Algebra I Notes

Shun/翔海(@shun4midx)

9-4-24 (WEEK 1)

SYMMETRIC GROUPS

DEFINITION

Let G be a nonempty set. If $\exists$ a map: $\begin{matrix} G\times G \to G \\ (x,y)\mapsto xy \end{matrix}$, s.t.

(1) $(xy)z = x(yz)$ $\forall x,y,z \in G$
(2) $\exists e \in G$, s.t. $xe = ex = x$ $\forall x \in G$
(3) $\forall x \in G$, $\exists y \in G$, s.t. $xy = yx = e$
(4) $\forall x,y \in G$, $xy = yx$

We call:
↳ (1) only a **semigroup**
↳ (1), (2) a **monoid**
↳ (1), (2), (3) a **group**
↳ (1), (2), (3), (4) an **abelian group**

FACT

(1) e is **unique**: if $\exists$ another e', then $e = ee' = e'$ ✓
(2) y is **unique** $\forall x$: if $\exists$ another y', then $y = ye = y(xy') = (yx)y' = ey' = y'$ ✓
↳ We denote $y := x^{-1}$
(3) $(x^{-1})^{-1} = x$ (b/c def, $xx^{-1} = x^{-1}x = e$)
(4) $xy = xz \Rightarrow y = z$: $x^{-1}(xy) = x^{-1}(xz) \Rightarrow ey = ez \Rightarrow y = z$ ✓

EXAMPLE 1 (SUBGROUPS)

$(\mathbb{Z}, +, 0)$ is a group, but $(\mathbb{Z}, \times, 1)$ is not a group
$(\mathbb{Q}\setminus\{0\}, \times, 1)$ is a group
$\cap$ ← subgroup
$(\mathbb{R}\setminus\{0\}, \times, 1)$ is a group

} Abelian!

DEFINITION

H is a **subgroup** if $\emptyset \neq H \subseteq G$, s.t.:
- $\forall x,y \in H$, $xy \in H$
- $e \in H$
- $\forall x \in H$, $x^{-1} \in H$

Notice, $(H, \cdot, e)$ is also a **group**

USEFUL LEMMA

$H \overset{\text{subgroup}}{\leq} G \iff \forall x,y \in H$, $xy^{-1} \in H$

Proof
"$\Rightarrow$": $\forall y \in H$, thus $y^{-1} \in H$. $\therefore \forall x,y \in H$, $xy^{-1} \in H$ ✓
"$\Leftarrow$": · Identity: $\forall x \in H$, $xx^{-1} = e \in H$ ✓
· Inverse: $\forall x \in H$, since $e \in H$, thus $ex^{-1} = x^{-1} \in H$ ✓
· "$xy \in H$": By above, $\forall y \in H$, $y^{-1} \in H$. $\therefore \forall x,y \in H$, $x(y^{-1})^{-1} = xy \in H$ ✓

EXAMPLE 2 (PERMUTATION GROUPS)

Let S be a nonempty set
A **permutation** of S is a **bijection** from S to S.
We denote $\text{Perm}(S)$ = the set of all permutations of S $\Rightarrow$ $(\text{Perm}(S), \circ, \text{id}_S)$ forms a **group**
(likely non-abelian; $\circ$: composition of functions)

For $|S| = n$, say $S = \{1, 2, \dots, n\}$, $S_n = \text{Perm}(S)$, i.e. the **symmetric group** of deg n

OBSERVE
For $S_n = \{\sigma : \{1, \dots, n\} \to \{1, \dots, n\} \mid \sigma \text{ is bijective}\}$,

CYCLIC NOTATION
For example, for $\sigma \in S_5$, say $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$, we say $\sigma = (1\ 4)(2\ 3\ 5)$

Note, any permutation is a product of disjoint cycles

EXAMPLE OF PRODUCTS
In S_8, for $\sigma = (1\ 2\ 3)(4\ 5\ 6)$, $\tau = (1\ 3\ 5\ 6)(2\ 4\ 7)$, then $\sigma\tau = (1)(2\ 5\ 4\ 7\ 3\ 6)$
(4-cycle, 3-cycle, 6-cycle)
Notice,
↳ $\sigma^{-1} = (1\ 3\ 2)(4\ 6\ 5)$
↳ $\tau^{-1} = (1\ 6\ 5\ 3)(2\ 7\ 4)$

DEFINITION
A 2-cycle is called a transposition

EXAMPLES OF 2-CYCLE DECOMPOSITION
$(1\ 2\ 3) = (1\ 2)(1\ 3)$, $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$

Note, any permutation is a product of transpositions

PROPOSITION
For $\sigma \in S_n$, the number of transpositions appearing in any product for σ is unique modulo 2. (Parity Check)
We call σ a(n) "even permutation" or "odd permutation", accordingly

PROOF
Define N (length): $S_n \longrightarrow \mathbb{Z}$
$(j_1 \cdots j_m) \longmapsto m-1$

Notice, if the cycles are disjoint, we define $(j_1 \cdots j_m)(i_1 \cdots i_n) \longmapsto (m-1)+(n-1) = N(\sigma)$
Claim: $N((a\ b)\sigma) = N(\sigma) - 1$ if a, b occur in the same disjoint decomposition cycle of σ
$= N(\sigma) + 1$ otherwise

Proof
observe: $(a\ b)(a\ c_1 \cdots c_h\ b\ d_1 \cdots d_k) = (a\ c_1 \cdots c_h)(b\ d_1 \cdots d_k)$, which also holds for $h, k = 0$
In this case, $N((a\ b)\sigma) = (h+1-1)+(k+1-1) = h+k$, meanwhile $N(\sigma) = h+k+2-1 = h+k+1 \Rightarrow$ The claim holds

However, notice that $(a\ b)^{-1} = (a\ b)$, thus $(a\ c_1 \cdots c_h\ b\ d_1 \cdots d_k) = (a\ b)(a\ c_1 \cdots c_h)(b\ d_1 \cdots d_k)$ (σ')
Now, in the case of $\sigma = \sigma'$, $N((a\ b)\sigma) = h+k+1$, but $N(\sigma) = h+k \Rightarrow$ The claim holds

$\therefore$ The claim holds true (all cases are considered)

Now, if $\sigma = (a_1\ b_1)(a_2\ b_2) \cdots (a_\ell\ b_\ell)$ (any possible decomposition), then $N((a_1\ b_1)) = 1$, $N((a_1\ b_1)(a_2\ b_2)) = 1 \pm 1, \dots$, thus $N(\sigma) = \sum_{i=1}^{\ell} \varepsilon_i$, $\varepsilon_i = \pm 1$
$\because -1 \equiv 1 \pmod 2$ $\therefore N(\sigma) \equiv \ell \pmod 2$ ✓

USEFUL FORMULA

$\sigma(j_1 \cdots j_m)\sigma^{-1} = (\sigma(j_1) \cdots \sigma(j_m))$

└ A conjugate of $(j_1 \cdots j_m)$

Proof

Let $i \in \{1, \ldots, n\}$

Case 1: $i \in \{\sigma(j_1), \cdots, \sigma(j_m)\}$, say $i = \sigma(j_t)$, then $RHS(i) = \begin{cases} \sigma(j_{t+1}) \\ \sigma(j_1) \end{cases}$; $\begin{matrix} t \neq m \\ t = m \end{matrix} = LHS(i)$

Case 2: $i \notin \{\sigma(j_1), \cdots, \sigma(j_m)\}$, then $\sigma^{-1}(i) \notin \{j_1, \ldots, j_m\} \Rightarrow RHS(i) = i = LHS(i)$

DEFINITION

A group G is said to be generated by $x_1, \ldots, x_n$, denoted by $G = \langle x_1 \cdots x_n \rangle$ if $\forall x \in G$, $\exists j_1, \ldots, j_r \in \{1, \ldots, n\}$, and $m_1, \ldots, m_r \in \mathbb{Z}$, s.t. $x = x_{j_1}^{m_1} \cdots x_{j_r}^{m_r}$

PROPOSITION

$S_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle$

Proof

$(a\ b) = (1\ a)(1\ b)(1\ a)$, done

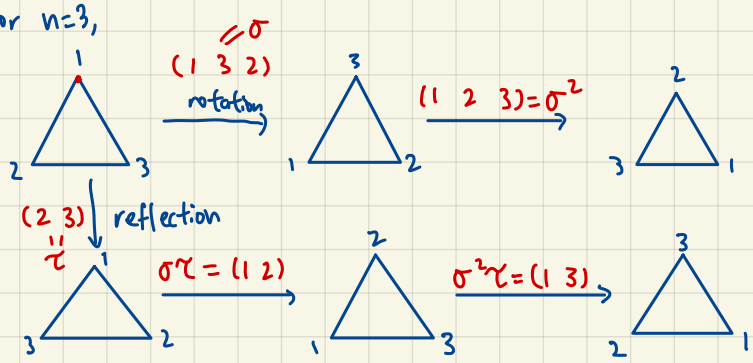
DIHEDRAL GROUPS

DEFINITION

The Dihedral group D_{2n} is the group of symmetries of the n-gon

EXAMPLE

For $n=3$,



Notice, $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$

$\therefore D_6 = \langle \underbrace{\sigma, \tau}_{\text{generators}} \mid \underbrace{\sigma^3 = id, \tau^2 = id, \tau\sigma\tau^{-1} = \sigma^{-1}}_{\text{relations}} \rangle = \{id, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ ($\because \tau\sigma = \sigma^{-1}\tau$, so all elements are in the form $\sigma^m\tau^n$)

SUMMARY

In general, $D_{2n} = \langle \underbrace{\sigma}_{\text{rotation}}, \underbrace{\tau}_{\text{reflection}} \mid \sigma^n = id, \tau^2 = id, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle = \{\sigma^i\tau^j \mid \begin{matrix} i=0,\ldots,n-1 \\ j=0,1 \end{matrix}\}$, so $|D_{2n}| = 2n$

DEFINITION

In S_n, we have $A_n = \{\text{even permutations}\} \Rightarrow |A_n| = \frac{n!}{2}$ and $A_n \trianglelefteq S_n$

9-6-24 (WEEK 1)

CYCLIC GROUPS AND INTERNAL DIRECT PRODUCT

DEFINITION

A group $G=\langle a\rangle := \{\dots, a^{-2}, a^{-1}, \underbrace{1}_{\text{identity } e=a^0}, a^1, a^2, \dots\}$ is a cyclic group generated by a (generator of G)

EXAMPLES

1. $\mathbb{Z}=\langle 1\rangle$ ($\mathbb{Z}$ alone is usually for addition unless specified, $\mathbb{Z}\setminus\{0\}$ is for multiplication)
2. $G=\langle \underbrace{\begin{pmatrix}\cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n}\\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n}\end{pmatrix}}_{A}\rangle \leq SO(2)=\{I_2, A, A^2, \dots, A^{n-1}\}$ (Notice $A^n=I_2$, $A^{-1}=A^{n-1}$)
3. $\mathbb{Z}/n\mathbb{Z}=\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{(n-1)}\}$, $\bar{i}+\bar{j}=\overline{i+j} \Rightarrow (\mathbb{Z}/n\mathbb{Z}, +, \bar{0})=\langle\bar{1}\rangle$ is a cyclic group
4. $\langle\underbrace{(1\ 2\ 3\ 4\ 5)}_{\sigma}\rangle \leq S_5$, where it is equal to $\{id, \sigma, \sigma^2, \sigma^3, \sigma^4\}$, $\sigma^5=id$
5. $(\mathbb{Z}/n\mathbb{Z})^\times$ (Notice this $\times$) multiplication: Notice $\forall \bar{j}\in\mathbb{Z}/n\mathbb{Z}$, $\exists\ \underbrace{\bar{j}'}_{(\bar{j})^{-1}}\in\mathbb{Z}/n\mathbb{Z}$, $\bar{j}\times\bar{j}'=\bar{1} \Leftrightarrow \gcd(n,j)=1 \Rightarrow ((\mathbb{Z}/n\mathbb{Z})^\times, \times, \bar{1})$ is a group

   Proof of Claim: "$\Leftarrow$": $jj'=kn+1 \Rightarrow \gcd(n,j)\mid jj'-kn=1 \Rightarrow \gcd(n,j)=1$

   "$\Rightarrow$": By Euclidean Algorithm, $\exists k,h\in\mathbb{Z}$, s.t. $kn+hj=1 \Rightarrow \bar{h}\times\bar{j}=\bar{1}$ in $\mathbb{Z}/n\mathbb{Z} \Rightarrow h=j'$

   Examples: $(\mathbb{Z}/6\mathbb{Z})^\times=\{\bar{1},\bar{5}\}=\langle\bar{5}\rangle$, $(\mathbb{Z}/9\mathbb{Z})^\times=\{\bar{1},\bar{2},\bar{4},\bar{5},\bar{7},\bar{8}\}=\langle\bar{2}\rangle$, $(\mathbb{Z}/12\mathbb{Z})^\times=\{\bar{1},\bar{5},\bar{7},\bar{11}\}$ is not cyclic

DEFINITION

The **order** of G is the **number of elements** in G, denoted by $|G|$

For $a\in G$, the order of a is the **least positive integer** n, s.t. $a^n=1$, written as $\text{ord}(a)$ (Notice $|\langle a\rangle|=n$)

If $a^n\neq 1\ \forall n\in\mathbb{N}$, then we say a has **infinite order**

PROPOSITION 1

Let $a\in G$ with $\text{ord}(a)=n$, then:

(1) $a^k=1 \Leftrightarrow n\mid k$

(2) $\text{ord}(a^r)=\frac{n}{\gcd(n,r)}$

Proof

(1): "$\Rightarrow$": Write $k=qn+r$, $0\leq r<n$. If $r\neq 0$, then $1=a^k=a^{qn+r}=\underbrace{(a^n)^q}_{1}a^r=a^r$ $\therefore r=0$

"$\Leftarrow$": Let $k=nq$, $a^k=(a^n)^q=1$

(2): Let $d=\gcd(n,r)$ and $n=n'd$, $r=r'd$, with $\gcd(n',r')=1$

Notice, $(a^r)^{n'}=a^{r'dn'}=(a^n)^{r'}=1 \Rightarrow \text{ord}(a^r)\mid n'$

However, $(a^r)^{\text{ord}(a^r)}=a^{r\,\text{ord}(a^r)}=1 \Rightarrow n\mid r\,\text{ord}(a^r) \Rightarrow n'\mid r'\,\text{ord}(a^r)$. However, $\gcd(n',r')=1$, thus $n'\mid\text{ord}(a^r)$ □

PROPOSITION 2

Any subgroup of a cyclic group is cyclic

Proof

Let $G=\langle a\rangle$, and $H\leq G$. If $H=\{1\}$, then done

Otherwise, by well-ordering axiom, $\exists\ d=\min\{m\in\mathbb{N}\mid a^m\in H\}$ ($\neq\emptyset$, since $a^r\in H\Leftrightarrow a^{-r}\in H$) ("only nonpositive")

Claim: $H=\langle a^d\rangle$

Proof

"$\supseteq$": ok

"$\subseteq$": For $a^m\in H$, write $m=qd+r$ with $0\leq r<d$

If $r\neq 0$, then $a^r=a^{m-qd}=\underbrace{a^m}_{H}(\underbrace{a^d}_{H})^{-1}\in H$ ↯ ($\because d$ is the least one) $\therefore r=0$, i.e. $d\mid m$

PROPOSITION 3

Let $G=\langle a\rangle$. If $|G|=n$, then $G\cong \mathbb{Z}/n\mathbb{Z}$ $(+, \bar{0})$

Proof

Define $f: G \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $a^i \longmapsto \bar{i}$

Well-defined: $a^i=a^j \Rightarrow a^{i-j}=1 \Rightarrow n \mid i-j \Rightarrow \bar{i}=\bar{j}$ ✓

Homomorphism: $f(a^i a^j)=f(a^{i+j})=\overline{i+j}=\bar{i}+\bar{j}=f(a^i)+f(a^j)$ ✓

1-1: $\bar{i}=\bar{j} \Rightarrow \overline{i-j}=\bar{0} \Rightarrow n \mid i-j \Rightarrow a^{i-j}=1 \Rightarrow a^i=a^j$ ✓

Onto: $\forall \bar{i} \in \mathbb{Z}/n\mathbb{Z}$, $f(a^i)=\bar{i}$

DEFINITION

Let $G_1, G_2 \leq G$, then G is said to be the **internal direct product** of G_1, G_2 if

$f: G_1 \times G_2 \longrightarrow G$ is an **isomorphism**

$(g_1, g_2) \longmapsto g_1 g_2$

(Notice $(g_1, g_2)\cdot(h_1, h_2)=(g_1h_1, g_2h_2)$)

REMARK

- Here, we get $G=G_1G_2=\{g_1g_2 \mid g_1\in G_1, g_2\in G_2\}$ since f is onto
- If $\exists\, 1\neq a\in G_1\cap G_2$, then $f((a,1))=a=f((1,a))$ ✱ since f is 1-1
- $\forall a\in G$, $a=g_1g_2$ and g_1, g_2 are unique for a, since $g_1g_2=g_1'g_2' \Rightarrow \underbrace{(g_1')^{-1}g_1}_{G_1}=\underbrace{g_2'(g_2)^{-1}}_{G_2}\in G_1\cap G_2=\{1\}$, i.e. $g_1=g_1'$, $g_2=g_2'$
- For $g_1\in G_1$, $g_2\in G_2$, $g_1g_2=f((g_1,1)\cdot(1,g_2))=f(g_1,g_2)$
  $g_2g_1=f((1,g_2)\cdot(g_1,1))=f(g_1,g_2)$ $\Rightarrow g_1g_2=g_2g_1$

EXAMPLES

1. $G=\mathbb{Z}/6\mathbb{Z}=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$, $G_1=\langle\bar{3}\rangle=\{\bar{0},\bar{3}\}$, $G_2=\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4}\}$ $\Rightarrow G_1\times G_2 \xrightarrow{\sim} G$
2. $(\mathbb{Z}/12\mathbb{Z})^\times=\{\bar{1},\bar{5},\bar{7},\bar{11}\}=\langle\bar{5}\rangle\times\langle\bar{7}\rangle$ ($\langle\bar{5}\rangle\cong C_2$, $\langle\bar{7}\rangle\cong C_2$)
3. $G=S_3$, $G_1=\langle(1\ 2)\rangle\cong C_2$, $G_2=\langle(1\ 2\ 3)\rangle\cong C_3$
   $\because (1\ 2\ 3)(1\ 2)\neq(1\ 2)(1\ 2\ 3)$
   $\therefore G\not\cong G_1, G_2$
   Example: $H=\langle(1\ 2)\rangle$, $K=\langle(1\ 2\ 3)\rangle \Rightarrow HK=\{id, (1\ 2), (2\ 3), (1\ 2\ 3)\}$

