rho}}(\underbrace{s^{-1}as}_{\in A}) = \chi_i(s^{-1}as)\chi_{\widetilde{\rho}}(1) = n_i(\chi_i)_s(a)$$

$$(\widetilde{\chi}_i \otimes \chi_{\widetilde{\rho}})|_A(a) = \widetilde{\chi}_i(a)\chi_{\widetilde{\rho}}(a) = \widetilde{\chi}_i(a)\chi_{\widetilde{\rho}}(1) = n_i\chi_i(a)$$

    Since $s \in G \setminus G_i$, if $s = ah \rightsquigarrow h \notin H_i \rightsquigarrow (\chi_i)_s = (\chi_i)_h \neq \chi_i \rightsquigarrow \langle (\chi_i)_s, \chi_i \rangle_A = 0$, since χ_i and $(\chi_i)_s$ are irr. rep. on A. Hence, $\langle (\widetilde{\chi} \otimes \chi_{\widetilde{\rho}})_s|_A, (\widetilde{\chi}_i \otimes \chi_{\widetilde{\rho}})|_A \rangle = 0$. □
    If these two rep. is not disjoint, then they have common irr. subrep. and thus there restrictions on A have non trivial common subrep. on A $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$.

Theorem 3.9.1 (Main theorem (1))**.** If $\theta_{i,\rho} \simeq \theta_{i',\rho'}$, then $i = i'$ and $\rho \simeq \rho'$.

Proof:

- split $\mathrm{Res}_A \theta_{i,\rho}$: $\forall a \in A$, by reciprocity formula,

$$\mathrm{Ind}_{G_i}^{G}(\chi_{\widetilde{\chi} \otimes \widetilde{\rho}})(a) = \frac{1}{|G_i|}\sum_{s \in G} \chi_i(s^{-1}as)\chi_{\widetilde{\rho}}(s^{-1}as) = \frac{1}{|G_i|}\sum_{s \in G} (\chi_i)_s(a)\underbrace{\chi_{\widetilde{\rho}}(1)}_{=n_i} \qquad (*)$$

  If we write $s = bh$, then $(\chi_i)_s = (\chi_i)_h$. Hence, the $\mathrm{Res}_A \theta_{i,\rho}$ only involves characters in the orbit $H\chi_i \rightsquigarrow i$ is uniquely decide.

- Let $\theta_{i,\rho} : G \to \mathrm{GL}(W)$. Define $W_i = \{v \in W | \theta_{i,\rho}(a)v = \chi_i(a)v \ \forall a \in A\}$ which is the subspace of W corresponding to all component of χ_i in $\mathrm{Res}_A \theta_{i,\rho}$.

  - $\dim W_i = n_i = \dim V_i$: To calculate $\dim W_i$, we need to calculate the coefficient of χ_i in $(*)$. $\because (\chi_i)_s = \chi_i \iff s \in G_i$ $\therefore$ there are $|G_i|$ elements h in G which contribute $(\chi)_h(a)\chi_{\widetilde{\rho}}(1) = n_i\chi_i(a)$. After multiplying $\frac{1}{|G_i|}$, $\exists$ exactly n_i irr. components isomorphic to χ_i i.e.

$$\mathrm{Res}_A \theta_{i,\rho} \simeq \chi_i^{\oplus n_i} \oplus \cdots$$

    and thus $\dim W_i = n_i$.

- W_i is H_i-invariant, i.e. $\theta_{i,\rho}(h)v \in W_i \ \forall h \in H_i, v \in W_i$: For all $a \in A$

$$\begin{aligned} &\theta_{i,\rho}(a)\theta_{i,\rho}(h)v = \theta_{i,\rho}(ah)v && (\theta_{i,\rho} \text{ is group rep.}) \\ =&\theta_{i,\rho}(h)\theta_{i,\rho}(h^{-1}ah)v = \theta_{i,\rho}(h)\chi_i(h^{-1}ah)\rho(1)v \\ =&\theta_{i,\rho}(h)(\chi_i)_h(a)v = \theta_{i,\rho}(h)\chi_i(a)v = \chi_i(a)(\theta_{i,\theta}(h)v) && (h \in H_i) \end{aligned}$$

- $\mathrm{Res}_{H_i}\theta_{i,\rho} : H_i \longrightarrow \mathrm{GL}(W_i)$ isomorphic to $\rho : H_i \to \mathrm{GL}(V_i)$:
  Claim : If $\{v_1, ..., v_{n_i}\}$ is a basis for V_i over $\mathbb{C}$, then $\{1 \otimes v_1, ..., 1 \otimes v_{n_i}\}$ is a basis for W_i over $\mathbb{C}$.
  subproof : Since $\forall a \in A$,

$$\theta_{i,\rho}(a)(1 \otimes v_j) = a \otimes v_j = 1 \otimes av_j = 1 \otimes \chi_i(a)\rho(1)v_j = \chi_i(a)(1 \otimes a)$$

  Hence, $1 \otimes v_j \in W_i$. Combine with $\{1 \otimes v_j : j = 1, ..., n_i\}$ are linearly independent over $\mathbb{C}$ and $\dim W_i = n_i \implies \{1 \otimes v_i\}$ is a basis for W_i. □
  $\forall h \in H_i$,

$$\theta_{i,\rho}(h)(1 \otimes v_j) = h \otimes v_j = 1 \otimes h \cdot v_j = 1 \otimes \underbrace{\widetilde{\chi}_i(h)}_{=\chi_i(1)=1}\widetilde{\rho}(h)v = 1 \otimes \rho(h)v_j$$

  So via the $\mathbb{C}[H_i]$-isom. $W_i \simeq V_i$ with $1 \otimes v_j \mapsto v_j$, $\mathrm{Res}_{H_i}\theta_{i,\rho} \simeq \rho \rightsquigarrow \rho$ is uniquely decide.

□

Theorem 3.9.2 (Main theorem (2))**.** Each irreducible representation of G is isomorphic to one of the $\theta_{i,\rho}$.

Proof: Let $\sigma : G \to \mathrm{GL}(U)$ be an irr. rep. of G. Write $\mathrm{Res}_A \sigma \simeq \chi_{i_1}^{\oplus r_1} \oplus \cdots \oplus \chi_{i_m}^{\oplus r_m}$ with $r_1, ..., r_m \in \mathbb{Z}_{>0}$ and $\chi_{i_1}, ..., \chi_{i_m} \in X$ are distinct. Then $U \simeq U_1 \oplus \cdots \oplus U_m$ as $\mathbb{C}[A]$-isomorphism.

- $\forall a \in A$, $v_j \in U_j$, $\sigma(a)v_j = \chi_{i_j}(a)v_j$
- $\forall s \in G$, $v_j \in U_j$

$$\begin{aligned} \sigma(a)\sigma(s)v_j =&\sigma(as)v_j = \sigma(ss^{-1}as)v_j = \sigma(s)\sigma(s^{-1}as)v_j \\ =&\sigma(s)\chi_{i_j}(s^{-1}as)v_j = \sigma(s)\underbrace{(\chi_{i_j})_s}_{:=\chi_{i_{j'}}}(a)v_j = \chi_{i_{j'}}(a)\sigma(s)v_j \end{aligned}$$

  Hence, $\sigma(s) : U_j \longrightarrow U_{j'}$, where $s \cdot (\chi_{i_j}) = \chi_{i_{j'}}$.

- If $\chi_{i_1} \in H\chi_i$ and thus $H\chi_{i_1} = H\chi_i$, after renaming $\begin{cases} H_i = \mathrm{Stab}_H \chi_{i_1} \\ \chi_i = \chi_{i_1} \end{cases}$. Then $\forall h \in H_i$,

$$\sigma(h) : U_1 \longrightarrow U_1 \text{ i.e. } \mathrm{Res}_{H_i}\sigma : H_i \mapsto \mathrm{GL}(U_1)$$

  Let $\overline{U}$ be an irr. $\mathbb{C}[H_i]$-subspace of U_1 and $\rho : H_i \longrightarrow \mathrm{GL}(\overline{U})$ be the corresponding rep. of H_i.
  Now, we found the index i and rep. ρ. We claim that $\sigma \simeq \theta_{i,\rho}$.

- For all $ah \in AH_i$, $v \in \overline{U}$,

$$\sigma(ah)v = \sigma(a)\sigma(h)\underbrace{v}_{\in\overline{U}} = \sigma(a)\underbrace{\rho(h)v}_{\in\overline{U}\subseteq U_1} = \chi_i(a)\rho(h)v = (\widetilde{\chi}_i \otimes \widetilde{\rho})(ah)v$$

$\implies \mathrm{Res}_{G_i}\sigma : G_i \longrightarrow \mathrm{GL}(\overline{U})$ contains $\widetilde{\chi}_i \otimes \widetilde{\rho}$ at least once. Hence,

$$1 \leq \langle \mathrm{Res}_{G_i}\sigma, \widetilde{\chi}_i \otimes \widetilde{\rho}\rangle_{G_i} = \langle \sigma, \mathrm{Ind}_{G_i}^{G}(\widetilde{\chi}_i \otimes \widetilde{\rho})\rangle_G$$

$\implies \sigma$ occurs at least once in $\theta_{i,\rho}$. Since $\sigma, \theta_{i,\rho}$ are irr. $\rightsquigarrow \sigma \simeq \theta_{i,\rho}$.

Note : By Main theorem (1), χ_{i_j} $j = 1, ..., m$ belongs to same orbit $H\chi_i$.

□

3.10 Brauer theorem (I)

3.10.1 Artin theorem

First, we formalize what we learned before.
Recall : G : finite group, $X(G)$ = the space of $\mathbb{C}$-valued class functions on G.

- $X(G)$ is a $\mathbb{C}$-algebra :
  $(f_1 + f_2)(s) = f_1(s) + f_2(s)$, $(f_1 f_2)(s) := f_1(s)f_2(s)$, $(cf)(s) = c \cdot f(s)$
- If $\chi_1, ..., \chi_r$ are distinct irr. characters of G, then $X(G) = \langle \chi_1, ..., \chi_r\rangle_{\mathbb{C}}$ and $\{\chi_i : i = 1, ..., r\}$ is a orthonormal basis.
- If $f \in X(G)$, then $f = \chi_\rho$ for some $\rho : G \to \mathrm{GL}(V) \iff f = \sum_{i=1}^{r} \alpha_i\chi_i$, $\alpha_i \in \mathbb{Z}_{\geq 0}$.
  - Define $\mathrm{Ch}^+(G) := \{f \in X(G) : f = \chi_\rho\}$ is a monoid under "+" and called **character set**.
  - Define $\mathrm{Ch}(G)$ = the group generated by $\mathrm{Ch}^+(G) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_r$ and called **generalized character set**.

  $\because \chi_\rho\chi_{\rho'} = \chi_{\rho\otimes\rho'} \therefore \mathrm{Ch}(G)$ is a commutative subring of $X(G)$.
- $X(G) \simeq \mathbb{C} \otimes_{\mathbb{Z}} \mathrm{Ch}(G)$.
- $H \leq G$,

$$\begin{array}{rccc} \mathrm{Res}: & \mathrm{Ch}(G) & \longrightarrow & \mathrm{Ch}(H) \\ & \chi & \longmapsto & \chi|_H \\ \mathrm{Ind}: & \mathrm{Ch}(H) & \longrightarrow & \mathrm{Ch}(G) \\ & \chi & \longrightarrow & \mathrm{Ind}_H^G\chi \\ & V & & \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V \end{array}$$

Reciprocity formula :

$$\mathrm{Ind}\,\chi(a) = \frac{1}{|H|}\sum_{\substack{s\in G \\ s^{-1}as\in H}} \chi(s^{-1}as)$$

- Res is a ring homomorphism.
- Ind is an abelian group homomorphism ($\mathrm{Ind}(\chi+\chi')=\mathrm{Ind}\,\chi+\mathrm{Ind}\,\chi'$).
- Ind and Res are adjoints of each other.
- The image of Ind is not only an abelian subgroup but also an ideal.
  pf. Let $\varphi\in\mathrm{Ch}(H)$, $\psi\in\mathrm{Ch}(G)$, then

$$\begin{aligned}((\mathrm{Ind}\,\varphi)\psi)(a)&=\frac{1}{|H|}\sum_{\substack{s\in G\\ s^{-1}as\in H}}\varphi(s^{-1}as)\psi(a)=\frac{1}{|H|}\sum_{\substack{s\in G\\ s^{-1}as\in H}}\varphi(s^{-1}as)\psi(s^{-1}as)\\&=\frac{1}{|H|}\sum_{\substack{s\in G\\ s^{-1}as\in H}}\varphi(s^{-1}as)\,\mathrm{Res}\,\psi(s^{-1}as)=\mathrm{Ind}(\varphi\cdot\mathrm{Res}\,\psi)(a)\end{aligned}$$

- In order to continue to use formal language, we give the following definition.

  If A is a commutative ring, the homomorphism Res and Ind extend by linearity to A-linear maps :

$$\begin{array}{rccc}A\otimes\mathrm{Res}: & A\otimes\mathrm{Ch}(G) & \longrightarrow & A\otimes\mathrm{Ch}(H)\\ A\otimes\mathrm{Ind}: & A\otimes\mathrm{Ch}(H) & \longrightarrow & A\otimes\mathrm{Ch}(G)\end{array}$$

Theorem 3.10.1 (Artin theorem)**.** If $\rho: G\to\mathrm{GL}(V)$, then χ_ρ is a rational linear combination of characters induced from representations of cyclic subgroups of G. In other word, if $\mathcal{F}:=$ the family of all cyclic subgroups of G, then

$$\begin{array}{rccc}\mathbb{Q}\otimes\mathrm{Ind}: & \bigoplus_{H\in\mathcal{F}}\mathbb{Q}\otimes\mathrm{Ch}(H) & \twoheadrightarrow & \mathbb{Q}\otimes\mathrm{Ch}(G)\\ & (\varphi_H)_{H\in\mathcal{F}} & \mapsto & \sum_{H\in\mathcal{F}}\mathrm{Ind}\,\varphi_H\end{array}$$

Before proving this theorem, we see some properties first.

Property 3.10.1. Let $H\in\mathcal{F}$. Define $\theta_H(h)=\begin{cases}|H| & ,\text{ if }\langle h\rangle=H\\ 0 & ,\text{ otherwise}\end{cases}$. Then

$$|G|=\sum_{H\in\mathcal{F}}\mathrm{Ind}\,\theta_H$$

Proof: $\forall a\in G$,

$$\sum_{H\in\mathcal{F}}\mathrm{Ind}\,\theta_H(a)=\sum_{H\in\mathcal{F}}\sum_{\substack{s\in G\\ s^{-1}as\in H}}\theta_H(s^{-1}as)|H|^{-1}=\sum_{H\in\mathcal{F}}\sum_{\substack{s\in G\\ \langle s^{-1}as\rangle=H}}1=\sum_{s\in G}\sum_{\langle s^{-1}as\rangle\in\mathcal{F}}1=|G|$$

□

Property 3.10.2. For $H\in\mathcal{F}$, $\theta\in\mathrm{Ch}(H)$

Proof: By induction on $|H|$. $|H| = 1 \rightsquigarrow H = \{e\} \rightsquigarrow \theta_H \equiv 1$ done!
Claim : $\theta_H = |H| - \sum_{\substack{K \in \mathcal{F} \\ K \lneq H}} \mathrm{Ind}_K^H \theta_K$.

pf. By Property 3.10.1, $|H| = \sum_{\substack{K \in \mathcal{F} \\ K \leq H}} \mathrm{Ind}_K^H \theta_K$. When $K = H$, $\mathrm{Ind}_H^H \theta_H = \theta_H$, so the claim is done! □
Since $|H|$ is the character of trivial rep. of degree $|H|$ and by induction hypothesis, $\theta_K \in \mathrm{Ch}(K) \rightsquigarrow \mathrm{Ind}_K^H \theta_K \in \mathrm{Ch}(H)\ \forall K \lneq H \rightsquigarrow \theta_H \in \mathrm{Ch}(H)$. □

Remark 3.10.1. By Property 3.10.1 and 3.10.2, we can say $|G| \in \sum_{H \in \mathcal{F}} \mathrm{Ind}\,\mathrm{Ch}(H)$.

Proof: (Artin theorem) $\because$ the constant function $|G| \in \sum_{H \in \mathcal{F}} \mathrm{Ind}\,\mathrm{Ch}(H) \leq \mathrm{Ch}(G)$ as a ideal $\therefore |G|\chi_\rho \in \sum_{H \in \mathcal{F}} \mathrm{Ind}\,\mathrm{Ch}(H) \implies \chi_\rho \in \frac{1}{|G|} \sum_{H \in \mathcal{F}} \mathrm{Ind}\,\mathrm{Ch}(H)$. □

3.10.2 General form of Artin theorem

Let $\mathcal{S}$ be a family of subgroups of G. Let

$$\begin{array}{rccc} \mathrm{Ind}: & \bigoplus_{H \in \mathcal{S}} \mathrm{Ch}(H) & \longrightarrow & \mathrm{Ch}(G) \\ & (\varphi_H)_{H \in \mathcal{S}} & \longmapsto & \sum_{H \in \mathcal{S}} \mathrm{Ind}\,\varphi_H \end{array}$$

Theorem 3.10.2 (general Artin theorem)**.** TEAE

(a) G is the union of the conjugates of the subgroups belonging to $\mathcal{S}$ i.e.

$$G = \bigcup_{s \in G} \bigcup_{H \in \mathcal{S}} sHs^{-1}$$

(b) $\mathbb{Q} \otimes \mathrm{Ind} : \bigoplus_{H \in \mathcal{S}} \mathbb{Q} \otimes \mathrm{Ch}(H) \twoheadrightarrow \mathbb{Q} \otimes \mathrm{Ch}(G)$.

Proof:

- $(b) \Rightarrow (a)$: Let $K \subsetneq G$ be the union of the cojugates of the subgroups in $\mathcal{S}$. Then $\forall a \in G \setminus K$, $s^{-1}as \notin H\ \forall H \in \mathcal{S}$ and $s \in G$, otherwise, $a \in sHs^{-1} \subseteq K$ $(\rightarrow\!\leftarrow) \rightsquigarrow \varphi_H(s^{-1}as) = 0\ \forall H \in \mathcal{S}$. So each function of the form $\sum_{H \in \mathcal{S}} \mathrm{Ind}\,\varphi_H$ vanishes outside K. By (b), $\forall \chi \in \mathrm{Ch}(G)$, say $\chi = \sum_{H \in \mathcal{S}} a_H \,\mathrm{Ind}\,\varphi_H$ for some $(\varphi_H) \in \bigoplus_{H \in \mathcal{S}} \mathbb{Q} \otimes \mathrm{Ch}(H)$ and $a_H \in \mathbb{Q} \rightsquigarrow \chi$ vanishes outside K $(\rightarrow\!\leftarrow)$.
- $(a) \Rightarrow (b)$: Regard $\bigoplus_{H \in \mathcal{S}} \mathbb{Q} \otimes \mathrm{Ch}(H)$ and $\mathbb{Q} \otimes \mathrm{Ch}(G)$ are vector space over $\mathbb{Q}$. Then

$$\begin{array}{ccccccc} & \underset{\hookrightarrow B \in M_{n_2 \times n_1}(\mathbb{Q})}{\mathbb{Q} \otimes \mathrm{Ind}} & : & \bigoplus_{H \in \mathcal{S}} \mathbb{Q} \otimes \mathrm{Ch}(H) & \twoheadrightarrow & \mathbb{Q} \otimes \mathrm{Ch}(G) \\ \iff & \underset{\hookrightarrow B}{\mathbb{Q} \otimes \mathrm{Ind}} & : & \bigoplus_{H \in \mathcal{S}} \frac{\mathbb{C} \otimes \mathrm{Ch}(H)}{=X(H)} & \twoheadrightarrow & \frac{\mathbb{C} \otimes \mathrm{Ch}(G)}{=X(G)} \\ \iff & \underset{\hookrightarrow B^*}{\mathbb{Q} \otimes \mathrm{Res}} & : & \frac{\mathbb{C} \otimes \mathrm{Ch}(G)}{=X(G)} & \hookrightarrow & \bigoplus_{H \in \mathcal{S}} \frac{\mathbb{C} \otimes \mathrm{Ch}(H)}{=X(H)} \end{array}$$

For $\Longleftrightarrow$: Since Ind and Res are adjoint and by linear algebra we have

$$\operatorname{rank} B + \operatorname{null}(B^*) = \dim X(G)$$

so $\mathbb{Q} \otimes \mathrm{Ind}$ is surjective $\iff \operatorname{rank} B = \dim X(G) \iff \operatorname{null}(B^*) = 0 \iff \mathbb{Q} \otimes \mathrm{Res}$ is $1-1$. If a class function f on G in $\ker \mathbb{C} \otimes \mathrm{Res}$, then f restricts to 0 on each $H \in \mathcal{S}$. By (a), $f \equiv 0$ on G. Hence, $\mathbb{Q} \otimes \mathrm{Ind}$ is surjective.

□

3.10.3 Introduction of Brauer theorem

By Artin theorem, every element in $\mathrm{Ch}(G)$ is rational linear combination of induce character from cycle subgroup of G. Now, we want it be integer linear combination, so we need to have a detailed study of the structure of subgroups of G and find suitable family of subgroups of G satisfy this condition.

Definition 3.10.1. Let p be a prime integer. $s \in G$ is said to be **p-regular** if $p \nmid o(s)$ and **p-unipotent (singular)** id $o(s) = p^m$ for some $m \in \mathbb{N}$.

Fact 3.10.1. $\forall s \in G$, $s = s_r s_u$ where $\begin{cases} s_r : p\text{-regular}, \ s_u : p\text{-unipotent} \\ s_r s_u = s_u s_r \end{cases}$

Proof: Let $o(s) = p^m \ell$, with $\gcd(o, \ell) = 1$. By Euclidean Algorithm, $\exists a, b \in \mathbb{Z}$ s.t. $ap^m + b\ell = 1$. Then $s = s^{ap^m + b\ell} = s^{ap^m} \cdot s^{b\ell} =: s_r s_u$.

- $(s_r)^\ell = e \rightsquigarrow o(s_r) | \ell \rightsquigarrow s_r$ is p-regular.
- $(s_u)^{p^m} = e \rightsquigarrow o(s_u) | p^m \rightsquigarrow s_u$ is p-unipotent.
- It's clear that $s_r s_u = s_u s_r$

□

Fact 3.10.2. s : p-regular, $H_s := \langle s \rangle P_s \simeq \langle s \rangle \times P_s$, where P_s is the p-Sylow subgroup of $C_G(s)$. Where H_s is unique up to conjugation in $C_G(s)$.
$(t \in C_g(s),\ t^{-1} H_s t = t^{-1} \langle s \rangle t t^{-1} P_s t = \langle s \rangle (t^{-1} P_s t)$ and $t^{-1} P_s t \in \mathrm{Syl}_p(C_G(s)))$

Definition 3.10.2. H is said to be p-elementary if $H \simeq C \times P$, where

$$\begin{cases} C : \text{cyclic group with } p \nmid |C| \\ P : p\text{-group} \end{cases}$$

$\rightsquigarrow$ if s : p-regular, then H_s is p-elementary.

Observation :

- Let $H = CP \simeq C \times P$ be p-elementary. Then $stst' = sstt' \rightsquigarrow st = ts \implies P \subseteq C_G(s)$. Let $C = \langle s \rangle$. By Sylow thm, $P \subseteq P_s$ for some p-Sylow subgroup P_s in $C_G(s)$ i.e. $H \leq H_s$.

- $\forall s \in G$, $s = s_r s_u \in \langle s_r \rangle \langle s_u \rangle$ and $\langle s_u \rangle$ is a p-group. By above, $s \in H_{s_r}$.

Now, our strategy is consider another ring A and consider $A \otimes \mathrm{Ind}$ to get the A-linear combination. This A satisfy $A \cap \mathbb{Q} = \mathbb{Z}$ and we can get the result.

Definition 3.10.3. Let $g = |G|$ and $A = \mathbb{Z}[\zeta : \zeta^g = 1]$ i.e. ζ : gth root of unity. Then $\begin{cases} \forall \chi \in \mathrm{Ch}(G),\ \chi(a) \in A\ \forall a \in G \\ \text{The elements in } A \text{ are algebraic integers, so } A \cap \mathbb{Q} = \mathbb{Z}. \end{cases}$

Definition 3.10.4.