PROPOSITION 4

Let $H, K\leq G$. Then, $HK\in G \Leftrightarrow HK=KH$, $h_1k_1=h_1'k_1'$

Proof

"$\Rightarrow$": Notice, $H\leq HK$, $K\leq HK \Rightarrow KH\subseteq HK$ (HK a group)

$\forall hk\in HK$, $\exists\, h'k'\in HK$, s.t. $(hk)(h'k')=1 \Rightarrow hk=(k')^{-1}(h')^{-1}$, so $HK\subseteq KH$

"$\Leftarrow$": For $h_1, h_2, k_1k_2\in HK$, $(h_1k_1)(h_2k_2)^{-1}=h_1\underbrace{k_1k_2^{-1}}_{KH=HK}h_2^{-1}=h_1h'k'\in HK$

REMARK

In this case $HK\leq G$, does not imply $HK\cong H\times K$

ZORN'S LEMMA ≡ AXIOM OF CHOICE

DEFINITIONS

A **choice C** is a collection of nonempty sets

A **choice function** is defined as $f: \mathcal{C} \to \bigcup_{x\in\mathcal{C}} x$, $X \mapsto f(x) \in X$ (e.g. $\{\{0\},\{1,2\}\} \to \{0,1\}$)

If $|\mathcal{C}|<\infty$, then $\mathcal{C}=\{x_1,\dots,x_n\}$, we can pick $x_1\in X_1,\dots,x_n\in X_n$, $f: X_i \mapsto x_i \in X_i$

If $|\mathcal{C}|=\infty$, $M\neq\emptyset$? (e.g. $\mathcal{C}\subset\{TCM : T\neq\emptyset\}$)

AXIOM OF CHOICE

$\forall \mathcal{C}$, a collection of nonempty sets, $\exists$ a choice function f

DEFINITIONS

For a set S,

1. **Binary relation**: "$x\leq y$" is **partially ordered** if
   i. $x\leq x$
   ii. $x\leq y$ and $y\leq x \Rightarrow x=y$
   iii. $x\leq y$ and $y\leq z \Rightarrow x\leq z$
   $(S,\leq)$ is a **"poset"**
2. $(S,\leq)$ is **totally ordered** if $\forall x,y\in S \Rightarrow x\leq y$ or $y\leq x$
3. **Upperbound**: $T\subset S$, $t\in S$ is an **upperbound** if $t'\leq t$ $\forall t\in T$
4. **Least upperbound**: $T\subset S$, $t\in S$ is a **least upperbound** if t is an upperbound and $\forall t'\in S$ upperbound, $t'\geq t$
5. **Chain**: A nonempty ordered subset $T\subset S$

ZORN'S LEMMA

$\forall$ nonempty poset $(S,\leq)$, s.t. every chain has a least upperbound, then $\exists$ maximal element $s\in S$ (i.e. $\forall t\in S$, $t\geq s \Rightarrow s=t$)

GOAL: ZL ≡ AC (idea: for $s_1\in S$, if max ⇒ OK, if not, $s_2>s_1\cdots s_1\leq s_2\leq\dots\supset C_1$, $\exists t\geq s_i$ $\forall i$, $t_1\leq t_2\leq\dots\supset C_2 \Rightarrow C_1\leq C_2\leq C_3\leq\dots$)

PART 1: ZL ⇒ AC

For $S=\{(D,f): D\subset\mathcal{C}, f:$ choice function on $D\}$

- $S\neq\emptyset$: Pick $x\in\mathcal{C}$, $\{x\}\subset\mathcal{C}$ ✓
- $(D_1,f_1)\leq(D_2,f_2)$ if $D_1\subset D_2$, $D_2 \xrightarrow{f_2} \bigcup_{x\in D_2} x$, $D_1 \xrightarrow{f_1} \bigcup_{x\in D_1} x$
- Every chain in S has an upperbound $\to (D_T,f_T)\in S$
  For all $T\subset S$ chain, $D_T=\bigcup\{D : (D,g)\in T$ for some $g\}$
  Here,
  $f_T: D_T \to \bigcup_{x\in D_T} x$
  $X \mapsto g(X)$ if $x\in D$, $(D,g)\in T$

⇒ By **Zorn's Lemma**, $\exists$ **maximal element** $S\in(D,f)$, $D\subset\mathcal{C}$

Claim: $D=\mathcal{C}$

Proof

If not, pick $x\in\mathcal{C}\setminus D \Rightarrow D\cup\{x\}\supset D$

For the choice function $f_x: D\cup\{x\}\to\bigcup_{Y\in D} Y\cup x$, $f_x|_D=f$, $f_x(x)=x\in X \Rightarrow (D\cup\{x\},f_x)>(D,f)$ ↯

BOURBAKI'S THEOREM (≡ ZORN'S LEMMA)

For $A \neq \emptyset$, poset, every chain has a least upperbound; $f: A \to A$, s.t. $f(x) \geq x$

Then, $\exists x_0 \in A$, s.t. $f(x_0) = x_0$

PART 2: AXIOM OF CHOICE ⇒ WEAK ZORN'S LEMMA

If not, $\forall x \in S$, $\exists S \ni y > x$.

By Axiom of Choice, $\exists\ f: S \to S$

$$x \longmapsto y_x,\ y_x > x$$

Then, $\mathcal{C} = \{\{y \in S : y > x\},\ x \in S\}$

However, by Bourbaki's Theorem, $\exists\ x$, s.t. $y_x = f(x) = x$ ↯

PART 3: WEAK ZORN'S LEMMA ⇒ ZORN'S LEMMA

Let $A = \{\text{chains in } S\} \neq \emptyset$. Then for $C_1, C_2 \in A$, $C_1 \subseteq C_2$ or $C_2 \subseteq C_1$ ⇒ $(A, \leq)$ is a poset

- "$B \subset A$ is a chain"

  Here, $S \supset \bar{C} = \bigcup_{C \in B} C^{**}$ is again a chain in S.

  If $x, y \in \bar{C}$, $\exists\ x \in C_1$, $y \in C_2$, assume $C_1 \subseteq C_2$ by symmetry

By Weak Zorn's Lemma, $\exists$ max $S \supset C_0 \in A$, $\exists s \in S$, s.t. s is an upperbound of C_0

⇒ s is a maximal element (if $t \geq s$, $C_0 \cup \{t\} \geq C_0 \in A \Rightarrow C_0 \ni t \Rightarrow t \leq s \Rightarrow t = s$) □

PROOF OF BOURBAKI'S THEOREM

We use the choice function $f: S \to S$, $f(x) \geq x$, and $S = A$

Case 1: S is totally ordered

↪ for $s =$ upperbound of S, $s \leq f(s) \leq s \Rightarrow f(s) = s$

Case 2: General S

Pick $a \in S_1$, let $M = \{x \in S \mid x \geq a\}$, $f(M) \subset M$ ⇒ Replace S by M ⇒ Assume S has least element

DEFINITION

$B \subset A$ is admissable if

1. $a \in B$
2. $f(B) \subset B$
3. If T is a chain in B, then least upperbound $\in B$

For $\{B_i\}_{i \in I}$ admissable subsets ⇒ $\bigcap_{i \in I} B_i$ is admissable

⇒ $M := \bigcap \{B \subset A \mid B$ is admissable$\}$. (M is the smallest admissable s.t. $B \subset M \Rightarrow B = M$)

Claim: M is totally ordered

Proof

$E := \{c \in M \mid f(x) \leq c\ \forall x \in M,\ x < c\} \ni a$

Claim 1: $\forall c \in E$, $x \in M$, $x \leq c$ or $f(c) \leq x$

Claim 2: $E = M$, i.e. E is admissable (if it is true, by claim 2, $\forall x, y \in M$, $x \leq y$ or $y \leq f(y) \leq x$)

Proof 1

For $c \in E$, $M_c = \{x \in M \mid x \leq c$ or $f(c) \leq x\}$

Then, $a \in M_c$, where $x \in M_c \Rightarrow x \leq c$ or $f(c) \leq x$

$\therefore c \in E \Rightarrow$ if $x < c$, $f(x) \leq f(c) \Rightarrow f(x) \in M_c$ (or $f(c) \leq x \leq f(x) \Rightarrow f(x) \in M_c$)

if $x = c$, $f(x) = f(c) \Rightarrow f(x) \in M_c$

9-11-24 (WEEK 2)

COSETS AND QUOTIENT GROUPS

DEFINITION

If $f: G_1 \to G_2$ is a map, s.t. $f(a_1a_2)=f(a_1)f(a_2)\ \forall a_1,a_2\in G$, then f is a **group homomorphism**
If f is bijective, then it is a **group isomorphism**

FACT 1

- $f(1)=1$: $f(1)=f(1\cdot 1)=f(1)f(1)\Rightarrow f(1)=1$ ✓
- $f(x^{-1})=f(x)^{-1}$: $1=f(1)=f(xx^{-1})=f(x)f(x^{-1})\Rightarrow f(x^{-1})=f(x)^{-1}$ ✓
- If $\exists f^{-1}$, then f^{-1} is also a group homo: $\forall c,d\in G_2$, say $c=f(a)$, $d=f(b)$, then $cd=f(a)f(b)=f(ab)\Rightarrow f^{-1}(cd)=ab=f^{-1}(c)f^{-1}(d)$

DEFINITION

$\ker f := \{a\in G_1 \mid f(a)=1\}$. We know $\ker f \leq G_1$ ($\because f(ab^{-1})=1\Rightarrow ab^{-1}\in \ker f$)

Notice, $f(a)=f(b)$, $a\neq b \Rightarrow f(a)f(b)^{-1}=1 \Rightarrow f(ab^{-1})=1$, i.e. $ab^{-1}\in\ker f \Rightarrow a\in(\ker f)b$
Conversely, for $a'\in(\ker f)b$, say $a'=\underbrace{h}_{\in\ker f}b \Rightarrow f(a')=f(hb)=\cancel{f(h)}1f(b)=f(b)$

DEFINITION

Let $H\leq G$. For $a\in G$, $Ha:=\{ha \mid h\in H\}$ is called a **right coset** of H in G.

FACT 2

(1) For two right cosets Ha, Hb, either $Ha=Hb$ or $Ha\cap Hb=\emptyset$
(2) $\{Ha \mid a\in G\}$ forms a partition of G.

Proof
(1) If $c\in Ha\cap Hb$, say $c=\underbrace{h_1}_{\in H}a=\underbrace{h_2}_{\in H}b \Rightarrow \begin{cases} a=h_1^{-1}h_2b \Rightarrow a\in Hb \Rightarrow Ha\subset Hb \\ b=h_2^{-1}h_1a \Rightarrow Hb\subset Ha \end{cases}$, so $Ha=Hb$
(2) It is easy to see that $G=\bigcup_{a\in G} Ha$

LAGRANGE'S THEOREM

Let G be a finite group and $H\leq G$, then $|H|\,|\,|G|$
Proof
Write $G=\bigcup_{i=1}^{r} Ha_i$, where $\{Ha_1,\dots,Ha_r\}$ is the set of all right cosets of H on G
Notice, $\begin{matrix} H & \longrightarrow & Ha_i \\ x & \longmapsto & xa_i \end{matrix}$ is 1-1 since $xa_i=ya_i\Rightarrow x=y$. By definition, it is also onto.
Hence, $|H|=|Ha_i| \Rightarrow |G|=r|H| \Rightarrow |H|\,|\,|G|$

DEFINITION

r, s.t. $|G|=r|H|$ is called the **index** of H in G, denoted by $[G:H]$

COROLLARY 1

If $|G|=p$ is a prime, then $G\cong C_p\cong \mathbb{Z}/p\mathbb{Z}$
Proof
$\exists\, 1\neq a\in G$, by Lagrange's Theorem, $|\langle a\rangle|\,|\,|G| \overset{=p}{\Rightarrow} |\langle a\rangle|=1$ or p $\not\Rightarrow \Rightarrow |\langle a\rangle|=p=|G|\Rightarrow \langle a\rangle=G$

COROLLARY 2

Let $|G|<\infty$ and $1\neq a\in G$, then $a^{|G|}=1$
Proof
By Lagrange's Theorem, $\operatorname{ord}(a)=|\langle a\rangle|\,|\,|G| \Rightarrow a^{|G|}=1$

EXAMPLE ($aH \neq Ha$)

In S_3, $H = \langle (1\ 2) \rangle = \{id, (1\ 2)\}$

$(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\} \neq H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}$

REMARK

{left cosets of H} $\longleftrightarrow$ {right cosets of H}

$aH = bH \longleftrightarrow Ha^{-1} = Hb^{-1}$ — $Ha^{-1}b = H \Rightarrow a^{-1}b \in H$

$H = a^{-1}bH \Rightarrow a^{-1}b \in H$

RECALL

$G_1 \xrightarrow{f} G_2 \Rightarrow$ "f is 1-1 $\Leftrightarrow \ker f = \{1\}$"

$(\ker f)a$, $(\ker f)b$, $(\ker f)ab$; $f(a)\ f(b) = f(ab)$

QUESTION

How do we make $\{aH \mid H \in G\}$ into a group?

EXAMPLE ($(aH)(bH) := abH$, $aH = a'H$, $b = b'H$, but $(a'H)(b'H) \neq a'b'H$)

$H = \langle (1\ 2) \rangle \leq S_3$.

$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H$

$(1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\} = (2\ 3)H$

Multiply: $LHS = (2\ 3)H$, $RHS = (1\ 3)H$

WHEN DOES $(aH)(bH) = abH = a'b'H$?

Say $a = a'h_1$, $b = b'h_2$. Then, $ab = a'h_1 b'h_2 = a'b'[(b')^{-1} h_1 b'] h_2$ ($(b')^{-1} h_1 b' \in H$, $h_2 \in H$)

DEFINITION

$H \leq G$ is said to be **normal**, denoted by $H \lhd G$ if $\forall x \in G$, $xHx^{-1} \subset x$

Let $H \lhd G$, then the **quotient group** of G by H is defined to be the group $\{aH \mid a \in G\}$ under $(aH)(bH) := abH$, which is denoted by G/H

PROPERTIES

Let $H \lhd G$. Consider $G/H = \{aH \mid a \in G\}$, then the identity is H, and $(aH)^{-1} = a^{-1}H$

REMARK

The study of homomorphic images of G $\longleftrightarrow$ The study of normal subgroups of G

$f: G \to G' \longleftrightarrow \ker f$

$G \xrightarrow{f} G'$, $G/\ker f \simeq G'$

so for $x \in G$, $y \in \ker f$, $f(xyx^{-1}) = f(x)f(y)f(x)^{-1} = 1$

So, for $H \lhd G$

$G \twoheadrightarrow G/H$

$a \mapsto aH$

QUESTION

How to find a normal subgroup of G?

PROPOSITION 1

(1) If G is abelian, then $\forall H \leq G \Rightarrow H \lhd G$ ($\forall x \in G, y \in H,\ xyx^{-1} = yxx^{-1} = y$)

(2) If $H \leq G$ with $[G:H] = 2$, then $H \lhd G$

Proof: Write $G = H \cup aH = H \cup Ha$, $a \notin H \Rightarrow aH = Ha \Rightarrow aHa^{-1} = H$. Also $\forall a \in H$, $aH = H = Ha$

PROPOSITION 2

Define the center of G to be $Z_G := \{a \in G \mid ax = xa\ \forall x \in G\}$

Then, (1) $Z_G \lhd G$; (2) if G/Z_G is cyclic, then G is abelian

Proof

(1): $a, b \in Z_G$, i.e. $\begin{cases} ax = xa \Rightarrow a = xax^{-1} \\ bx = xb \Rightarrow b = xbx^{-1} \end{cases} \Rightarrow ab^{-1} = (xax^{-1})(xb^{-1}x^{-1}) = x(ab^{-1})x^{-1} \Rightarrow ab \in Z_G$

(2): Let $G/Z_G = \langle aZ_G \rangle = \{Z_G, aZ_G, a^2Z_G, \dots\}$ with $a \in G$

Then $G = \bigcup_{k \in \mathbb{Z}} a^k Z_G$

For $x, y \in G$, say $x = a^{k_1} z_1$ ($z_1 \in H$), $y = a^{k_2} z_2$ ($z_2 \in H$), $xy = (a^{k_1} z_1)(a^{k_2} z_2) = a^{k_1+k_2} z_1 z_2 = yx$

PROPOSITION 3

The commutator of G is defined to be $[G,G] := \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$ (Notice: These elements are the generators, not all elements are in this form)

Then, $[G,G] \lhd G$ and $G/[G,G]$ is abelian

Proof

$\forall x \in G$, $a \in [G,G]$, $xax^{-1} = \underbrace{(xax^{-1}a^{-1})}_{\in [G,G]} a \in [G,G]$

"$xy[G,G] = yx[G,G]$" $\longleftrightarrow$ $(xy)^{-1}yx = y^{-1}x^{-1}yx \in [G,G]$

$(x[G,G])(y[G,G]) = (y[G,G])(x[G,G])$

9-13-24 (WEEK 2)

ISOMORPHISM THEOREMS

DEFINITION

Let $H \leq G$. The normalizer of H in G is $H \leq N_G(H) := \{x \in G \mid xHx^{-1} = H\} \leq G$

FACT

$\forall H \leq K \leq N(H) \Rightarrow H \trianglelefteq K$, in particular, $H \trianglelefteq N(H)$ and "$N(H) = G \Rightarrow H \trianglelefteq G$"

FIRST ISOMORPHISM THEOREM

Let $\varphi: G_1 \to G_2$ be a group homomorphism. Then, $G_1/\ker\varphi \cong \operatorname{Im}\varphi \leq G_2$

Proof

Define $\bar{\varphi}: G_1/\ker\varphi \longrightarrow \operatorname{Im}\varphi$, $a\ker\varphi \longmapsto \varphi(a)$

- well-defined: $a\ker\varphi = b\ker\varphi \Rightarrow a^{-1}b \in \ker\varphi \Rightarrow \varphi(a^{-1}b) = 1 \Rightarrow \varphi(a)^{-1}\varphi(b) = 1 \Rightarrow \varphi(a) = \varphi(b)$
- Group homo: $\bar{\varphi}((a\ker\varphi)(b\ker\varphi)) = \bar{\varphi}(ab\ker\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(a\ker\varphi)\,\bar{\varphi}(b\ker\varphi)$
- 1-1: $\varphi(a) = \varphi(b) \Rightarrow \varphi(a)^{-1}\varphi(b) = 1 \Rightarrow \varphi(a^{-1}b) = 1 \Rightarrow a^{-1}b \in \ker\varphi \Rightarrow a\ker\varphi = b\ker\varphi$
- Onto: $\forall g \in \operatorname{Im}\varphi$, $g = \varphi(a)$ for some $a \in G_1$, so $\bar{\varphi}(a\ker\varphi) = g$

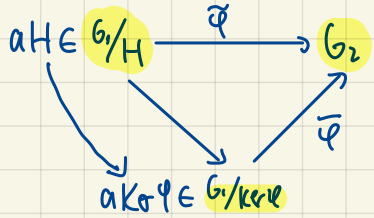
Note: $a\ker\varphi =: \bar{a}$

FACTOR THEOREM

Let $\varphi: G_1 \to G_2$ be a group homo and $H \trianglelefteq G_1$, $H \leq \ker\varphi$, then $\exists\, \bar{\varphi}: G_1/H \longrightarrow G_2$, $aH \longmapsto \varphi(a)$ ($aH = bH \Rightarrow a^{-1}b \in H \leq \ker\varphi \Rightarrow \varphi(a^{-1}b) = 1 \Rightarrow \varphi(a) = \varphi(b)$)

REMARK

$aH = bH \Rightarrow \bar{a} = \bar{b}$



Note: Group Homo means identity $\longmapsto$ identity

EXAMPLE 1

Let $G = \langle a \rangle$ with $\operatorname{ord}(a) = n$. Then $\varphi: \mathbb{Z} \longrightarrow G$, $k \longmapsto a^k$ $\Rightarrow \mathbb{Z}/n\mathbb{Z} \cong G$ ($k \in \ker\varphi \Rightarrow a^k = 1 \Rightarrow n \mid k$, i.e. $\ker\varphi = n\mathbb{Z}$)

EXAMPLE 2

$\det: GL_n(\text{over } F) \longrightarrow F^\times$

$\det(AB) = \det(A)\det(B) \Rightarrow \det$ is a group homo

Thus, $\ker\det = SGL_n(F)$. By first isom thm, $GL_n(F)/SL_n(F) \cong F^\times$

SECOND ISOMORHISM THEOREM

Let $H \leq G$ and $K \lhd G$. Then, $HK/K \cong H/H\cap K$

Proof

First, $H\leq G$ and $K\leq G \Rightarrow HK \leq G$; $K \lhd G \Rightarrow K \lhd HK$, so it is well-defined

Define $\varphi: H \to HK/K$, $h \mapsto hK$, which is a group homo

- φ is onto: $\forall hkK \in HK/K$, $hkK = hK$, so $\varphi(h) = hk = hkK$
- Find $\ker\varphi$: $h \in \ker\varphi \Leftrightarrow hK = K \Leftrightarrow h \in K \Rightarrow \ker\varphi = H\cap K$

By first isom thm, $HK/K \cong H/H\cap K$ □

EXAMPLE 3

$m\mathbb{Z}+n\mathbb{Z}/m\mathbb{Z} \cong n\mathbb{Z}/n\mathbb{Z}\cap m\mathbb{Z}$

($m\mathbb{Z}+n\mathbb{Z} = \gcd(m,n)\mathbb{Z}$, $n\mathbb{Z}\cap m\mathbb{Z} = \mathrm{lcm}(n,m)\mathbb{Z}$)

EXAMPLE 4

$G = GL_2(\mathbb{C})$, $H = SL_2(\mathbb{C})$, $K = \mathbb{C}^\times I_2$ (B)

$K = ZG \Rightarrow K \lhd G$; $\forall A \in GL_2(\mathbb{C})$, $\frac{1}{\det A} I_2 A \in SL_2(\mathbb{C}) \Rightarrow G = HK$ ($A \mapsto B(\frac{1}{\det A} I_2)$)

$\therefore$ By second isom thm, $G/K \cong H/H\cap K$ ($H\cap K = \{\pm I_2\}$)

We call $G/K = PGL_2(\mathbb{C})$, $H/H\cap K = PSL_2(\mathbb{C})$

THIRD ISOMORPHISM THEOREM

Let $K \lhd G$.

(1) $\exists$ 1-1 correspondence between $\{H \leq G \mid K \leq H\}$ and $\{\text{subgroups of } G/K\}$

(2) If $H \lhd G$ and $K \leq H$, then $\frac{G/K}{H/K} \cong G/H$

Proof

(1) Define $\varphi: \{H \leq G \mid K \leq H\} \to \{\text{subgroups of } G/K\}$, $H \mapsto H/K \leq G/K$ ($(aK)(bK)^{-1} = (ab^{-1})K$)

- φ is 1-1: Assume $H_1/K = H_2/K$. For $h_1 \in H_1$, $h_1K \in H_1/K \Rightarrow h_1K = h_2K$ for some $h_2 \in H_2$. $\Rightarrow h_1 = h_2k$ for some $k \in K \subseteq H_2 \Rightarrow h_1 \in H_2$
  $\therefore H_1 \subseteq H_2$. By symmetry, $H_1 = H_2$
- φ is onto: $\forall Q \leq G/K$, $H := f^{-1}(Q) = \{x \in G \mid xK \in Q\}$
  - ↳ $H \leq G$: $a, b \in H$, i.e. $f(a), f(b) \in Q \Rightarrow f(a)f(b)^{-1} \in Q \Rightarrow ab^{-1} \in H$ ✓
  - ↳ $K \leq H$: For $f(a) = \bar{1} \in Q$ (K (since it is $\bar{0}$ in G/K)), $a \in H \Rightarrow K \leq H$ ✓
  - ↳ $H/K \leq Q$: "$\subseteq$": $\forall x \in H$, i.e. $f(x) = xK \in Q$, so $H/K \subseteq Q$
    "$\supseteq$": $\forall xK \in Q$, i.e. $f(x) \in Q \Rightarrow x \in H$, so $Q \subseteq H/K$ ✓
- $H \lhd G$ with $K \leq H \Leftrightarrow \forall x \in G$, $xHx^{-1} = H$ and $K \leq H$
  $\Leftrightarrow \forall \bar{x} \in G/K$, $\bar{x}\, H/K\, x^{-1} = (xK)\, H/K\, (xK)^{-1} = H/K \Leftrightarrow H/K \lhd G/K$

(2) Define $\psi: G \to \frac{G/K}{H/K}$, $a \mapsto (aK)(H/K)$

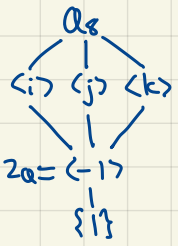
- ψ is a group homo: OK
- Onto: For $x = (aK)(H/K) \in \frac{G/K}{H/K}$, $\psi(a) = x$ ✓
- $\ker\psi$: $a \in \ker\psi \Leftrightarrow (aK)(H/K) = H/K \Leftrightarrow aK \in H/K \Leftrightarrow a \in H$

EXAMPLE 5

$\mathbb{Z}/6\mathbb{Z}/\langle\bar{3}\rangle = \mathbb{Z}/6\mathbb{Z}/3\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$

EXAMPLE 6

(1) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, $ij = k$, $jk = i$, $ki = j$, $i^2 = j^2 = k^2 = -1$



Thus, $Q_8/\langle -1\rangle = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

(2) $D_8 = \langle x, y \mid x^4 = 1, y^2 = 1, yxy^{-1} = x^{-1}\rangle$

Here, $K = \langle x^2\rangle \lhd D_8$.

Example: $(x^2y)x^2(x^2y)^{-1} = x^2(yx^2y^{-1})x^2 = x^2x^2x^2 = x^2$

So, $D_8/K \cong \langle \bar{x}, \bar{y}\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ... However, $Q_8 \not\cong D_8$.

Here, we can conclude that $G/K \cong G'/K'$, $K \cong K' \not\Rightarrow G \cong G'$

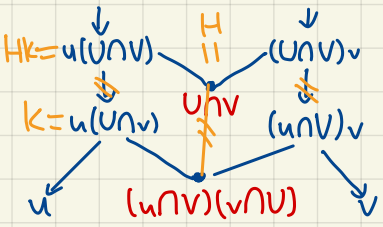
EXTENSION PROBLEM

Given two groups A, B (here $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), how to find G and $K \lhd G$, s.t. $A \cong K$ and $B \cong G/K$ (an extension of A by B)

$$1 \longrightarrow A \longrightarrow G \longrightarrow B \longrightarrow 1$$

BUTTERFLY LEMMA

Let $U, V \leq G$, $u \lhd U$, $v \lhd V$.



- $(u(U\cap V)\cap(U\cap V)v) = (U\cap V)(uU\cap v) = U\cap V$
- $(u(U\cap v)\cap(u\cap V)v) = (u\cap V)(v\cap U)$

Let $H = U\cap V$, $K = u(U\cap v) \leq UU = U \Rightarrow H \leq N(K)$: $x \in H$, $xu(U\cap v)x^{-1} = xux^{-1}(xUx^{-1})\cap(xvx^{-1}) = u(U\cap v)$

- $HK = (U\cap V)u(U\cap v) = u(U\cap V)(U\cap v) = u(U\cap V)$
- $H\cap K = (U\cap V)\cap u(U\cap v) = ((U\cap V)\cap u)(U\cap v) = (u\cap V)(U\cap v)$

By 2nd isom thm, $HK/K \cong H/H\cap K$

$$\therefore \frac{u(U\cap V)}{u(U\cap v)} \cong \frac{U\cap V}{(u\cap V)(U\cap v)}$$

9-18-24 (WEEK 3)

GROUP ACTION

DEFINITION

A group G is said to act on a set $X \neq \emptyset$, if $\exists$ a map $G \times X \longrightarrow X$, $(g, x) \longmapsto gx$, s.t.

(1) $1x = x \quad \forall x \in X$

(2) $(g_1 g_2)x = g_1(g_2 x) \quad \forall g_1, g_2 \in G, x \in X$

PROPOSITION 1

Let G be a group and $X \neq \emptyset$. Then, $\{\text{actions on } X\} \longleftrightarrow \{\text{group homo } G \longrightarrow \text{Perm}(X)\}$

Proof

Given an action of G on X, we consider $\varphi: G \longrightarrow \text{Perm}(X)$, $g \longmapsto \tau_g: X \longrightarrow X$, $x \longmapsto gx$

- $\tau_g \in \text{Perm}(X)$: 1-1: $gx = gy \Rightarrow g^{-1}(gx) = g^{-1}(gy) \Rightarrow x = y$
  Onto: $\forall y \in X$, $\tau_g(g^{-1}y) = y$
- φ is a group homo: $\varphi(g_1 g_2)(x) = \tau_{g_1 g_2}(x) = g_1 g_2 (x) = g_1(g_2 x) = \tau_{g_1}(\tau_{g_2}(x)) = \varphi(g_1)\varphi(g_2)(x) \quad \forall x \in X$

Conversely, given a group homo $\varphi: G \to \text{Perm}(X)$, $g \longmapsto \varphi(g)$, we consider $G \times X \longrightarrow X$, $(g, x) \longmapsto \varphi(g)(x) := gx$ (only define, we haven't proved it is an action)

- $1x = \varphi(1)(x) = id(x) = x \quad \forall x \in X$
- $(g_1 g_2)x = \varphi(g_1 g_2)(x) = \varphi(g_1)\varphi(g_2)(x) = g_1(g_2 x) \quad \forall x \in X, g_1, g_2 \in G$

EXAMPLE 1

$\mathbb{Z}/m\mathbb{Z} \longrightarrow GL_2(\mathbb{R})$, $\bar{k} \longmapsto \begin{pmatrix} \cos\frac{2k\pi}{m} & -\sin\frac{2k\pi}{m} \\ \sin\frac{2k\pi}{m} & \cos\frac{2k\pi}{m} \end{pmatrix}$ is a type of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ (a group action of $\mathbb{Z}/m\mathbb{Z}$ on $\mathbb{R}^2$ linearly)

A representation

EXAMPLE 2

$S_n \longrightarrow GL_n(\mathbb{R})$ ($\mathbb{R}^n \longrightarrow \mathbb{R}^n$ invertible), $\sigma \longmapsto \tau_\sigma: e_i \longmapsto e_{\sigma(i)}$ (swap cols like in σ) (a representation of S_n on $\mathbb{R}^n$)

REMARK

(1) Group actions

- φ is 1-1 $\Rightarrow$ a faithful action
- $\ker\varphi := \{g \in G \mid gx = x \ \forall x \in X\} = \bigcap_{x \in X} \{g \in G \mid gx = x\} \leq G$ (fixing x)
  $\hookrightarrow$ $G/\ker\varphi \times X \longrightarrow X$, $(\bar{g}, x) \longmapsto gx$ is faithful ($\bar{g} = \bar{g}' \Rightarrow g^{-1}g' \in \ker\varphi \Rightarrow g^{-1}g'x = x \Rightarrow g'x = gx$)

$:G_x$, stabilizer of G at x or isotropy subgroup of G at x

(2) $C(X) := \{f: X \longrightarrow \mathbb{C}\}$

If $G \curvearrowright X$, then $G \curvearrowright C(X)$ by $G \times C(X) \longrightarrow C(X)$, $(g, f) \longmapsto gf: x \longmapsto f(g^{-1}x)$ (Notice this is to preserve the order correctly)

Since $(g_1 g_2)f(x) = f((g_1 g_2)^{-1}(x)) = f(g_2^{-1} g_1^{-1}(x)) = g_2 f(g_1^{-1}x) = g_1(g_2 f)(x)$

DEFINITION

Let $G \curvearrowright X$ and $x \in X$. $Gx := \{gx \mid g \in G\}$ is called the orbit of x. (group actions)

$G \curvearrowright X$ is called a transitive action if $\exists$ only one orbit, i.e. $\forall x, y \in X, \exists g \in G$, s.t. $y = gx$ (simply)

EXAMPLE 3 (σ)

$G=\langle(1\ 2\ 3\ 4\ 5)\rangle \leq S_5$, $G \curvearrowright \{1,2,3,4,5\}$, $2=\sigma^{-3}(5)$ (transitive) (simply)

$\hookrightarrow S_5 \curvearrowright \{1,2,3,4,5\}$

└ May be only $(2\ 5)$ or have other permutations, so $\exists g \neq \sigma$.

PROPOSITION 2

Let $G \curvearrowright X$ and $x \in X$. Then, $|G_x| = [G:G_x]$. In particular, if $|G| < \infty$, then $|G| = |G_x||G_x|$

Proof

Define $\varphi = \{\text{left cosets of } G_x\} \longrightarrow G_x$

$gG_x \longmapsto gx$

- φ is well-defined and 1-1: $gG_x = g'G_x \Leftrightarrow g^{-1}g' \in G_x \Leftrightarrow g^{-1}g'x = x \Leftrightarrow gx = g'x$
- φ is onto: $\forall gx \in G_x$, $\varphi(gG_x) = gx$

ACTION BY LEFT MULTIPLICATION (Cayley Theorem)

$G \times G \longrightarrow G$, $(g, g') \longmapsto gg'$ $\Rightarrow \varphi: G \hookrightarrow \text{Perm}(G)$ (faithful) $(g \longrightarrow l_g: g' \to gg')$ (If $l_g = l_h$, i.e. $gg' = hg' \Rightarrow g = h$ $\forall g' \in G$)

(Transitive: $a, b \in G$, $g = ba^{-1} \Rightarrow ga = b$)

- Let $H \leq G$ and $X = \{\text{left cosets of } H\}$

  $G \times X \longrightarrow X$, $(g, aH) \longmapsto (ga)H$ $\Rightarrow \varphi: G \to \text{Perm}(X)$

  $a^{-1}ga \in H \Leftrightarrow g \in aHa^{-1}$; $|H| = |H^{-1}|$

  $\ker\varphi := \{g \in G \mid gaH = aH\ \forall a \in G\} = \bigcap_{a \in G} aHa^{-1} \leq H$, which is the largest normal subgroup of G contained in H

  $\because \ker\varphi \trianglelefteq G$ and $\{N \trianglelefteq G,\ N \leq H \Rightarrow N \leq \ker\varphi$

  $\therefore$ Done!

  └ $\forall a \in G$, $aNa^{-1} \leq aHa^{-1} \Rightarrow N \leq aHa^{-1}$ (normal) $\Rightarrow N \leq \bigcap_{a \in G} aHa^{-1} = \ker\varphi$

PROPOSITION 3

Let $|G| < \infty$, $H \leq G$ and $[G:H] = p$ which is the smallest prime dividing $|G|$. Then $H \trianglelefteq G$.