- $E_p = \{H : p\text{-elementary subgroups of } G\}$
- $V_p = \mathrm{Ind}\left(\bigoplus_{H \in E_p} \mathrm{Ch}(H)\right) = \sum_{H \in E_p} \mathrm{Ind}\,\mathrm{Ch}(H)$ is an ideal of $\mathrm{Ch}(G)$

  Define $A \otimes \mathrm{Ind} : \bigoplus_{H \in E_p} A \otimes \mathrm{Ch}(H) \longrightarrow A \otimes \mathrm{Ch}(G)$, then

- $\mathrm{Im}(A \otimes \mathrm{Ind}) = (A \otimes V_p)$
- $(A \otimes V_p) \cap \mathrm{Ch}(G) = V_p$:

  Let $\zeta_1 = 1, ..., \zeta_g$ be roots of $x^g = 1$ in $\mathbb{C}$. Then $A = \mathbb{Z}\zeta_1 + \cdots + \mathbb{Z}\zeta_g = \mathbb{Z} \cdot 1 \oplus \mathbb{Z}\zeta_{i_1} \oplus \cdots \oplus \mathbb{Z}\zeta_{i_c}$ to get the free $\mathbb{Z}$ basis. Then

  $$(A \otimes V_p) \cap \mathrm{Ch}(G) = (1 \otimes V_p \oplus \zeta_{i_1} \otimes V_p \oplus \cdots \oplus \zeta_{i_c} \otimes V_p) \cap (1 \otimes \mathrm{Ch}(G)) = 1 \otimes V_p = V_p$$

Theorem 3.10.3 (Brauer theorem)**.** $\mathrm{Ch}(G) = \sum_{p:\text{prime}} V_p = \sum_{H \in \bigcup_{p \in \mathbf{P}} E_p} \mathrm{Ind}\,\mathrm{Ch}(H)$

Property 3.10.3 (key property (1))**.** $[\mathrm{Ch}(G) : V_p]$ is finite and prime to p.

Remark 3.10.2. Key property (1) $\Longrightarrow$ Brauer theorem :
Let $V = \sum_{p:\text{prime}} V_p$. Then $V_p \leq V \leq \mathrm{Ch}(G)\ \forall p$: prime. Then

$$[\mathrm{Ch}(G) : V] \big| [\mathrm{Ch}(G) : V_p] \rightsquigarrow [\mathrm{Ch}(G) : V] \text{ is prime to } p\ \forall p$$

$\rightsquigarrow [\mathrm{Ch}(G) : V] = 1$ i.e. $V = \mathrm{Ch}(G)$.

To prove key property (1), we need key property (2) to help us.

Property 3.10.4 (key property (2))**.** Let $g = p^n \ell$ with $\gcd(p, \ell) = 1$. Then $\ell \in V_p$.

Remark 3.10.3. key property (2) $\Longrightarrow$ key property (1) :
V_p is an ideal of $\mathrm{Ch}(G)$, so $\forall \chi \in \mathrm{Ch}(G)$, $\ell\chi \in V_p \rightsquigarrow \ell\,\mathrm{Ch}(G) \subseteq V_p \Longrightarrow [\mathrm{Ch}(G) : V_p] \leq \ell$. Moreover, $o(\overline{\chi}) | \ell\ \forall \overline{\chi} \in \mathrm{Ch}(G)/V_p \rightsquigarrow [\mathrm{Ch}(G) : V_p]$ is prime to p.

Hence, to prove Brauer theorem, we need to show that key property is true.

3.11 Brauer theorem (II)

3.11.1 Proof ot Brauer theorem

Recall : p : a prime number, $g = |G|$

- $E_p := \{H \leq G : H \text{ is } p\text{-elementary}\}$ i.e. $H = CP$, where $C = \langle s \rangle$ with $p \not| o(s)$ and $P : p$-subgroup in $C_G(s)$
- $H_s = \langle s \rangle P_s$, $P_s : p$-Sylow subgroup of $C_G(s)$.
- $V_p := \operatorname{Ind}\left(\bigoplus_{H \in E_p} \operatorname{Ch}(H)\right) = \sum_{H \in E_p} \operatorname{Ind} \operatorname{Ch}(G) \leq \operatorname{Ch}(G)$ as a ideal.

Theorem 3.11.1 (Brauer theorem)**.** $\operatorname{Ch}(G) = \sum_{p \in \mathbb{P}} V_p = \sum_{H \in \bigcup_{p \in \mathbb{P}} E_p} \operatorname{Ind} \operatorname{Ch}(H)$

Goal : The constant function $\ell \in A \otimes V_p$, where $A = \mathbb{Z}[\zeta : \zeta^g = 1]$, $g = p^n \ell$ with $\gcd(p, \ell) = 1$. Then $\ell \in (A \otimes V_p) \cap \operatorname{Ch}(G) = V_p$ and thus key property (2) holds.

Lemma 3.11.1. Let $\mathcal{F} = \{\text{cyclic subgroups of } G\}$ and $\chi : G \to \mathbb{Z}$ be a class function with integer values divisible by g. Then

$$\chi \in A \otimes \sum_{H \in \mathcal{F}} \operatorname{Ind} \operatorname{Ch}(H)$$

Proof: Recall : $g = |G| = \sum_{H \in \mathcal{F}} \operatorname{Ind} \theta_H$, where $\theta_H(h) = \begin{cases} |H| & \text{, if } H = \langle h \rangle \\ 0 & \text{, otherwise} \end{cases}$. So

$$\chi = g\chi_1 = \sum_{H \in \mathcal{F}} (\operatorname{Ind} \theta_H)\chi_1 = \sum_{H \in \mathcal{F}} \operatorname{Ind}(\theta_H \operatorname{Res} \chi_1)$$

Now, for a fixed $H \in \mathcal{H}$, let $\{\varphi_1, ..., \varphi_r\}$ be the set of all irr. characters of H, then

$$\langle \varphi_i, \theta_H \operatorname{Res} \chi_1 \rangle_H = \frac{1}{|H|} \sum_{h \in H} \varphi_i(h) \overline{\theta_H(h) \chi_i(h)} = \sum_{h \in H} \underbrace{\varphi_i(h)}_{\in A} \underbrace{\left(\frac{\theta_H(h^{-1})}{|H|}\right)}_{\in \{0,1\}} \underbrace{\chi_i(h^{-1})}_{\in \mathbb{Z}} \in A$$

Hence, $\theta_H \operatorname{Res} \chi_1 \in A \otimes \operatorname{Ch}(H) \rightsquigarrow \chi \in A \otimes \sum_{H \in \mathcal{F}} \operatorname{Ch}(H)$ □

Lemma 3.11.2. Let $\chi \in A \otimes \operatorname{Ch}(G)$ have integer values, p be a prime and $s \in G$. Then

$$\chi(s) \equiv \chi(s_r) \pmod{p}$$

where s_r is p-regular part of s.

Proof: Let $H = \langle s \rangle$ and $\chi_0 = \mathrm{Res}_H \chi$. The irr. characters of $H = \{\varphi_1, ..., \varphi_{|H|}\}$, since H is abelian. Write $\chi_0 = \sum_{i=1}^{|H|} a_i \varphi_i$ with $a_i \in A$ (by $\chi \in A \otimes \mathrm{Ch}(G)$). Say $o(s) = p^m \ell \rightsquigarrow s^{p^m} = s_r^{p^m} s_u^{p^m} = s_r^{p^m}$. Now, we take pA modulo,

$$\chi_0(s)^{p^m} - \chi_0(s_r)^{p^m} = \left(\sum_{i=1}^{p^m \ell} a_i \varphi_i(s)\right)^{p^m} - \left(\sum_{i=1}^{p^m \ell} a_i \varphi_i(s_r)\right)^{p^m} \equiv \sum_{i=1}^{p^m \ell} a_i^{p^m} \left(\varphi_i(s)^{p^m} - \varphi_i(s_r)^{p^m}\right) = 0$$

Since χ has integer values, $\chi_0(s)^{p^m} - \chi_0(s_r)^{p^m} \in pA \cap \mathbb{Z} = p\mathbb{Z}$. Hence,

$$\chi(s) = \chi_0(s) \equiv \chi_0(s)^{p^m} \equiv \chi_0(s_r)^{p^m} \equiv \chi_0(s_r) = \chi(s_r) \pmod{p}$$

□

Recall : s is p-regular, $H_s = \langle s \rangle P_s$, where P_s is a p-Sylow subgroup of $C_G(s)$. Now, we will using the notation in above : $d = |\langle s \rangle_{:=C}|$, $p^a = |P_s|$.

Lemma 3.11.3. For fixed s : p-regular, $\exists \psi \in A \otimes \mathrm{Ch}(H_s)$ with integer values s.t. $\psi' = \mathrm{Ind}_{H_s}^G \psi$ satisfies

- $\psi'(s) \not\equiv 0 \pmod{p}$
- $\psi'(t) = 0$ for each t : p-regular which is not conjugate to s.

Proof: Define $\psi_C(s) = d$ and $\psi_C(t) = 0 \, \forall t \in C \backslash \{s\}$. Let $\chi_k(s) = \zeta_d^k$ $(0 \le k \le d-1)$ be distinct irr. characters of C. If $\psi_C = \sum_{i=0}^{d-1} a_i \chi_i$, then

$$a_i = \langle \psi_C, \chi_i \rangle = \frac{1}{d} \sum_{j=1}^{d} \psi_C(s^j) \chi_i(s^{-j}) = \chi_i(s^{-1})$$

i.e. $\psi = \sum_{i=0}^{d-1} \chi_i(s^{-1}) \chi_i \in A \otimes \mathrm{Ch}(C)$. Define $\psi : H_s \to \mathbb{Z}$ by $\psi(s^j z) = \psi_C(s^j)$, where $s^j \in C$, $z \in P_s \rightsquigarrow \psi \in A \otimes \mathrm{Ch}(H_s)$.

- If $t \in G$ is p-regular, then $\because o(u^{-1}tu) = o(t) \ \forall u \in G \therefore u^{-1}tu$ is also p-regular. So if $u^{-1}tu \in H_s = CP_s$, then $u^{-1}tu \in C$. Then

$$\psi'(t) = \frac{1}{|H_s|} \sum_{\substack{u \in G \\ u^{-1}tu \in C}} \psi_C(\underbrace{u^{-1}tu}_{\neq s}) = 0$$

- $\psi'(s) = \dfrac{1}{dp^a} \displaystyle\sum_{\substack{u \in G \\ u^{-1}su = s}} \psi_C(s) = \frac{1}{p^a} \sum_{\substack{u \in G \\ u^{-1}su = s}} 1 = \frac{|C_G(s)|}{p^a} \not\equiv 0 \pmod{p}$

□

Lemma 3.11.4. For fixed s : p-regular, $\exists \psi \in A \otimes V_p$ with integer values s.t.

$$\psi(s) \neq 0 \pmod{p} \ \forall s \in G$$

Proof: Let $\{\{s_i\} : i \in I\}$ be the set of distinct conjugacy classes for p-regular elements. By Lemma 3.11.3, $\forall i \in I$, $\exists \psi_i \in A \otimes \mathrm{Ind}_{H_{s_i}}^G \mathrm{Ch}(H_{s_i}) \leq A \otimes V_p$ with integer values s.t. $\psi_i(s_i) \neq 0 \pmod p$ and $\psi_i(s_j) = 0 \ \forall j \neq i$. Let $\psi = \sum_{i \in I} \psi_i \in A \otimes V_p$ and have integer values. For $s \in G$, $s_r \in \{s_i\}$ for some $i \in I$. By Lemma **??**,

$$\psi(s) \equiv \psi(s_r) = \psi_i(s_i) \not\equiv 0 \pmod p$$

□

Theorem 3.11.2. $g = p^n \ell$ with $\gcd(p, \ell) = 1 \rightsquigarrow \ell \in A \otimes V_p$.

Proof: Let ψ be constructed in Lemma 3.11.4 and $N = \varphi(p^n)$. Since $\psi(s) \not\equiv 0 \pmod p \therefore \psi(s)^N \equiv 1 \pmod p \rightsquigarrow g | \ell(\psi^N - 1)$. By Lemma 3.11.1,

$$\ell(\psi^N - 1) \in A \otimes \sum_{C \in \mathcal{F}} \mathrm{Ind}\, \mathrm{Ch}(C) \subseteq A \otimes V_p \text{ (Since } \mathcal{F} \subseteq E_p)$$

However, $A \otimes V_p \leq A \otimes \mathrm{Ch}(G)$ as an ideal, so $\ell\psi^N \in A \otimes V_p \rightsquigarrow \ell = \ell\psi^N - \ell(\psi^N - 1) \in A \otimes V_p$. □

3.11.2 Application

Definition 3.11.1. A character χ is said to be monomial if it is induced from a character of deg 1 of some subgroup.

Observation : For a finite solvable group G,

$$\{e\} = G_0 \lhd G_1 \lhd \cdot \lhd G_n = G \text{ with } G_i/G_{i-1} : \text{cycle}$$

If $G_i \lhd G \ \forall i$, then we call G supersolvable.

- If G is a nonabelian supersolvable group with $Z = Z(G)$, then

  $$G_0 Z/Z \lhd G_1 Z/Z \lhd \cdots \lhd G/Z$$

  Let i be the largest index s.t. $G_i Z/Z = \{\overline{e}\}$, then $G_{i+1}Z/Z \neq \{e\}$ is cyclic $\rightsquigarrow G_{i+1}$ is abelian and $G_{i+1} \lhd G$. Since $0 \neq G_{i+1}Z/Z \simeq G_{i+1}/(G_{i+1} \cap Z)$, $G_{i+1} \neq G_{i+1} \cap Z \implies G_{i+1} \not\leq Z$.

  i.e. $\exists$ a normal abelian subgroup H of G with $H \not\leq Z(G)$.

Property 3.11.1. Let G be a finite supersolvable group. Then each irr. rep. ρ of G is monomial (i.e. induced by a deg 1 rep. of a subgroup of G).

Proof: By induction on $|G|$, $|G| = 1 \rightsquigarrow G = \{e\}$ done! Let $\rho : G \to \mathrm{GL}(V) \rightsquigarrow \overline{\rho} : G/\ker\rho \to \mathrm{GL}(V)$. If $\ker\rho \neq \{e\}$, then $|G/\ker\rho| < |G|$, then by induction hypothesis, done! So we may assume that ρ is faithful.

- G : abelian : $\dim V = 1$, done!

- G : non-abelian : Let $H \lhd G$ and H be abelian with $H \not\leq Z(G)$. Since ρ is faithful, $\rho(H) \not\leq \rho(Z(G))$. Say $\exists a \in H$ s.t. $\rho(a) \notin \rho(Z(G)) \rightsquigarrow \rho(a) \neq \lambda I_n \rightsquigarrow \rho|_H \not\simeq \rho_0^{\oplus n}$ (direct sum of identity), say $\rho \simeq \rho_0^{\oplus n_0} \oplus \cdots \oplus \rho_{\alpha-1}^{\oplus n_{\alpha-1}} \longleftrightarrow V = V_0 \oplus \cdots \oplus V_{\alpha-1}$ for $\alpha > 1$. Since H is abelian, ρ_i : deg 1 and thus $\rho_i = \chi_i$.

  - $a \in H$, $\rho(a)v_i = \chi_i(a)v_i \ \forall v_i \in V_i$
  - $s \in G$, $\rho(a)\rho(s)v_i = \rho(s)\rho(s^{-1}as)v_i = (\chi_i)_s(a)\rho(s)v_i \rightsquigarrow \rho(s) : V_i \longrightarrow V_j$.

  Let $K = \{s \in G : \rho(s)V_0 = V_0\} = \mathrm{Stab}_G(\chi_0) \geq H$.

  (問號) $\left\{\varphi : K \longrightarrow \mathrm{GL}(V_0)\right.$

□

Property 3.11.2. Each p-elementary group H is supersolvable.

Proof: Let $H = CP$ with $p \not| |C|$ and $C = \langle s \rangle$, $|P| = p^a$ and $P \leq C_G(s)$.

- Recall : $Z(P) \neq \{e\}$, if $P = Z(P)$ i.e. P is abelian, then P us supersolvable. If $P/Z(P) \neq \{e\}$, then $Z(P/Z(P)) \neq \{e\}$, say $Z_1(P)/Z(P) = Z(P/Z(P)) \lhd P/Z(P) \rightsquigarrow \{e\} \lhd Z(P) \lhd Z_1(P) \lhd P$. If $P = Z_1(P)$, then P is supsersolvable. Otherwise, $Z_1(P) \lhd Z_2(P) \lhd P, \cdots$. So P is supersolvable.

- Now, $C \lhd H, H/C$ is a p-group. Say

$$\{\overline{e}\} \lhd Z(H/C) \lhd Z_1(H/C) \lhd \cdots \lhd Z_s(H/C) = H/C$$

  Say $Z_i(H/C) = H_i/C$, then $\{e\} \lhd C \lhd H_0 \lhd H_1 \lhd \cdots \lhd H$ i.e. H is supersolvable.

□

Theorem 3.11.3. Each character of G is a linear combination with integer coefficient of monomial characters.

Proof: By Brauer theorem, $\mathrm{Ch}(G) = \sum_{H \in \bigcup_{\mathbb{P}} E_p} \mathrm{Ind}\,\mathrm{Ch}(H)$. Since H is supersolvable, by Property 3.11.2, each irreducible rep of H is monomial. And by transitivity of induction, the theroem follows. □

3.12 GL_2 over a finite field

Let $G = \mathrm{GL}_2(\mathbb{F}_q)$ with $2 \not| q = p^n \rightsquigarrow |G| = (q^2-1)(q^2-q) = q(q+1)(q-1)^2$. For $\alpha \in G$, the characteristic polynomial of α is

- reducible : α is conjugate to

$$\underbrace{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}}, \underbrace{\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}}_{\text{Jordan form}}, \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}_{a \neq d},$$

- irreducible : α is conjugate to

$$\underbrace{\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}}_{\text{rational form}} \text{ with char. poly.} = x^2 + ax + b$$

Now, we want to calculate the number of conjugacy classes and number in each class. To calculate the number of elements in class, we need to calculate the centralizer.

α	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$	$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$
# of class	$q-1$	$q-1$	$\frac{1}{2}(q-1)(q-2)$	$\frac{1}{2}q(q-1)$
# of elements in class	1	q^2-1	q^2+q	q^2-q

- $\begin{pmatrix} x & z \\ y & u \end{pmatrix} \in C_G\left(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}\right) \rightsquigarrow \begin{pmatrix} x & z \\ y & u \end{pmatrix}^{-1} = \frac{1}{D}\begin{pmatrix} u & -z \\ -y & x \end{pmatrix}$, where $D = xu - yz \neq 0$.

$$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \begin{pmatrix} x & z \\ y & u \end{pmatrix}\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)\begin{pmatrix} x & z \\ y & u \end{pmatrix}^{-1}$$

$$\Longrightarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \frac{-xy}{D} & \frac{x^2}{D} \\ \frac{-y^2}{D} & \frac{xy}{D} \end{pmatrix}$$

Then $y^2 = 0 \rightsquigarrow y = 0$ and $x^2 = xu \rightsquigarrow x = 0 (\rightsquigarrow D = 0\ (\not\rightarrow))$ or u. Hence,

$$C_G\left(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}\right) = \left\{\begin{pmatrix} x & z \\ 0 & x \end{pmatrix}\middle| x \neq 0\right\} \rightsquigarrow \# = q(q-1)$$

and thus # of elements in class is $\frac{|G|}{q(q-1)} = q^2 - 1$.

- Similarly,

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} x & z \\ y & u \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} x & z \\ y & u \end{pmatrix}^{-1} = \begin{pmatrix} \frac{axu-dzy}{D} & \frac{-axz+dzx}{D} \\ \frac{ayu-duy}{D} & \frac{-ayz+dux}{D} \end{pmatrix}$$

$$\Longrightarrow \begin{cases} ayu - dyu = 0 \rightsquigarrow (a-d)yu = 0 \rightsquigarrow yu = 0 \\ axz - dxz = 0 \rightsquigarrow (a-d)xz = 0 \rightsquigarrow xz = 0 \\ \frac{axu-dzy}{xu-zy} = a \rightsquigarrow zy = 0 \\ \frac{-ayz-dux}{xu-zy} = d \rightsquigarrow zy = 0 \end{cases}$$

Then $y = z = 0$. Hence,

$$C_G\left(\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right) = \left\{\begin{pmatrix} x & 0 \\ 0 & u \end{pmatrix}\middle| x \neq 0, u \neq 0\right\} \rightsquigarrow \# = (q-1)^2$$

Notice that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix}$. So there is $\binom{q-1}{2}$ classes and each class have $\frac{|G|}{(q-1)^2} = q(q+1)$ elements.

- For last case, it is too complicated to calculate it's centralizer. We give another method.

  For given $\alpha \in G$. By Cayley Hamilton theorem, $\alpha^2+a\alpha+b=0 \rightsquigarrow \alpha = \frac{-a\pm\sqrt{a^2-4b}}{2}$. Let $d=a^2-4b \notin \mathbb{F}_q^2$ and $K=\mathbb{F}_q(\sqrt{d})=\mathbb{F}_q \oplus \mathbb{F}_q\sqrt{d} \simeq \mathbb{F}_{q^2}$. Now, $\alpha^+ := \frac{-a}{2}+\frac{1}{2}\sqrt{d}$ can be regard as the element in $\mathrm{GL}(K)$ by multiply on left side

$$\alpha^+(x+y\sqrt{d}) = \left(\frac{-a}{2}x+\frac{d}{2}y\right)+\left(\frac{1}{2}x-\frac{a}{2}y\right)\sqrt{d} \rightsquigarrow \alpha \longleftrightarrow \begin{pmatrix} \frac{-a}{2} & \frac{d}{2} \\ \frac{1}{2} & \frac{-a}{2} \end{pmatrix}$$

  Then every type of $\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$ can be regard as the element in $\mathbb{F}_{q^2} \simeq K$ with form $u+v\sqrt{d} \neq 0$ with $v \neq 0$. Notice that

$$\alpha^{-1} = \frac{-a}{2}-\frac{1}{2}\sqrt{d} \longleftrightarrow \begin{pmatrix} \frac{-a}{2} & \frac{d}{2} \\ \frac{1}{2} & \frac{-a}{2} \end{pmatrix}$$

  which have same char. poly ($x^2+ax+b=0$) with the matrix corresponding to α^+. So there have exactly $\frac{p(p-1)}{2}$ different classes of this type. By counting all element in G, we have each classes have q^2-q elements.

Now, we start to find all irreducible representation of $\mathrm{GL}_2(\mathbb{F}_q)$. First, we define

- Z = center of $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \neq 0 \right\}$ which is abelian.
- A = diagonal subgroup of $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a,b \neq 0 \right\}$.
- U = group of unipotent elements $= \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in \mathbb{F}_q \right\}$.
- B = Borel subgroup $= AU = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| a,b \neq 0 \right\}$ collect all upper triangular matrix in G.

Fact 3.12.1. $U \lhd B$ and $B/U \simeq A$

$$\begin{pmatrix} x & z \\ 0 & y \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & z \\ 0 & y \end{pmatrix}^{-1} = \begin{pmatrix} 1 & by^{-1} \\ 0 & 1 \end{pmatrix}$$

Our goal is using irreducible representation of subgroup of G with degree one and induced to G.

- 1st type : $\mu : \mathbb{F}_q^\times \to \mathbb{C}^\times$: group homomorphism

$$\rho : G \xrightarrow{\det} \mathbb{F}_q^\times \xrightarrow{\mu} \mathbb{C}^\times \quad : \text{deg 1 rep. of } G$$

	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$	$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$
ρ	$\mu(a)^2$	$\mu(a)^2$	$\mu(ad)$	$\mu(d)$

$\because \mathbb{F}_q^\times = \langle r \rangle$ with $r^{q-1} = 1 \rightsquigarrow \mu(r) : (q-1)$-th root of unity $\rightsquigarrow$ # of $\mu = q-1 \therefore$ There are $q-1$ characters of 1st type.

- 2nd type : $\mu : \mathbb{F}_q^\times \longrightarrow \mathbb{C}^\times$: group homomorphism. Let $\psi_\mu = \mathrm{Res}_A(\mu \circ \det)$. Consider

$$\widetilde{\psi_\mu} : B \xrightarrow{\pi} B/U \simeq A \xrightarrow{\psi_\mu} \mathbb{C}^\times \quad : \text{group homomorphism}$$

$$\Longrightarrow \widetilde{\psi_\mu}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = \psi_\mu\left(\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right) = \mu(ad)$$

The induced character $\psi_\mu^G := \mathrm{Ind}_B^G(\widetilde{\psi_\mu})$

$\because \langle \mathrm{Ind}_B^G(\widetilde{\psi_\mu}), \mu \circ \det \rangle_G = \langle \widetilde{\psi_\mu}, \mathrm{Res}_B(\mu \circ \det) \rangle_B = \langle \widetilde{\psi_\mu}, \widetilde{\psi_\mu} \rangle_B = 1 \therefore \psi_\mu^G$ contains one $\mu \circ \det$. We plan to pick $\chi = \psi_\mu^G - \mu \circ \det$. $\forall \alpha \in G$

$$\chi(a) = \psi_\mu^G(\alpha) - \mu \circ \det(a) = \frac{1}{q(q-1)^2} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in B}} \mu \circ \det(\beta^{-1}\alpha\beta) - \mu \circ \det(\alpha)$$

- $\alpha = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$:

$$\chi(\alpha) = (q+1)(\mu \circ \det(a)) = \mu \circ \det(\alpha) = q\mu(a)^2$$

- $\alpha = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} : \beta = \begin{pmatrix} x & z \\ y & u \end{pmatrix}$, then $\beta^{-1}\alpha\beta \in B \iff y = 0$ i.e. $\beta \in B$. Then

$$\chi(\alpha) = \mu \circ \det(\alpha) - \mu \circ \det(\alpha) = 0$$

- $\alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : \beta^{-1}\alpha\beta \in B \iff \begin{cases} y = 0 \\ u \neq 0 \end{cases}$ or $\begin{cases} u = 0 \\ y \neq 0 \end{cases}$ $\rightsquigarrow$ # of $\beta = 2|B|$

$$\chi(\alpha) = 2\mu \circ \det(\alpha) - \mu \circ \det(\alpha) = \mu(ad)$$

- $\alpha = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} : \beta^{-1}\alpha\beta \notin B \iff u^2 + by^2 + ayu = 0 \iff y = 0\ u = 0\ (\rightarrow\!\leftarrow)$ or uy^{-1} is a root of $x^2 + ax + b$ $(\rightarrow\!\leftarrow)$. So

$$\chi(\alpha) = -\mu \circ \det(\alpha) = -\mu(b)$$

Hence,

$$\langle\chi,\chi\rangle = \frac{1}{|G|}\left((q-1)q^2\mu(a)^2\overline{\mu(a)}^2 + (q-1)(q^2-1)\cdot 0 \right.$$
$$\left. + \frac{1}{2}(q-1)(q-2)(q^2+q)\mu(ad)\overline{\mu(ad)} + \frac{1}{2}(q-1)q(q^2-q)(-\mu(b))(\overline{-\mu(b)})\right) = 1$$

since $|\mu(a)| = 1\ \forall a \in G$. So χ is irr.
$\because \#$ of $u = q-1 \therefore$ There are $(q-1)$ of χ of degree $([G:B]-1) = q$.

- 3rd type : $\psi : A \to \mathbb{C}^\times$: group homomorphism. Notice that $[N(A):A] = 2$ and $N(A) = A \cup \omega A$, where $\omega = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ and $\omega^{-1}\operatorname{diag}(a,d)\omega = \operatorname{diag}(d,a)$. Then

$$\psi_\omega(\operatorname{diag}(a,d)) = \psi(\operatorname{diag}(d,a))$$

Recall : $\mu : A \to \mathbb{C}^\times$ define by $\operatorname{diag}(a,d) = \mu(a)\mu(d) \rightsquigarrow \mu_\omega = \mu$. Now, we want $\psi \neq \psi_\omega$. Since $\operatorname{diag}(a,d)\operatorname{diag}(a',d') = \operatorname{diag}(aa',dd')$, we can write

$$\psi\left(\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}\right) = \psi_1(a)\psi_2(d)$$

with $\psi_i : \mathbb{F}_q^\times \to \mathbb{C}^\times$. To let $\psi \neq \mu$, we may assume $\psi_1 \neq \psi_2$. Also, ψ can we regard as representation of B by $\psi : B \xrightarrow{\pi} B/U \to \mathbb{C}^\times$ i.e.

$$\psi\left(\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\right) = \psi\left(\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}\right) = \psi_1(a)\psi_2(d)$$

Let $\psi_1 \neq \psi_2$ and $\psi^G = \operatorname{Ind}_B^G \psi$.

•• $\alpha = \begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$:

$$\psi^G(\alpha) = \frac{1}{|B|}\sum_{\substack{\beta\in G\\ \beta^{-1}\alpha\beta\in B}} \psi(\alpha) = \frac{|G|}{|B|}\psi_1(a)\psi_2(a) = (q+1)\psi_1(a)\psi_2(a)$$

•• $\alpha = \begin{pmatrix}a & 1\\ 0 & a\end{pmatrix}$:

$$\psi^G(\alpha) = \frac{1}{|B|}\sum_{\substack{\beta\in G\\ \beta^{-1}\alpha\beta\in B\\ (\beta\in B)}} \psi(\beta^{-1}\alpha\beta) = \frac{|B|}{|B|}\psi_1(a)\psi_2(a) = \psi_1(a)\psi_2(a)$$

•• $\alpha = \begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}$: Let $B' = B\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$

$$\psi^G(\alpha) = \frac{1}{|B|}\sum_{\substack{\beta\in G\\ \beta^{-1}\alpha\beta\in B\\ (\beta\in B \text{ or } B')}} \psi(\beta^{-1}\alpha\beta) = \psi_1(a)\psi_2(d) + \psi_1(d)\psi_2(a)$$

•• $\alpha = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$: no $\beta \in G$ s.t. $\beta^{-1}\alpha\beta \in B$, $\psi^G(\alpha) = 0$.

Then

$$\langle \psi^G, \psi^G \rangle = \frac{1}{|G|}\Big((q-1)(q+1)^2|\psi_1(a)|^2|\psi_2(a)|^2 + (q-1)(q^2-1)|\psi_1(a)|^2|\psi_2(a)|^2 + \frac{1}{2}(q^2+q)\sum_{a\neq d \text{ in } \mathbb{F}_q^\times}(\psi_1(a)\psi_2(d)+\psi_1(d)\psi_2(a))(\overline{\psi_1(a)\psi_2(d)} + \overline{\psi_1(d)\psi_2(a)}) + \frac{1}{2}(q-1)q(q^2-q)\cdot 0\Big)$$

For 3rd term, it can be rewrite as

$$|\psi_1(a)|^2||\psi_2(d)|^2 + |\psi_1(d)|^2||\psi_2(a)|^2 + \psi(\alpha)\psi((\alpha^{-1})^\omega) + \psi(\alpha^\omega)\psi(\alpha^{-1})$$

Now, consider $\psi' : A \to \mathbb{C}^\times$ define by $\alpha \mapsto \psi(\alpha^{1-\omega})$, since $\psi \neq \psi^\omega$, so ψ' is non-trivial degree one representation, then $\langle \chi_A^{\text{trivial}}, \chi' \rangle = 0$ i.e. $\sum_{\alpha\in A}\psi(\alpha^{1-\omega})$. Similarly, $\sum_{\alpha\in A}\psi(\alpha^{\omega-1}) = 0$. So the 3rd term is equal to

$$2(q-1)(q-2) - \sum_{a\in F_q^\times}(\psi(\alpha^{1-\omega}) + \psi(\alpha^{\omega-1})) = 2(q-1)(q-2) - 2(q-1)$$

Then

$$\langle \psi^G, \psi^G \rangle = \frac{1}{|G|}\Big(2q(q-1)(q+1) + q(q+1)(q-1)(q-3)\Big) = 1$$

So φ^G is irr. of deg $q+1$. And # of φ^G is $\binom{q-1}{2}$, since $|\psi_i| = (q-1)$ and $(\psi_1\psi_2)^\omega = (\psi_2\psi_1)$.

- **Observation** : Let $[K : \mathbb{F}_q] = 2 \rightsquigarrow K \simeq \mathbb{F}_{q^2}$ which is unique. We can regard $K^\times$ as an abelian subgroup of $\mathrm{GL}_2(\mathbb{F}_q) : K = \mathbb{F}_q \oplus \zeta\mathbb{F}_q$. $\forall \alpha \in K^\times$, say $\alpha = a + b\zeta$ with $(a,b) \neq (0,0)$.

$$\begin{array}{rccc} \alpha : & K & \longrightarrow & K \\ & u+v\zeta & \longmapsto & (a+b\zeta)(u+v\zeta) = (au+bv\zeta^2) + (av+bu)\zeta \end{array}$$

$$\longleftrightarrow \begin{pmatrix} a & b\zeta^2 \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$$

(for convenience, we let $\zeta^2 \in \mathbb{F}_q \setminus \mathbb{F}_q^2$).

- 4th type : Let $\theta : K^\times \longrightarrow \mathbb{C}^\times$: group homo. with $\theta_\omega \neq \theta$. Let $\theta^G = \mathrm{Ind}_K^G(\theta)$.

•• $\alpha = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$:

$$\theta^G(\alpha) = \frac{1}{|K^\times|}\sum_{\substack{\beta\in G \\ \beta^{-1}\alpha\beta\in K^\times}}\theta(\beta^{-1}\alpha\beta) = \frac{|G|}{|K^\times|}\theta(\alpha) = (q^2-q)\theta(\alpha)$$

- $\alpha = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} : \beta = \begin{pmatrix} x & z \\ y & u \end{pmatrix} \rightsquigarrow \beta\alpha\beta^{-1} \in K^\times \implies xy = 0 \implies x = y = 0$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$). So

$$\theta^G(\alpha) = \frac{1}{|K^\times|} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in K^\times}} \theta(\beta^{-1}\alpha\beta) = 0$$

- $\alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : \beta = \begin{pmatrix} x & z \\ y & u \end{pmatrix} \rightsquigarrow \beta\alpha\beta^{-1} \in K^\times \implies axu - dzy = -ayz + dux \implies xu + yz = 0, -xz = \zeta^2 yu \implies x^2 z = \zeta^2 y^2 z$. Since $\zeta^2 \in \mathbb{F}_q \setminus \mathbb{F}_q^2 \implies z = 0$ i.e. $D = 0$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$). So

$$\theta^G(\alpha) = \frac{1}{|K^\times|} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in K^\times}} \theta(\beta^{-1}\alpha\beta) = 0$$

- $\alpha = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$:

$$\theta^G(\alpha) = \frac{1}{|K^\times|} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in K^\times}} \theta(\beta^{-1}\alpha\beta) = \theta(\alpha) + \theta(\alpha^\omega)$$

Let $\mu : \mathbb{F}_q^\times \longrightarrow \mathbb{C}^\times$ be a group homo. and $\lambda : \mathbb{F}_q^+ \to \mathbb{C}^\times$ be a nontrivial group homo.. Define

$$\begin{array}{rccc} (\mu, \lambda) : & ZU & \longrightarrow & \mathbb{C}^\times \\ & \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} & \longmapsto & \mu(a)\lambda(x) \end{array}$$

Let $(\mu, \lambda)^G = \mathrm{Ind}_{ZU}^G(\mu, \lambda)$

- $\alpha = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$:

$$(\mu, \lambda)^G(\alpha) = \frac{1}{|ZU|} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in ZU}} (\mu, \lambda)(\alpha) = \frac{|G|}{|ZU|}\mu(a) = (q^2 - 1)\mu(a)$$

- $\alpha = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} : \beta^{-1}\alpha\beta \in ZU \iff \beta \in B$. So

$$(\mu, \lambda)^G(\alpha) = \frac{1}{|ZU|} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in ZU}} (\mu, \lambda)(\beta^{-1}\alpha\beta) = \mu(a) \sum_{c \in \mathbb{F}_q^\times \setminus \{1\}} = -\mu(a)$$

- $\alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : \beta\alpha\beta^{-1} \in ZU \iff yu = 0, xu + yz = 0$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$)

$$(\mu, \lambda)^G(\alpha) = \frac{1}{|ZU|} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in ZU}} (\mu, \lambda)(\beta^{-1}\alpha\beta) = 0$$

•• $\alpha = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} : \beta\alpha\beta^{-1} \in ZU \implies u^2 + by^2 + auy = 0$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$).

$$(\mu, \lambda)^G(\alpha) = \frac{1}{|ZU|} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in ZU}} (\mu, \lambda)(\beta^{-1}\alpha\beta) = 0$$

Let $\theta' = (\operatorname{Res} \theta, \lambda)^G - \theta^G$

•• $\alpha = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$:

$$\theta'(\alpha) = (q-1)\theta(a)$$

•• $\alpha = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$:

$$\theta'(\alpha) = -\theta(a)$$

•• $\alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$:

$$\theta'(\alpha) = 0$$

•• $\alpha = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$:

$$\theta'(\alpha) = -\theta(a) - \theta(a^\omega)$$

By similar method,

$$\sum_{\alpha \in G} |\theta'(\alpha)|^2 = (q-1)(q-1)^2 + (q-1)(q^2-1) + 0 + \frac{q^2-q}{2} \sum_{\alpha \in (K^\times \setminus \mathbb{F}_q^\times)} |\theta(\alpha) + \theta(\alpha^\omega)|^2 = |G|$$

Hence, θ' is irr of degree $([G : ZU] - [G : K^\times]) = q - 1$ and # of $\theta' = \frac{1}{2}(|K^\times| - |F^\times|) = \frac{1}{2}(q^2 - q)$.

- Now,

$$(q-1) \cdot 1^2 + (q-1) \cdot q^2 + \frac{1}{2}(q-1)(q-2) \cdot (q+1)^2 + \frac{1}{2}(q^2-q) \cdot (q-1)^2 = |G|$$

Hence, those four types are all irreducible representation of $\mathrm{GL}_2(\mathbb{F}_q)$.

Chapter 4

Presentation

Contents

4.1 Hilbert's nullstellensatz

4.1.1 Motivation

Let F be an algebraically closed field and $P_1, P_2, ..., P_n \in F[x_1, ..., x_d]$. When is it possible to solvable $P_1 = P_2 = \cdots = P_n = 0$ in $F[x_1, ..., x_d]$. First, if there exists $Q_1, ..., Q_n \in F[x_1, ..., x_d]$ such that

$$\sum_{i=1}^{n} P_i Q_i = 1$$

then it is impossible to solve. Now, we may ask : is this cases be the only obstacle to solve $P_i = 0 \ \forall i$. It will be answer by Hilbert's nullstellensatz.

4.1.2 Solvability test for a system of equations and inequations

Lemma 4.1.1. Let $f, g \in R[x]$, R be a ring and $g \neq 0$. Let $b_m x^m$ be the leading term of g. Then there exists $k \in \mathbb{Z}$ and $q, r \in R[x]$ with $\deg r < \deg g$ such that $b_m^k f = qg + r$.

Proof: By induction on $n = \deg f$. $n < m$: OK! $n \geq m$: Let $a_n x^n$ be the leading term of f, then $\deg(b_m f - a_n g) < \deg f$. By induction hypothesis, $\exists k \in \mathbb{Z}$, $q, r \in R[x]$ with $\deg r < \deg g$ s.t.

$$b_m^k(b_m f - a_n g) = qg + r \implies b_m^{k+1} f = (b_m^k a_n + q)g + r$$

Hence, $(k+1, b_m^k a_n + q, r)$ as required. □

Lemma 4.1.2. Let F be a field and $f, g \in F[x]$ with $f, g \neq 0$. Let $h = \deg f$. Then $f \nmid g^h$ if and only if there exists a in some algebraic extension field E/F such that $f(a) = 0$ and $g(a) \neq 0$.

Proof:

- ($\Rightarrow$) : Assume $f \nmid g^h$. Let $p_1, ..., p_m$ be all distinct irreducible of f, We claim that there exists p_i such that $p_i \nmid g$. If $p_i | g \ \forall i$, then $(p_1 \cdots p_m) | g$.

  $$\implies f | (p_1 \cdots p_m)^h | g^h \ (\rightarrow\!\!\!\!\leftarrow)$$

  Let $p_i \nmid g$ and $E = F[x]/\langle p_i \rangle$, then by Kronecker's theorem, E is an algebraic extension that has a root $a = x + \langle p_i \rangle$ of f, but $g(a) \neq 0$.

- ($\Leftarrow$) : Assume that $f(a) = 0$ and $g(a) \neq 0$, then $0 | g(0)^h \neq 0$ ($\rightarrow\!\!\!\!\leftarrow$).

□

Theorem 4.1.1 (Solvability test for a system of equations and inequations)**.** Let $K = \mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ and let $A = K[\underline{t}]$ and $B = A[\underline{x}]$, where $\underline{t} = t_1, ..., t_r$, $\underline{x} = x_1, ..., x_n$. Let $\Gamma = \{F_1, ..., F_m; G\} \subseteq B$. Then we can determine in a finite number of steps with finite collection $\{\Delta_1, \Delta_2, ..., \Delta_s\}$, where

$$\Delta_j = \{f_{j1}, ..., f_{j,m_j}; g_j\} \subseteq A$$

such that for any extension field F of K and any $\underline{c} = c_1, ..., c_r \in F$, the system of equations and inequations

$$\Gamma(\underline{c}) : F_1(\underline{c}; \underline{x}) = F_2(\underline{c}; \underline{x}) = \cdots = F_m(\underline{c}; \underline{x}) = 0,\ G(\underline{c}; \underline{x}) \neq 0 \qquad (*)$$

is solvable for $\underline{x}$ in some extension field E/F if and only if $\underline{c}$ satisfies one of the systems

$$\Delta_j(\underline{c}) : f_{j1}(\underline{c}) = f_{j2}(\underline{c}) = \cdots = f_{jm_j}(\underline{c}) = 0,\ g_j(\underline{c}) \neq 0$$

$1 \leq j \leq s$. Moreover, when the condition are satisfied, then a solution exists for $(*)$ in some algebraic extension E'/F.

Proof: We induct on n.

- $n = 1$: We induct on $\deg \Gamma \equiv \sum_{i=1}^{m} \deg_x F_i + \deg_x G$.
  - If $\deg \Gamma = 0$, then let $\Delta_1 \equiv \Gamma$.
    The system $\Gamma(\underline{c})$ is solvable $\iff$ $\Delta_1(c)$ is satisfied.
    If $\Delta_1(c)$ is satisfied, then any $x \in F$ is a solution of $\Gamma(\underline{c})$ and F is algebraic over itself. Therefore it has a solution in an algebraic extension field.
  - If $\deg \Gamma > 0$, we split it into 4 cases :
    - $\deg_x F_1, \deg_x F_2 > 0$: Let ax^α, bx^β be the leading terms of F_1, F_2 respectively and we may assume $\alpha > \beta$ by Lemma 4.1.1. Now, we want using induction hypothesis by Euclidean algorithm. Intuitively, we will consider Γ'' in below. But Γ'' is solvable will not implies Γ solvable, since b may be 0 (input $\underline{c}$). So we need consider Γ'.

      $$\begin{cases} \Gamma' = \{b, F_1, F_2, F_2 - bx^\beta, F_3, ...; G\} \\ \Gamma'' = \{bF_1 - ax^{\alpha-\beta}F_2, F_2, F_3, ...; G\} \end{cases}$$

      Since $\deg \Gamma', \deg \Gamma'' < \deg \Gamma$, by induction hypothesis, there exists $\{\Delta'_j\}_{j=1}^{s'}$ and $\{\Delta''_j\}_{j=1}^{s''}$ for Γ' and Γ'' respectively. For any F/K and $\underline{c} \in F$, we have

      $$b(\underline{c}) = 0, \Gamma(\underline{c}) \text{ is solvable} \iff \Gamma'(\underline{c}) \text{ is solvable} \iff \underline{c} \text{ satisfy one of } \Delta'_j$$

      $$b(\underline{c}) \neq 0, \Gamma(\underline{c}) \text{ is solvable} \iff \Gamma''(\underline{c}) \text{ is solvable} \iff \underline{c} \text{ satisfy one of } \Delta''_j$$

      Let $\{\Delta_j\}_{j=1}^{s} \equiv \{\Delta'_j\}_{j=1}^{s'} \cup \{\Delta''_j\}_{j=1}^{s''}$, then $\Gamma(\underline{c})$ is solvable if and only if $\underline{c}$ satisfy one of the system in $\{\Delta_j\}_{j=1}^{s}$. When the condition hold, by induction hypothesis, $\Gamma(\underline{c})$ has a solution in an algebraic extension field.

- $\deg_x F_1 > 0, \deg_x F_i = 0\ \forall i > 1$ and $\deg_x G > 0$: Let ax^α, bx^β be the leading terms of F_1, G respectively. By Lemma 4.1.1, there exists $Q, R \in B$ such that $a^{\alpha\beta}G^\alpha = QF_1 + R$. Let $R = r_{\alpha-1}x^{\alpha-1} + \cdots + r_0$ and

$$\begin{cases}\Gamma' = \{a, F_1 - ax^\alpha, F_2, ..., F_m; G\} \\ \Delta''_j = \{F_2, ..., F_m; ar_j\} \text{ for } 0 \le j < \alpha\end{cases}$$

Since $\deg \Gamma' < \deg \Gamma$, there exists a set $\{\Delta'_j\}$ for Γ'. For any F/K and $\underline{c} \in F$, we have

$$a(\underline{c}) = 0, \Gamma(\underline{c}) \text{ is solvable} \iff \Gamma'(\underline{c}) \text{ is solvable} \iff \underline{c} \text{ satisfies one of } \Delta'_j$$

and

$$\begin{aligned} & a(\underline{c}) \neq 0 \text{ and } \Gamma(\underline{c}) \text{ is solvable} \\ \iff & a(\underline{c}) \neq 0 \text{ and } F_2(\underline{c}) = \cdots = F_m(\underline{c}) = 0 \text{ and } F_1(\underline{c}; x) \not| G(\underline{c}; x)^\alpha \\ \iff & a(\underline{c}) \neq 0 \text{ and } F_2(\underline{c}) = \cdots = F_m(\underline{c}) = 0 \text{ and } R(\underline{c}; x) \neq 0 \\ \iff & a(\underline{c}) \neq 0 \text{ and } F_2(\underline{c}) = \cdots = F_m(\underline{c}) = 0 \text{ and } r_i(\underline{c}) \neq 0 \text{ for some } i \\ \iff & \underline{c} \text{ satisfies one of } \Delta''_i \end{aligned}$$

where " $\iff$ " is by Lemma 4.1.2. Hence, let $\{\Delta_j\} \equiv \{\Delta'_j\} \cup \{\Delta''_j\}$, then $\Gamma(\underline{c})$ is solvable if and only if $\underline{c}$ satisfies one of Δ_i. By induction hypothesis and Lemma 4.1.2, if the condition are satisfied, then there exists a solution x in some algebraic extension.

- $\deg_x F_1 > 0, \deg_x F_i = 0\ \forall i > 1$ and $\deg_x G = 0$: Let ax^α be the leading term of F_1 and

$$\begin{cases}\Gamma' = \{a, F_1 - ax^\alpha, F_2, ..., F_m; G\} \\ \Gamma'' = \{F_2, ..., F_m; aG\}\end{cases}$$

Since $\deg \Gamma', \deg \Gamma'' < \deg \Gamma$, there exists sets $\{\Delta'_j\}$, $\{\Delta''_j\}$ for Γ' and Γ''. For any F/K and $\underline{c} \in F$, we have

$$a(\underline{c}) = 0, \Gamma(\underline{c}) \text{ is solvable} \iff \Gamma'(\underline{c}) \text{ is solvable} \iff \underline{c} \text{ satisfies one of } \Delta'_j$$

$$a(\underline{c}) \neq 0, \Gamma(\underline{c}) \text{ is solvable} \iff \Gamma''(c) \text{ is solvable} \iff \underline{c} \text{ satisfies one of } \Delta''_j$$

where "$\impliedby$" is by Kronecker theorem (F_i, G is independent on $x\ \forall i > 1$). Then by same argument in above.

- $\deg_x F_i = 0\ \forall i$ and $\deg_x G > 0$: Let ax^α be the leading term of G and

$$\begin{cases}\Gamma' = \{a, F_1, ..., F_m; G - ax^\alpha\} \\ \Gamma'' = \{F_1, ..., F_m; a\}\end{cases}$$

Since $\deg \Gamma', \deg \Gamma'' < \deg \Gamma$, there exists sets $\{\Delta'_j\}$, $\{\Delta''_j\}$ for Γ' and Γ''. For any F/K and $\underline{c} \in F$, we have

$$a(\underline{c}) = 0, \Gamma(\underline{c}) \text{ is solvable} \iff \Gamma'(\underline{c}) \text{ is solvable} \iff \underline{c} \text{ satisfies one of } \Delta'_j$$

$a(\underline{c}) \neq 0, \Gamma(\underline{c})$ is solvable $\Longleftrightarrow \Gamma''(\underline{c})$ is solvable $\iff \underline{c}$ satisfies one of Δ_j''

"$\Leftarrow$" : If $a(\underline{c}) \neq 0$, then $G(\underline{c}, x)$ at most α distinct roots. So $G(\underline{c}, x) \neq 0$ solvable in a field with cardinality bigger than α. Since we can always find an algebraic extension field E/F satisfying this condition (since finite field is not algebraically closed), therefore $\Gamma(\underline{c})$ is solvable. By same argument in above.

- For $n > 1$, we treat $x_1, ..., x_{n-1}$ as additional t's and apply the case for $n = 1$, then we get $\{\Lambda_i\}_{i=1}^{s} \subseteq K[\underline{t}][x_1, ..., x_{n-1}]$ that satisfies the properties in the theorem statement.

  Since each Λ_i has $n-1$ x's. By induction hypothesis, there exists $\{\Delta_{ij}\}_{j=1}^{s_j} \subseteq A$ satisfies the properties in the theorem statement. We claim that $\{\Delta_{ij}\}$ satisfies the condition : For any F/K and $\underline{c} \in F$

$$\begin{aligned} & \underline{c} \text{ satisfies one of } \Delta_{ij} \\ \iff & \exists x_1, ..., x_{n-1} \text{ that solves } \Lambda_i(\underline{c}) \\ \iff & \exists x_1, ..., x_{n-1} \text{ that } \underline{c}, x_1, ..., x_{n-1} \text{ satisfies } \Lambda_i \\ \iff & \exists x_1, ..., x_n \text{ that solves } \Lambda(\underline{c}) \\ \iff & \Gamma(\underline{c}) \text{ is solvable} \end{aligned}$$

  We can check that if the conditions are satisfied, then there exists a solution of $\Gamma(\underline{c})$ in some algebraic extension field.