Proof

Let $X = \{a_1H, \dots, a_pH\}$ be the set of all left cosets of H. By left multiplication on X, we have $\varphi: G \longrightarrow S_p$

By first isom thm, $G/\ker\varphi \cong \text{Im}\varphi \leq S_p$. By Lagrange's Thm, $|G/\ker\varphi| \mid |S_p| = p! \Rightarrow |G/\ker\varphi| = 1$ or p ($\because [G:H]$ is smallest prime)

If $|G/\ker\varphi| = 1$, then $G = \ker\varphi$ ↯ ($\because \ker\varphi \leq H \lneq G$)

$\therefore |G/\ker\varphi| = p$. But we know $[G:\ker\varphi] = [G:H][H:\ker\varphi]$, thus $[H:\ker\varphi] = 1$, i.e. $H = \ker\varphi$ $\therefore H \trianglelefteq G$ □ (Ker is normal)

ACTION BY CONJUGATION

Consider $G \times G \longrightarrow G$, $(g, x) \longmapsto gxg^{-1}$ $\Rightarrow$ $\varphi: G \longrightarrow \text{Perm}(G)$, $g \longmapsto \tau_g: G \to G$, $x \mapsto gxg^{-1}$

(Orbit is all the $G \curvearrowright X$, stabilizer is when "$G \curvearrowright$" is identity)

Notice, orbit of $x = \{gxg^{-1} \mid g \in G\} = \{\text{conjugates of } x\}$

stabilizer $= \{g \in G \mid gxg^{-1} = x\} = Z_G(x)$ $\mathcal{C\ell}(x)$ ("class")

Thus, $|\mathcal{C\ell}(x)| = [G:Z_G(x)] \Rightarrow |G| = |\mathcal{C\ell}(x)||Z_G(x)|$

In fact, τ_g is a group isom with $\tau_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \tau_g(x)\tau_g(y)$

↳ We call this an automorphism, for every group isom to itself, i.e. $G \longrightarrow G$

That is, $\varphi: G \longrightarrow \text{Aut}(G) \leq \text{Perm}(G)$

$\text{Inn}(G)$ — inner automorphism

$\therefore$ By first isom thm, $G/\ker\varphi \cong \text{Inn}(G)$, and $\ker\varphi = \{g \in G \mid gx = xg\ \forall x \in G\} = Z_G$, i.e. $G/Z_G \cong \text{Inn}(G)$

H IS A NORMAL SUBGROUP

For $H \lhd G$, consider:

$$\begin{aligned} G \times H &\longrightarrow H \\ (g, x) &\longmapsto gxg^{-1} \end{aligned} \Rightarrow \varphi : G \longrightarrow \mathrm{Aut}(H) \text{ with } \ker\varphi = \{g \in G \mid gxg^{-1} = x \ \forall x \in H\} = Z_G(H)$$

($Z_G(H)$: the centralizer of H in G)

$$\Rightarrow G/Z_G(H) \leq \mathrm{Aut}(H)$$

EXAMPLE

($\tau(1\ 2\ 3\ 4\ 5)\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ \tau(5))$ is also a 5-cycle, applicable to all 5-cycles)

$\sigma = (1\ 2\ 3\ 4\ 5) \in S_5 \Rightarrow Cl_{S_5}(\sigma) = \{5\text{-cycles}\} \Rightarrow |Cl_{S_5}(\sigma)| = (5-1)! = 24$

So, $|Z_{S_5}(\sigma)| = \frac{|S_5|}{24} = 5 \Rightarrow Z_{S_5}(\sigma) = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4\}$

Now, consider $\sigma = (1\ 2\ 3\ 4\ 5) \in A_5$

Notice, $\{1, \sigma, \sigma^2, \sigma^3, \sigma^4\} \subset A_5$. As $S_5 \geq A_5$, thus $Z_{A_5}(\sigma) = Z_{S_5}(\sigma)$. Hence, $|Cl_{A_5}(\sigma)| = \frac{|A_5|}{|Z_{A_5}(\sigma)|} = \frac{60}{5} = 12$

9-20-24 (WEEK 4)

CLASS EQUATION AND CAUCHY THEOREM

OBSERVE

Consider $G \curvearrowright X$ with $|G|<\infty$, $|X|<\infty$. Write $\text{Fix}\, G = \{x \in X \mid gx = x \ \forall g \in G\}$

- For $x \in \text{Fix}\, G$, $G_x = \{x\}$ (orbit) Orbit (Gx): Elements of gx
- For $x \notin \text{Fix}\, G$, $|Gx| = \frac{|G|}{|G_x|} > 1$ (orbit, stabilizer) Stabilizer (G_x): Elements s.t. $gx = x$

Assume that $\{Gx_1, \dots, Gx_r, Gx_{r+1}, \dots, Gx_n\}$ be a set of different orbits ($Gx_1, \dots, Gx_r$: $\text{Fix}\, G$; $Gx_{r+1}, \dots, Gx_n$: not $\text{Fix}\, G$)

Then, $X = (\bigcup_{i=1}^{r} Gx_i) \cup (\bigcup_{i=r+1}^{n} Gx_i) \Rightarrow |X| = r + \sum_{i=r+1}^{n} \frac{|G|}{|G_{x_i}|}$

CLASS EQUATION

For $|G|<\infty$, consider $G \times G \xrightarrow{\text{(action by conjugation)}} G$, $(g, x) \mapsto gxg^{-1}$.

($gx = xg$)

Then, $\text{Fix}\, G = \{x \in G \mid gxg^{-1} = x \ \forall g \in G\} = Z_G$

For $x \in G$, $G_x = \{g \in G \mid gxg^{-1} = x\} = Z_G(x)$

If G is abelian, then $G = Z_G \Rightarrow G$ is easy

Otherwise, $\exists x_{r+1}, \dots, x_n \notin Z_G$, s.t. $\boxed{|G| = |Z_G| + \sum_{i=r+1}^{n} \frac{|G|}{|Z_G(x_i)|}}$ ← Class Equation (We will normally write $|G| = |Z_G| + \sum_{i=1}^{m} [G : Z_G(x_i)]$ instead)

PROPOSITION 1

Let $|G| = p^n$ (called a p-group) with p being a prime. Then $Z_G \neq \{1\}$

Proof

If $G = Z_G$, then done. Otherwise, $|G| = |Z_G| + \sum_{i=1}^{m} [G : Z_G(x_i)]$, $x_i \notin Z_G$

Notice, $x_i \notin Z_G$. $\therefore Z_G(x_i) \subsetneq G \Rightarrow p \mid \frac{|G|}{|Z_G(x_i)|}$ $\forall i$

Hence, $|Z_G| = |G| - \sum_{i=1}^{m} \frac{|G|}{|Z_G(x_i)|} \Rightarrow p \mid |Z_G|$, so $|Z_G| \neq 1$, i.e. $Z_G \neq \{1\}$

PROPOSITION 2

Let $|G| = p^2$. Then G is abelian

Proof

Assume that G is not abelian. Then, $\{1\} \subsetneq Z_G \subsetneq G \Rightarrow 1 < |Z_G| < |G| = p^2 \Rightarrow |Z_G| = p$ (Lagrange (Multiples!)), so $|G/Z_G| = p$

$\therefore G/Z_G$ is cyclic, so G is abelian. ↯

PROPOSITION 3

If $|G| = p^3$, G is not abelian, then $|Z_G| = p$

Proof

$|Z_G| = p$ or p^2. If $|Z_G| = p^2$, $|G/Z_G| = p \Rightarrow G/Z_G$ is cyclic $\Rightarrow G$ is abelian ↯ $\therefore |Z_G| = p$ □

PROPOSITION 4

If $|G| = p^n$, then $\forall 0 \le k \le n$, $\exists G_k \lhd G$, s.t. $|G_k| = p^k$ and $G_i \subsetneq G_{i+1}$ $\forall i = 0, \dots, n-1$ (i.e. $\{1\} \lhd G_1 \lhd \dots \lhd G_{n-1} \lhd G_n = G$ (G_{n-1}: p^{n-1}, G_n: p^n)) G is "solvable"

Proof

By induction on n,

- $n=1$: $G = C_p$ ✓
- $n>1$: Assume that the statement holds for $n-1$.

  By prop 1, $Z_G \neq \{1\} \Rightarrow \exists 1 \neq a \in Z_G$, say $\text{ord}(a) = p^k \Rightarrow \text{ord}(a^{p^{k-1}}) = p$. We denote $a' = a^{p^{k-1}} \in Z_G \Rightarrow \langle a' \rangle \lhd G$, $|\langle a' \rangle| = p \Rightarrow |G/\langle a' \rangle| = p^{n-1}$

  $\therefore$ By induction hypothesis, $\exists \overline{G_k} \lhd G/\langle a' \rangle$, s.t. $|\overline{G_k}| = p^k$ and $\overline{G_i} \subsetneq \overline{G_{i+1}}$ $\forall i = 0, \dots, n-2$

  ($\overline{G_{k+1}} = G_{k+1}/\langle a' \rangle \Rightarrow G_{k+1} \lhd G$, $G_0 := \{1\}$)

Then, $|G_{k+1}| = p^{k+1}$ and $G_i \trianglelefteq G_{i+1}$ $\forall i = 0, \dots, n-1$. □

USEFUL PROPOSITION

Let G be a p-group. If G acts on a finite set X, then $|\mathrm{Fix}\, G| \equiv |X| \pmod p$

Proof

If $X = \mathrm{Fix}\, G$, then $|X| = |\mathrm{Fix}\, G|$ ✓

Otherwise, $|X| = |\mathrm{Fix}\, G| + \sum_{i=k+1}^{n} [G : G_{x_i}]$, $x_{k+1}, \dots, x_n \notin \mathrm{Fix}\, G$ $\therefore |X| \equiv |\mathrm{Fix}\, G| \pmod p$

($\equiv 0 \pmod p$, since it is $\sum \frac{|G|}{|G_{x_i}|}$, G is a p-group, so $|G|$ only has mod $p \equiv 0$ factors)

CAUCHY THEOREM

If $p \mid |G|$ with p being a prime, then $\exists\, a \in G$, s.t. $\mathrm{ord}(a) = p$ ($|G| = 2468 \Rightarrow \exists\, a \in G$, $\mathrm{ord}(a) = 617$)

Proof

Let $X = \{(a_1, \dots, a_p) \in G \times \dots \times G \mid a_1 a_2 \cdots a_p = 1\}$

Consider the action of $\mathbb{Z}/p\mathbb{Z}$ on X:

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} \times X &\longrightarrow X \\ (\bar{k}, (a_1, \dots, a_p)) &\longmapsto (a_{k+1}, \dots, a_p, a_1, \dots, a_k) \end{aligned}$$

(Well-defined: $ab = 1 \Rightarrow ba = 1$ in a group $\therefore a_{k+1} \cdots a_p a_1 \cdots a_k = 1$)

By the above proposition, $|X| \equiv |\mathrm{Fix}^{\mathbb{Z}/p\mathbb{Z}}| \pmod p$

Also, $|X| = |G|^{p-1}$ since $a_1, \dots, a_{p-1}$ can be chosen arbitrarily, then $a_p = (a_1 \cdots a_{p-1})^{-1}$

Observe, $(a_1, \dots, a_p) \in \mathrm{Fix}^{\mathbb{Z}/p\mathbb{Z}} \Rightarrow (a_1, \dots, a_p) = (a_2, \dots, a_p, a_1) = \dots$

$\Rightarrow a_1 = a_2 = \dots = a_p$, i.e. $(a_1, \dots, a_p) = (a, \dots, a)$ and $a^p = 1$

$\because |X| \equiv |\mathrm{Fix}^{\mathbb{Z}/p\mathbb{Z}}| \pmod p$, $|X| = |G|^{p-1} \equiv 0 \pmod p$, and also $(1, \dots, 1) \in \mathrm{Fix}^{\mathbb{Z}/p\mathbb{Z}}$ ($|\mathrm{Fix}^{\mathbb{Z}/p\mathbb{Z}}| \neq 0$)

$\therefore |\mathrm{Fix}^{\mathbb{Z}/p\mathbb{Z}}| \geq p$, i.e. $\exists\, 1 \neq a$, s.t. $(a, \dots, a) \in \mathrm{Fix}^{\mathbb{Z}/p\mathbb{Z}}$, $a^p = 1$ □

APPLICATION (G IS NON-ABELIAN, $|G| = p^3$, odd p, $\exists\, a \in G$ s.t. $\mathrm{ord}(a) = p^2 \Rightarrow |Z_G| = p$)

Notice, $|G/Z_G| \neq p^2$: If $\exists\, \bar{a} \in G/Z_G$ with $\mathrm{ord}(\bar{a}) = p^2$, then $G/Z_G = \langle \bar{a} \rangle$ is cyclic $\Rightarrow G$ is abelian ↯

$\therefore \forall\, 1 \neq \bar{a} \in G/Z_G$, $\mathrm{ord}(\bar{a}) = p$, i.e. $\bar{a}^p = \bar{1} \Rightarrow a^p Z_G = Z_G \Rightarrow a^p \in Z_G$

We can define φ:

$$\begin{aligned} G &\longrightarrow Z_G \\ a &\longmapsto a^p \end{aligned}$$

(Hope φ is a group homo, i.e. $\forall a, b \in G$, $a^p b^p = (ab)^p$)

(Surjective: not possible $\because \forall g \in G$, $\mathrm{ord}(g) = n$)

Also, $|G/Z_G| = p^2 \Rightarrow G/Z_G$ is abelian $\Rightarrow [G, G] \leq Z_G$

However, $\because G$ is not abelian, $|Z_G| = p$ $\therefore |[G, G]| = p \Rightarrow [G, G] = Z_G$

Define $[b, a] := b^{-1} a^{-1} b a$. (commutative, since in Z_G)

Then, $a^p b^p = a^p b^p [b, a]^{\frac{p(p-1)}{2}} = a^p b [b, a] b^{p-1} [b, a]^{p-1} = a^{p-1} b [b, a] a b^{p-1} [b, a]^{p-2} = a^{p-2} b a^2 b^{p-1} [b, a]^{p-2} = \dots = aba^{p-1} b^{p-1} [b, a]$ ($[b, a]^{p+1}$)

$= (ab)^2 a^{p-2} b^{p-2} [a, b]^3 = \dots = (ab)^{p-1} (ab) [b, a]^{1+2+\dots+(p-1)} = (ab)^p$

Thus, $\exists\, a^p \in Z_G \Rightarrow \mathrm{Im}\, \varphi = Z_G$ ($a^p \in \mathrm{Im}\, \varphi$, but $|\mathrm{Im}\, \varphi| = 1$ or p, so $|\mathrm{Im}\, \varphi| = p \Rightarrow \mathrm{Im}\, \varphi = Z_G$)

Now, if $|\ker \varphi| = p^2$, then $\ker \varphi$ is abelian, and $\forall\, b \in \ker \varphi$, $b^p = 1$

Pick $1 \neq b \in \ker \varphi$ and $1 \neq c \in \ker \varphi \setminus \langle b \rangle$ ($|\ker \varphi| \geq |\langle b \rangle| > 1$)

Set $H = \langle b \rangle$, $K = \langle c \rangle$

- $H \cap K = \{1\}$ since $|H \cap K| \mid |H| = p$ ($\because K \neq H$, so $H \cap K \neq H$)
- $HK = KH$

} $\Rightarrow \ker \varphi = HK$, $\exists!\, h \in H$, $k \in K$, s.t. $x = hk$

- $\ker \varphi \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (Notice if $x_1 = h_1 k_1$, $x_2 = h_2 k_2 \Rightarrow x_1 x_2 = h_1 k_1 h_2 k_2 = (h_1 h_2)(k_1 k_2)$)

$$\begin{aligned} x &\longmapsto (h, k) \end{aligned}$$

For abelian G, if $|G| = p^2$, then $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

Similarly, for abelian G, if $|G| = p^3$, then $G \cong \mathbb{Z}/p^3\mathbb{Z}$ or $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

9-25-24 (WEEK 4)

SYLOW THEOREM AND SEMIDIRECT PRODUCT

DEFINITION

Let $|G|=p^\alpha r$ with $p \nmid r$

- A subgroup of order p^α is called a Sylow p-subgroup of G
- $\mathrm{Syl}_p(G)$ = the set of all Sylow p-subgroups
- $n_p := |\mathrm{Syl}_p(G)|$

KEY LEMMA

Let $P \in \mathrm{Syl}_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$

Proof

"$\supseteq$": OK, since $P \subseteq N_G(P)$

"$\subseteq$": Let $H = Q \cap N_G(P)$

By Lagrange's Thm, $|H| \mid |Q| \Rightarrow H$ is a p-subgroup or $\{1\}$

$\because P \trianglelefteq N_G(P)$ $\therefore HP \leq N_G(P) \leq G$ and in $N_G(P)$, $HP/P \cong H/H \cap P \Rightarrow |HP| = \frac{|H||P|}{|H \cap P|}$

Assume $|H| = p^k$, $|P| = p^\alpha$, $|H \cap P| = p^s \Rightarrow |HP| = p^{\alpha+k-s} \mid |G| = p^\alpha r$, thus $k = s \Rightarrow H = H \cap P$. $\because H \subseteq Q$ $\therefore H \subseteq P \cap Q$ ✓ ($k \geq s$ by def)

SYLOW I

$\forall 0 \leq k \leq \alpha$, $\exists H \leq G$, s.t. $|H| = p^k$. In particular, $\mathrm{Syl}_p(G) \neq \emptyset$ (Special case of converse of Lagrange's Thm)

Proof

By induction on $|G|$,

- $|G| = 1$: Thus, $G = \{1\}$, $k = 0 \Rightarrow H = \{1\}$ ✓
- Assume that $|G| > 1$, $\alpha \geq 1$, $k \geq 1$
- **Case 1: $p \mid |Z_G|$**

  By Cauchy Thm, $\exists a \in Z_G$, with $\mathrm{ord}(a) = p$

  Since $\langle a \rangle \trianglelefteq G$ and $|G/\langle a \rangle| < |G|$, and if $k = 1$, $H = \{a\}$ (order p), by induction hypothesis, $\exists H' \leq G/\langle a \rangle$, s.t. $|H'| = p^{k-1}$ ($|G/\langle a \rangle| = p^{\alpha-1} r$)

  By the third isom thm, we can write $H' = H/\langle a \rangle \Rightarrow |H| = p^k$

Case 2: $p \nmid |Z_G|$

By the class equation, $|G| = |Z_G| + \sum_{i=1}^{m} \frac{|G|}{|Z_G(a_i)|}$, $a_i \notin Z_G$

Thus, $p \nmid \sum_{i=1}^{m} \frac{|G|}{|Z_G(a_i)|}$, which means $\exists j$, s.t. $|Z_G(a_j)| = p^\alpha r'$ (max, so dividing would not have remainder k)

$\because Z_G(a_j) \nleq G$

$\therefore$ By induction hypothesis, $\exists H \leq Z_G(a_j) \leq G$, s.t. $|H| = p^k$

SYLOW II

OBSERVE

$P \leq G \Rightarrow aPa^{-1} \leq G$ (all Syl_p can be conj?)

P: Syl_p $\quad$ aPa^{-1}: Syl_p

THEOREM

Let $P \in Syl_p(G)$ and Q be p-subgroups of G. Then $\exists\, a \in G$, s.t. $Q \leq aPa^{-1}$. In particular, $Q \in Syl_p(G)$, $|Q| = |aPa^{-1}| \Rightarrow Q = aPa^{-1}$

Proof

Let $X = \{\text{left cosets of } P\}$ and consider $\begin{aligned} Q \times X &\longrightarrow X \\ (a,\ xP) &\longmapsto axP \end{aligned}$ (Recall useful proposition: $|X| \equiv |Fix\, Q| \pmod p$)

Also, $xP \in Fix\, Q \Leftrightarrow axP = xP\ \forall a \in Q \Leftrightarrow x^{-1}ax \in P\ \forall a \in Q \Leftrightarrow a \in xPx^{-1}\ \forall a \in Q \Leftrightarrow Q \leq xPx^{-1}$

Notably, since $|X| = \frac{|G|}{|P|} = r \not\equiv 0 \pmod p$, thus $|Fix\, Q| \neq 0$.