□

Example 4.1.1. Consider $\Gamma = \{x^2 + y - t, x^2 - y - t; x\}$. By repeating the proof of the theorem, we can obtain : given $t \in F/K$,

$$\begin{aligned} & x^2 + y - t = x^2 - y - t = 0, x \neq 0 \text{ is solvable over some } E/F \\ \iff & y = 0, y + t = 0 \text{ is solvable over some } E/F \\ \iff & t \neq 0 \end{aligned}$$

Theorem 4.1.2. Let F be an algebraically closed field and let $f_1, .., f_m, g \in F[\underline{x}]$, where $\underline{x} = x_1, ..., x_n$. Suppose the system of equation and inequation

$$f_1(\underline{x}) = f_2(\underline{x}) = \cdots = f_m(\underline{x}) = 0, \ g(\underline{x}) \neq 0$$

has a solution in some extension field E/F, then it has a solution in F.

Proof: Let K be $\mathbb{Z}/p\mathbb{Z}$ if char$F$ => 0, or $\mathbb{Z}$ is char$F$ = 0. By adding enough indeterminates $\underline{t} = t_1, ..., t_r$, we can define polynomials $F_1, ..., F_m, G \in K[\underline{x}][\underline{x}]$ such that there exists $\underline{c} = c_1, ..., c_r \in F$ and $F_i(\underline{c}; \underline{x}) = f_i(\underline{x})$ $\forall i$, $G(\underline{c}, \underline{x}) = g(\underline{x})$. By assumption, the system $\Gamma(\underline{c})$ has a solution in some extension field E/F, where $\Gamma = \{F_1, ..., F_m; G\}$. By Theorem 4.1.1, it has a solution in some algebraic extension field E'/F. In other words, $f_1 = \cdots = f_m = 0$, $g \neq 0$ has a solution in E'. Since F is algebraically closed, $E' = F$ i.e. it has a solution in F. □

4.1.3 Hilbert's nullstellensatz

Definition 4.1.1. Let F be an algebraically closed field. Let S be a subset of $F[x_1, ..., x_n]$, we define $V(S)$ to be the set of points $(a_1, ..., a_n) \in F^n$ such that $f(a_1, ..., a_n) = 0$ for all $f \in S$. We call $V(S)$ is the **(affine algebraic) variety** define by S.

Theorem 4.1.3 (Hilbert's nullstellensatz, 1900)**.** Let I be an ideal in the polynomial ring $F[x_1, ..., x_n]$ over an algebraically closed field F and let $g \in F[x_1, ..., x_n]$. Suppose $g(a_1, ..., a_n) = 0$ for all $(a_1, ..., a_n) \in V(I)$. Then $g \in \sqrt{I}$.

Proof:

- Suppose $g \notin \sqrt{I} = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}$, then $\exists \mathfrak{p} \in \operatorname{Spec} k[x_1, ..., x_n]$ containing I s.t. $g \notin \mathfrak{p}$. Since F is a field which is Noetherian, by Hilbert basis theorem, $F[x_1, ..., x_n]$ is Noetherian. Hence, $I = \langle f_1, ..., f_m \rangle$ which is finitely generated. Let $D = F[x_1, ..., x_n]/\mathfrak{p}$ is integral domain, then $D = F[\overline{x_1}, ..., \overline{x_n}]$ and $f_i(\overline{x_1}, ..., \overline{x_n}) = 0 \ \forall i$, $g(\overline{x_1}, ..., \overline{x_n}) \neq 0$.
- Now, $\Gamma := \{f_1, ..., f_m; g\}$ is solvable in D and we want apply Theorem 4.1.2 but D is only integral domain. So we let E be the field of fraction of D, then F can embedded in E and Γ is solvable in E. Since F is algebraically closed, E is also algebraically closed. By Theorem 4.1.2, Γ has a solution in F, that is exists $\underline{a} = (a_1, ..., a_n) \in F^n$ s.t. $f_i(\underline{a}) = 0$ and $g(\underline{a}) \neq 0 \rightsquigarrow \underline{a} \in V(I)$. Then $g(\underline{a}) = 0$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$. Hence, $g \in \sqrt{I}$.

□

Corollary 4.1.1. Let I_1, I_2 be ideals in $F[x_1, ..., x_n]$ over an algebraically closed field F. Then $V(I_1) = V(I_2) \iff \sqrt{I_1} = \sqrt{I_2}$.

Proof:

- $(\Leftarrow)$: We claim that $V(I) = V(\sqrt{I})$:

  subproof : Since $I \subseteq \sqrt{I} \implies V(\sqrt{I}) \subseteq V(I)$. If $a \in V(I)$, then $\forall f \in \sqrt{I}$, say $f^n \in I \rightsquigarrow f(a)^n = 0 \rightsquigarrow f(a) = 0$ i.e. $a \in V(\sqrt{I})$. □

  By Claim, $V(I_1) = V(\sqrt{I_1}) = V(\sqrt{I_2}) = V(I_2)$.
- $(\Rightarrow)$: For $f \in \sqrt{I_1}$. Since $V(\sqrt{I_1}) = V(I_1) = V(I_2)$, f annihilates $V(I_2)$. By Hilbert's nullstellensatz, $f \in \sqrt{I_2}$ i.e. $\sqrt{I_1} \subseteq \sqrt{I_2}$. By symmetry, $\sqrt{I_2} = \sqrt{I_1}$.

□

Corollary 4.1.2. [weak Hilbert's nullstellensatz] If I is a proper ideal in $F[x_1, ..., x_n]$ over an algebraically closed field F, then $V(I) \neq \varnothing$.

Proof: Assume I is proper and $V(I) = \varnothing$. Since $f = 1$ annihilates $V(I)$. By Hilbert's nullstellensatz, $1^m \in I$ i.e. $I = k[x_1, ..., x_n]$ $(\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow)$. □

Remark 4.1.1. Back to motivation, weak nullstellensatz states that the only obstacle when solving $P_1 = \cdots = P_n = 0$ is that there exists $Q_1, ..., Q_n$ such that $\sum_{P_iQ_i} = 1$. In other words, exactly one of the following two things happens :

- $P_1 = \cdots = P_m = 0$ is solvable over F.
- There exists $Q_1, ..., Q_m \in F[x_1, ..., x_n]$ such that $\sum_{i=1}^{m} P_iQ_i = 1$.

Corollary 4.1.3. If F is an algebraically closed field, then the map

$$\varphi : (a_1, ..., a_n) \longmapsto \langle x_1 - a_1, ..., x_n - a_n \rangle$$

is a bijection of F^n onto $\operatorname{Max} F[x_1, ..., x_n]$

Proof:

- Let $M_a = \langle x_1 - a_1, ..., x_n - a_n \rangle$, where $a = (a_1, ..., a_n)$. Notice that

  $$F[x_1, ..., x_n]/M_a \simeq F[a_1, ..., a_n] \simeq F$$

  Hence, M_a is a maximal ideal $\rightsquigarrow \varphi$ is well-defined.
- Since $V(M_a) = (a_1, ..., a_n) \rightsquigarrow \varphi$ is $1 - 1$.
- Let $\mathfrak{m} \in \operatorname{Max} k[x_1, ..., x_n]$. By Corollary 4.1.2, $V(\mathfrak{m}) \neq \varnothing$. Say $a \in V(\mathfrak{m})$. Then $V(M_a) = \{a\} \subseteq V(\mathfrak{m})$. Since every polynomial in $\mathfrak{m}$ annihilates $V(M_a)$. By Hilbert's nullstellensatz, $\mathfrak{m} \subseteq \sqrt{M_a} = M_a$. Since $\mathfrak{m}$ and M_a are maximal ideal $\rightsquigarrow \mathfrak{m} = M_a$ i.e. φ is onto.

□

Theorem 4.1.4. Weak Hilbert's nullstellensatz and Hilbert's nullstellensatz are equivalent.

Proof:

- ($\Leftarrow$) : By above.
- ($\Rightarrow$) : Let I be the ideal in $F[x_1, ..., x_n]$ and $f \in F[x_1, ..., x_n]$ annihilates $V(I)$. If $f = 0 \rightsquigarrow f^1 \in I$. If $f \neq 0$, consider the ring $F[x_1, ..., x_n, y]$. Let J be the ideal generated by I and $1 - yf$ in $F[x_1, ..., x_n, y]$. We claim that $J = F[x_1, ..., x_n]$. If not, then by weak Hilbert's nullstellensatz, $V(J) \neq \varnothing$. Say $(a_1, ..., a_n, c) \in V(J)$, by $I \subseteq J \rightsquigarrow (a_1, ..., a_n) \in V(I)$. But $1 - yf$ doesn't annihilate $(a_1, ..., a_n, c)$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$). Hence, $J = k[x_1, ..., x_n, y]$. Say

  $$1 = g_0(1 - yf) + \underbrace{g_1h_1 + \cdots + g_rh_r}_{\in I}$$

Let $y = f^{-1}$ and see the relation in the field of fractions of $F[x_1, ..., x_n]$. Then we have

$$1 = \sum_{i=1}^{r} g_i(x_1, ..., x_n, f^{-1}) h_i(x_1, ..., x_n)$$

Notice that in the right hand side, the only powers of f appear in the denominators. Rewriting the right hand side to have a common denominator, then we get

$$1 = \frac{1}{f^m} \sum_{i=1}^{r} f_i(x_1, ..., x_n) h_i(x_1, ..., x_n)$$

for some $f_i \in F[x_1, ..., x_n]$. Then $f^m \in I$ i.e. $f \in \sqrt{I}$. This proves Hilbert's nullstellensatz.

□

Remark 4.1.2. The method of proving Hilbert's nullstellensatz from weak Hilbert's nullstellensatz is called the Rabinowitsch trick, introduced by George Yuri Rainich in 1929. We can prove a simplified version of Theorem 4.1.1 (for system of polynomial equations), then prove Weak nullstellensatz, then use the Rabinowitsch trick to prove Hilbert's nullstellensatz.

4.2 Integral & going up and going down theorem

In this section, every ring is commutative.

4.2.1 Introduction and motivation

Since I haven't studied algebraic geometry, I can't realize the meaning of integral in algebraic geometry. Let's see how it is introduced in Atiyah-MacDonald.

> In classical algebraic geometry curves were frequently studied by projecting them onto a line and regarding the curve as a (ramified) covering of the line. This is quite analogous to the relationship between a number field and the rational field-or rather between their rings of integers-and the common algebraic feature is the notion of integral dependence.

In the first half of this report, we will focus on the property of integral extension and derive the going up and going down theorem. In the second half, we will give some application for integral and going up, going down theorem. Which includes Noether's normalization lemma and Zariski's lemma, and our ultimate goal is Hilbert's nullstellensatz.

4.2.2 Extension and contraction

Before going to introduce the concept of integral, let's first introduce a concept that we will often use later. Given a ring homomorphism $f : A \to B$. Notice that if $\mathfrak{a}$ is the ideal of A, then $f(\mathfrak{a})$ may not be the ideal of B. For example, $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ by $z \mapsto z/1$. Then $f(2\mathbb{Z})$ is not an ideal in $\mathbb{Q}$, since the only ideal in $\mathbb{Q}$ are 0 and $\mathbb{Q}$. But we can check that if $\mathfrak{b}$ is the ideal of B, then $f^{-1}(\mathfrak{b})$ is the ideal of A.

Definition 4.2.1. Let $f : A \to B$ be a ring homomorphism, $\mathfrak{a}, \mathfrak{b}$ be the ideal of A, B respectively. Define

- the **extension** $\mathfrak{a}^e$ of $\mathfrak{a}$ is the ideal $Bf(\mathfrak{a})$ which is generated by $f(\mathfrak{a})$ in B i.e.

$$\mathfrak{a}^e = \{\sum_{\text{finite}} b_i f(a_i) : a_i \in \mathfrak{a}, b_i \in B\}$$

- the **contraction** $\mathfrak{b}^c$ of $\mathfrak{b}$ is the ideal $f^{-1}(\mathfrak{b})$ i.e.

$$\mathfrak{b}^c = \{a \in A : f(a) \in \mathfrak{b}\}$$

Property 4.2.1.

- $\mathfrak{b} \in \operatorname{Spec} B \implies \mathfrak{b}^c \in \operatorname{Spec} A$. Conversely, $\mathfrak{a} \in \operatorname{Spec} A$ will not implies $\mathfrak{a}^e \in \operatorname{Spec} B$.
- $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$, $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$
- $\mathfrak{a}^e = \mathfrak{a}^{ece}$, $\mathfrak{b}^c = \mathfrak{b}^{cec}$
- $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$, $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$

- $(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e$, $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$

Proof: By definition. □

Recall. Let $\rho : R \to S^{-1}R,\ x \mapsto \frac{x}{1}$ is natural canonical map

$$\begin{array}{ccc} \operatorname{Spec} S^{-1}R & \longleftrightarrow & \{\mathfrak{p} \in \operatorname{Spec} R : \mathfrak{p} \cap S = \varnothing\} \\ \mathfrak{q} & \longmapsto & \rho^{-1}(\mathfrak{q}) \\ S^{-1}\mathfrak{p} & \longmapsfrom & \mathfrak{p} \end{array}$$

So $\forall \mathfrak{p} \in \operatorname{Spec} R$ with $\mathfrak{p} \cap S = \varnothing$, $\mathfrak{p}^{ec} = \mathfrak{p}$.
If $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} R$ and $\mathfrak{p} \cap S = \mathfrak{q} \cap S = \varnothing$, then $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q} \iff \mathfrak{p} = \mathfrak{q}$

Theorem 4.2.1. Let $A \to B$ be a ring homomorphism and let $\mathfrak{p} \in \operatorname{Spec} A$. Then $\mathfrak{p}$ is the contraction of a prime ideal of $B \iff \mathfrak{p}^{ec} = \mathfrak{p}$.

Proof:

- $(\Rightarrow)$: If $\mathfrak{p} = \mathfrak{q}^c$ for some $\mathfrak{q} \in \operatorname{Spec} B$. Then $\mathfrak{p}^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c = \mathfrak{p}$.
- $(\Leftarrow)$: Let $S = f(A - \mathfrak{p})$ which is multiplicative closed subset of B. If $f(a) \in \mathfrak{p}^e \cap S$, then $a \in \mathfrak{p}^{ec} = \mathfrak{p}$, but $a \in A - \mathfrak{p}$ $(\rightarrow\!\leftarrow)$. So $\mathfrak{p}^e \cap S = \varnothing$ and thus the extension of $\mathfrak{p}^e$ in $S^{-1}B$ is a proper ideal $\mathfrak{n}$ in $S^{-1}B$. Say $\mathfrak{n} \subseteq \mathfrak{m}$ for some $\mathfrak{m} \in \operatorname{Max} S^{-1}B$. Let $\mathfrak{q}$ be the contraction of $\mathfrak{m}$ in B, then $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{p}^e \subseteq \mathfrak{q}$. Notice that $\mathfrak{q} \cap S = \varnothing$ (otherwise $\mathfrak{m} = S^{-1}B$), then $\mathfrak{q}^c \cap (A - \mathfrak{p}) = \varnothing$. Combine with $\mathfrak{q}^c \supseteq \mathfrak{p}^{ec} = \mathfrak{p}$, we have $\mathfrak{q}^c = \mathfrak{p}$.

□

4.2.3 Integral dependence

Definition 4.2.2. Let B be a ring and A is a subring of A. We say $x \in B$ is **integral** over A if

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

for some $a_i \in A$.

Example 4.2.1. $\mathbb{Z} \subseteq \mathbb{Q}$, if $t = r/s \in \mathbb{Q}$ is integral over $\mathbb{Z}$ with $\gcd(r, s) = 1$, then

$$\left(\frac{r}{s}\right)^n + a_1 \left(\frac{r}{s}\right)^{n-1} + \cdots + a_n = 0 \text{ with } a_i \in \mathbb{Z}$$

Multiply s^n in both side we have $s | r^n \implies s | 1$ i.e. $t \in \mathbb{Z}$.

Similar to algebraic over a field, we have some equivalent statement for integral and property similar to algebraic. But before the equivalent, we see the important lemma first.

Lemma 4.2.1. M : finitely generated A-module, $\mathfrak{a}$ be an ideal of A, $\phi \in \operatorname{End}_A(M)$ such that $\phi(M) \subseteq \mathfrak{a}M$. Then ϕ satisfies

$$\phi^n + a_1 \phi^{n-1} + \cdots + a_n = 0 \text{ for some } a_i \in \mathfrak{a}$$

Proof: Let $M = \langle x_1, ..., x_n \rangle_A$ and for all i, say $\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j$ for $a_{ij} \in \mathfrak{a}$. Then

$$\underbrace{\begin{pmatrix} \phi - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \phi - a_{22} & & \\ \vdots & & \ddots & \\ -a_{n1} & & & \phi - a_{nn} \end{pmatrix}}_{:=N} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{:=\mathbf{x}} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Then $0 = \text{adj}(N)N\mathbf{x} = \det(N)\mathbf{x} \implies \det(N)$ annihilates $x_1, ..., x_n$ i.e $\det N$ is zero endomorphism. Then $\det N = 0$ is polynomial of ϕ with coefficient in $\mathfrak{a}$ which is what we want. □

Proposition 4.2.1. TFAE

(1) $x \in B$ is integral over A

(2) $A[x]$ is finitely-generated A-module

(3) $A[x]$ is containing in a subring C of B which is finitely generating A-module

(4) exists a faithful $A[x]$-module M is finite generated A-module

Proof:

- (1) $\Rightarrow$ (2) : If x is a root of monic polynomial $f(t) \in A[t]$ with degree n, then $A[x] = \langle 1, x, ..., x^{n-1} \rangle_A$ which is finitely generated A-module.
- (2) $\Rightarrow$ (3) : Choose $C = A[x]$.
- (3) $\Rightarrow$ (4) : Choose $M = C$. If $y \in \text{Ann}_{A[x]}(C)$, then $y \cdot 1 = 0$. Hence, C is faithful $A[x]$-module.
- (4) $\Rightarrow$ (1) : Since $xM \subseteq M$. By Lemma 4.2.1 ($\phi : m \mapsto xm$ and $\mathfrak{a} = A$),

  $$f(\phi) = \phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

  for some $a_i \in A$. Then $f(x)M = f(\phi)M = 0$. Since M is faithful $A[x]$-module, $f(x) = 0$ i.e. x is integral over A.

□

Corollary 4.2.1. Let $x_1, ..., x_n \in B$ such that x_i is integral over A for all $i = 1, ..., n$. Then $A[x_1, ..., x_n]$ is finitely generated A-module.

Proof: By induction on n. Using Proposition 4.2.1 and the fact that x_i is integral over $A[x_1, ..., x_{i-1}]$. □

Corollary 4.2.2. Let $C = \{x \in B : x \text{ is integral over } A\}$ is a subring of B containing A.

Proof: If $x, y \in C$, then by Corollary 4.2.1, $A[x, y]$ is finitely generating A-module. Notice that $A[x \pm y], A[xy] \subseteq A[x, y] \subseteq B$, by Proposition 4.2.1, $x \pm y$, xy are integral over A. Clearly every element of A is integral over A. □

Definition 4.2.3.

- C in Corollary 4.2.2 is called the **integral closure** of A in B.
- If $C = A$, then we say A is **integrally closed** in B.
- If $C = B$, then we say B is **integral** over A.

Example 4.2.2. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{5}]$ is $\mathbb{Q}[\frac{1+\sqrt{5}}{2}]$:
If $z = a + b\sqrt{5}$ is integral over $\mathbb{Z}$, let $f(x) \in \mathbb{Z}[x]$ be the monic polynomial s.t. $f(z) = 0$. Notice that $(x - a)^2 - 5b^2 \in \mathbb{Q}[x]$ has root z. View f as the polynomial with coefficient Q, then $f(x) = ((x - a)^2 - 5b^2)g(x)$ for some monic polynomial g in $Q[x]$. By Guass lemma, f is reducible in $Z[x]$. So exists $c \in C$ s.t. $c((x - a)^2 - 5b^2), g(x)/c \in \mathbb{Z}[x]$. Consider the leading coefficient of two polynomial, $c = \pm 1$ i.e. $(x - a)^2 - 5b^2 \in \mathbb{Z}[x]$. Hence, $2a \in \mathbb{Z}$ and $a^2 - 5b^2 \in \mathbb{Z}$. Say $a = m/2$, $b = p/q$ with $\gcd(p, q) = 1$ and $q \in \mathbb{N}$.

$$a^2 - 5b^2 \in \mathbb{Z} \implies \frac{m^2q^2 - 20p^2}{4q^2} \in \mathbb{Z} \implies q^2 | 20p^2 \implies q|2$$

- If $q = 1$, then $a^2 \in \mathbb{Z} \implies a \in \mathbb{Z}$. Hence, $(x - a)^2 - 5b^2 \in \mathbb{Z}[x]$ has root z. And

$$a + b\sqrt{5} = (a + b)\frac{1 + \sqrt{5}}{2} + (a - b)\frac{2}{1 + \sqrt{5}} \in \mathbb{Q}\left(\frac{1 + \sqrt{5}}{2}\right) = \mathbb{Q}\left[\frac{1 + \sqrt{5}}{2}\right]$$

- If $q = 2$, say $a^2 - 5b^2 = k$ i.e. $m^2 - 5p^2 = 4k$. Then we can check that $m + p, m - p \in 2\mathbb{Z}$ and

$$a + b\sqrt{5} = \left(\frac{m + p}{2}\right)\frac{1 + \sqrt{5}}{2} + \left(\frac{m - p}{2}\right)\frac{2}{1 + \sqrt{5}} \in \mathbb{Q}\left(\frac{1 + \sqrt{5}}{2}\right) = \mathbb{Q}\left[\frac{1 + \sqrt{5}}{2}\right]$$

Remark 4.2.1. Let $f : A \to B$ be the ring homomorphism, so that B is A-algebra. Then f is said to be **integral**, and B is said to be an **integral** A-algebra, if B is integral over $f(A)$. We say f is **finite type** if B is finitely generated A-algebra and f is **finite** if B is finitely generated A-module. So finite type + integral = finite.

Property 4.2.2. If $A \subseteq B \subseteq C$ are rings. B is integral over A and C is integral over $B \iff C$ is integral over A.

Proof:

- ($\Leftarrow$) : Trivial.

- ($\Rightarrow$) : For all $x \in C$, since x integral over B, say

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0 \text{ with } b_i \in B$$

Let $B' = A[b_1, ..., b_n]$ which is f.g. A-module, since b_i are integral over A. Since x is integral over B', $B'[x]$ is f.g B'-module. Hence, $B'[x]$ is f.g. A-module containing $A[x]$ and $B'[x] \subseteq C$. By Proposition 4.2.1, x is integral over A.

□

Property 4.2.3. Let $A \subseteq B$ are rings and C is integral closure of A in B. Then C is integrally closed in B.

Proof: If $x \in B$ is integral over C. By Property 4.2.2, x is integral over $A \implies x \in C$. □

Proposition 4.2.2. Let $A \subseteq B$ are rings and B is integral over A.

- If $\mathfrak{b}$ is an ideal of B and $\mathfrak{a} = \mathfrak{b}^c$ (i.e. $\mathfrak{a} = \mathfrak{b} \cap A$). Then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.
  (Note: $A/\mathfrak{a} = A/(A \cap \mathfrak{b}) \simeq (A + \mathfrak{b})/\mathfrak{b} \subseteq B/\mathfrak{b}$)
- If S is multiplicative closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.

Proof:

- For all $x \in B$, say

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \text{ with } a_i \in A$$

Reduce the equation by mod $\mathfrak{b}$. Then $\overline{x}$ is integral over $(A + \mathfrak{b})/b \simeq A/\mathfrak{a}$.

- For all $x/s \in S^{-1}B$, then

$$\left(\frac{x}{s}\right)^{n-1} + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0$$

Then x/s is integral over $S^{-1}A$.

□

4.2.4 Going up theorem

Motivation: Given a ring extension $A \subseteq B$, we know if $\mathfrak{q} \in \operatorname{Spec} B$, then $\mathfrak{q} \cap A \in \operatorname{Spec} A$. So we have a map $\operatorname{Spec} B \to \operatorname{Spec} A$. Now, you may ask, will this map is surjuctive? The answer is no. But if we require for some property, then it may holds.

Proposition 4.2.3. Let $A \subseteq B$ be integral domains and B is integral over A. Then A is a field $\iff$ B is a field.

Proof:

- For all $0 \neq x \in B$, since x integral over A, choose the monic polynomial with smallest degree $n \geq 1$ such that exists $a_1, ..., a_n \in A$ s.t.

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

Then $a_n \neq 0$, otherwise by B is integral domain, $x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1} = 0$ contradict with the definition of n. So

$$x^{-1} = a_n^{-1}(x^{n-1} + \cdots + a_2 x + a_1) \in B$$

i.e. B is a field.

- For all $0 \neq x \in A \subseteq B$, $x^{-1} \in B$, say

$$x^{-m} + a_1 x^{-m+1} + \cdots + a_m = 0 \text{ for some } m \geq 1$$

Then $1 = x(-a_m x^{m-1} - \cdots - a_1) \implies x^{-1} = -(a_m x^{m-1} + \cdots + a_1) \in A$ i.e. A is a field.

□

Corollary 4.2.3. Let $A \subseteq B$ be rings and B is integral over A, $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{p} \in \operatorname{Max} A \iff \mathfrak{q} \in \operatorname{Max} B$.

Proof: By Proposition 4.2.2, $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$ and $A/\mathfrak{p}$, $B/\mathfrak{q}$ are all integral domain. By Proposition 4.2.3, $B/\mathfrak{q}$ is a field $\iff$ $A/\mathfrak{p}$ is a field. Hence, $\mathfrak{q} \in \operatorname{Max} B \iff \mathfrak{p} \in \operatorname{Max} A$. □

Corollary 4.2.4. Let $A \subseteq B$ and B is integral over A, let $\mathfrak{q}, \mathfrak{q}' \in \operatorname{Spec} B$ such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}^c = \mathfrak{q}'^c = \mathfrak{p}$. Then $\mathfrak{q} = \mathfrak{q}'$.

Proof: By Proposition 4.2.2, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. Let $\mathfrak{m} = \mathfrak{p}_\mathfrak{p}$ be the extension of $\mathfrak{p}$ in $A_\mathfrak{p}$ and $\mathfrak{n}, \mathfrak{n}'$ is the extension of $\mathfrak{q}, \mathfrak{q}'$ in $B_\mathfrak{p}$ $\implies$ $\mathfrak{n}^c = \mathfrak{n}'^c = \mathfrak{m}$ and $\mathfrak{n} \subseteq \mathfrak{n}'$. Since $\mathfrak{m}$ is maximal in $A_\mathfrak{p}$, by Corollary 4.2.3, $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal in $B_\mathfrak{p}$ $\implies$ $\mathfrak{n} = \mathfrak{n}'$ and thus $\mathfrak{q} = \mathfrak{q}'$ □

Theorem 4.2.2. Let $A \subseteq B$ be rings and B is integral over A, $\mathfrak{p} \in \operatorname{Spec} A$, then $\exists \mathfrak{q} \in \operatorname{Spec} B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$.

Proof: By Proposition 4.2.2, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ and the diagram commute.

$$\begin{array}{ccc} A & \hookrightarrow & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A_\mathfrak{p} & \hookrightarrow & B_\mathfrak{p} \end{array}$$

Let $\mathfrak{m}$ be the maximal ideal in $B_\mathfrak{p}$, then the contraction of $\mathfrak{m}$ in $A_\mathfrak{p}$ is also maximal. Notice that $(A_\mathfrak{p}, \mathfrak{p}_\mathfrak{p})$ is local ring, so $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$. Let $\mathfrak{q} = \beta^{-1}(\mathfrak{m})$, then $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{m} = \mathfrak{q}_\mathfrak{p}, \mathfrak{q} \cap (A - \mathfrak{p}) = \varnothing \implies \mathfrak{p}_\mathfrak{p} = \mathfrak{q}_\mathfrak{p} \cap A_\mathfrak{p} = (\mathfrak{q} \cap A)_\mathfrak{p}$. Since $\mathfrak{q} \cap A, \mathfrak{p} \in \operatorname{Spec} A$ and $(\mathfrak{q} \cap A) \cap (A - \mathfrak{p}), \mathfrak{p} \cap (A - \mathfrak{p}) = \varnothing \implies \mathfrak{p} = \mathfrak{q} \cap A$. □

Theorem 4.2.3. [Going-up theorem] Let $A \subseteq B$ be rings and B integral over A. Let $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ $(m < n)$ be a chain of primes ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$. Then we can extended $\{\mathfrak{q}_i\}_{i=1}^m$ to $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.

Proof: By induction, we only need to do the case for $m = 1$ and $n = 2$. By Proposition 4.2.2, $B/\mathfrak{q}_1$ is integral over $A/\mathfrak{p}_1$. By Theorem 4.2.2, $\exists \overline{q}_2 \in \operatorname{Spec} B/\mathfrak{q}_1$ s.t. $\overline{q}_2 \cap A/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. Lift back $\overline{q}_2$ to B, we get a prime ideal $\mathfrak{q}_2$ in B s.t. $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ and $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$. □

4.2.5 Integrally closed integral domains and going down theorem

First, we can do more in Property 4.2.3 :

Property 4.2.4. Let $A \subseteq B$ be rings and C is integral closure of A in B, S is multiplicative closed subset of A. Then $S^{-1}C$ is integral closure of $S^{-1}A$ in $S^{-1}B$.

Proof: Since C is integral over A, by Proposition 4.2.2, $S^{-1}C$ is integral over $S^{-1}A$. If $x/s \in S^{-1}B$ is integral over $S^{-1}A$, say

$$(x/s)^n + (a_1/s_1)(x/s)^{n-1} + \cdots + (a_n/s_n) = 0$$

for some $a_i \in A, s_i \in S$. Let $t = s_1 s_2 \cdots s_n \in S$ and rewrite as

$$\frac{tx^n + a_1' x^{n-1} + \cdots + a_n'}{ts^n} = 0 \text{ in } S^{-1}A$$

Then exists $u \in S$ such that $utx^n + ua_1' x^{n-1} + \cdots + ta_n' = 0$. Multiply $(ut)^{n-1}$, then it becomes an equation of integral dependence for utx over A i.e. $utx \in C$. Then $x/s = (utx)/(uts) \in S^{-1}C$. □

Definition 4.2.4. An integral domain is said to be **integrally closed** if it is integrally closed in its field of fractions.
(Note : Since A is integral domain, $A \setminus \{0\}$ is multiplicative closed set and thus field of fractions exists.)

Example 4.2.3. As we discuss in Example 4.2.1, every UFD is integrally closed. In particular, if k is a field. By Gauss lemma $k[x_1, ..., x_n]$ is UFD and thus is integrally closed.

Proposition 4.2.4. (local property) Let A be an integral domain. TFAE

(1) A is integrally closed

(2) $A_{\mathfrak{p}}$ is integrally closed $\forall \mathfrak{p} \in \operatorname{Spec} A$

(3) $A_{\mathfrak{m}}$ is integrally closed $\forall \mathfrak{m} \in \operatorname{Max} A$

Proof: Let C be the integral closure of A in field of fraction of A and $f : A \to C$ be inclusion. A is integrally closed $\iff$ f is surjective $\iff$ $f_{\mathfrak{p}}$ (resp. $f_{\mathfrak{m}}$) is surjective $\forall \mathfrak{p} \in \operatorname{Spec} A$ (resp. $\forall \mathfrak{m} \in \operatorname{Max} A$) $\iff$ $A_{\mathfrak{p}}$ (resp. $A_{\mathfrak{m}}$) is integrally closed $\forall \mathfrak{p} \in \operatorname{Spec} A$ (resp. $\forall \mathfrak{m} \in \operatorname{Max} A$). □

Now, we generalize the definition of integral.

Definition 4.2.5. Let $A \subseteq B$ be rings and let $\mathfrak{a}$ be an ideal of A. $x \in B$ is said to be **integral** over $\mathfrak{a}$ if

$$x^n + a_1 x^{n-1} + \cdots + a_n x^n = 0 \text{ for some } a_i \in \mathfrak{a}$$

The **integral closure** of $\mathfrak{a}$ in B is

$$\{b \in B : b \text{ is integral over } \mathfrak{a}\}$$

Lemma 4.2.2. Let C be the integral closure of A in B and let a^e denote the extension of $\mathfrak{a}$ in C. Then the integral closure of $\mathfrak{a}$ in B is the radical of $\mathfrak{a}^e$. Therefore, $\mathfrak{a}$ is closed under addition and multiplication.

Proof: If $x \in B$ is integral over $\mathfrak{a}$, say

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \text{ for some } a_i \in \mathfrak{a}$$

Then $x^n \in \mathfrak{a}^e$ i.e. $x \in \sqrt{\mathfrak{a}^e}$. Conversely, if $x \in \sqrt{\mathfrak{a}^e}$, say $x^n = \sum_{i=1}^{m} a_i x_i$ for some $n > 0$, $a_i \in \mathfrak{a}$ and $x_i \in C$. Since x_i are integral over A, by Corollary 4.2.1, $M = A[x_1, ..., x_m]$ is f.g. A-module. Then we have $x^n M \subseteq \mathfrak{a}M$. By Lemma 4.2.1 and $1 \in M$, x^n is integral over $\mathfrak{a}$ and thus x is integral over $\mathfrak{a}$. □

Proposition 4.2.5. Let $A \subseteq B$ be integral domains and A integrally closed. Let $x \in B$ is integral over an ideal $\mathfrak{a}$ of A. Then x is algebraic over the field of fraction K of A, and the minimal polynomial of x over K is form

$$t^n + a_1 t^{n-1} + \cdots + a_n$$

with $a_1, ..., a_n \in \sqrt{\mathfrak{a}}$ in K.

Proof: It's clear that x algebraic over K. Let monic polynomial $f(t) \in A[t]$ s.t. $f(x) = 0$ and $\overline{f}(t) \in K[x]$ with is f with coefficient in K. Let $x_1, ..., x_n$ be all roots of $m_{x,K}(t)$. Since $m_{x,K}(t) | \overline{f}(t)$, $\overline{f}(x_i) = 0$ for all i. Then exists $u_i \in A \setminus \{0\}$ such that $u_i f(x_i) = 0$. Since A is domain, $f(x_i) = 0$ i.e. x_i integral over $\mathfrak{a}$. Notice that the coefficient a_i of $m_{x,K}$ is symmetric polynomial of $x_1, ..., x_n$ which is also integral over A and $a_i \in K$. By A is integrally closed and Lemma 4.2.2 ($C = A$, $\mathfrak{a}^e = \mathfrak{a}$), $a_i \in \sqrt{\mathfrak{a}}$ w.r.t. K. □

Theorem 4.2.4. [Going-down theorem] Let $A \subseteq B$ be integral domains and A integrally closed, B integral over A. Let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be chain of primes ideals of A, and let $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ ($m < n$) be chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ ($1 \leq i \leq m$). Then the chain $\{\mathfrak{q}_i\}_{i=1}^m$ can be extended to a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.

Proof: By induction, we only need to prove the case for $m = 1$ and $n = 2$. Consider $A \to B \to B_{\mathfrak{q}_1}$, if we find a prime ideal $(\mathfrak{q}_2)_{\mathfrak{q}_1}$ in $B_{\mathfrak{q}_1}$ such that the contraction of $(\mathfrak{q}_2)_{\mathfrak{q}_1}$ is $\mathfrak{p}_2$. Then $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$ and $\mathfrak{q}_2$ is contraction of $(\mathfrak{q}_2)_{\mathfrak{q}_1}$ in B, $\mathfrak{q}_2 \cap A$ is contraction of $\mathfrak{q}_2$ in $A \implies \mathfrak{q}_2 \cap A = \mathfrak{p}_2$ and thus $\mathfrak{q}_2$ as required. By Theorem 4.2.1, it is suffices to show that $\mathfrak{p}_2^{ec} = \mathfrak{p}_2$ i.e. $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$.

- For all $y/s \in B_{\mathfrak{q}_1}\mathfrak{p}_2$ with $y \in B\mathfrak{p}_2$ and $s \in B \backslash \mathfrak{q}_1$. Since $y \in B\mathfrak{p}_2 = \mathfrak{p}_2^e \subseteq \sqrt{\mathfrak{p}_2^e}$ (where extension w.r.t. B) and by Lemma 4.2.2, y is integral over $\mathfrak{p}_2$. By Proposition 4.2.5, the minimal polynomial of y is form
$$t^n + u_1 t^{n-1} + \cdots + u_n$$
with $u_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$ (since $\mathfrak{p}_2$ is primes ideal).

- If $x \in B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$, write $x = y/s$ and thus $sx = y$ (by B is integral domain). Rewrite $s = yx^{-1}$ with $x^{-1} \in K$. Then the minimal polynomial of s over K is
$$t^n + \frac{u_1}{x} t^{n-1} + \cdots + \frac{u_n}{x^n} \tag{1}$$
Let $v_i = u_i/x^i$, then $x^i v_i = u_i \in \mathfrak{p}_2$. Since $s \in B$ is integral over A. By Proposition 4.2.5, $v_i \in \sqrt{A} = A$. Suppose that $x \notin \mathfrak{p}_2$, then $v_i \in \mathfrak{p}_2$ $\forall i = 1, ..., n$. By (1), $s^n \in B\mathfrak{p}_2 \subseteq B\mathfrak{p}_1 \subseteq \mathfrak{q}_1 \implies s \in \mathfrak{q}_1$ which is contradict to $s \in B \setminus \mathfrak{q}_1$. Hence, $x \in \mathfrak{p}_2$ and thus $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$ as required.

□

Proposition 4.2.6. Let A be an integrally closed domain and K is field of fraction. Let L/K : Galois, B is the integral closure of A in L. Then there exists a basis $v_1, ..., v_n$ of L over K such that $B \subseteq \sum_{j=1}^{n} Av_j$.

Proof:

- For all $v \in L$ which is algebraic over K, then it must satisfy the condition form
$$a_0 v^r + a_1 v^{r-1} + \cdots + a_n = 0 \text{ for some } a_i \in A$$
Multiply a_0^{r-1}, then $a_0 v$ is integral over A. Thus, given basis $\{v_1, ..., v_n\}$ for L over K, there exists a_i s.t. $u_i := a_i v_i \in B$

- Let T denote the trace form L to K. Since L/K is separable, the bilinear form $(x, y) \mapsto T(xy)$ is nondegenerate, and thus we have the dual basis $w_1, ..., w_n$ define by $T(w_i u_j) = \delta_{ij}$. Given $x \in B$, say $x = \sum_{j=1}^{n} x_j w_j$ for some $x_j \in K$. Then $xu_i \in B$ (since $u_i \in B$). By Proposition 4.2.5, $T(xu_i) \in A$ since the trace of element y is the coefficient of $x^{\deg m_{y,K}-1}$ in $m_{y,K}$and multiply (-1). Combine with
$$T(xu_i) = \sum_{j=1}^{n} T(x_j w_j u_i) = \sum_{j=1}^{n} x_j T(w_j u_i) = \sum_{j=1}^{n} x_j \delta_{ji} = x_i$$
we have $x_i \in A$. Hence, $B \subseteq \sum_{j=1}^{n} Av_j$.

□

4.2.6 Application

In this section, we will prove based on what we have learned above. Ultimately we will derive Hilbert's nullstellensatz theorem from these.

Krull dimension & Noether's normalization lemma

Definition 4.2.6. Let A be a ring. Define **Krull dimension** of A to be the supremum of the lengths of all chains of prime ideals in A and denoted by $\dim A$. We allow $\dim A = \infty$.

Example 4.2.4.

- If k is a field, them $\dim k = 0$.
- If A is a PID and not a field, then $\dim A = 1$.
  Since if $I \neq 0$, then $I \in \operatorname{Spec} A \iff I \in \operatorname{Max} A$.
- If A is Noetherian, then $\dim A[x] = \dim A + 1$.
  In particular, if k is a field, then $\dim k[x_1, ..., x_n] = n$.
- Notice that every proper ideal in nontrivial ring A will contain in a maximal ideal, so $\dim A = 0 \iff \operatorname{Max} A = \operatorname{Spec} A$. Hence, A : Artinian $\iff$ A : Noetherian $+ \dim A = 0$.

Property 4.2.5. If $A \subseteq B$ be rings and B is integral over A, then $\dim A = \dim B$.

Proof: By Corollary 4.2.4 and going-up theorem. □

Theorem 4.2.5 (Noether's normalization lemma)**.** Let k be a field and let $A \neq 0$ be a finitely generated k-algebra. Then there exists $y_1, ..., y_r \in A$ which are algebraically independent over k and such that A is integral over $k[y_1, ..., y_r]$.

Proof: We induct on the number of generators m of A over k. If $m = 0$ i.e. $A = k$, then done! If $m > 0$, let $x_1, ..., x_m$ be the generators of A over k. If $x_1, ..., x_m$ are algebraically independent over k. Since A is integral over $A = k[x_1, ..., x_m]$, and done! Otherwise, there exists $f \in k[t_1, ..., t_m]$ such that

$$f(x_1, ..., x_m) = 0$$

Let $r > \deg f$ and $z_1 = x_1$, $z_i = x_i - x_1^{r^{i-1}}$ for all $i = 2, ..., m$. Notice that $z_1, ..., z_m$ also generators of A over k and satisfies

$$f(x_1, z_2 + x_1^r, ..., z_m + x_1^{r^{m-1}}) = 0. \tag{1}$$

Since $r > \deg f$, there exists unique term $\prod_{i=1}^{m} t_i^{\alpha_i}$ in $f(t_1, ..., t_m)$ has maximum of $\sum_{i=1}^{m} \alpha_i r^{i-1}$ among all terms in f. So, after expand (1), it is the polynomial of x_1

with coefficient in $k[z_2, ..., z_m]$ and leading coefficient in k. Hence, x_1 is integral over $k[z_2, ..., z_m]$. Since $z_2, ..., z_m$ also integral over $k[z_2, ..., z_m]$, A is integral over $k[z_2, ..., z_m]$. By induction hypothesis, $k[z_2, ..., z_m]$ integral over $k[y_1, ..., y_r]$ for some $y_1, ..., y_r \in A$ are algebraically independent over k. Hence, A integral over $k[y_1, ..., y_r]$ as required. □

Corollary 4.2.5 (Zariski's lemma)**.** Let k be a field and K is finitely generated k-algebra. Suppose that K is a field, then K/k is finite extension.

Proof: By Noether's normalization lemma, K is integral over $k[y_1, ..., y_r]$ for some $y_1, ..., y_r \in B$ are algebraically independent over k. Since K is a field, $\dim K = 0$. By Property 4.2.5, $\dim k[y_1, ..., y_r] = 0$. Since $y_1, ..., y_r$ are algebraically independent, $\dim k[y_1, ..., y_r] = r \implies r = 0$. Hence, K is integral over k and thus K/k is finite extension (integral + finite-type = finite). □

Hilbert's nullstellensatz

Definition 4.2.7. Let k be an algebraically closed field, $A = k[t_1, ..., t_n]$ be the polynomial ring and S is a subset of A. Define **zero locus** of S be the set

$$Z(S) = \{x \in k^n : f(x) = 0 \ \forall f \in S\}$$

If a subset $X \subseteq k^n$ has the form $V = Z(S)$ for some S, then X is called **affine algebraic variety**. Define **ideal of variety** X by

$$I(X) = \{g(x) \in k[t_1, ..., t_n] : g(\mathbf{x}) = 0 \ \forall \mathbf{x} \in X\}$$

Theorem 4.2.6. [weak Hilbert's nullstellensatz] Let k be the algebraically closed field and $\mathfrak{a}$ be the ideal in the polynomial ring $A = k[x_1, ..., x_n]$. Then $\mathfrak{a} \neq A \iff Z(\mathfrak{a}) \neq \varnothing$.

Proof: Let $\mathfrak{a} \subsetneq k[x_1, ..., x_n]$ and $\mathfrak{a}$ contains in $\mathfrak{m} \in \operatorname{Max} A$. Then $A/\mathfrak{m}$ is a field with generator $\overline{x}_1, ..., \overline{x}_n$ as k-algebra. By Zariski's lemma, $A/\mathfrak{m}$ is finite extension of k i.e. $k \subseteq A/\mathfrak{m} \subseteq \overline{k} = k$. Hence, $A/\mathfrak{m} \simeq k$ as k-algebra. Consider $\varphi : A/\mathfrak{m} \xrightarrow{\sim} k$ and let $a_i = \varphi(\bar{t}_i)$, then for all $f \in \mathfrak{m}$ we have

$$f(a_1, ..., a_n) = f(\varphi(\bar{t}_1), ..., \varphi(\bar{t}_n)) = \varphi(f(\bar{t}_1, ..., \bar{t}_n)) = 0$$

i.e. $(a_1, ..., a_n) \in Z(\mathfrak{m}) \subseteq Z(\mathfrak{a})$. If $\mathfrak{a} = A$, then consider the root of x_1 and $x_1 + 1 \implies Z(\mathfrak{a}) = \varnothing$. □

Corollary 4.2.6. Let k be algebraic closed field, then every maximal ideal in $k[x_1, ..., x_n]$ is form $\mathfrak{m} = (x_1 - a_1, ..., x_n - a_n)$.

Proof: For all $a = (a_1, ..., a_n) \in F^n$, consider the evaluation map

$$\begin{array}{rccc} ev_a : & k[x_1, x_2, ..., x_n] & \longrightarrow & k \\ & f(x_1, ..., x_n) & \longmapsto & f(a) \end{array}$$

is k-algebra epimorphism and let $\mathfrak{m}_a = \ker ev_a$. Then $k[x_1, ..., x_n]/\mathfrak{m}_a \simeq k \implies \mathfrak{m}_a$ is maximal. Conversely, $\forall \mathfrak{m} \in \operatorname{Max} k[x_1, ..., x_n]$. Let $\varphi : A/\mathfrak{m} \to k$ and $a = (a_1, ..., a_n)$ defined in Theorem 4.2.6. Then $\forall f \in \mathfrak{m}_a$,

$$\varphi(\overline{f}(x_1, ..., x_n)) = f(a_1, ..., a_n) = 0 \implies \overline{f}(x_1, ..., x_n) = 0 \text{ in } k[x_1, ..., x_n]/\mathfrak{m}$$

Hence, $\mathfrak{m}_a \subseteq \mathfrak{m}$. Since $\mathfrak{m}_a$ is maximal and $\mathfrak{m} \neq k[x_1, ..., x_n]$, $\mathfrak{m} = \mathfrak{m}_a$ as required. □

Lemma 4.2.3. Let k be a field, B be a finitely generated k-algebra and $\mathfrak{b}$ be an ideal in B. Then

$$\sqrt{\mathfrak{b}} = \bigcap_{\mathfrak{b} \subseteq \mathfrak{m} \in \operatorname{Max} B} \mathfrak{m}$$

Proof: Notice that

$$\left(\bigcap_{\mathfrak{b} \subseteq \mathfrak{m} \in \operatorname{Max} B} \mathfrak{m} \right) \Big/ \mathfrak{b} = \bigcap_{\mathfrak{m} \subseteq \mathfrak{m} \in \operatorname{Max} B} \mathfrak{m}/\mathfrak{b} = \bigcap_{\mathfrak{m}/\mathfrak{b} \in \operatorname{Max} B/\mathfrak{b}} \mathfrak{m}/\mathfrak{b}$$

and

$$\left(\bigcap_{\mathfrak{b} \subseteq \mathfrak{m} \in \operatorname{Spec} B} \mathfrak{m} \right) \Big/ \mathfrak{b} = \bigcap_{\mathfrak{m} \subseteq \mathfrak{m} \in \operatorname{Spec} B} \mathfrak{m}/\mathfrak{b} = \bigcap_{\mathfrak{m}/\mathfrak{b} \in \operatorname{Spec} B/\mathfrak{b}} \mathfrak{m}/\mathfrak{b}$$

So we only need to proof the cases for $\mathfrak{b} = 0$ i.e. nilradical of B equal to Jacobson radical of B. Let $f \in B$ s.t. $f \notin \sqrt{0}$. Let $S = \{f^n : n \in \mathbb{Z}_{\geq 0}\}$ which is multiplicative closed set in B and $S^{-1}B$ is a non-trivial k-algebra, hence it has a maximal ideal $\mathfrak{m}$. Consider $\phi : B \to S^{-1}B$. Since B is f.g k-algebra, the field $S^{-1}B/\mathfrak{m}$ is also f.g. k-algebra. By Zariski's lemma, $S^{-1}B/\mathfrak{m}$ is a finite extension over k and notice that $k \subseteq B/\phi^{-1}(\mathfrak{m}) \subseteq S^{-1}B/\mathfrak{m} \implies B/\phi^{-1}(\mathfrak{m})$ is integral over k. Since $\phi^{-1}(\mathfrak{m}) \in \operatorname{Spec} B \implies B/\phi^{-1}(\mathfrak{m})$ is integral domain. By Proposition 4.2.3, k is a field $\implies B/\phi^{-1}(\mathfrak{m})$ is a also a field i.e. $\phi^{-1}(\mathfrak{m}) \in \operatorname{Max} B$. Notice that if $f \in \phi^{-1}(\mathfrak{m})$, then $f/1 \in \mathfrak{m}$ and thus $1 = 1/f \cdot f/1 \in \mathfrak{m}$ ($\rightarrow\!\leftarrow$). Hence, $f \notin \phi^{-1}(\mathfrak{m}) \in \operatorname{Max} B$ i.e. $f \notin J_B$. Which means $\mathfrak{N}_B = J_B$. □

Theorem 4.2.7 (Hilbert's nullstellensatz)**.** Let k be an algebraically closed field, A be the polynomial ring $A = k[t_1, ..., t_n]$ and $\mathfrak{a}$ be an ideal of A. Then

$$I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$$

Proof: We continue to use the notation in above. Observe that if $a \in Z(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{m}_a$ and $f \in I(V) \iff f(a) = 0 \ \forall a \in V \iff f \in \bigcap_{a \in V} \mathfrak{m}_a$. Hence,

$$I(Z(\mathfrak{a})) = \bigcap_{a \in Z\mathfrak{a}} \mathfrak{m}_a = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m}_a} \mathfrak{m}_a$$

By Corollary 4.2.6, every maximal ideal in A is form $\mathfrak{m}_a$ for some $a \in k^n$. Hence,

$$\bigcap_{\mathfrak{a} \subseteq \mathfrak{m}_a} \mathfrak{m}_a = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m}} \mathfrak{m} = \sqrt{\mathfrak{a}} \qquad \text{(By Lemma 4.2.3)}$$

□

Extend the ring homomorphism when integral

Recall that we learn in field theory. Let $\sigma : F \to L$ is homomorphism and $F(\alpha)/F$ is algebraic. Then $\exists \tau : F(\alpha) \to L$ s.t. $\sigma|_F = f \iff m^{\sigma}_{\alpha,F}(\beta) = 0$ for some $\beta \in L$. Then we have similar property for integral extension.