Take $aP \in Fix\, Q \Rightarrow Q \leq aPa^{-1}$

SYLOW III

$n_p \equiv 1 \pmod p$, $n_p \mid |G| \Rightarrow n_p \mid r$ ($\because n_p \nmid p$)

Proof

- For $P \in Syl_p(G)$, consider $\begin{aligned} P \times Syl_p(G) &\longrightarrow Syl_p(G) \\ (a,\ Q) &\longmapsto aQa^{-1} \end{aligned}$ (Always find Fix when doing group actions!)

  Notice, $Q \in Fix\, P \Leftrightarrow aQa^{-1} = Q \Leftrightarrow P \leq N_G(Q)$

  By key lemma, $P = P \cap N_G(Q) = P \cap Q \Rightarrow P = Q$ ($\because Q$ is also Sylow, and P has max card for Sylow)

  That is, $Fix\, P = \{P\}$, then by useful proposition, $|Syl_p G| \equiv |Fix\, P| \pmod p \Rightarrow n_p \equiv 1 \pmod p$
- Otherwise, consider (G: larger) $\begin{aligned} G \times Syl_p(G) &\longrightarrow Syl_p(G) \\ (a,\ P) &\longmapsto aPa^{-1} \end{aligned}$

  By Sylow II, the orbit of $P = Syl_p(G)$. Hence, $n_p = |Syl_p(G)| = \frac{|G|}{|G_p|}$, $G_p = \{a \in G \mid aPa^{-1} = P\} = N_G(P)$ (stabilizers), so $n_p = \frac{|G|}{|N_G(P)|}$

  As $|G| = p^\alpha r$, $|N_G(P)| = p^\alpha r' \Rightarrow n_p \mid r$

COROLLARY

$n_p = 1$, i.e. $Syl_p(G) = \{P\} \Leftrightarrow P \trianglelefteq G$

EXAMPLE

No group G of order 48 is simple (No proper normal subgroup)

Proof

Let $|G| = 48 = 2^4(3)$

If $n_2 = 1$, then $P \in Syl_2(G) \Rightarrow P \trianglelefteq G$

Otherwise, $n_2 = 1 + 2k \mid 3 \Rightarrow n_2 = 3$

Let $X = \{\text{left cosets of } P \in Syl_2(G)\}$, and consider $\begin{aligned} G \times X &\longrightarrow X \\ (a,\ xP) &\longmapsto axP \end{aligned} \Rightarrow \varphi : G \longrightarrow Perm(X) = S_3$

$\because |G| = 48 > |S_3| = 6$

$\therefore Ker\, \varphi \neq \{1\}$

We know $Ker\, \varphi \leq P$, thus $Ker\, \varphi \trianglelefteq G$

SEMI-DIRECT PRODUCT

FACT 1

$K \trianglelefteq G$, $H \trianglelefteq G$, $K \cap H = \{1\} \Rightarrow KH \cong K \times H$ ($\forall k \in K, h \in H$, $\underbrace{khk^{-1}}_{\in K} h^{-1} \in H \cap K = \{1\} \Rightarrow hk = kh$)

FACT 2

For two groups K, H, consider $G = K \times H$, which is a group, under $(k_1, h_1)(k_2, h_2) = (k_1k_2, h_1h_2)$

Now, let $K' = K \times \{1\} \trianglelefteq (K \times H)$, $H' = H \times \{1\} \trianglelefteq (K \times H) \Rightarrow \underbrace{K' \cap H' = \{1\}}_{\text{makes it a direct product}}$. Actually, $K'H' = G = K \times H$

OBSERVE

$\begin{cases} K \leq G,\ H \trianglelefteq G \\ K \cap H = \{1\} \end{cases} \Rightarrow KH \leq G$ and $KH \xleftrightarrow{\text{1-1 correspondence}} K \times H$ as a set

$kh \longleftrightarrow (k, h)$

Consider its group operation,

$(k_1h_1)(k_2h_2) = k_1k_2(k_2^{-1}h_1k_2)h_2 = k_1k_2h_3h_2$ ✯ Notice how h_1 needs to be converted into $h_3 = k_2^{-1}h_1k_2$

(H is normal)

If we define the inner automorphism $\tau_{k_2^{-1}}$, $(\mathrm{Aut}(H))$

$\tau_{k_2^{-1}} : H \longrightarrow H$

$h \longmapsto k_2^{-1}hk_2$

Then, we can have $(k_1h_1)(k_2h_2) = k_1k_2\tau_{k_2}(h_1)h_2$

$\therefore$ We can write $KH \cong K \overset{\times}{\tau} H$ (semi-direct product)

DEFINITION

For two groups K, H and a group homo $\tau : K \longrightarrow \mathrm{Aut}(H)$, $K \overset{\times}{\tau} H = \{(k,h) \mid k \in K,\ h \in H\}$ (Normal $\times$)

$(k_1, h_1)(k_2, h_2) = (k_1k_2, [\tau(k_2^{-1})(h_1)]h_2)$

- Identity : $(1, 1)$ ✓
- $(k,h)^{-1} = (k^{-1}, \tau(k)(h^{-1}))$: $(k,h)(k^{-1}, \tau(k)(h^{-1})) = (1, \tau(k)(h)\tau(k)(h^{-1})) = (1, \tau(k)(1)) = (1,1)$ ✓

  $(k^{-1}, \tau(k)(h^{-1}))(k,h) = (1, \tau(k^{-1})(\tau(k)(h^{-1}))\,h) = (1, k^{-1}(kh^{-1}k^{-1})kh) = (1,1)$ ✓
- $K \cong K \times \{1\}$: $(k_1, 1)(k_2, 1) = (k_1k_2, \tau(1^{-1})(1)(1) = (k_1k_2, 1)$ ✓
- $H \cong \{1\} \times H$: $(1, h_1)(1, h_2) = (1, \tau(1^{-1})(h_1)(h_2)) = (1, h_1h_2)$ ✓
- $\tau(k)(h) = khk^{-1}$: $(k,1)(1,h)(k,1)^{-1} = (k, \tau(1^{-1})(1)(h))(k^{-1}, \tau(k)(1^{-1})) = (k,h)(k^{-1}, 1) = (1, \tau(k)(h)(1)) = (1, khk^{-1})$ ✓
- $H \trianglelefteq (K \overset{\times}{\tau} H)$: $(k,h)(1,h')(k,h)^{-1} = (k, hh')(k^{-1}, \tau(k)(h^{-1})) = (1, \tau(k)(hh')\tau(k)(h^{-1})) = (1, \tau(k)(hh'h^{-1})) \in H$ ✓

COROLLARY

If τ is trivial, i.e. $\tau : K \longrightarrow \mathrm{Aut}(H)$, $k \longmapsto \mathrm{id}$ (id), then $K \overset{\times}{\tau} H \cong K \times H$ since $(k_1, h_1)(k_2, h_2) = (k_1k_2, \tau(k_2^{-1})(h_1)(h_2) = (k_1k_2, h_1h_2)$

EXAMPLE

Construction of a non-abelian group of order 21

Let $H = C_7$, $K = C_3$. We need "$\tau : K \longrightarrow \mathrm{Aut}(H)$".

$\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/7\mathbb{Z}^{\times}$

$\tau \longmapsto \varphi_2$

Notice, to find something in $\mathbb{Z}/7\mathbb{Z}$ of order 3

$\mathbb{Z}/7\mathbb{Z} \xrightarrow{\varphi_2} \mathbb{Z}/7\mathbb{Z}$

$\bar{1} \longmapsto \bar{1}\ (=\bar{8})$

Then, $G = K \overset{\times}{\tau} H$

REMARK

Notice, $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^{\times}$

$\varphi_k \longmapsto \bar{k}$

- $\varphi_{k_1} \circ \varphi_{k_2}(\bar{1}) = \varphi_{k_1}(\underbrace{\bar{1} + \ldots + \bar{1}}_{k_2 \text{ times}}) = \varphi_{k_1}(\bar{1}) + \ldots + \varphi_{k_1}(\bar{1}) = \bar{k}_1 + \ldots + \bar{k}_1 = \overline{k_1k_2} = \varphi_{k_1k_2}(\bar{1})$

9-27-24 (WEEK 4)

CLASSIFICATIONS

PROPOSITION 1

Let $|G|=pq$ where p,q are prime with $p<q$, $q\not\equiv 1 \pmod p$. Then, $G\cong \mathbb{Z}/pq\mathbb{Z}$

Proof

By Sylow III, $\begin{cases} n_p = 1+pk \mid q \Rightarrow n_p = 1 \Rightarrow \exists!\, H\in Syl_p(G),\ H\trianglelefteq G \\ n_q = 1+qh \mid p \Rightarrow n_q = 1 \Rightarrow \exists!\, K\in Syl_p(G),\ K\trianglelefteq G \end{cases}$

Notice, $|H\cap K| \mid \frac{|H|}{|K|} \Rightarrow |H\cap K|=1 \Rightarrow H\cap K=\{1\}$

So, $KH\cong K\times H\cong C_q\times C_p\cong \mathbb{Z}/q\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z} \Rightarrow |KH|=pq \Rightarrow G=\underbrace{KH}_{\langle a\rangle}\cong \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ (Note: $(\mathrm{ord}(a),\mathrm{ord}(b))=1$ + "$ab=ba$" $\Rightarrow \mathrm{ord}(ab)=\mathrm{ord}(a)\mathrm{ord}(b)$)

EXAMPLE 1

$|G|=255=3(5)(17) \Rightarrow G$ is abelian

By Sylow III, $n_{17}=1+17k \mid 15 \Rightarrow n_{17}=1 \Rightarrow \exists!\, H\in Syl_p(G),\ H\trianglelefteq G$

Also, $|G/H|=15 \Rightarrow G/H$ is abelian $\Rightarrow [G,G]\le H$, i.e. $|[G,G]|\mid |H|=17$

Claim: At least one of Sylow 3-subgroup or Sylow 5-subgroup is normal

Proof

$n_3=1+3k \mid 85 \Rightarrow n_3=1$ or 85

$n_5=1+5k \mid 51 \Rightarrow n_5=1$ or 51

If not, $n_3=85$ and $n_5=51$.

$\Rightarrow \exists$ 170 elements of order 3 ; $\exists$ 204 elements of order 5

However, $170+204>255$ ↯ Thus, the claim is true. □

Now, assume that $\exists!\, K\in Syl_3(G)$ with $K\trianglelefteq G \Rightarrow |G/K|=5(17) \Rightarrow G/K$ is abelian

$\therefore |[G,G]|\,|K|=3$ and $|[G,G]|\,|17 \Rightarrow [G,G]=\{1\}$, i.e. G is abelian

Moreover, $G\cong H\times K\times \underbrace{Q}_{\in Syl_5(G)}\cong C_{17}\times C_3\times C_5\cong C_{255}$

PROPOSITION 2

If $|G|=30$, then both $P\in Syl_3(G)$ and $Q\in Syl_5(G)$ are normal

Proof

By Sylow III, $n_5=1+5k \mid 6 \Rightarrow n_5=1$ or 6

$n_3=1+3h \mid 10 \Rightarrow n_3=1$ or 10

However, $4(6)+2(10)=44>30 \Rightarrow$ either P or Q is normal

Hence, $PQ\le G$ and $|PQ|=15 \Rightarrow \begin{cases} PQ\trianglelefteq G \text{ since } [G:PQ]=2 \\ PQ\cong \mathbb{Z}/15\mathbb{Z} \end{cases}$

Now, $\forall a\in G$, $aPa^{-1}\le aPQa^{-1}=PQ \Rightarrow aPa^{-1}\in Syl_3(PQ)=\{P\}$, so $aPa^{-1}=P$. Similarly, $Q\trianglelefteq G$

PROPOSITION 3

$|G|=12=2^2(3) \Rightarrow$ either G has a normal Sylow 3-subgroup or $G\cong A_4$

Proof ⌜ normal Sylow 3-subgroup

By Sylow III, $n_3=1+3k \mid 4 \Rightarrow n_3=1$ or 4

Assume $n_3=4$, $H\in Syl_p(G)$, let $X=\{\text{left cosets of } H\}$. Consider $G\times X\longrightarrow X \Rightarrow \varphi: G\to S_4$

$(a, xH)\longmapsto axH$

Recall, $\ker\varphi$ is the largest normal subgroup contained in H. However, $|H|=3$ and $H\not\trianglelefteq G$ ($n_3=4$) $\Rightarrow \ker\varphi=\{1\}$. Thus, $G\hookrightarrow S_4$

Notice, there are $(3-1)(4)=8$ elements of order 3 in G and there are precisely 8 elements of order 3 in S_4 (i.e. 3-cycles) all contained in A_4. So, $|\mathrm{Im}\varphi \cap A_4| \geq 8$. However, $|\mathrm{Im}\varphi \cap A_4| \,|\, |A_4| = 12 \Rightarrow \mathrm{Im}\varphi \cap A_4 = A_4 \Rightarrow \mathrm{Im}\varphi = A_4$

EXAMPLE 2

$|G|=8$: Case 1: G is abelian $\Rightarrow G \cong \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ($\{1, a, a^2, a^3, b, ab, b^3, ab^2\}$)

Case 2: G is non-abelian

- $\nexists\, a \in G$, s.t. $\mathrm{ord}(a)=8$
- Not all $a \in G$ has $\mathrm{ord}(a)=2$ ($\because \forall a \in G,\ a^2=1 \Rightarrow G$ is abelian)
- $\exists\, a \in G$ with $\mathrm{ord}(a)=4$.

Thus, let $H=\langle a \rangle \Rightarrow H \lhd G$ since $[G:H]=2$

Take $b \notin H$ and $K=\langle b \rangle$. Then, $H \lneq KH \leq G \Rightarrow [G:H]=[G:KH][KH:H] \Rightarrow (G:KH]=1 \Rightarrow G=KH$ ($[KH:H]=1$)

↳ Case 2a: $\mathrm{ord}(b)=2$: $\because K \cap H = \{1\}$ $\therefore G \cong K \rtimes_{\varphi} H$ for $\tau: K=\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong C_2$ ($\because$ Either $\bar{1} \mapsto \bar{1}$ or $\bar{3}$)

$\bar{b} \longmapsto \varphi_{\bar{3}}(b): a \longmapsto a^3$

(identity is trivial, ignore)

Thus, $\varphi_{\bar{3}}(b)(a) = bab^{-1} = a^3$, so $G = \langle a, b \mid a^4=1,\ b^2=1,\ bab^{-1}=a^3=a^{-1} \rangle \cong D_8$

↳ Case 2b: $\mathrm{ord}(b)=4$

Notice, $K \cap H \neq \{1\}$, since $|KH| = 16 > 8$ ⟶

$\therefore |K \cap H| = 2 \Rightarrow a^2 = b^2 \in K \cap H$

Also, $H \lhd G \Rightarrow bab^{-1} = 1, \cancel{a}, a^2, a^3$

If $bab^{-1}=a^2$, then $a = a^2 a a^{-2} = b^2 a b^{-2} = ba^2b^{-1} = (bab^{-1})^2 = a^4 \Rightarrow a^3 = 1$ ⟶

Hence, $bab^{-1}=a^3=a^{-1}$ and $G = \langle a, b \mid a^4=b^4=1,\ a^2=b^2,\ bab^{-1}=a^{-1} \rangle \cong Q_8$

$\varphi: G \longrightarrow Q_8$

$1 \longmapsto 1$ $\quad a^2 \longmapsto -1$

$a \longmapsto i$ $\quad a^3 \longmapsto -i$

$b \longmapsto j$ $\quad a^2b \longmapsto -j$

$ab \longmapsto k$ $\quad a^3b \longmapsto -k$

PROPOSITION 4

We classify groups of order p^3, for odd p

- G is abelian $\Rightarrow G \cong \mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Proof

Case 1: G is abelian

We know that $|Z_G| = p$ and $\varphi: G \longrightarrow Z_G$ is a group homo, $x \longmapsto x^p$

Case 1.1: $\exists\, a \in G$, s.t. $\mathrm{ord}(a)=p^2$

Let $H=\langle a \rangle$. Since $[G:H]=p$ is the smallest prime dividing $|G|$, $H \lhd G$

Also, $\because 1 \neq a^p \in Z_G$ $\therefore \ker\varphi \neq G$, $\mathrm{Im}\varphi = Z_G \Rightarrow |G/\ker\varphi| = |Z_G| = p \Rightarrow |\ker\varphi| = p^2$.

However, $\forall x \in \ker\varphi$, $\mathrm{ord}(x) = p$. Thus, $\ker\varphi \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

It is clear that $H \cap E = \langle a^p \rangle$

Pick $b \in E \setminus H$ and $K = \langle b \rangle \Rightarrow K \cap H = \{1\} \Rightarrow G \cong K \rtimes_{\tau} H$ for $\tau: K \longrightarrow \mathrm{Aut}(H) \cong \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$

$\forall f \in \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$, $f: \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z}$, where $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^{\times}$

$\bar{1} \longmapsto \bar{k} \leftarrow (k, p^2) = 1$

Fact: $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is cyclic

Claim: $(\mathbb{Z}/p^2\mathbb{Z})^{\times}$ is cyclic

Proof

Notice, $|(\mathbb{Z}/p^2\mathbb{Z})^{\times}| = p(p-1)$

Observe: $(1+p)^p \equiv 1 \pmod{p^2}$, $(1+p) \not\equiv 1 \pmod{p^2} \Rightarrow \langle \overline{(1+p)} \rangle$ is a cyclic p-subgroup of $(\mathbb{Z}/p^2\mathbb{Z})^{\times}$

Consider $(\mathbb{Z}/p^2\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$

$\overline{k} \mapsto \overline{k}$

We notice that all Sylow $p \neq q$-subgroups of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ correspond to all Sylow q-subgroups of $(\mathbb{Z}/p\mathbb{Z})^\times$ which are cyclic

$\therefore (\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/p\mathbb{Z} \times C_{q_1^{k_1}} \times \dots \times C_{q_m^{k_m}} \cong C_{pq_1^{k_1}\cdots q_m^{k_m}} = C_{p(p-1)}$ □

Since $\mathrm{Aut}(H) \cong \mathbb{Z}/p(p-1)\mathbb{Z}$, $\exists!$ subgroup of order p in $\mathbb{Z}/p(p-1)\mathbb{Z}$ that is $\langle \overline{(1+p)} \rangle$

Thus, $\tau : K \xrightarrow{\cong \langle b \rangle} \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong \mathbb{Z}/p(p-1)\mathbb{Z}$

$b \mapsto \tau(b)(a) = a^{1+p}$

$\therefore G = \langle a, b \mid a^{p^2} = 1, b^p = 1, bab^{-1} = a^{p+1} \rangle$

Case 1.1.1: $\forall$ elements of G, G has order p

$\because G$ is a p-group $\therefore \exists H < G$ with $|H| = p^2 \Rightarrow H \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ← 2D vector space over $\mathbb{Z}/p\mathbb{Z}$

$\langle a, b \mid a^p = 1, b^p = 1, ab = ba \rangle$

$|GL_2(\mathbb{Z}/p\mathbb{Z})| = p(p-1)^2(p+1)$

As $H \trianglelefteq G$, let $c \in G \setminus H$ and $K = \langle c \rangle$. Then, $H \cap K = \{1\} \Rightarrow G \cong K \ltimes_\tau H$ for some $\tau : K \longrightarrow \mathrm{Aut}(H) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$

Observe, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ and $\mathrm{ord}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = p$

$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{Aut}(H) \to \rho : \begin{matrix} a \mapsto ab \\ b \mapsto b \end{matrix} \Rightarrow \tau(c)(a) = ab \Rightarrow cac^{-1} = ab,\ \tau(c)(b) = b \Rightarrow cbc^{-1} = b$

Hence, $G = \langle a, b, c \mid a^p = 1, b^p = 1, c^p = 1, ab = ba, cb = bc, cac^{-1} = ab \rangle$

(The rest are isom, since $\tau(K) \in \mathrm{Syl}_p(\mathrm{Aut}(H))$)

10-2-24 (WEEK 5)

RINGS AND MODULES

A ring is made of an Abelian group, denoted with addition and an operation called multiplication which only has identity and associative operation.