Theorem 4.2.8. Let A be a subring of a ring B such that B is integral over A, and let $f : A \mapsto \Omega$ be a homomorphism of A into an algebraically closed field Ω. Show that f can be extended to a homomorphism of B into Ω.

Proof:

- Notice that Ω is integral domain, so 0 is prime ideal and thus $\ker f = f^{-1}(0)$ is also prime ideal in A. By Theorem 4.2.2, there exists $\mathfrak{q} \in \operatorname{Spec} B$ s.t. $\mathfrak{q} \cap A = \ker f$. By Proposition 4.2.2, $B/\mathfrak{q}$ is integral over $A/\ker f$. By 1st isomorphism, $\exists \overline{f} : A/\ker f \hookrightarrow \Omega$. So it is suffices to show the cases for $A \subseteq B$ be integral domain and f is $1-1$.

- Define $\mathcal{S} = \{(C, \sigma) : A \subseteq C \subseteq B, \sigma : C \hookrightarrow \Omega \text{ and } \sigma|_A = f\}$ and partial order $(C, \sigma) \leq (C', \sigma') \iff C \subseteq C'$ and $\sigma'|_C = \sigma$. By the routine argument of Zorn's lemma, $\exists$ a maximal element (C, σ) in $\mathcal{S}$. We claim that $C = B$ and thus $\exists \sigma : B \to \Omega$ and $\sigma|_A = f$.

- If not, $\exists b \in B \setminus C$. Notice that b is integral over C and C is also integral domain. Notice that we can find at least one polynomial $m(x)$ with least degree in $C[x]$ s.t. $m(b) = 0$, say $\deg m = d$ and m_0 be the leading coefficient. We claim that for all $g(x) \in C[x]$ with $g(b) = 0$, there exists $0 \neq c \in C$ and $h(x) \in C[x]$ s.t.

$$cg(x) = h(x)m(x)$$

  We induct on $\deg g = n$. If $n = d$, let the leading coefficient of $g(x)$ is g_0, then

$$m_0 g(b) - g_0 m(b) = 0 \text{ and } \deg(m_0 g(x) - g_0 m(x)) < \deg m(x)$$

  By definition of $m(x)$, $m_0 g(x) - g_0 m(x) = 0$ i.e. $m_0 g(x) = g_0 m(x)$. For $n > d$, let the leading coefficient of $g(x)$ is g_0, then

$$m_0 g(b) - g_0 b^{n-d} m(b) = 0 \text{ and } d' := \deg(m_0 g(x) - g_0 x^{n-d} m(x)) < n$$

  Case1. $d' < d$: Then $m_0 g(x) = g_0 x^{n-d} m(x)$.

  Case2. $d' \geq d$: By induction hypothesis, $\exists 0 \neq c \in C, h(x) \in C[x]$ s.t.

$$c(m_0 g(x) - g_0 x^{n-d} m(x)) = h(x)m(x) \implies cm_0 g(x) = (h(x) + cg_0 x^{n-d})m(x)$$

  Since C is integral domain, $cm_0 \neq 0$. By induction, our claim holds.

- Since $\Omega = \overline{\Omega}$, let β be the arbitrary root of $m^{\sigma}(x) = 0$. Now, define $\tau : C[b] \to \Omega$ by $f(b) \mapsto f^{\sigma}(\beta)$. Then $\tau(c) = \sigma(c)$ for all $c \in C$.

  - well-defined : If $g(b) = 0$. By claim, $\exists 0 \neq c \in C$ and $h(x) \in C[x]$ s.t. $cg(x) = h(x)m(x)$ and thus $\tau(c)g^{\sigma}(\beta) = h^{\sigma}(\beta)m^{\sigma}(\beta) = 0$. Since $\tau(c) = \sigma(c) \neq 0$ by σ is injective, $g^{\sigma}(\beta) = 0$

- τ is $1-1$: Notice that $\sigma(C)$ is also integral domain. Let $g(x) \in \sigma(C)[x]$ (say $g(x) = p^\sigma(x)$) has least degree s.t. $g(\beta) = 0$. By same argument, $\sigma(c)m^\sigma(x) = h^\sigma(x)g(x)$ for some $0 \neq c \in C$, $h(x) \in C[x]$. Then $cm(x) = h(x)p(x)$ by σ is $1-1 \implies h(b)p(b) = cm(b) = 0 \implies p(b) = 0$ or $h(b) = 0$.
  - If $p(b) = 0$, combine $\deg p \leq \deg m \implies m_0 p(x) = p_0 m(x) \implies p(b) = 0$.
  - If $h(b) = 0 \implies \deg h = \deg m \implies p(x) = c'$ for some $c' \in C$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$).

  Now, $q(b) \in \ker \tau \iff q^\sigma(\beta) = 0 \iff f(c)q^\sigma = r^\sigma(x)g(x)$ for some $c \neq 0$, $r(x) \in C[x] \implies cq(x) = r(x)p(x) \implies cq(b) = r(b)p(b) = 0 \implies q(b) = 0$. Hence, τ is $1-1$.

Hence, $(C, \sigma) \lneq (C[b], \tau) \in \mathcal{S}$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$). Which means $C = B$.

□

4.3 Dedekind domain

4.3.1 Valuation rings

Definition 4.3.1. A **valuation** of a field K is a map v from $K^\times$ into an abelian totally order group Γ, such that the axioms below are satisfied

- $v(ab) = v(a) + v(b)$
- $v(a+b) \geq \min(v(a), v(b))$, where the equality holds when $v(a) \neq v(b)$.

For notational simplicity, we sometimes say $v(0) = \infty$.

Example 4.3.1. Given a prime number p, then

$$\begin{array}{rccc} v: & \mathbb{Q}^\times & \longrightarrow & \mathbb{Z} \\ & \frac{a}{b} & \longmapsto & v_p(a) - v_p(b) \end{array}$$

is a valuation of $\mathbb{Q}$, where $v_p(a) \in \mathbb{Z}_{\geq 0}$ s.t. $p^{v_p(a)} | a$ and $p^{v_p(a)+1} \nmid a$

Definition 4.3.2. Given a valuation $v : K^\times \longrightarrow \Gamma$

- $\{a \in K | v(a) \geq 0\}$ is a subring of K which is called **valuation ring** of the valuation v.
- $v(K^\times)$ is a subgroup of Γ, which is called the **valuation group** of the valuation v.

Property 4.3.1. Let $v : K^\times \to \Gamma$ be a valuation with valuation ring A.

- $v(1) = 0$.
- $\forall x \in K$, either x or x^{-1} belongs to A.
  $v(x) + v(x^{-1}) = v(1) = 0 \implies x$ or x^{-1} belongs to A.
- $\forall x \in A,\ v(x) = 0 \iff x \in A^\times$.
- $K \simeq \operatorname{Frac} A$.
  Clearly. $\operatorname{Frac} A \hookrightarrow K$. From (b), $\forall x \in K$, $x \in \operatorname{Frac} A$.
- $\mathfrak{m} := \{a \in A | v(a) > 0\}$ is the unique maximal ideal of A.
  It's clear that $\mathfrak{m}$ is a ideal and $A \setminus \mathfrak{m}$ are all units in A.
- $(A, \mathfrak{m})$ is a local ring.
- A is integrally closed.
  If $x \in \operatorname{Frac} A \simeq K$ is integral over A, say $x^n + a_1 x^{n-1} + \cdots + a_n$. If $x \notin A$, then $x^{-1} \in A$ and
  $$x = -(a_1 + a_2 x^{-1} + \cdots + a_n x^{n-1}) \in A \ (\rightarrow\!\leftarrow)$$

Proposition 4.3.1. Let A be a integral domain with $K = \operatorname{Frac} A$. TFAE

(a) A is the valuation ring for some valuation of K.

(b) For all $x \in K$, either x or x^{-1} belongs to A.

(c) The principal ideals of A are totally ordered by inclusion.

(d) The ideals of A are totally ordered by inclusion.

(e) A is local and all finitely generated ideals of A are principal (A is a local **Bézout domain**)

Proof:

- $(a) \Rightarrow (b)$: OK!
- $(b) \Rightarrow (a)$: First, we claim A is local ring (we claim that all non-unit form a ideal $\mathfrak{m}$ of A). If $a \in A$ and $x \in \mathfrak{m}$, then $ax \in \mathfrak{m}$. If $x, y \in \mathfrak{m}$, one of $xy^{-1}, yx^{-1} \in A$, say $xy^{-1} \in A$ and $x + y = (xy^{-1} + 1)y \in \mathfrak{m}$.

  Now, let $\Gamma = K^\times \setminus A^\times$. This can given a total order via divisibility by element in A (by assumption). Then the projection $K^\times \to \Gamma$ is a valuation with valuation ring A since

  - group homo. : OK
  - If $v(a) \geq v(b)$, $ab^{-1} \in A$. Then $(a+b)b^{-1} \in A$ i.e. $v(a+b) \geq v(b)$. If $v(a) \neq v(b)$, then $a = xb$ with $x \notin A^\times \rightsquigarrow 1 + x$ is unit and thus $v(a+b) = v((1+x)b) = v(b)$.
  - If $v(a) \geq 0 = v(1)$, then $a \cdot 1^{-1} \in A$. Hence, A is the valuation ring via this valuation.
- $(b) \Rightarrow (c)$: Given $\langle x \rangle, \langle y \rangle \subseteq A$. Either $xy^{-1} \in A$ or $yx^{-1} \in A$ which is corresponding to $\langle x \rangle \subseteq \langle y \rangle$ or $\langle y \rangle \subseteq \langle x \rangle$.
- $(c) \Rightarrow (b)$: Given $x/y \in K$, either $\langle x \rangle \subseteq \langle y \rangle$ ($\iff xy^{-1} \in A$) or $\langle y \rangle \subseteq \langle x \rangle$ ($\iff yx^{-1} \in A$).
- $(c) \Rightarrow (d)$: Given $I, J \subseteq A$. If $x \in I \setminus J$ and $y \in J \setminus I$. WLOG $\langle x \rangle \subseteq \langle y \rangle$, then $\langle x \rangle \subseteq \langle y \rangle \subseteq J$ ($\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$).
- $(d) \Rightarrow (c)$: OK!
- $(e) \Rightarrow (c)$: Say $\langle x, y \rangle = \langle g \rangle$, then $x = ag, y = bg \rightsquigarrow \langle a, b \rangle = A$. Then one of $a, b \in A^\times$ since A is local ring. Hence, one of $\langle x \rangle, \langle y \rangle$ is $\langle g \rangle$ will contain another one.
- $(a), (c) \Rightarrow (e)$: Since A is valuation ring for some valuation of $K \rightsquigarrow A$ is local. Since $\langle x \rangle \subseteq \langle y \rangle$ or $\langle y \rangle \subseteq \langle x \rangle \implies \langle x, y \rangle = \langle x \rangle$ or $\langle y \rangle$ and by induction.

□

Definition 4.3.3. A **discrate valuation** of a field K is a valuation $K^\times \longrightarrow \mathbb{Z}$. A **discrete valuation ring (DVR)** is the valuation ring of some discrete valuation.

Proposition 4.3.2. Let A be a domain that is not a field. TFAE

(a) A is a DVR.

(b) A is a local ED.

(c) A is a local PID.

(d) A is a PID with a unique non-zero prime ideal.

(e) A is a Noetherian valuation ring.

(f) A is a UFD with a unique irreducible element.

Proof:

- $(a) \Rightarrow (b)$: A is local. Define norm by the valuation and $\|0\| = -\infty$. If $v(x) \geq v(y)$, then $v(xy^{-1}) \geq 0 \rightsquigarrow xy^{-1} \in A$. Then $x = (xy^{-1})y + 0$.
- $(b) \Rightarrow (c)$: OK
- $(c) \Rightarrow (d)$: Since non-zero prime ideal is non-zero maximal ideal in PID and A is local.
- $(d) \Rightarrow (e)$: PID $\implies$ Noetherian and A is local Bézout domain.
- $(e) \Rightarrow (f)$: Bézout domain is GCD domain. Noetherian + GCD $\implies$ UFD. Valuation ring has at most one irreducible element.
- $(f) \Rightarrow (a)$: Let p be the unique irreducible element. $\forall x/y \in \operatorname{Frac} A$, say $x = ap^n, y = bp^m$ with $a, b \in A^\times$. Define $v(x/y) = n - m \in \mathbb{Z}$ which is a discrete valuation.

□

Proposition 4.3.3. Let $(A, \mathfrak{m})$ be a Noetherian local domain that is not a field. TFAE

(a) A is a DVR

(b) A is integrally closed of dimension one.

(c) $\mathfrak{m}$ is principal.

(d) $\dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$ i.e. A is regular local ring of dim 1.

(e) every nonzero ideal of A is the power of $\mathfrak{m}$.

Proof:

- $(a) \Rightarrow (b)$: valuation $\implies$ integrally closed. DVR and not field $\implies$ local PID and not field $\implies \dim A = 1$.

- $(b) \Rightarrow (c)$: Let $a \in \mathfrak{m}$, then $\sqrt{\langle a \rangle}$ is a prime ideal $\rightsquigarrow \sqrt{\langle a \rangle} = \mathfrak{m}$. By Noetherian, $\mathfrak{m}^n \subseteq \langle a \rangle$ for some n and we may assume n be the smallest number satisfy. If $\mathfrak{m} \subseteq \langle a \rangle$ then done! Otherwise, take $b \in \mathfrak{m}^{n-1} \setminus \langle a \rangle$, then $x = b/a \notin A$ which is not integral over A. This implies $x\mathfrak{m} \nsubseteq \mathfrak{m}$, otherwise there exists a matrix M present $f : \mathfrak{m} \to \mathfrak{m}$ by $m \mapsto xm$ (by Noetherian). In particular, $\det(xI - M)$ is an integral relation of x ($\multimap$). Since $x\mathfrak{m} \subseteq A$ ($b\mathfrak{m} \subseteq m^n \subseteq \langle a \rangle$), $x\mathfrak{m} = A \rightsquigarrow \mathfrak{m} = \langle x^{-1} \rangle$ is principal.
- $(c) \Rightarrow (d)$: Let $\mathfrak{m} = \langle x \rangle$. Then $\mathfrak{m}/\mathfrak{m}^2$ is generated by $x + \mathfrak{m}^2$ over $A/\mathfrak{m} \rightsquigarrow \dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \leq 1$. If $\mathfrak{m} = \mathfrak{m}^2$, then by Nakayama's lemma (by Noetherian, $\mathfrak{m}$: f.g.), $\mathfrak{m} = 0 \rightsquigarrow A$ is a field ($\multimap$).
- $(d) \Rightarrow (c)$: If $\mathfrak{m}/\mathfrak{m}^2 = xA/\mathfrak{m}$, then $m = \langle x \rangle + \mathfrak{m}^2$. By Nakayama's lemma, $\mathfrak{m} = \langle x \rangle$.
- $(c) \Rightarrow (e)$: Let $\mathfrak{m} = \langle x \rangle$. By Noetherian, every $y \in A \setminus (A^\times \cup 0)$ is a product of irreducible elements, and thus it associated to a power of x. In particular, any ideal $I \subseteq A$ is generated by x^k, where k is the least integer such that $x^k \in I$.
- $(e) \Rightarrow (a)$: The ideals of A are totally order by inclusion i.e. A is valuation ring. Also, Noetherian valuation ring $\implies$ DVR.

□

4.3.2 Fractional ideals and invertible ideals

In this subsection, A denotes an integral domain with $K = \operatorname{Frac} A$ be it's fractional field.

Definition 4.3.4. A **fractional ideal** is an A-submodule of K such that there exists a nonzero $x \in A$ satisfying $xI \subseteq A$.

Remark 4.3.1. Do not get confused about the terminology. Fractions ideals are in general not regular "ideals" that we usually talk about. To clarify things up, we usually call the regular ideals

Definition 4.3.5. Let I, J be the fractional ideal. Define

$$IJ = \{\sum_{\text{finite}} x_i y_i | x_i \in I, y_i \in J\}$$

which is still a fractional ideal. A nonzero fractional ideal I is **invertible** if there exists another fractional ideal J such that $IJ = A$. Note that since product of ideals is associative, the inverse is unique, which will be denoted by I^{-1}.

Proposition 4.3.4. If I is invertible, then $I^{-1} = \{x \in K | xI \subseteq A\}$.

Proof: Let $J = \{x \in K | xI \subseteq A\}$. $\forall x \in I$, $xJ \subseteq A \implies J$ is fractional ideal. Since $A = II^{-1} \subseteq IJ \subseteq A$. By uniqueness of the inverse, $I^{-1} = J$. □

Proposition 4.3.5. Invertible ideals are finitely generated.

Proof: Since $II^{-1} = A$, $1 = \sum_{\text{finite}} a_i b_i$ for some $a_i \in I, b_i \in I^{-1}$. Then $\forall x \in I$, we have $x = \sum a_i(xb_i)$ with $xb_i \in A \ \forall i$ i.e. a_i's generated I. □

Proposition 4.3.6. A nonzero fractional ideal is invertible $\iff$ it is projective.

Proof:

- ($\Rightarrow$) : Let $1 = \sum_{i=1}^{n} a_i b_i$ for some $a_i \in I$, $b_i \in I^{-1}$. Consider the A-module maps

$$f: \begin{array}{ccc} A^n & \longrightarrow & I \\ e_i & \longmapsto & a_i \end{array} \text{ and } g: \begin{array}{ccc} I & \longrightarrow & A^n \\ x & \longmapsto & \sum (b_i x) e_i \end{array}$$

  Then $f \circ g$ is the identity, and thus $0 \to \ker f \to A^n \to I \to 0$ is split and thus I is projective.

- Suppose $I \oplus J = A^{\oplus S}$. Let $g : A^{\oplus S} \longrightarrow I$ be the projection, and $f_i : I \to A^{\oplus S} \longrightarrow A$ denote the projection into the i-th coordinate. Note that f_i is A-module homomorphism, so $bf_i(a/b) = f_i(a)$ and $a' f_i(a) = f_i(a'a) = f_i(aa') = af_i(a')$, then $f_i(a)/a = f_i(a')/a'$ in K, so $f_i(x) = k_i x$ for some $k_i \in K$. Notice that $g \circ \left(\sum_{i}^{n} f_i(x) e_i \right) = x \ \forall x \in I$. Then

$$x = \sum_{i \in S} f_i(x) g(e_i) = \left(\sum k_i g(e_i) \right) x \implies \sum_{i \in S} k_i g(e_i) = 1$$

  Hence, it only finitely many of k_i are nonzero. Say $\sum_{i \in S'} k_i g(e_i) = 1$. This implies I is invertible and $\langle k_i \rangle$ is its inverse.

□

Proposition 4.3.7. In a integral domain, if an (integral) ideal is a product of invertible prime ideals, then the product is unique.

Proof: Suppose $\prod p_i = \prod q_i$. WLOG let p_1 be the biggest in the sense that $p_1 \subseteq p_i \implies p_i = p_1$. By prime avoidance lemma, $p_1 \subseteq q_i \subseteq p_j$ for some i, j. By the choice of p_1, $p_1 = q_i$. Multiplying p_1^{-1} on both sides and we can then proceed by induction. □

4.3.3 Dedekind domain

Proposition 4.3.8. Let A be a integral domain that is not a field. TFAE

(a) A is Noetherian, integrally closed and of dimension one.

(b) A is Noetherian, and every $A_{\mathfrak{p}}$ is a DVR for all prime ideals $\mathfrak{p} \neq 0$.

(c) A is Noetherian, and every $A_{\mathfrak{m}}$ is DVR for all maximal ideals $\mathfrak{m}$.

(d) A is Noetherian, and every and every non-zero primary ideal in A is a power of a maximal ideal.

(Then every prime ideal is maximal ideal.)

(e) Every non-zero ideal can be uniquely written as a finite product of prime ideals.

(f) Every non-zero ideal can be uniquely written as a finite product of maximal ideals.

(g) Every non-zero fractional ideal is invertible.

(h) For any two ideals $I \subseteq J \subseteq A$, there exists an integral ideal H such that $I = JH$. (A is called **containment-division ring (CDR)**)

(i) A is integrally closed, and A/I is Artinian for all non-zero ideal I.

(j) A/I is a principal ideal ring for all non-zero ideal I.

Proof:

- (a) $\Rightarrow$ (b) : Since A_p is a Noetherian local domain and A_p is integral closed of dimension one. By Proposition 4.3.3, $A_{\mathfrak{p}}$ is DVR $\forall 0 \neq \mathfrak{p} \in \operatorname{Spec} A$
- (b) $\Rightarrow$ (c) : OK
- (c) $\Rightarrow$ (d) : Let $0 \neq I$ be p-primary. Let $\mathfrak{m}$ be a maximal ideal containing I, then $I_{\mathfrak{m}}$ is p-primary in $A_{\mathfrak{m}} \rightsquigarrow p = \mathfrak{m}$. By Proposition 4.3.3, $I_{\mathfrak{m}} = \mathfrak{m}_{\mathfrak{m}} \rightsquigarrow I = \mathfrak{m}^n$.
- (d) $\Rightarrow$ (e) By primary decomposition, $I = \bigcap \mathfrak{m}^n$. Then $\sqrt{\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j}} = \sqrt{\sqrt{\mathfrak{m}_i^{n_i}} + \sqrt{\mathfrak{m}_j^{n_j}}} = \sqrt{\mathfrak{m}_i + \mathfrak{m}_j} = A$. Hence, $\mathfrak{m}_i^{n_i}$, $\mathfrak{m}_j^{n_j}$ coprime $\rightsquigarrow I = \prod \mathfrak{m}^n$. Uniqueness by Proposition 4.3.7
- (e) $\Rightarrow$ (f) : We claim that every non zero prime ideal is maximal and invertible :

  subproof : If $\mathfrak{p}$ is invertible and $x \notin A \setminus \mathfrak{p}$. By assumption, say $\mathfrak{p} + \langle x \rangle = p_1 \cdots p_n$, $\mathfrak{p} + \langle x^2 \rangle = q_1 \cdots q_m$. Then

  $$\overline{p_1}^2 \cdots \overline{p_n}^2 = \langle \overline{x}^2 \rangle = \overline{q_1} \cdots \overline{q_m} \text{ in } A/\mathfrak{p} : \text{integral domain}$$

  Notice that $\overline{p_1}^{-1} = \langle \overline{x}^{-2} \rangle \overline{p_1 p_2}^2 \cdots \overline{p_n}^2$ i.e. $\overline{p_1}$ is invertible. By Proposition 4.3.7, they are the same prime ideals up to permutation, and thus

  $$\mathfrak{p} \subseteq \langle x^2 \rangle + \mathfrak{p} = q_1 \cdots q_m = (p_1 \cdots p_n)^2 = (\langle x \rangle + \mathfrak{p})^2 \subseteq \langle x \rangle + \mathfrak{p}^2$$

  Notice that if $ax + bp'p'' \in \mathfrak{p}$, then $ax \in \mathfrak{p} \rightsquigarrow a \in \mathfrak{m}$. Thus, $\mathfrak{p} \subseteq x\mathfrak{p} + \mathfrak{p}^2 \subseteq \mathfrak{p}$. Multiplying $\mathfrak{p}^{-1}$ gives $A = \langle x \rangle + \mathfrak{p}$. Thus, $\mathfrak{p}$ is maximal. It remains to show that every nonzero prime $\mathfrak{p}$ is invertible. Let $0 \neq x \in \mathfrak{p}$, then $\mathfrak{p} \supseteq \langle x \rangle = p_1 \cdots p_n$. By prime avoidance lemma, $p_i \subseteq \mathfrak{p}$. Since p_i is invertible with the inverse $x^{-1} p_1 \cdots p_{i-1} p_i \cdots p_n$, it is maximal and hence $\mathfrak{p} = p_i$ is invertible.

  (f) $\Rightarrow$ (e) : OK

- $(e) \Rightarrow (g)$: $\exists x \in A$ s.t. $xI \subseteq A$. By assumption, $xI = p_1 \cdot p_n \rightsquigarrow I^{-1} = x^{-1}p_2^{-1} \cdot p_n^{-1}$ (By $(e) \Rightarrow (f)$).
- $(g) \Rightarrow (h)$: Assume $I, J \neq 0$. Let $H = IJ^{-1} \subseteq II^{-1} = A$ (by Proposition 4.3.4)
- $(h) \Rightarrow (g)$: Let $0 \neq I$ be fractional ideal and $x \in A$ s.t. $xI \subseteq I$. Let $y \in xI$, then $\langle x \rangle \subseteq xI$. By assumption, $\exists J$ s.t. $xIJ = \langle y \rangle$, then $I^{-1} = y^{-1}xJ$.
- $(g), (h) \Rightarrow (a)$: $\forall I$: fractional is invertible and thus is f.g. $\implies A$ is Noetherian. Let $x = a/b \in K$ s.t. $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Then $I = \langle 1, x, ..., x^{n-1} \rangle$ is fractional $\implies I$ is invertible. Also, $I^2 = I \rightsquigarrow I = I^{-1}(I^2) = I^{-1}I = A \implies x \in A$. Let be the set of ideals that cannot be written as a finite product of maximal ideals. Since A is Noetherian, if $\sum \neq \varnothing$, then it has a maximal element I, say $I \subsetneq \mathfrak{m}$, then $\exists J$ s.t. $I = \mathfrak{m}J \subseteq J$. If $I = J$, by Nakayama's lemma, $I = 0$ $(\rightarrow\!\!\!\!\!\!\!\!\leftarrow)$. Hence, $J \supsetneq I$ and $J \in \sum$ $(\rightarrow\!\!\!\!\!\!\!\!\leftarrow)$. Then every nonzero prime ideal is maximal ideal and thus $\dim A = 1$.
- $(a) \iff (i)$: A Noetherian and $\dim A = 1 \iff \forall I \neq 0$ A/I is Noetherian and $\dim A/I = 0 \iff A/I$ is Artinian.
- $(f), (g) \Rightarrow (j)$: If $I \subseteq J$, then $IJ^{-1} \subseteq II^{-1} = A \rightsquigarrow IJ^{-1} \rightsquigarrow IJ^{-1}$ is ideal of A. By assumption, $IJ^{-1} = \prod p_i^{e_i}$. Let $a_i \in J \prod_{j \neq i} p_j \setminus J \prod p_j$, then $a := \sum a_i \notin p_i$. Since p_i are all maximal ideal containing IJ^{-1} and $a \notin p_i$ $\forall i \rightsquigarrow aJ^{-1} + IJ^{-1} = A \rightsquigarrow \langle a \rangle + I = J$. Hence, A/I is principal ideal ring.
- $(j) \Rightarrow (c)$: Given I be the ideal of A and $x \in I$, then $I/\langle x \rangle$ is principal, say $I/\langle x \rangle = \langle \bar{b} \rangle$, then I is generated by $x, b \rightsquigarrow A$ is Noetherian. Since localizing preserves this property i.e. every ideal in $A_{\mathfrak{p}}/I_{\mathfrak{p}}$ is principal. Then $\mathfrak{m}_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}^2$ is principal in $A_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}^2$. Then $\mathfrak{m}_{\mathfrak{m}} = \langle a \rangle + \mathfrak{m}_{\mathfrak{m}}\mathfrak{m}_m$ and by Nakayama's lemma, $\mathfrak{m}_{\mathfrak{m}} = \langle a \rangle$ is principal. By Proposition 4.3.3, $A_{\mathfrak{m}}$ is DVR.

□

Remark 4.3.2. The containment-division property and the unique-factorization property still holds for factorial ideals if inverse powers of prime ideals are allowed.

Definition 4.3.6. Any domain that satisfies one of the conditions above is called a **dedekind domain**.

Remark 4.3.3. Note that a local ring is a dedekind domain $\iff$ it is a DVR. Thus, any condition above together with localness implies that A is a DVR.

Proposition 4.3.9. A domain is a PID $\iff$ it is a dedekind UFD.

Proof:

- $(\Rightarrow)$: Since $A_{\mathfrak{m}}$ are all PID and thus is DVR. PID $\implies$ Noetherian. Hence, A is dedekind domain. Also, PID $\implies$ UFD.

- ($\Leftarrow$) : Since every nonzero ideal is product of maximal ideal, so we only need to show that maximal ideal is principal. Let $x \in \mathfrak{m} \in \operatorname{Max} A$, say $x = \prod p_i^{e_i}$, then $\langle x \rangle = \prod \langle p_i \rangle^{e_i} \subseteq \mathfrak{m}$. By prime avoidance lemma, $\langle p_i \rangle \subseteq \mathfrak{m}$. Also, every nonzero prime ideal is maximal, then $\mathfrak{m} = \langle p_i \rangle$ is principal.

□

Definition 4.3.7. The nonzero fractional ideals of a dedekind domain A form under ideal products. It is called the **group of ideals** of A and denoted by $\mathcal{J}_A$. Let $\mathcal{P}_A := \{\langle x \rangle_A : x \in K\}$ is a subgroup of $\mathcal{J}_A$. The quotient group $\mathcal{J}_A/\mathcal{P}_A$ is called the **ideal class group** of A.

Proposition 4.3.10. Let A be a dedekind domain and $K = \operatorname{Frac} A$. There is an exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A^\times & \longrightarrow & K^\times & \longrightarrow & \mathcal{J}_A & \longrightarrow & \mathcal{J}_A/\mathcal{P}_A & \longrightarrow & 1 \\ & & & & x & \longmapsto & \langle x \rangle & & & & \end{array}$$

Remark 4.3.4. Let A be a dedekind domain. $|\mathcal{J}_A/\mathcal{P}_A| = 1 \iff A$ is PID $\iff A$ is UFD.

Chapter 5

Appendix

5.1 Definition of Categories and Functors

Definition 5.1.1. A **category** C consists of :

- $\mathrm{Ob}(C)$: a **class** of object
- Set of morphisms : $C(X, Y)$ for order pair (X, Y)
- Composition of morphisms : $\forall (X, Y, Z)$: ordered pair

$$\begin{array}{ccc} C(X,Y) \otimes C(Y,Z) & \longrightarrow & C(X,Z) \\ (f,g) & \longmapsto & g \circ f \end{array}$$

  satisfies associativity and $\forall X \in \mathrm{Ob}(C)\ \exists 1_X \in C(X,X)$ s.t. $f \circ 1_X = f, 1_X \circ g = g$.

Remark 5.1.1. C is called a small cat. if $\mathrm{Ob}(C)$ is a set. Otherwise, we called it large cat.

Definition 5.1.2. For $X, Y \in C$, $f : X \to Y$ is called an **isomorphism** if $\exists g : Y \to X$ s.t. $f \circ g = 1_Y$ and $g \circ f = 1_X$.

Example 5.1.1.

- Set with functions between then.
- Topological space with continuous map.
- poset with $X \to Y \iff x \leq Y$, then it form a small cat.

Definition 5.1.3. Let C, D : category. A **covariant functor** $F : C \to D$ consists of

- $F : \mathrm{Ob}(C) \to \mathrm{Ob}(D)$
- $F : C(X, Y) \to D(F(X), F(Y))$

which satisfies

- $\forall X \in C$, $F(1_X) = 1_{F(x)}$
- $F(g \circ f) = F(g) \circ F(f)$ which is called **functoriality**

We say $F : C \to D$ is a **contravariant functor** if we change the condition to

- $F : C(X, Y) \to D(F(Y), F(X))$
- $F(g \circ f) = F(f) \circ F(g)$

Example 5.1.2. $\mathrm{Hom}(\_, N) : M \mapsto \mathrm{Hom}(M, N)$ is a convariant functor and $\_ \otimes N : M \to M \otimes N$ is a contravariant functor.

Definition 5.1.4. For given C is a category, define **opposite category** of C by

- $\mathrm{Ob}(C^{op}) = \mathrm{Ob}(C)$
- $C^{op}(Y, X) = C(X, Y)$

So F is contravariant functor if F is convariant functor define on C^{op}.

Chapter 6

Homework

6.1

Problem 6.1.1. Let A be a ring and M be a left A-module.

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

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

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 6.1.2. Let $k = \mathbb{R}$ and $V = \mathbb{R}^2$.

(a) Let T be the rotation clockwise about the origin by $\pi/2$ radians. We know that the linear transformation T gives rise to a $k[x]$-submodules for this T. Show that V and 0 are the only $k[x]$-submodules for this T.

(b) Let T be the projection onto the y-axis. Show that $V, 0$, the x-axis and the y-axis are the only $k[x]$-submodules for this T.

(c) Let T be the rotation clockwise about the origin by π radians. Show that every subspace of V is a $k[x]$-submodule for this T.

Problem 6.1.3.

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

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

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

6.2

Problem 6.2.1. Construct a ring A such that for all $m, n \in \mathbb{N}, A^n \simeq A^m$

Problem 6.2.2. If A is a division ring, then A has IBN.

Problem 6.2.3. Let I be an ideal of A.

(a) Let M be an A-module. Show that M/IM has an A/I-module structure.

(b) Show that if I is proper and A/I has IBN, then A also has IBN.

(c) Show that if $f : B \to A$ is a ring epimorphism and A is a division ring, then B has IBN.

Problem 6.2.4. Let $\{M_i\}$ be a directed family of modules over a ring. For any module N show that

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

6.3

Problem 6.3.1. Let G be an abelian group and

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

Please write G as a direct sum of cyclic groups.

Problem 6.3.2. Let R be a PID and M be a finitely generated R-module with rank n. Show that if N is a submodule of M and has rank m, then M/N has rank $n - m$.

Problem 6.3.3. Let A be an additive subgroup of Euclidean space $\mathbb{R}^n$, and assume that in every bounded region of space, there is only a finite number of elements of A. Show that A is a free abelian group on $\leq n$ generators.

Hint: Induction on the maximal number of linearly independent elements of A over $\mathbb{R}$. Let $v_1, ..., v_m$ 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 6.3.4. 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.)

6.4

Problem 6.4.1.

(a) Let $k = \mathbb{C}$. Find the Jordan canonical form J of

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix}$$

and the matrix Q such that $J = Q^{-1}AQ$

(b) Let $k = \mathbb{R}$. Find the Rational canonical form C of

$$A = \begin{pmatrix} 0 & -7 & 14 & -6 \\ 1 & -4 & 6 & -3 \\ 0 & -4 & 9 & -4 \\ 0 & -4 & 11 & -5 \end{pmatrix}$$

and the matrix Q such that $J = Q^{-1}AQ$

Problem 6.4.2. Let R be a PID and M be a finitely generated R-module. Show that if $M \simeq Rz_1 \oplus \cdots \oplus Rz_r$ with $\text{ann}(z_i) = \langle d_i \rangle \neq R$ and $d_i | d_{i+1}$ for all $i = 1, ..., r-1$, then the ring $(\text{Hom}_R(M, M), +, \circ)$ 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 $\text{diag}\{d_1, ..., d_r\}C = B\,\text{diag}\{d_1, ..., d_r\}$ and I is the ideal of matrices of the form $\text{diag}\{d_1, ..., d_r\}Q, Q \in M_{r\times r}(R)$.

Problem 6.4.3. Let $A \in M_{n\times n}(k)$ with k being a field. Assume that $d_1(x), ..., d_r(x)$ are the non-unit monic invariant factors of $(xI_n - A)$ with $\deg d_i(x) = n_i > 0$. Show that

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

6.5

Problem 6.5.1.

(a) Let M be a right A-module, N an A-B bimodule and L a left B-module. Show that

$$(M \otimes_A N) \otimes_B L \simeq M \otimes_A (N \otimes_B L)$$

(b) Let R be a commutative ring and M, N be two R-modules. Show that

$$M \otimes_R N \simeq N \otimes_R M$$

Problem 6.5.2. Justify your answers.

(a) Compute $\dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ and $\dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.

(b) Compute $\dim_{\mathbb{C}} \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ and $\dim_{\mathbb{C}} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

(c) Compute $\dim_{\mathbb{C}} \mathbb{C}[x]/\langle x^2 + x + 1\rangle \otimes_{\mathbb{R}} \mathbb{R}[z]/\langle z + 1\rangle$

(d) Let V and W be two k-vector spaces with $\dim_k V = n$ and $\dim_K W = m$. Compute $\dim_k V \otimes_k W$

Problem 6.5.3. Let $R = \bigoplus_{k=0}^{\infty} R_k$ be a graded ring with $R_i R_j \subset R_{i+j}$ and I be an ideal of R generated by some homogeneous elements. Show that the quotient ring R/I has a natural graded ring structure via $R/I = \bigoplus_{k=0}^{\infty} R_k/(R_k \cap I)$.

Problem 6.5.4. Let R be a commutative ring.

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

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

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

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

6.6

Problem 6.6.1. Let N, L be two R-submodules of M and S be a multiplicatively closed set in the commutative ring R. Show that

(a) $(N + L)_S = N_S + L_S$

(b) $(N \cap L)_S = N_S \cap L_S$

(c) $(M/N)_S \simeq M_S/N_S$

Problem 6.6.2. Let R be a commutative ring. Show that

(a) If M is a proper ideal of R such that for all $x \in R - M$ are units in R, then R is a local ring.

(b) If M is a maximal ideal of R such each element of $1 + M$ is a unit in R, then R is a local ring.

Problem 6.6.3 (Prime avoidance lemma)**.** Let R be a commutative ring. Show that

(a) If $P_1, ..., P_n \in \operatorname{Spec} R$ 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 6.6.4. Let R be a commutative ring and I be an ideal of R. Define

$$\sqrt{I} := \{x \in R : x^n \in I \text{ for some } n > 0\}$$

Show that

(a) $\sqrt{\sqrt{I}} = \sqrt{I}$

(b) For another ideal J, $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

(c) For another ideal J, $\sqrt{I + J} = \sqrt{\left(\sqrt{I} + \sqrt{J}\right)}$

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

6.7

Problem 6.7.1. Show that of A is a (left) Noetherian ring, then the formal power series ring $A[[x]]$ is (left) Noetherian.

Problem 6.7.2. Let R be a commutative 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

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

Problem 6.7.3. 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

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

Problem 6.7.4. Let R be a commutative Noetherian ring and M be a finitely generated R-module. Show that $\mathrm{Ass}(M)$ is a finite set.

6.8

Problem 6.8.1. Show that if A is a commutative Noetherian ring, then the set of zero-divisors in A is the set-theoretical union of all primes belongs to primary ideals in a reduced primary decomposition of $\langle 0 \rangle$.

Problem 6.8.2.

(a) Let $\mathfrak{p}$ be a prime ideal, and $\mathfrak{a}, \mathfrak{b}$ ideals of A. If $\mathfrak{ab} \subseteq \mathfrak{p}$, 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 $\mathfrak{ab} \subseteq \mathfrak{p}$. Assume that $\mathfrak{b}$ is finitely generated. Show that $\mathfrak{a} \subseteq \mathfrak{p}$ or there exists some positive integer n such that $\mathfrak{b}^n \subseteq \mathfrak{p}$

Problem 6.8.3. Let A be Noetherian, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Show that there exists some $n \geq 1$ such that $\mathfrak{p}^n \subseteq \mathfrak{q}$.

Problem 6.8.4.

(a) Let A be an arbitrary commutative ring and let S be a multiplicative subset. Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Then $\mathfrak{p}$ intersects S if and only if $\mathfrak{q}$ intersects S. Furthermore, if $\mathfrak{q}$ does not intersect S, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary in $S^{-1}A$.

(b) Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ be a reduced primary decomposition of an ideal. Assume that $\mathfrak{q}_1, ..., \mathfrak{q}_i$ do not intersect S, but that $\mathfrak{q}_j$ intersects S for $j > i$. Show that

$$S^{-1}\mathfrak{a} = S^{-1}\mathfrak{q}_1 \cap \cdots \cap S^{-1}\mathfrak{q}_i$$

is a reduced primary decomposition of $S^{-1}\mathfrak{a}$.

6.9

Problem 6.9.1. Let R be a commutative ring and I be an ideal of R.

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

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

Problem 6.9.2. Let $\varphi : S_I(R) \to \mathrm{gr}_I(R)$ 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 $S_I(R)/IS_I(R) \simeq \mathrm{gr}_I(R)$.

Problem 6.9.3. Show that $\mathrm{gr}_I(M) \simeq S_I(R)M/IS_I(R)M$
(Here, $S_I(R)M = M \oplus IMt \oplus I^2Mt^2 \oplus \cdots$)

Problem 6.9.4. Show that if R is Noetherian and M is a finitely generated R-module, then $\mathrm{gr}_I(M)$ is a finitely generated $\mathrm{gr}_I(R)$-module.

6.10

Problem 6.10.1. Let (R, m) be a Noetherian local ring and Q be an m-primary ideal.

(1) Show that R/Q is an Artinian R-module and thus $\ell(R/Q)$ is well-defined.

(2) Show that $\ell(Q^i/Q^{i+1})$ is well-defined for all $i = 1, 2, ...$ 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.

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

6.11

Problem 6.11.1. Let A, B be local rings with maximal ideals $\mathfrak{m}_A, \mathfrak{m}_B$, respectively. Let $f : A \to B$ 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 6.11.2. Let A be a Noetherian local ring. Let E be a finite A-module. Assume that A has no nilpotent elements. For each prime ideal $\mathfrak{p}$ of A, let $k(\mathfrak{p})$ be the residue class field. If $\dim_{k(\mathfrak{p})}(E_\mathfrak{p}/\mathfrak{p}E_\mathfrak{p})$ is constant for all $\mathfrak{p}$, show that E is free.

Problem 6.11.3. Let R be a commutative ring. Show that R is Artinian if and only if R is Noetherian and $\operatorname{Spec} R = \operatorname{Max} R$.

Problem 6.11.4. Let $(R, \mathfrak{m})$ be an Artinian local ring. Show that TFAE :

(1) R is a PID

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

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

6.12

Problem 6.12.1. Show that for a short exact sequence of R-modules

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$$

the following are equivalent :

(a) $M_2 = \alpha(M_1) \oplus N$ with $N \simeq M_3$.

(b) $\exists \lambda : M_3 \to M_2$ such that $\beta \circ \lambda = \mathrm{id}_{M_3}$.

(c) $\exists \mu : M_2 \to M_1$ such that $\mu \circ \alpha = \mathrm{id}_{M_1}$

(In this case, this sequence is said to be split exact)

Problem 6.12.2. Show that for a short exact sequence of R-modules

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$$

(a) For all M : R-modules,

$$0 \to \mathrm{Hom}_R(M, M_1) \to \mathrm{Hom}_R(M, M_2) \to \mathrm{Hom}_R(M, M_3) \text{ is exact.}$$

(b) For all N : R-modules,

$$0 \to \mathrm{Hom}_R(M_3, N) \to \mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M_1, N) \text{ is exact.}$$

(c) For all M : right R-modules,

$$M \otimes_R M_1 \to M \otimes_R M_2 \to M \otimes_R M_3 \to 0 \text{ is exact.}$$

Problem 6.12.3. Show that if M is S-R bimodule, $A \in {}_R\mathfrak{M}, B \in {}_S\mathfrak{M}$, then

$$\mathrm{Hom}_S(M \otimes_R A, B) \simeq \mathrm{Hom}_R(A, \mathrm{Hom}_S(M, B))$$

6.13

Problem 6.13.1.

(a) State the property of morphisms being homotopic in the case of cochain complexes.

(b) Let $M \in {}_R\mathcal{M}$. Show that there exists an injective resolution of M

$$0 \to M \xrightarrow{\mu} I^0 \xrightarrow{d_1} I^1 \xrightarrow{d_2} I^2 \xrightarrow{d_3} \cdots .$$

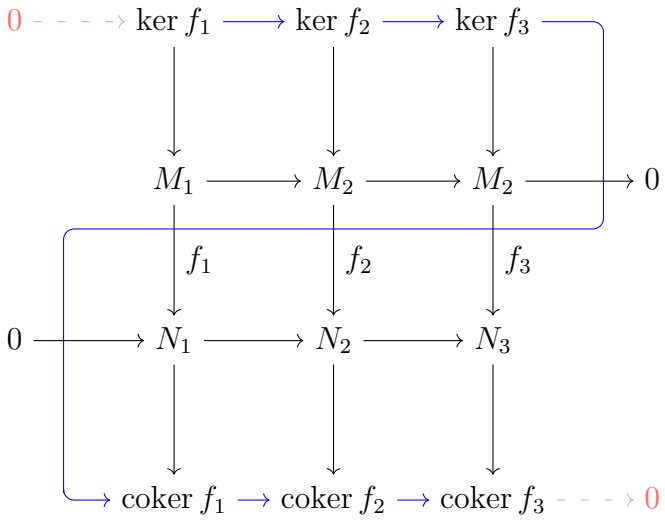
Problem 6.13.2. State and show the dual version of Comparison theorem for injective resolutions.

Problem 6.13.3.

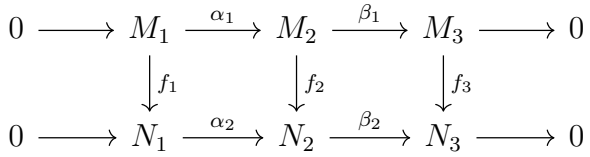
(a) (Snake Lemma) Suppose the following diagram commutes in $\mathcal{M}_R$

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{\alpha_1} & M_2 & \xrightarrow{\beta_1} & M_3 \longrightarrow 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ 0 & \longrightarrow & N_1 & \xrightarrow{\alpha_2} & N_2 & \xrightarrow{\beta_2} & N_3 \end{array}$$

Show that there exists a long exact sequence (in blue color):

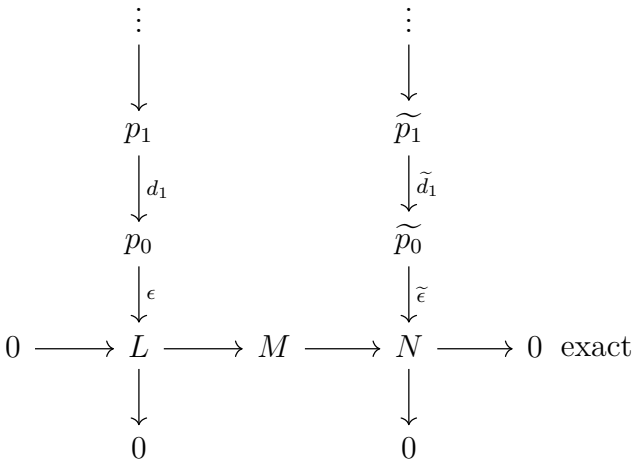


Furthermore, if those two exact sequences are short exact sequence:



Then we can extend the blue exact sequence by adding two red "0" on it.

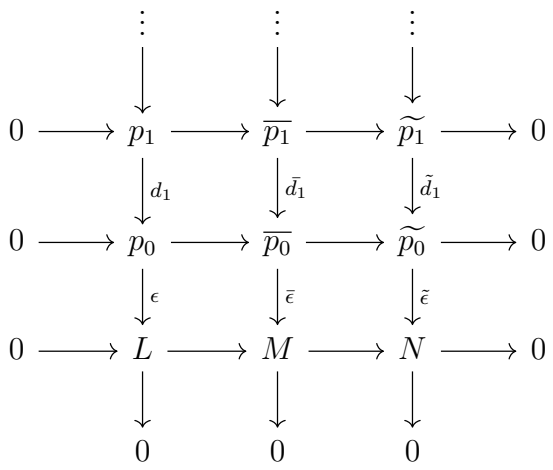
(b) Show the Horseshoe Lemma: Let two projective resolutions of L and N respectively combined with a short exact sequence as follows:



then there is a projective resolution of M:

$$\cdots \to \bar{p}_1 \xrightarrow{\bar{d}_1} \bar{p}_0 \xrightarrow{\bar{\epsilon}} M \to 0$$

such that the completed diagram



commutes, and horizontal sequences are all short exact sequences.

Problem 6.13.4 (standard complex). Let S be a set. For $i = 0, 1, 2, ...$ let E_i be the free module over $\mathbb{Z}$ generated by $(i+1)$-tuples $(x_0, ..., x_i)$ with $x_0, ..., x_i \in S$. Thus such $(i+1)$-tuples form a basis of E_i over $\mathbb{Z}$. There is a unique homomorphism

$$d_{i+1} : E_{i+1} \to E_i$$

such that

$$d_{i+1}(x_0, ..., x_{i+1}) = \sum_{j=0}^{i+1} (-1)^j (x_0, ...\hat{x}_j, ..., x_{i+1})$$

where the symbol $\hat{x}_j$ means that this term is to be omitted. For $i = 0$, we define $d_0 : E_0 \to \mathbb{Z}$ to be the unique homomorphism such that $d_0(x_0) = 1$. The map d_0 is sometimes called the **augmentation**, and is also denoted by ε. Check that

$$\cdots \to E_{i+1} \to E_i \to \cdots \to E_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

is a resolution of $\mathbb{Z}$ by the complex.

6.14

Problem 6.14.1.

(a) Let $P_\bullet \to M \to 0$ be a projective resolution of M. Show that for $N \in \mathfrak{M}_R$, the definition

$$\operatorname{Tor}_n(M, N) := H_n(P_M \otimes N) \quad \text{for } n \geq 0$$

is independent of the choices of projective resolutions.