DEFINITION

A ring is a nonempty set R with two operations $R \times R \to R$, $(a,b) \mapsto a+b,\ a\cdot b$, s.t.

(1) $(R,+,0)$ is an abelian group
(2) $(R,\cdot,1)$ is a monoid
(3) Distributive Laws: $\forall a,b,c \in R$, we have $a\cdot(b+c)=a\cdot b+a\cdot c$ and $(b+c)\cdot a = b\cdot a + c\cdot a$

↳ $a \in R$ is called a unit if $\exists\, a^{-1} \in R$
↳ $R^\times = \{\text{units of } R\}$
↳ R is called a division ring if $R^\times = R\setminus\{0\}$
↳ R is said to be commutative if $\forall a,b \in R$, $a\cdot b = b\cdot a$
↳ R is called a field (perfect multiplication) if R is a commutative division ring

Let $a \in R$. If $\exists\, b \neq 0 \in R$, s.t. $a\cdot b = 0$, then a is called a left zero divisor
Let $a \in R$. a is called a zero divisor if it is a left zero divisor or a right zero divisor

R is an integral domain if it is commutative with no zero divisor

FACTS

1. $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a \Rightarrow 0\cdot a = 0$ $\forall a \in R$
2. $a\cdot(-b)+a\cdot b = a\cdot(-b+b) = a\cdot 0 = 0 \Rightarrow a\cdot(-b) = -a\cdot b$
3. All fields are integrable domains
   - Commutative: By def
   - No zero divisor: $\forall a \neq 0$, $a\cdot b = 0 \Rightarrow a^{-1}\cdot(a\cdot b) = 0 \Rightarrow (a^{-1}\cdot a)\cdot b = 1\cdot b = b = 0$

EXAMPLES

1. $(\mathbb{Z},+,\times)$, $(\mathbb{Z}/n\mathbb{Z},+,\times)$, $(M_{n\times n}(F),+,\times)$ (F: field) are rings
2. If G is an abelian group, then $(\mathrm{End}(G),+,\circ)$ is a ring where $\forall f,g \in \mathrm{End}(G)$, $a \in G$, $(f+g)(a) := f(a)+g(a)$, $(f\cdot g)(a) = f(g(a))$
3. $\mathbb{Z}[x] = \{a_0 + a_1 x + \dots + a_n x^n \mid a_i \in \mathbb{Z},\ n \in \mathbb{N}\}$
4. $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\} = \{a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + \dots + a_n\sqrt{2}^n \mid a_i \in \mathbb{Z},\ n \in \mathbb{N}\}$

PROPOSITION 1

TFAE
(1) $\mathbb{Z}/n\mathbb{Z}$ is an integral domain
(2) $\mathbb{Z}/n\mathbb{Z}$ is a field
(3) $n = p$ is prime

Proof (Finite + integral domain ⇒ Field; At least one of them is 1.)

- (1) ⇒ (2): Let $R = \{0, a_1, \dots, a_n\}$. For any a_i, $\{0, a_i a_1, \dots, a_i a_n\} = R$
  If $a_i \neq 0$, $a_i a_j = a_i a_k \Rightarrow a_i(a_j - a_k) = 0 \Rightarrow a_j - a_k = 0 \Rightarrow a_j = a_k$, thus $\forall a,b,c \in R$, $ab = ac \Rightarrow b = c$
  Hence, for all a_i, $\exists a_j$, s.t. $a_i a_j = 1$ ✓
- (2) ⇒ (3): Assume n is not prime, say $n = kl$, $1 < k, l < n$. Then $\bar{k} \neq \bar{0}$, $\bar{l} \neq \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$. However, $\bar{n} = \overline{kl} = \bar{k}\cdot\bar{l} = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$.
  ∴ $\bar{k}$ is a zero divisor ∴ $\bar{k}^{-1}$ does not exist ↯
- (3) ⇒ (1): If $\bar{k}\cdot\bar{l} = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$, then $p \mid kl \Rightarrow p \mid k$ or $p \mid l$. Thus, $\bar{k} = 0$ or $\bar{l} = 0$ ✓

DEFINITION

- $\varphi: R_1 \to R_2$ is called a ring homomorphism if $\forall a,b \in R_1$, $\varphi(a+b)=\varphi(a)+\varphi(b)$, $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$, $\varphi(1)=1$ (Not necessary for certain rings but for now assume it's true.)
- $\ker\varphi := \{a \in R_1 \mid \varphi(a)=0\}$ is an additive subgroup of R. ($\ker\varphi$ is used to check if φ is (-1))
- $\mathrm{Im}\,\varphi$ is a subring of R_2 since $\varphi(a)\cdot\varphi(b)=\varphi(a\cdot b)\in \mathrm{Im}\,\varphi$, $1=\varphi(1)\in \mathrm{Im}\,\varphi$

OBSERVE

$\ker\varphi$ does not only have an addition abelian group, it even maintained multiplication within itself!
In multiplication: $\forall r\in R_1$, $a\in\ker\varphi$, $\varphi(r\cdot a)=\varphi(r)\cdot\varphi(a)=\varphi(r)\cdot 0=0$, similarly, $\varphi(a\cdot r)=0$. Thus, by def, $r\cdot a,\ a\cdot r\in\ker\varphi$

DEFINITION

Let I be an additive subgroup of R. I is called an ideal of R if $\forall r\in R, a\in I$, $r\cdot a,\ a\cdot r\in I$
↳ Since $(R,+,0)$ is abelian, I is a normal additive subgroup and $(R/I,+,\bar{0})$ is an abelian group
↳ In R/I, we define $(r_1+I)\cdot(r_2+I)=r_1\cdot r_2+I$
It is well-defined. Consider the following for $r_1+I=r_1'+I$, $r_2+I=r_2'+I$, say $r_1-r_1'=a\in I$, $r_2-r_2'=b\in I$
We have $r_1r_2=(r_1'+a)\cdot(r_2'+b)=r_1'\cdot r_2'+\underbrace{a\cdot r_2'+r_1'\cdot b+a\cdot b}_{\in I}$. Thus, $r_1r_2+I=r_1'r_2'+I$

Note that $(R/I,+,\cdot)$ is called the quotient ring of R by I.
Similarities in rings and groups: $H\lhd G \Rightarrow G/H$ is a group, I: ideal in $R \longrightarrow R/I$ is a ring

PROPOSITION 2

$\exists!$ ring homomorphism $\varphi:\mathbb{Z}\to R$, s.t. $\varphi(1)=1_R$

Proof

Since $\mathbb{Z}=\langle 1\rangle$, $\varphi(1):=1_R$, it forms an additive homomorphism $\varphi:\mathbb{Z}\to R$
That is, for $m\in\mathbb{N}$, $\varphi(m)=\varphi(\underbrace{1+\dots+1}_{m\text{ times}})=\underbrace{\varphi(1)+\dots+\varphi(1)}_{m\text{ times}}=\underbrace{1_R+\dots+1_R}_{m\text{ times}}$ in R. Similarly, $\varphi(-m)=\underbrace{(-1_R)+\dots+(-1_R)}_{m\text{ times}}$ in R

Hence, $\varphi(m\times n)\overset{\mathbb{N}}{=}\underbrace{1_R+\dots+1_R}_{mn\text{ times}}=(\underbrace{1_R+\dots+1_R}_{m\text{ times}})(\underbrace{1_R+\dots+1_R}_{n\text{ times}})=\varphi(m)\varphi(n)$
$\varphi((-m)\times n)=\varphi(-mn)=\underbrace{(-1_R)+\dots+(-1_R)}_{mn\text{ times}}=(\underbrace{(-1_R)+\dots+(-1_R)}_{m\text{ times}})(\underbrace{1_R+\dots+1_R}_{n\text{ times}})=\varphi(-m)\varphi(n)$
Similarly, $\varphi(m\times(-n))=\varphi(m)\cdot\varphi(-n)$, $\varphi((-m)\times(-n))=\varphi(-m)\varphi(-n)$, i.e. φ is a ring homomorphism □

DEFINITION

In proposition 2, if $\ker\varphi=m\mathbb{Z}$ then m is called the characteristic of R, denoted by $\mathrm{char}\,R=m$, i.e. smallest integer m, s.t. $\underbrace{1_R+\dots+1_R}_{m\text{ times}}=0$

PROPOSITION 3

(1) If R is an integral domain, then $\mathrm{char}\,R=0$ or a prime number
(2) If $\mathrm{char}\,R=p$, then $(a+b)^p=a^p+b^p$ $\forall a,b\in R$

Proof

(1) Assume $\mathrm{char}\,R=n\neq 0$ If n is not prime, say $n=k\cdot l$, then $\underbrace{(\underbrace{1_R+\dots+1_R}_{k\text{ times}})}_{\neq 0}\underbrace{(\underbrace{1_R+\dots+1_R}_{l\text{ times}})}_{\neq 0}=\underbrace{1_R+\dots+1_R}_{n\text{ times}}=0$ ⟶ ×

For convenience, denote $n1_R:=\underbrace{1_R+\dots+1_R}_{n\text{ times}}$
(2) By the binomial thm, $(a+b)^p=a^p+\binom{p}{1}a^{p-1}b+\dots+b^p$.
For $1\le i\le p-1$, $p\nmid i!$ and $\binom{p}{i}=\frac{p(p-1)\cdots(p-i+1)}{i!}\Rightarrow p\mid\binom{p}{i}$.
Notice, $px=x\cdot p1_R=x\cdot 0=0$, so $\binom{p}{i}a^{p-i}b^i=0$ $\forall 1\le i\le p-1$
In other words, $(a+b)^p=a^p+b^p$ □

EXTENSION TO MODULES

Like how fields extend to the more general ring, vector spaces extend to the more general modules

DEFINITION

An **R-module** is an abelian group M (written additively) on which R acts **linearly**: $R \times M \longrightarrow M$, $(r, m) \longmapsto rm$

(1) $r(x+y) = rx + ry$ $\forall r \in R,\ x, y \in M$
(2) $(r+s)x = rx + sx$ $\forall r, s \in R,\ x \in M$
(3) $(r \cdot s)x = r(sx)$ $\forall r, s \in R,\ x \in M$
(4) $1x = x$ $\forall x \in M$

EXAMPLES

1. Any **abelian group** G is a **$\mathbb{Z}$-module**
   $\forall a \in G,\ n \in \mathbb{Z}$, $na := \underbrace{a + \dots + a}_{n \text{ times}}$ $\forall n \in \mathbb{N}$, $(-n) \cdot a = \underbrace{(-a) + \dots + (-a)}_{n \text{ times}}$
2. Let I be an ideal of R. Then, **I is an R-module** By def, $\forall r \in R,\ a \in I,\ ra \in I$. In particular, **$R$ is an R-module**

☆ A ring is also a module

10-4-24 (WEEK 5)

MODULES OVER PID

DEFINITION / PROPOSITION

Let M be an R-module and $\emptyset \neq S \subseteq M$. The submodule is generated by S is defined to be
$\langle S \rangle_R := \{\sum_{\text{finite}} r_i x_i \mid r_i \in R, x_i \in S\}$ = the least submodule of M containing $S = \bigcap_{S \subseteq N} N$ (submodule)

DEFINITION

An R-module is said to be finitely generated if $M = \langle x_1, \dots, x_n \rangle_R = Rx_1 + \dots + Rx_n$

EXAMPLE 1

R can be regarded as an R-module generated by 1

DEFINITION

An integral domain R is a principal ideal domain (PID) (GCD domain) if each ideal I in R, $\exists a \in R$, s.t. $I = \langle a \rangle_R$ (principal = generated by 1 element)

FACT

If $\langle a, b \rangle_R = \langle d \rangle_R$, then $d = \gcd(a, b)$

Proof

- $a, b \in \langle d \rangle_R \Rightarrow \exists r_1 \in R, r_2 \in R$, s.t. $a = r_1 d$, $b = r_2 d \Rightarrow d \mid a$ and $d \mid b$
- For $c \in R$ with $c \mid a$ and $c \mid b$ ($a = ck_1$, $b = ck_2$), write $d = l_1 a + l_2 b = l_1 k_1 c + l_2 k_2 c = (l_1 k_1 + l_2 k_2) c \Rightarrow c \mid d$ (ideal is commutative)

EXAMPLE 2

$\mathbb{Z}$ is a PID

Proof

Let I be an ideal in $\mathbb{Z}$. In particular, I is an additive subgroup of $\mathbb{Z} \Rightarrow I = m\mathbb{Z} = \langle m \rangle_{\mathbb{Z}}$

DEFINITION

M is said to be a free R-module of rank n if if $M \cong \underbrace{R \times \cdots \times R}_{n \text{ times}} =: R^n$ (R-module isom) Notice $r(r_1, \dots, r_n) = (rr_1, \dots, rr_n)$, $R^n = Re_1 + \dots + Re_n$ ($e_1 = (1, 0, \dots, 0)$)

Strategy: $R^n \xrightarrow{\varphi} M$, $e_i \mapsto x_i$ $\Rightarrow M \cong R/\inf \varphi$ (first isom)

EXAMPLE (Basis cannot exist...)

$R = \mathbb{Z}[x_1, x_2, \dots] \Rightarrow R = R \cdot 1$, but $I = \langle x_1, x_2, \dots \rangle$ is not a f.g submodule of R

THEOREM 1

If R is a PID and $n \in \mathbb{N}$, then any submodule of R^n is free of rank at most n

Proof

By induction on n,

($R \xrightarrow{\varphi} Ra$, $a \mapsto a \Rightarrow \ker\varphi = \{0\}$ since R is an integral domain)

- $n = 1$: Let $\langle 0 \rangle \neq I \subset R$, then $I = \langle a \rangle_R = Ra \cong R$
- Let $n > 1$ and N be a submodule of R^n (Submodules may not have a smaller rank! But we want rank↓ so we can use MI)

  Consider $\pi_1 : R^n \to R$, $(x_1, \dots, x_n) \mapsto x_1$ and $\pi = \pi_1|_N : N \to R$

  Case 1: $\operatorname{Im}\pi = \langle 0 \rangle$ (Only 2 to n are nonzero)

  In this case, $N \subset \ker\pi_1 \cong R^{n-1}$, so by induction hypothesis, N is free of rank $\leq n-1 < n$

  Case 2: $\operatorname{Im}\pi \neq \langle 0 \rangle$, say $\operatorname{Im}\pi = \langle x \rangle_R$, $x = \pi(a)$ for some $a \in N$

  Claim: $N \cong Ra \oplus \ker\pi$ ($\ker\pi \subseteq \ker\pi_1 \cong R^{n-1}$)

  Proof

  - $Ra \cap \ker\pi = \{0\}$: $\pi(ra) = 0 \Rightarrow r\pi(a) = rx = 0$, but $x \neq 0$, so $r = 0 \Rightarrow ra = 0$ ✓

- "$\supseteq$": OK
- "$N \subseteq Ra \oplus \ker\pi$": $\forall b \in N$, let $\pi(b) \in \mathrm{Im}\,\pi = \langle x \rangle_R$, where $\pi(b) = r_0 x$ for some $r_0 \in R$

  Notice, $r_0 x = r_0 \cdot \pi(a) = \pi(r_0 a) \Rightarrow b - r_0 a \in \ker\pi \Rightarrow b \in Ra \oplus \ker\pi$ ✓

Now, $Ra \cong R$ and $\ker\pi \subseteq R^{n-1}$ is free of rank $\leq n-1 \Rightarrow N$ is free for rank $\leq n$. □

GAUSSIAN ELIMINATION OVER PID

Recall that the **elementary matricies** are:
- $D_i(u) = \mathrm{diag}(1, \dots, 1, \underline{u}, 1, \dots, 1)$ (ith place) (Left Multiply: ith row $\times u$; Right Multiply: ith col $\times u$)
- $B_{ij}(a) = I_n + a e_{ij}$, $a \in R$, $i \neq j$ (Left Multiply: jth row $\times a$ + ith row; Right Multiply: ith col $\times a$ + jth col)
- $P_{ij} = I_n - e_{ii} - e_{jj} + e_{ij} + e_{ji}$ (Left Multiply: Swap ith, jth rows; Right Multiply: Swap ith, jth cols)

Notice, $D_i(u)$ can only have an inverse if u is a **unit** in R

Although, $B_{ij}(a)^{-1} = B_{ij}(-a)$, $P_{ij}^{-1} = P_{ij}$, so they are OK

THEOREM 2

Let R be a PID and $A \in M_{m\times n}(R)$. Then $\exists P \in GL_n(R)$, $Q \in GL_m(R)$, s.t. $PAQ = \mathrm{diag}(d_1, d_2, \dots, d_r, 0, \dots, 0)$ with $d_i \mid d_{i+1}$, $\forall i = 1, \dots, r-1$

Proof

Define the length $\ell(a)$ of $0 \neq a$ to be r if $a = p_1 p_2 \cdots p_r$ where $p_1, \dots, p_r$ are prime elements (PID $\Rightarrow$ UFD)

If a is a unit, then set $\ell(a) = 0$

(1) We may assume $a_{11} \neq 0$, and $\ell(a_{11}) \leq \ell(a_{ij})$ $\forall a_{ij} \neq 0$ (Use elementary matricies)

$$\begin{pmatrix} \vdots \\ a_{i1} \cdots \end{pmatrix} \rightsquigarrow P_{1i}(\ ) \rightsquigarrow (\ ) P_{1i} \rightarrow \begin{pmatrix} a_{11} \cdots \\ \vdots \end{pmatrix}$$

(range with length)

(2) We may assume $a_{11} \mid a_{1k}$ $\forall k = 2, \dots, m$, and $a_{11} \mid a_{k1}$ $\forall k = 2, \dots, n$

If $a_{11} \nmid a_{1k}$, then we interchange the 2^{nd} and k^{th} columns to assume $a_{11} \nmid a_{12}$ ($a \neq b$)

Write $a = a_{11}$, $b = a_{12}$. Let $d = \gcd(a, b)$. We have $\ell(d) < \ell(a)$ and $d = ax + by$ for some $x, y \in R$

$\Rightarrow 1 = (\frac{a}{d})x + (\frac{b}{d})y := -a'x + b'y$ ($-a' := \frac{a}{d}$, $b' := \frac{b}{d}$)

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

$\therefore \left(\begin{array}{cc|c} x & b' & \\ y & a' & \\ \hline & & I \end{array}\right)$ is invertible.

Consider the following:

$$\begin{pmatrix} a & b & a_{13} \cdots \\ a_{21} & a_{22} & \\ \vdots & & \ddots \end{pmatrix}\left(\begin{array}{cc|c} x & b' & \\ y & a' & \\ \hline & & I \end{array}\right) = \left(\begin{array}{cc|c} d & 0 & a_{13} \cdots a_{1m} \\ a_{21}' & a_{22}' & \\ \vdots & & \end{array}\right) \cdots$$

(changed; finally $a_{11} \mid a_{12}$; unchanged)

But $\ell(d)$ may not be min

If $\ell(a_{k1}') < \ell(d)$, then change the matrix to $\begin{pmatrix} a_{k1}' & a_{12} & a_{13} \cdots \end{pmatrix}$

Since we keep the length of the $(1,1)$-entry s.t. it decreases, after a finite number of steps, $a_{11} \mid a_{1k}$, $a_{11} \mid a_{k1}$ ($\forall a, u(u^{-1}a) = a$)

(3) By the assumption of 2,

$$\begin{pmatrix} & \end{pmatrix} \rightarrow \left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{array}\right)$$

(4) We can also arrange to have $a_{11} \mid b_{k1}$ $\forall k, l$

If $a_{11} \nmid b_{k1}$, then we add the k^{th} row to the 1^{st} one, i.e. $\left(\begin{array}{c|ccc} a_{11} & b_{k2} & \cdots & b_{km} \\ \hline 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{array}\right)$ (b_{k1})

With $d' = \gcd(a_{11}, b_{k1})$, $\left(\begin{array}{c|ccc} d' & 0 & \cdots & 0 \\ \hline * & & & \end{array}\right)$

However, $\ell(d') < \ell(a_{11})$ (so continue doing it)

After that, we obtain: $\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{pmatrix}$

(5) Apply (1), (2), (3), (4) on (b_{ij}) to get $\begin{pmatrix} b_{22} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & c_{ij} & \\ 0 & & & \end{pmatrix}$, $b_{22} \mid c_{kl}$ $\forall k, l$

All transformations we use do not affect the divisibility condition by a_{11}. Hence, $a_{11} \mid b_{22}$

Now, by induction, we have $PAQ = \begin{pmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \ddots & & \\ & & & d_r & \\ & & & & 0 \end{pmatrix}$. $\square$ (i.e. we can do Gaussian Elimination in PID!)

10-9-24 (WEEK 6)

FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS (FTOFAG)

RECALL

Let R be a PID and $A \in M_{n\times n}(R) \Rightarrow \exists P \in GL_n(R), Q \in GL_m(R)$, s.t. $PAQ = \operatorname{diag}(d_1, d_2, \dots, d_r, 0, \dots, 0)$ with $d_i \mid d_{i+1}$ $\forall i = 1, \dots, r-1$

PROPOSITION 1

$d_1, \dots, d_r$ are unique up to associates ($a \sim b$ if $a = bu$ for some unit u)

Proof

Let $\Delta_k(A)$ = the gcd of all k-th order minors of A (unique up to associates due to the units (eg $\gcd(12, 16) = 4, -4$? units $= 1, -1$))

Let $P = (P_{ij})_{n\times n}$. Then, $PA = \begin{pmatrix} \sum_j P_{1j}(a_{j1}, a_{j2}, \dots, a_{jn}) \\ \vdots \\ \sum_j P_{mj}(a_{j1}, a_{j2}, \dots, a_{jn}) \end{pmatrix}$, and a k-th order minor of $PA = \begin{vmatrix} \sum_j P_{s_1 j}(a_{jt_1}, a_{jt_2}, \dots, a_{jt_k}) \\ \vdots \\ \sum_j P_{s_k j}(a_{jt_1}, a_{jt_2}, \dots, a_{jt_k}) \end{vmatrix}$

This means, k-th order minor = a linear combination of some k-th order minors of A

Hence, $\Delta_k(A) \mid$ any k-th order minor of $\Delta_k(PA)$, meaning $\Delta_k(A) \mid \Delta_k(PA)$. Similarly, $\Delta_k(A) \mid \Delta_k(AQ)$

If $PAQ = B$, then $\Delta_k(A) \mid \Delta_k(B)$. Likewise, $A = P^{-1}BQ^{-1}$, so $\Delta_k(B) \mid \Delta_k(A)$

$\Rightarrow \Delta_k(A) \sim \Delta_k(B) = d_1 d_2 \cdots d_k$ ($= \operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0)$), $k = 1, \dots, r$, i.e. $d_i = \Delta_i(A)/\Delta_{i-1}(A)$

Not "$=$" since units ($-4 \mid 4$, $4 \mid -4$, $4 \neq -4$)

DEFINITION

$\operatorname{Tor}(M) = \{0 = m \in M \mid \exists\, 0 \neq r \in R$, s.t. $rm = 0\}$ forms a submodule of M (integral domain)

($m_1, m_2 \in \operatorname{Tor}(M)$, say $r_1 m_1 = 0$, $r_2 m_2 = 0$, $r_1 r_2 (m_1 + m_2) = 0$)

MAIN THEOREM (over modules, not just abelian groups)

Let R be a PID and M be a finitely generated R-module

Then, $M \cong \underbrace{R/\langle d_1\rangle_R \oplus \dots \oplus R/\langle d_k\rangle_R}_{\text{torsion part (up to associates)}} \oplus \underbrace{R^s}_{\text{free part (unique)}}$ for some $s \in \mathbb{Z}^{\geq 0}$, $d_i \mid d_{i+1}$ $\forall i = 1, \dots, k-1$, d_i is not a unit (Otherwise, $dR = R \Rightarrow R/dR = \langle 0\rangle$ ($1 = dd^{-1}$))

($rd_1 + \langle d_1\rangle_R = \langle d_1\rangle_R$)

REMARK

$R^s \cong M/\operatorname{Tor}(M)$. If $\exists\, t \in \mathbb{Z}^{\geq 0}$, s.t. $R^t \cong M/\operatorname{Tor}(M) \cong R^s$, then if R is commutative, then $t = s$, so t is unique

PROPOSITION 2 (needed for determinant)

Let R be a commutative ring. If $R^s \cong R^t$ (e_i, f_j standard bases), then $s = t$ (R/M^{max} is a field: $R^s \otimes R/M \cong R^t \otimes R/M \Rightarrow (R/M)^s \cong (R/M)^t \Rightarrow s = t$) (field)

Proof

If $s < t$, then $f_i = \sum_{j=1}^{s} a_{ji} e_j \Rightarrow (f_1 \cdots f_t) = (e_1 \cdots e_s)(a_{ij})_{s\times t}$

Also, $e_i = \sum_{j=1}^{t} b_{ij} f_j \Rightarrow (e_1 \cdots e_s) = (f_1 \cdots f_t)(b_{ij})$

$\therefore$ We obtain $(f_1 \cdots f_t) = (f_1 \cdots f_t)(b_{ij})(a_{ij}) \Rightarrow BA = I_t$

Let $\bar{A} = \left(\begin{array}{c} a_{ij} \\ \hline 0 \\ \vdots \\ 0 \end{array}\right)_{t\times t}$, $\bar{B} = \left(\begin{array}{c|c} b_{ij} & 0 \cdots 0 \end{array}\right)_{t\times t} \Rightarrow \bar{B}\bar{A} = I_t$, $\bar{A}\bar{B} = I_t$, $\bar{A}^{-1} = \bar{B}$

As R is commutative, we can define the determinant by multilinear maps.

Thus, by Cramer's rule, $A(\operatorname{adj} A) = (\det A \cdots \det A)$ ($\det A$ a unit), meaning $A^{-1} = \frac{1}{\det A} \operatorname{adj} A$

Notice, as $\bar{B}\bar{A} = I_t$, $\det(\bar{B})\det(\bar{A}) = 1$, $\det \bar{A}$ is a unit. However, with the added zeroes, $\det \bar{A} = 0$ $\rightarrow\!\leftarrow$ $\therefore s \neq t$, thus $s = t$ $\square$

PROOF OF MAIN THEOREM

Let $M=\langle x_1,\dots,x_n\rangle_R$ and define $f: R^n \twoheadrightarrow M \Rightarrow R^n/\ker f \cong M$

$e_i \longmapsto x_i$

We know $\ker f \cong R^m$ for some $m \le n$

$f_i \longmapsto e'_i$

$\{f_j\}$ $\quad$ $\{e_i\}$

$\because \ker f \subseteq R^n$

$\therefore$ We can write $f_i = \sum_{j=1}^{n} a_{ji} e_j \ \forall i$, so $(f_1 \cdots f_m) = (e_1 \cdots e_n)(a_{ij})$ (A)

$\because R$ is a PID

$\therefore \exists P \in GL_n(R), Q \in GL_m(R)$, s.t. $PAQ = \begin{pmatrix} d'_1 & & & \\ & \ddots & & \\ & & d'_r & \\ & & & 0 \end{pmatrix}$, $d'_i \mid d'_{i+1}, \forall i=1,\dots,r-1$

We can also say $PAQ = [Id_{R^m}]_{\{e_i\}}^{\{w_j\}} [T]_{\{f_j\}}^{\{e_i\}} [Id_{\ker f}]_{\{u_i\}}^{\{f_j\}}$ and $id = T: \ker f \hookrightarrow R^n$

Thus, $(u_1 \cdots u_m) = (f_1 \cdots f_n)Q$, $(w_1 \cdots w_n) = (e_1 \cdots e_n)P^{-1}$

Hence, $[T]_{\{u_i\}}^{\{w_j\}} = \begin{pmatrix} d'_1 & & & \\ & \ddots & & \\ & & d'_r & \\ & & & 0 \end{pmatrix} \Rightarrow (u_1 \cdots u_m) = (w_1 \cdots w_n)\begin{pmatrix} d'_1 & & & \\ & \ddots & & \\ & & d'_r & \\ & & & 0 \end{pmatrix} \Rightarrow r=m,\ u_i = d'_i w_i \ \forall i=1,\dots,m$

(Made the basis s.t. $R^n/\ker f$ can be quotiented systematically)

We can rewrite $R^n/\ker f = Rw_1 \oplus \cdots \oplus Rw_n / Rd'_1 w_1 \oplus \cdots \oplus Rd'_m w_m \oplus 0 \cdots 0 \cong Rw_1/Rd'_1 w_1 \oplus \cdots \oplus Rw_m/Rd'_m w_m \oplus Rw_{m+1} \oplus \cdots \oplus Rw_n$

$d'_i R = R$ (units), so $Rd'_i w_i = Rw_i$

Assume that $d'_1, \dots, d'_k$ are units and $d'_{k+1}, \dots, d'_n$ are non-units. Then, $Rw_i/Rd'_i w_i = Rw_i/Rw_i \cong \langle 0 \rangle \ \forall i=1,\dots,k$

Now, let $d_1 = d'_{k+1}, \dots, d_\ell = d'_m$, we have for $i=1,\dots,\ell$, $R \twoheadrightarrow Rw_i/Rd_i w_i$, where $\ker \varphi_i = \langle d_i \rangle_R$

$1 \longmapsto w_i$

$\therefore$ By first isom thm, $R/\langle d_i \rangle_R \cong Rw_i/Rd_i w_i$ (Rd_i)

Hence, $R^n/\ker f \cong R/\langle d_1 \rangle_R \oplus \cdots \oplus R/\langle d_\ell \rangle_R \oplus R^{n-m}$

(finitely generated)

FUNDAMENTAL THEOREM OF F.G. ABELIAN GROUPS

Let G be a f.g. abelian group. Then, $G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_\ell\mathbb{Z} \oplus \mathbb{Z}^s$ for some $s \in \mathbb{Z}^{\ge 0}$, $d_i \in \mathbb{Z}$ with $d_i \mid d_{i+1} \ \forall i=1,\dots,\ell-1$

↳ This is a generalization for the theorem above

EXAMPLE 1

Classify abelian G of $|G|=72$

We know it has invariant factors: $72/2(36)/3(24)/2(2)(18)/6(12)/2(6)(6)$

Thus, these are the classifications: $\mathbb{Z}/72\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$

Notice, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$, so: $\mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/3^2\mathbb{Z}$ . . . . . $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

(These are elementary divisors! You just "expand" each $\mathbb{Z}_k$ for composite k, no difference)

DEFINITION

The exponent of G with $|G|<\infty$ is $\exp(G) := \min\{m \in \mathbb{N} \mid g^m = 1 \ \forall g \in G\}$, which exits since $g^{|G|}=1 \ \forall g \in G$

REMARK

If $n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$, then $\mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{m_s}\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ (Specific version of Chinese Remainder Theorem)

CHINESE REMAINDER THEOREM (Feel like full proof may be tested)

Let R be a commutative ring and $I_1, \dots, I_n$ be ideals of R.

Then, $\varphi: R \to R/I_1 \times \dots \times R/I_n$ is a ring homo

$r \mapsto (r+I_1, \dots, r+I_n)$

$\Rightarrow \exists r$, s.t. $r-1 \in I_1$, $r \in I_2, \dots I_n \leftarrow I_1 + I_i = R \ \forall i \geq 2$

$\varphi(r) = (\bar{1}, \bar{0}, \dots, \bar{0})$ $\quad x_i + y_i = 1$, then $r = y_2 \cdots y_n$

$= (1-x_2) \cdots (1-x_n)$

$= 1 + x$ ($x \in I_i$)

and (1) if I_i, I_j are coprime $\forall i \neq j$ $(I_i + I_j = R)$, then $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \dots \cap I_n$

(2) φ is surjective $\Leftrightarrow$ I_i, I_j are coprime $\forall i \neq j$ (e.g. $\langle 3 \rangle + \langle 5 \rangle = \langle 1 \rangle$)

(3) φ is injective $\Leftrightarrow I_1 \cap I_2 \cap \dots \cap I_n = \{0\}$

We conclude that if I_i, I_j are coprime $\forall i \neq j$, then $R/I_1 I_2 \cdots I_n \cong R/I_1 \times \cdots \times R/I_n$

Proof

By induction on n,

- $n=2$: By def, $I_1 \cap I_2 \supseteq I_1 I_2$. However, notice $(I_1 \cap I_2) R \subseteq (I_1 \cap I_2)(I_1 + I_2)$, so $I_1 \cap I_2 \subseteq I_1 I_2$ ✓
- For $n > 2$, notice $I_1 I_2 \cdots I_n = (I_1 I_2 \cdots I_{n-1}) I_n = (I_1 \cdots I_{n-1}) \cap I_n \overset{\text{ind hyp}}{=} I_1 \cap \dots \cap I_{n-1} \cap I_n$

However, notice $\because I_i + I_n = R$ ($I_1 \cdots I_{n-1} + I_n = R$)

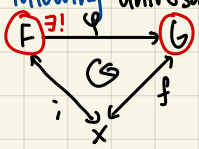
$\therefore \exists x_i, y_i$, s.t. $x_i + y_i = 1 \Rightarrow (x_1 \cdots x_{n-1}) = (1-y_1) \cdots (1-y_{n-1}) = 1 + y$ for some $y \in I_n$ ($x_1 \cdots x_{n-1} \in I_1 \cdots I_{n-1}$, $y_1 \in I_n$, $y_{n-1} \in I_n$)

10-11-24 (WEEK 6)

FREE GROUPS

DEFINITION

A **free group** on X is a **group** F with an **inclusion group** $i: X \hookrightarrow F$ satisfying the following universal property: for any **group** G and any **map** $f: X \to G$, $\exists!$ group homomorphism $\varphi: F \to G$, s.t. $F \xrightarrow{\exists!\ \varphi} G$ commutes with i and f.