(b) For $0 \to M_1 \to M_2 \to M_3 \to 0$ exact in $\mathfrak{M}_R$, show that we have the long exact sequence :

$$\cdots \longrightarrow \mathrm{Tor}_2(M_1, N) \longrightarrow \mathrm{Tor}_2(M_2, N) \longrightarrow \mathrm{Tor}_2(M_3, N)$$
$$\mathrm{Tor}_1(M_1, N) \longrightarrow \mathrm{Tor}_1(M_2, N) \longrightarrow \mathrm{Tor}_1(M_3, N)$$
$$M_1 \otimes N \xrightarrow{i\otimes 1} M_2 \otimes N \xrightarrow{\epsilon\otimes 1} M_3 \otimes N \longrightarrow 0$$

(c) If M is flat, show that $\mathrm{Tor}_n(M, N) = 0 \ \forall n > 0, N \in \mathfrak{M}_R$

Problem 6.14.2. Show that

(a) $\mathrm{Ext}^1(M, N) = 0 \ \forall N \iff M$ is projective.

(b) $\mathrm{Ext}^1(M, N) = 0 \ \forall M \iff N$ is injective.

(c) $\mathrm{Tor}_1(M, N) = 0 \ \forall N \iff M$ is flat.

Problem 6.14.3. Show that the two ways to define $\mathrm{Tor}_n(M, N)$ with $M, N \in \mathfrak{R}$ (by $H_n(P_M \otimes N)$ and by $H_n(M \otimes P_N)$) are equivalent.

Problem 6.14.4. Let R be an integral domain and Q be its field of fractions. Show that

(a) if M is a torsion R-module, then $\mathrm{Tor}_1(Q/R, M) \simeq M$.

(b) for any $M \in \mathfrak{M}_R$, $\mathrm{Tor}_n(Q/R, M) = 0 \ \forall n \geq 2$ and $\mathrm{Tor}_1(Q/R, M) \simeq \mathrm{Tor}(M)$.

(c) if M is torsion-free, then $\mathrm{Tor}_1(Q/R, M) \simeq 0$.

6.15

Problem 6.15.1.

(a) Show that $B(G)$ is a chain complex.

(b) Show that in $P(G)$, ∂_n is a $\mathbb{Z}[G]$-module homomorphism.

(c) Show that $P(G)$ is a chain complex.

Problem 6.15.2.

(a) Show that τ_n and τ_n^{-1} are $\mathbb{Z}[G]$-module homomorphisms.

(b) Show that $\tau = \{\tau_n\}$ is a chain map from $P(G)$ to $B(G)$.

(c) Show that $\tau^{-1} = \{\tau_n^{-1}\}$ is a chain map from $B(G)$ to $P(G)$

(d) Show that for $P(G)$, there us $s_n : P_n \to P_{n+1}$ such that

$$1_{P_n} = s_{n-1} \circ \partial_n + \partial_{n+1} \circ s_n$$

Problem 6.15.3.

(a) Show that $d_n(U_n) \subseteq U_{n+1}$ for the normalized bar resolution of $\mathbb{Z}$.

(b) Show that $B^*(G)$ is a chain complex.

(c) Shoe that there is $t_n^* : B_n^* \to B_{n+1}^*$ such that

$$1_{B_n^*} = t_{n-1}^* d_n^* + d_{n+1}^* t_n^*$$

and $B^*(G)$ is an exact sequence.

Problem 6.15.4.

(a) Show that if $G = \langle g_1, ..., g_n \rangle$, then $IG = \langle g_1 - 1, ..., g_n - 1 \rangle_{\mathbb{Z}[G]}$

(b) Show that $H_1(G, \mathbb{Z}/m\mathbb{Z}) \simeq G/[G,G]G^m$, where $G^m = \langle g^m : g \in G \rangle$. (For $H_1(G, \mathbb{Z}/m\mathbb{Z})$, G acts on $\mathbb{Z}/m\mathbb{Z}$ trivially.)

6.16

Problem 6.16.1.

(a) For $f : M \to R$, show that $d_f \circ d_f = 0$.

(b) For two chain complexes of R-modules $(C_\bullet, d), (C'_\bullet, d')$, show that $(d \circ d') \circ (d \circ d') = 0$.

(c) Let $M_1, M_2 \in \mathfrak{M}_R$, $f_1 \in \mathrm{Hom}_R(M_1, R)$, $f_2 \in \mathrm{Hom}_R(M_2, R)$. Show that $df_1 \otimes df_2 = df$ with $f = f_1 + f_2 \in \mathrm{Hom}_R(M_1 \oplus M_2, R)$ under the isomorphism

$$\bigoplus_{i=0}^{n} \bigwedge^i M_1 \otimes \bigwedge^{n-i} M_2 \simeq \bigwedge^n (M_1 \oplus M_2) \ \forall n.$$

Problem 6.16.2. Let $\{a_1, ..., a_n\}$ be an R-regular sequence and $I = \langle a_1, ..., a_n \rangle \subseteq R$. Show that

(a) I/I^2 is free of rank n over R/I.

(b) $\mathrm{gr}_I(R) \simeq R/I[x_1, ..., x_n]$ as graded rings.

Problem 6.16.3. Let $\{a_1, ..., a_n\}$ be an R-regular sequence and $I = \langle a_1, ..., a_n \rangle \subseteq R$. Show that R/I does not have any projective resolution of length shorter than n.

Problem 6.16.4. Let $\{x_1, x_2, x_3\}$ be an R-regular sequence. Write down explicitly

$$K_\bullet(\underline{x}) \to R/\langle x_1, x_2, x_3 \rangle \to 0$$

where $\underline{x} = x_1, x_2, x_3$.

6.17

Problem 6.17.1. Let a group G act on an abelian group M. Show that $B^2(G,M) \leq Z^2(G,M)$.

Problem 6.17.2. Let $1 \to M \to E \xrightarrow{p} G \to 1$ with two liftings $\ell_1 : G \to E . \ell_2 : G \to E$, whose corresponding factor sets are f_1, f_2, respectively. Show that there is $h : G \to M$ with $h(1) = 1$ and for all $\overline{x}, \overline{y} \in G$,

$$f_2(\overline{x},\overline{y}) f_1(\overline{x},\overline{y})^{-1} = \theta_{\overline{x}}(h(\overline{y}))h(\overline{xy})^{-1}h(\vec{x})$$

Problem 6.17.3. Show that there are inequivalent extensions of M by G with isomorphic middle group.

6.18

Problem 6.18.1. Two group-homomorphism liftings : $\ell_1, \ell_2 : G \to E$ are **M-conjugate** if there is an $a \in M$ such that $(a,1)\ell_1(x)(a,1)^{-1} = \ell_2(x)\ \forall x \in G$. Show that

$$H^1(G,M) \longleftrightarrow \{M\text{-conjugacy classes of group-homomorphism liftings}\}$$

Problem 6.18.2. Let $1 \to M \to E \to G \to 1$ be split and $\ell : G \to E, \ell' : G \to E$ be two liftings with $K = \ell(G), K' = \ell'(G)$. Show that if $H^1(G,M) = H^2(G,M) = 0$, then K and K' are conjugate in E.

Problem 6.18.3.

(a) Let $d|m$ and N be a $\mathbb{Z}/m\mathbb{Z}$-module. Compute

$$\mathrm{Ext}^n_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, N),\ \forall n \geq 0$$

(b) Compute $\mathrm{Ext}^n_{\mathbb{Z}/p^2\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}),\ \forall n \geq 0$.

6.19

Problem 6.19.1. Let $M = \mathbb{Z}/4\mathbb{Z}$ and $G = \mathbb{Z}/2\mathbb{Z}$.

(a) Find all linear actions of G on M.

(b) For each such action, compute $H^2(G,M)$.

(c) For each such action, describe all extensions of M by G.

(d) For each extension E of M by G, compute $\mathrm{Stab}_E(G,M)/\mathrm{Inn}(G,M)$.

Problem 6.19.2. Compute

(a) $H_n(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})\ \forall n \geq 0$.

(b) $H^n(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})\ \forall n \geq 0$.

Problem 6.19.3.

(a) Show that if G acts on M trivially, then

$$H^1(G, M) \simeq \mathrm{Der}(G, M) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M).$$

(b) Let $C_2 = \langle \sigma \rangle$ with $\sigma^2 = 1$ and act on $\mathbb{Z}$ by $\sigma \cdot n = -n$.
Compute $\mathrm{Der}(C_2, \mathbb{Z}), \mathrm{PDer}(C_2, \mathbb{Z})$ and $H^1(C_2, \mathbb{Z})$.

Problem 6.19.4. Define $\mathrm{Ind}^G(M) = \mathbb{Z}[G] \otimes_Z M$ and $\mathrm{CoInd}^G(M) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)$ which have natural $\mathbb{Z}[G]$-module structure.

(a) Compute $H^n(G, \mathrm{CoInd}^G(M))$ and $H_n(G, \mathrm{Ind}^G(M))$ for every $n \geq 0$.

(b) Let $|G| < \infty$. Show that

$$\mathrm{CoInd}^G(M) \simeq \mathrm{Ind}^G(M)$$

as $\mathbb{Z}[G]$-modules.

6.20

Problem 6.20.1. Let M be a semisimple A-module and N be a submodule of M. Show that N and M/N are also semisimple.

Problem 6.20.2. Let A be a division ring and M be a free A-module of rank 1. Show that $\mathrm{Hom}_A(M, M) \longleftrightarrow A$.
Is this corrsepondence a ring homomorphism?

Problem 6.20.3.

(a) Let $M = N^{\oplus n}$ with N being a simple submodule of M. Let $D' = \mathrm{End}_A(N)$ which is a division ring. Show that

$$\mathrm{End}_A(M) \simeq M_{n \times n}(D') \quad \text{as rings.}$$

(b) Let $M = N_1^{\oplus m_1} \oplus \cdots \oplus N_r^{\oplus m_r}$ with $N_1, ..., N_r$ be simple submodules of M and $N \not\simeq N_j\ \forall i \neq j$. Let $D_i' = \mathrm{End}_A(N_i),\ \forall i = 1, ..., r$. Show that $\mathrm{End}_A(M)$ is isomorphic to a ring of matrices, of type

$$\begin{pmatrix} I_1 & & & O \\ & I_2 & & \\ & & \ddots & \\ O & & & I_r \end{pmatrix}$$

where $I_i \in M_{m_i \times m_i}(D_i')$.

Problem 6.20.4.

(a) Show that every finitely generated semisimple A-module is both Noetherian and Artinian.

(b) Show that if D is a division ring, then the only two-sided ideals of $M_{n\times n}(D)$ are $\{0\}$ and $M_{n\times n}(D)$

6.21

Problem 6.21.1.

(a) When is an abelian group semisimple (as a $\mathbb{Z}$-module)?

(b) Show that a module M is semisimple, if and only if every cyclic submodule of M is semisimple.

Problem 6.21.2.

(a) Show that the radical of $A/r(A)$ is zero.

(b) Show that $x \in r(A) \iff 1 - yx$ is invertible for every $y \in A$.

(c) Show that $r(A)$ is the largest two-sided ideal I such that $1 - x$ is invertible for all $x \in I$.

(d) Show that if M is a finitely generated A-module such that $r(A)M = M$, then $M = 0$.

Problem 6.21.3. Let R be a semisimple commutative ring. Show that R is a direct product of fields.

Problem 6.21.4. Let R be a finite dimensional commutative algebra over a field k. If R has no nonzero nilpotent element, show that R is semisimple.

6.22

Problem 6.22.1. Show that the only finite dimensional division algebra over an algebraically closed field k is k itself.

Problem 6.22.2. Let E be a finite dimensional vector space over a field k. Let R be a semisimple subalgebra of $\mathrm{End}_k(E)$. Let $a, b \in R$. Assume that

$$\ker b_E \supseteq \ker a_E$$

where a_E, b_E is multiplication by a, b on E, respectively. Show that there exists an element $s \in R$ such that $sa = b$.

Problem 6.22.3. Let E be a finite-dimensional vector space over a field k. Let $A \in \mathrm{End}_k(E)$, we say that A is semisimple if E is a semisimple A-space, or equivalently, let R be the k-algebra generated by A, then E is a semisimple over R. Show that A is semisimple if and only if its minimal polynomial has no factors of multiplicity > 1 over k.

Problem 6.22.4. Let E be a finite-dimensional vector space over a field k, and let S be a commutative set of endomorphisms of E. Let $R = k[S]$. Assume that R is semisimple. Show that every subset of S is semisimple.

6.23

Problem 6.23.1.

(a) Let $\varphi : G \to \mathrm{GL}_n(F)$ be a matrix representation. Prove that the map $g \mapsto \det(\varphi(g))$ is a degree 1 representation.

(b) Prove that the degree 1 representations of G are in bijective correspondence with the degree 1 representations of the abelian group $G/[G, G]$.

Problem 6.23.2.

(a) Let V be a (possibly infinite dimensional) $F[G]$-module (G is finite group). Prove that for each $v \in V$, there is an $F[G]$-submodule containing v of dimension $\leq |G|$.

(b) Prove that if $|G| > 1$, then every irreducible $F[G]$-module has dimension $< |G|$.

Problem 6.23.3.

(a) Exhibit all 1-dimensional complex representations of a finite cyclic group; make sure to decide which are inequivalent (not isomorphic).

(b) Exhibit all 1-dimensional complex representations of a finite abelian group. Deduce that the number of inequivalent (non-isomorphic) degree 1 complex representations of a finite abelian group equals the order of the group.

Problem 6.23.4.

(a) Let p be a prime, let P be a p-group and let F be a field of characteristic p. Prove that the only irreducible representation of P over F is the trivial representation.

(b) Let p be a prime, let P be a nontrivial p-group and let F be a field of characteristic p. Prove that the regular representation is not completely reducible.

(c) Let p be a prime, let P be a nontrivial p-group and let F be a field of characteristic p. Prove that the regular representation is indecomposable.

6.24

Problem 6.24.1. Assume V is a $\mathbb{C}[G]$-module on which G acts by permuting the basis $B = \{e_1, ..., e_n\}$. Write $\mathcal{B}$ as a disjoint union of the orbits $\mathcal{B}_1, ..., \mathcal{B}_t$ of G on $\mathcal{B}$.

(a) Prove that V decomposes as a $\mathbb{C}[G]$-module as $V_1 \oplus \cdots \oplus V_t$, where $V_i = \text{span}(\mathcal{B}_i)$.

(b) Prove that if v_i is the sum of the vectors in $\mathcal{B}_i$, then the 1-dimensional subspace of V_i spanned by v_i is the unique $\mathbb{C}[G]$-submodule of V_i affording the trivial representation.

(In other words, any vector in V_i that is fixed under the action of G is a multiple of v_i.)

(c) Let $W = \{v \in V : \varphi(g)(v) = v \ \forall g \in G\}$ be the subspace of V fixed pointwise by all elements of G. Deduce that $\dim W = t =$ the number of orbits of G on $\mathcal{B}$.

Problem 6.24.2.

(a) Let $\varphi : G \to \text{GL}(V)$ be a representation with character ψ. Let W be the subspace $\{v \in V | \varphi(g)(v) = v \ \forall g \in G\}$ of V. Prove that $\dim_{\mathbb{C}} W = \langle \psi, \chi_1 \rangle$, where χ_1 is the principal character of G.

(b) Prove the following result (sometimes called Burnside's Lemma although its origin is with Frobenius) by the preceding results : Let G be a subgroup of S_n and for each $\sigma \in G$ let $\text{Fix}(\sigma)$ denote the number of fixed points of σ on $\{1, ..., n\}$. Let t be the number of orbits of G on $\{1, ..., n\}$. Then

$$t|G| = \sum_{g \in G} \text{Fix}(g)$$

Problem 6.24.3. Let ψ be the character of any 2-dimensional representation of a group G and let x be an element of order 2 in G. Prove that $\psi(x) = 0$ or ± 2. Generalize this to n-dimensional representations.

Problem 6.24.4. Let V be a vector space over $\mathbb{C}$, $\varphi : G \to \text{GL}(V)$ be a representation and $\chi : G \to \mathbb{C}^\times$ be a degree 1 representation.

(a) Show that $\chi\varphi : G \to \text{GL}(V) : G \to \text{GL}(V)$ define by $\chi\varphi(g) = \chi(g)\varphi(g)$ is a representation.

(b) Show that $\chi\varphi$ is irreducible if and only if φ is irreducible.

(c) Show that if ψ is the character afforded by φ then $\chi\varphi$ is the character afforded by $\chi\varphi$.

(d) Deduce that the product of any irreducible character with a character of degree 1 is also an irreducible character.

6.25

Problem 6.25.1. Prove that the elements x and y are conjugate in a group G if and only if $\chi(x) = \chi(y)$ for all irreducible character χ of G.

Problem 6.25.2. Prove that every irreducible character of both Q_8 and D_8 is rational valued. Prove that D_{10} has an irreducible character that is not rational valued.

Problem 6.25.3. Show for any positive integer n that every character of the symmetry group S_n is rational valued.
(i.e. $\psi(g) \in \mathbb{Q}$ for all $g \in S_n$ and all characters ψ of S_n.)

Actually, we can do more in Problem 6.25.3.

Problem 6.25.4. Show that every character of the symmetric group S_n is integer-valued.

6.26

Problem 6.26.1. The group S_3. Let S_3 be the symmetric group on 3 elements,

(a) Show that there are three conjugacy classes.

(b) There are two characters of dimension 1, on S_3/A_3.

(c) Let d_i $(i = 1, 2, 3)$ be the dimensions of the irreducible characters. Since $\sum d_i^2 = 6$, the third irreducible character has dimension 2. Show that the third representation can be realized by considering a cubic equation $X^3+aX+b = 0$, whose Galois group is S_3 over a field k. Let V be the k-vector space generated by the roots. Show that this space is 2-dimensional and gives the desired representation, which remains irreducible after tensoring with k^a

(d) Let $G = S_3$. Write down an idempotent for each one of the simple components of $\mathbb{C}[G]$. What is the multiplicity of each irreducible representation of G in the regular representation on $\mathbb{C}[G]$?

Problem 6.26.2. The group S_4 and A_4. Let S_4 be the symmetric group on 4 elements.

(a) Show that there are 5 conjugacy classes.

(b) Show that A_4 has a unique subgroup of order 4, which is not cyclic, and which is normal in S_4. Show that the factor group is isomorphic to S_3, so the representations of Problem 6.26.1 give rise to representations of S_4.

(c) Using the relation $\sum d_i^2 = 24$, conclude that there are only two other irreducible characters of S_4, each of dimensional 3.

(d) Let $X^4 + a_2X^2 + a_1X + a_0$ be an irreducible polynomial over a field k, with Galois group S_4. Show that the roots generate a 3-dimensional vector space V over k, and that the representation of S_4 on this space is irreducible, so we obtain one of the two missing representations.

(e) Let ρ be the representation of (d). Define ρ' by

$$\rho'(\sigma) = \begin{cases} \rho(\sigma) & \text{, if } \sigma \text{ is even} \\ -\rho(\sigma) & \text{, if } \sigma \text{ is odd} \end{cases}$$

Show that ρ' is also irreducible, remains irreducible after tensoring with k^a, and is non-isomorphic to ρ. This concludes the description of all irreducible representations of S_4.

(f) Show that the 3-dimensional irreducible representations of S_4 provide an irreducible representation of A_4.

(g) Show that all irreducible representations of A_4 are given by the representations in (f) and three others which are one-dimensional.

Problem 6.26.3. The quaternion group. Let $\mathbb{Q} = \{\pm 1, \pm x, \pm y, \pm z\}$ be the quaternion group, with $x^2 = y^2 = z^2 = -1$ and $xy = -yx, xz = -zx, yz = -zy$.

(a) Show that Q has 5 conjugacy classes.

Let $A = \{\pm 1\}$. Then Q/A is of type $(2, 2)$, and hence has 4 simple characters, which can be viewed as simple characters of Q.

(b) Show that there is only one more simple character of Q, of dimension 2. Show that the corresponding representation can be given by a matrix representation such that

$$\rho(x) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \rho(y) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \rho(z) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

(c) Let $\mathbb{H}$ be the quaternion field, i.e. the algebra over $\mathbb{R}$ having dimension 4, with basis $\{1, x, y, z\}$, and the corresponding relations as above, Show that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \simeq M_2(\mathbb{C})$. Relate this to (b).

Problem 6.26.4. Let G be a finite group operating on a finite set S. Let $\mathbb{C}[S]$ be the vector space generated by S over $\mathbb{C}$. Let ψ be the character of the corresponding representation of G on $\mathbb{C}[S]$.

(a) Let $\sigma \in G$. Show that $\psi(\sigma) =$ number of fixed points of σ in S.

(b) Show that $\langle \psi, 1_G \rangle_G$ is the number of G-orbits in S.

6.27

Problem 6.27.1. Let $G = S_3$, $H = A_3$ and V be the 3-dimensional $\mathbb{C}[H]$-module which affords the natural permutation representation of A_3. Let 1 and (12) be cosets representatives of A_3 in S_3 and write out the explicit matrices described in basic proposition for the action of S_3 on the induced module W, for each of the elements of S_3.

Problem 6.27.2. In each of parts (a) to (f), a character ψ of a subgroup H of a particular group G is specified. Compute the values of the induced character $\mathrm{Ind}_H^G(\psi)$ on all the conjugacy classes of G ans use the character tables to write $\mathrm{Ind}_H^G(\psi)$ as a sum of irreducible characters :

classes	1	(12)	(123)	(1234)	(12)(34)
sizes	1	6	8	6	3
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

Table 6.1: character table of S_4

(a) ψ is the unique nonprincipal degree 1 character of the subgroup $\langle(12)\rangle$ of S_3.

(b) ψ is the degree 1 character of the subgroup $\langle r\rangle$ of D_8 defined by $\psi(r) = i$, where $i \in \mathbb{C}$ is a square root of -1.

(c) ψ is the degree 1 character of the subgroup $\langle r\rangle$ of D_8 defined by $\psi(r) = -1$.

(d) ψ is any of the nonprincipal degree 1 characters of the subgroup $V_4 = \langle(12), (34)\rangle$ of S_4.

(e) $\psi = \chi_4$ in the character table of $H = S_4$ above and H is a subgroup of $G = S_5$.

(f) ψ is any of the nonprincipal degree 1 characters of the subgroup $V_4 = \langle(12), (34)\rangle$ of S_5.

Problem 6.27.3.

- Let H be a subgroup of G, let φ be a representation of H and suppose that N is a normal subgroup of G with $N \leq H$ and N is contained in the kernel of φ. Prove that N is also contained in the kernel of the induced representation of φ.
- Let N be a normal subgroup of G and let ψ_1 be the principal character of N. Let Ψ be the induced character $\mathrm{Ind}_N^G(\psi_1)$ so that by the preceding exercise, we may consider Ψ as the character of a representation of G/N. Prove that Ψ is the character of the regular representation of G/N.

Problem 6.27.4. Let Z be any subgroup of the center of G, let $[G : Z] = m$ and let ψ be a character of Z. Prove that

$$\mathrm{Ind}_Z^G(\psi)(g) = \begin{cases} m\psi(g) & \text{, if } g \in Z \\ 0 & \text{, if } g \notin Z \end{cases}$$

6.28

Problem 6.28.1. Use the method of $\mathrm{Ind}_{G_i}^G(\widetilde{\chi_i} \otimes \widetilde{\rho})$ to recompute the irreducible representations of D_n, A_n, S_n.

Problem 6.28.2. Let $|H| = u, |H| = u_i, |A| = t$.

(a) Show that $t = \sum_{i=1}^{\ell} \frac{u}{u_i}$.

(b) Show that, for fixed i, the sum of the squares of the degree of the representations is $\frac{u^2}{u_i}$.

(c) Deduce from this, give another proof of Main theorem (2).

6.29

Let $\mathcal{F}$ be the family of cyclic subgroups of G.

Problem 6.29.1. Let $G = A_4$ and let $\{\underbrace{\chi_0, \chi_1, \chi_2}_{\deg 1}, \underbrace{\psi}_{\deg 3}\}$ be the distinct irreducible characters of G.

(a) Show that the image of $\bigoplus_{H \in \mathcal{F}} \mathrm{Ch}(H)$ under Ind is generated by the five characters :

$$\chi_0 + \chi_1 + \chi_2 + \psi, 2\psi, \chi_0 + \psi, \chi_1 + \psi, \chi_2 + \psi$$

(b) Conclude that an element χ of $\mathrm{Ch}(G)$ belongs to the image of Ind if and only if $\chi(1) \equiv 0 \pmod 2$.

(c) Show that none of χ_0, χ_1, χ_2 is a linear combination with positive rational coefficients of characters induced from cyclic subgroups.

Problem 6.29.2. Denote by N be the kernel of

$$\mathbb{Q} \otimes \mathrm{Ind} : \bigoplus_{H \in \mathcal{F}} \mathbb{Q} \otimes \mathrm{Ch}(H) \longrightarrow \mathbb{Q} \otimes \mathrm{Ch}(G)$$

(a) Let $H, H' \in \mathcal{F}$ with $H' \subseteq H'$. Let $\chi' \in \mathrm{Ch}(H')$ and $\chi = \mathrm{Ind}_{H'}^H(\chi') \in \mathrm{Ch}(H)$. Show that $\chi - \chi' \in N$.

(b) Let $H \in \mathcal{F}$ and $s \in G$. Let $\chi \in \mathrm{Ch}(H)$ and let $\chi_s(shs^{-1}) = \chi(h)$ for all $shs^{-1} \in sHs^{-1}$. Show that $\chi - \chi_s \in N$.

(c) Show that N is generated over $\mathbb{Q}$ by the elements of type (a) and type (b).