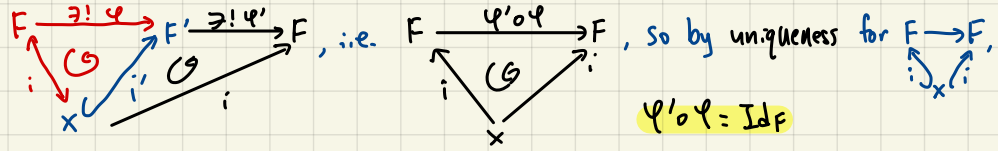


MAIN THEOREM

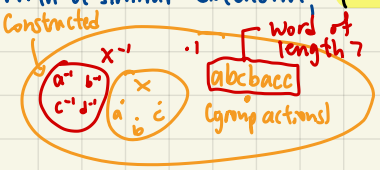
F exists and is unique up to isomorphism

Proof

- **Uniqueness**: If $\exists$ another F', then $F \xrightarrow{\exists!\ \varphi} F' \xrightarrow{\exists!\ \varphi'} F$, i.e. $F \xrightarrow{\varphi' \circ \varphi} F$, so by uniqueness for $F \to F$, $\varphi' \circ \varphi = \mathrm{Id}_F$



- **Existence**: With a similar extension, $\varphi \circ \varphi' = \mathrm{Id}_F$ too. Hence, $F \xrightarrow{\varphi}_{\simeq} F$



(Not so effective XD)

For X, we create a new disjoint set $X^{-1} := \{x^{-1} \mid x \in X\}$ and an element $1 \notin X \cup X^{-1}$ (can redefine e.g. $aa^{-1} := e \neq 1$)

Define $F(X) = \{1\} \cup \{x_1^{\delta_1} x_2^{\delta_2} \dots x_m^{\delta_m} \mid m \in \mathbb{N},\ x_i \in X,\ \delta_i = \pm 1,\ x_{i+1}^{\delta_{i+1}} \neq (x_i^{\delta_i})^{-1}\}$ (free group, not field) (Note: $x' := x$, $(x^{-1})^{-1} := x'$)

and "$x_1^{\delta_1} x_2^{\delta_2} \dots x_m^{\delta_m} = y_1^{\varepsilon_1} y_2^{\varepsilon_2} \dots y_n^{\varepsilon_n} \iff n = m,\ x_i = y_i,\ \delta_i = \varepsilon_i\ \forall i$"

For each $y \in X \cup X^{-1}$, we define $\sigma_y: F(X) \longrightarrow F(X)$ by: $\sigma_y(x_1^{\delta_1} \dots x_m^{\delta_m}) = \begin{cases} y x_1^{\delta_1} \dots x_m^{\delta_m}, & x_1^{\delta_1} \neq y \\ x_2^{\delta_2} \dots x_m^{\delta_m}, & x_1^{\delta_1} = y^{-1} \end{cases}$ (case 2: $m = 1$, $m \geq 2$)

CLAIM 1

σ_y is a permutation of $F(X)$, i.e. $\sigma_y \in \mathrm{Perm}(F(X))$

Proof

- 1-1: $\sigma_y(x_1^{\delta_1} \dots x_m^{\delta_m}) = \sigma_y(y_1^{\varepsilon_1} \dots y_n^{\varepsilon_n})$ (len $m-1$ or $m+1$ / len $n-1$ or $n+1$)
  - ↳ $m = n$: Either "$x_1^{\delta_1} = y_1^{\varepsilon_1} = y^{-1}$" or "$x_1^{\delta_1} \neq y^{-1}$ and $y_1^{\varepsilon_1} \neq y^{-1}$"
    - $\Rightarrow$ Either $x_2^{\delta_2} \dots x_m^{\delta_m} = y_2^{\varepsilon_2} \dots y_m^{\varepsilon_m}$ or $y x_1^{\delta_1} \dots x_m^{\delta_m} = y y_1^{\varepsilon_1} \dots y_m^{\varepsilon_m}$
    - $\Rightarrow \delta_i = \varepsilon_i,\ x_i = y_i\ \forall i$
  - ↳ $m = n+2$: By def, $x_2^{\delta_2} \dots x_m^{\delta_m} = y' y_1^{\varepsilon_1} \dots y_n^{\varepsilon_n}$
    - Thus, $x_1^{\delta_1} = y^{-1}$, $y' = x_2^{\delta_2}$, but $x_1^{\delta_1} = y^{-1} \Rightarrow x_1^{\delta_1} = (x_2^{\delta_2})^{-1}$ ✗
- Onto: $\forall x_1^{\delta_1} x_2^{\delta_2} \dots x_m^{\delta_m} \in F(X)$
  - ↳ Case 1: $x_1^{\delta_1} \neq y$, then $\sigma_y(y^{-1} x_1^{\delta_1} \dots x_m^{\delta_m}) \in \mathrm{Im}\,\sigma_y$ ✓
  - ↳ Case 2: $x_1^{\delta_1} = y$, then $\sigma_y(x_2^{\delta_2} \dots x_m^{\delta_m})$

Note: $\sigma_{y^{-1}} \circ \sigma_y = \mathrm{id}_{F(X)} \Rightarrow \sigma_{y^{-1}} = \sigma_y^{-1}$ ($\sigma_{x^{-1}} = \sigma_x^{-1}$)

Now, define $A = \langle \sigma_x \mid x \in X \rangle \leq \mathrm{Perm}(F(X))$ and define $\varphi: F(X) \longrightarrow A$

$1 \longmapsto \mathrm{id}_{F(X)}$

$x_1^{\delta_1} \dots x_m^{\delta_m} \longmapsto \sigma_{x_1}^{\delta_1} \dots \sigma_{x_m}^{\delta_m} = \sigma_{x_1}^{\delta_1} \circ \dots \circ \sigma_{x_m}^{\delta_m}$

CLAIM 2

Ψ is a bijection

Proof

- 1-1: $\sigma_{x_1}^{\delta_1} \cdots \sigma_{x_m}^{\delta_m} = \sigma_{y_1}^{\varepsilon_1} \cdots \sigma_{y_n}^{\varepsilon_n}$ ★ then WLOG $(x_m^{-\delta_m}, x_{m-1}^{-\delta_{m-1}})$

  $\Rightarrow 1 = \sigma_{y_1}^{\varepsilon_1} \circ \cdots \circ \sigma_{y_n}^{\varepsilon_n} (x_m^{-\delta_m} x_{m-1}^{-\delta_{m-1}} \cdots x_1^{-\delta_1})$

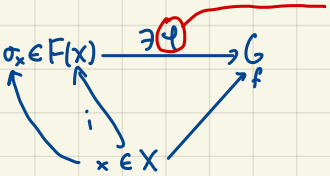
  $y_n^{\varepsilon_n} x_m^{-\delta_m} \cdots x_1^{-\delta_1}$ if $y_n^{\varepsilon_n} \neq x_m^{\delta_m}$ ↯ ($\because y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n} x_m^{-\delta_m} \cdots x_1^{-\delta_1} \neq 1$)

  By the same argument, ★ holds $\Leftrightarrow n=m$, $x_i^{\delta_i} = y_i^{\varepsilon_i}$ $\forall i = 1, \ldots, m$
- Onto: $\forall \sigma \in A$, $\sigma = \sigma_{x_1}^{\delta_1} \circ \cdots \circ \sigma_{x_m}^{\delta_m}$, $x_i \in X$, $\delta_i = \pm 1$, since $A = \langle \sigma_x \mid x \in X \rangle$

  Since A is a group, $\sigma_{i+1}^{\delta_{i+1}} \neq (\sigma_i^{\delta_i})^{-1}$

  ∴ Now we may give some binary operation on $F(x)$ as "$\circ$" on A via $\Psi: \sigma_{x_1}^{\delta_1} \circ \cdots \circ \sigma_{x_m}^{\delta_m} \longmapsto x_1^{\delta_1} \cdots x_m^{\delta_m}$

- **Universal Property:**



$\forall x \in X$, $\varphi(x) = f(x) \in G$, $\varphi(x^{-1}) = f(x^{-1}) \in G$, $\varphi(xx') = f(x)f(x')$,

i.e. $\varphi(x_1^{\delta_1} \cdots x_m^{\delta_m}) = f(x_1)^{\delta_1} \cdots f(x_m)^{\delta_m}$

↳ Group homo: Notice, $\varphi(x_1^{\delta_1} \cdots x_m^{\delta_m}) = f(x_1)^{\delta_1} \cdots f(x_m)^{\delta_m}$, $\varphi(y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}) = f(y_1)^{\varepsilon_1} \cdots f(y_n)^{\varepsilon_n}$

Thus, $\varphi(x_1^{\delta_1} \cdots x_m^{\delta_m} y_1^{\delta_1} \cdots y_n^{\delta_m}) = \varphi(x_1^{\delta_1} \cdots x_m^{\delta_m}) \varphi(y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n})$

By universal property, $F(X) \cong A$, then we get $f(x_1)^{\delta_1} \cdots f(y_n)^{\varepsilon_n}$

PROPOSITION

Let $G = \langle a_1, \ldots, a_n \rangle$ and $X = \{x_1, \ldots, x_n\}$. Then, $G \cong F(x)/K$ — the subgroup of relations for $\{a_1, \ldots, a_n\}$

Proof

Let $f: X \longrightarrow G$ ($x_i \longmapsto a_i$) $\Rightarrow \exists!\ \varphi: F(X) \longrightarrow G$ ($x_i \longmapsto a_i$) By first isom thm, $F(x)/\ker\varphi \cong G$

X: enumeration

DEFINITION

Let $|X| < \infty$, say $\{X = x_1, \ldots, x_n\}$ and $R \subset F[x]$.

Let R be the smallest normal subgroup of $F[X]$ containing R

Here, $G = F(x)/N(R) = \langle x_1, \ldots, x_n \mid$ elements of R (relations)$\rangle$ ⟶ a presentation of G

If $|R| < \infty$, then G is said to be finitely presented

EXAMPLE

$D_n = \langle \begin{pmatrix} \sin\frac{2\pi}{n} & -\cos\frac{2\pi}{n} \\ \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle \leq O(2)$

(ρ_n, σ)

Let $X = \{x_1, x_2\}$ and $F(x) \longrightarrow D_n$

$x \longmapsto \rho_n$

$y \longmapsto \tau$

We find that $R = \{x^n, y^2, yxyx\} \in \ker\varphi$ ($\because yxy^{-1} = x^{-1}$)

By Factor Thm, $\exists \bar{\varphi}: F(x)/N(R) \longrightarrow D_n$, where $|\frac{F(x)}{N(R)}| \leq 2n$, $|D_n| = 2n$

↑ $y^j x^i$, $0 \leq i \leq n-1$, $0 \leq j \leq 1$

PROPOSITION 2

Let $X = \{x_1, \ldots, x_n\}$. Then, $F(x)/[F(x), F(x)] \cong \mathbb{Z}^n$

Proof

Define $f: X \longrightarrow \mathbb{Z}^n$ ($x_i \longmapsto e_i$)

By universal property, $\exists!\ \varphi: F(x) \longrightarrow \mathbb{Z}^n \Rightarrow F(x)/\ker\varphi \cong \mathbb{Z}^n \Rightarrow [F(x), F(x)] \leq \ker\varphi \Rightarrow$ $F(x)/[F(x),F(x)] \xrightarrow{\bar{\varphi}} \mathbb{Z}^n$, G, φ, $F(x)$

Claim: $\bar{\varphi}$ is 1-1

Proof

Since $F(x)/[F(x), F(x)]$ is abelian, $\forall a \in F(x)/(F(x), F(x))$, we can write $a = \bar{x}_1^{m_1} \cdots \bar{x}_n^{m_n}$ for some $m_i \in \mathbb{Z}$

Now, if $\varphi(a) = 0$, then $\varphi(a) = (m_1, \ldots, m_n) = (0, \ldots, 0) \Rightarrow a = 1$

10-16-24 (WEEK 7)

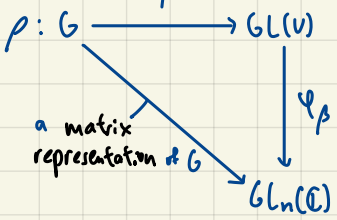
LINEAR REPRESENTATIONS

DEFINITION

$G \curvearrowright V$ n-dimensional over $\mathbb{C} \Rightarrow \varphi: G \longrightarrow \mathrm{Perm}(V)$, assume $\rho: G \longrightarrow GL(V)$, $\deg \rho := \deg V$

($GL(V)$: a representation space; ρ: a linear representation of G)

Fix a fixed basis β,



EXAMPLES

1. A representation of degree 1 of a finite group G is a group homo

   Here, $\rho: G \longrightarrow GL_1(\mathbb{C}) \cong \mathbb{C}^\times$

   If $|G|=m$, $g \longmapsto \rho(g) \Rightarrow \rho(g)^{|G|}=1$, i.e. $\rho(g)^m=1$ (m^{th} root of unity)

   So, honestly, it is just $\rho: G \longrightarrow S_1$

   For example, for $|G|=p$, i.e. $G \cong \mathbb{Z}/p\mathbb{Z}$, $\rho: G \longrightarrow S^1$

   $\tau \longmapsto \xi^p$ with $\xi^p=1$

2. $G=S_3 \cong D_6$, we have $V=\mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3$, $\rho: G \longrightarrow GL(V)$

   $\sigma \longmapsto \rho(\sigma): e_i \longmapsto e_{\sigma(i)}$

   Thus, $R: G \longrightarrow GL_3(\mathbb{C})$

   $1 \longmapsto \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$

   $(12) \longmapsto \begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix}$

   $(123) \longmapsto \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}$

   $1 \quad (12) \quad (13) \quad (23) \quad (123) \quad (132)$

3. $G=S_3$, and $V=\bigoplus_{\sigma \in S_3} \mathbb{C}e_\sigma = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3 \oplus \mathbb{C}e_4 \oplus \mathbb{C}e_5 \oplus \mathbb{C}e_6$ (Covers all multiplication but too large)

   Thus, $\rho^{reg}: G \longrightarrow GL(V)$ (reg: regular representation)

   $\tau \longmapsto \rho(\tau): e_\sigma \longmapsto e_{\tau\sigma}$

   For example:

   $R: (1\ 2) \longmapsto \begin{pmatrix} & 1 & & & & \\ 1 & & & & & \\ & & & & & \\ & & & & 1 & \\ & & & 1 & & \\ & & & & & 1 \end{pmatrix}$

☆ For a general G, $\rho^{reg}: G \longrightarrow GL(V)$ with $V=\bigoplus_{g \in G} \mathbb{C}e_g$

$g \longmapsto \rho(g): e_h \longmapsto e_{gh}$

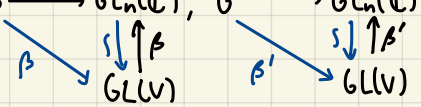
DEFINITION

- This is the trivial representation $\rho: G \longrightarrow GL(V)$, $g \longmapsto id$
- This is the faithful representation $\rho: G \hookrightarrow GL(V)$
- For $\rho: G \longrightarrow GL(V)$, $\rho': G \longrightarrow GL(V')$, we say ρ, ρ' are isomorphic if $\exists T: V \to V'$ such that

$$\begin{array}{ccc} V & \xrightarrow{\rho(g)} & V \\ {\scriptstyle T}\downarrow\uparrow{\scriptstyle S} & \circlearrowright & {\scriptstyle S}\downarrow\uparrow{\scriptstyle T} \\ V' & \xrightarrow{\rho(g)} & V' \end{array}$$

REMARK

When we choose two bases $\beta=\{e_i\}$, $\beta'=\{e_i'\}$ for V,



Let $T: V \xrightarrow{\sim} V$ (with $e_i \mapsto e_i'$). For $g \in G$, $R(g) = (a_{ij}) = A$

Now, consider $(T \circ \rho(g))(\sum_{i=1}^n x_i e_i) = T(\sum_{i=1}^n (\sum_{j=1}^n a_{ij} x_j) e_i) = \sum_{i=1}^n (\sum_{j=1}^n a_{ij} x_j) e_i' = (\rho'(g))(\sum_{i=1}^n x_i e_i') = (\rho'(g) \circ T)(\sum_{i=1}^n x_i e_i) \Rightarrow T \circ \rho(g) = \rho'(g) \circ T \ \forall g$

DEFINITION-PROPOSITION

Let $\langle \cdot, \cdot \rangle$ be a positive-definite Hermitian form

Then, $T: V \longrightarrow V$ is called a **unitary operator** if $\langle T(x), T(y) \rangle = \langle x, y \rangle \ \forall x, y \in V$

or **orthonormal** if $[T]_\beta [T]_\beta^* = [T]_\beta^* [T]_\beta = I_n$, i.e. $[T]_\beta \in I_n$

From now on, G is a finite group

THEOREM 1

$\forall \rho: G \longrightarrow GL(V)$, $\exists$ a matrix representation $R: G \longrightarrow U_n$

Proof

We only need a G-invariant definite Hermitian form on V, i.e. $\forall g \in G$, $\langle \rho(g)(x), \rho(g)(y) \rangle = \langle x, y \rangle \ \forall x, y \in V$

We start with an arbitrary positive definite Hermitian form $\langle \cdot, \cdot \rangle'$ on V. ($V \cong \mathbb{C}^n \leftarrow \langle \vec{a}, \vec{b} \rangle := \sum_{i=1}^n a_i \overline{b_i}$)

Define a new $\langle \cdot, \cdot \rangle$ by $\langle x, y \rangle := \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)(x), \rho(g)(y) \rangle'$

Check: $\langle y, x \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)(y), \rho(g)(x) \rangle' = \frac{1}{|G|} \sum_{g \in G} \overline{\langle \rho(g)(x), \rho(g)(y) \rangle'} = \overline{\langle x, y \rangle}$ (positive definite Hermitian form)

We check if $\langle \cdot, \cdot \rangle$ is G-invariant: $\forall g' \in G$, $\langle \rho(g')(x), \rho(g')(y) \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)\rho(g')(x), \rho(g)\rho(g')(y) \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho(gg')(x), \rho(gg')(y) \rangle = \langle x, y \rangle$

DEFINITION

Let $\rho: G \longrightarrow GL(V)$

For subspace $W \subset V$, if $x \in W$, $\rho(g)(x) \in W \ \forall g \in G$, then W is G-invariant and $\rho^W: G \longrightarrow GL(W)$ ($g \mapsto \rho(g)|_W$) is called a **subrepresentation** of ρ

EXAMPLE

Let ρ be the reg. rep. of S_3, then $W = \{\alpha_1 e_1 + \ldots + \alpha_6 e_6 \mid \alpha_1 + \ldots + \alpha_6 = 0\}$ ($\dim W = 5$) is a subrepresentation of V

$W' = \langle e_1 + \ldots + e_6 \rangle_{\mathbb{C}}$ ($\dim W' = 1$) too

THEOREM 2

Let $\rho: G \longrightarrow GL(V)$ and $W \subset V$ be G-invariant. Then $\exists W^\circ \subset V$ that is still G-invariant and $V = W \oplus W^\circ$ ($\rho = \rho^W \oplus \rho^{W^\circ}$)

Proof

We can pick an arbitrary W' with $V = W \oplus W'$ and projection $\pi_1: V \longrightarrow W$ ($y + y' \mapsto y$)

Define $\pi^\circ := \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} \circ \pi_1 \circ \rho(g)$. $V \longrightarrow W$ ($\rho(g)(x) \in V$)

- π° is well-defined: $\forall x \in V$, $\pi_1 \circ \rho(g)(x) \in W$ and $\rho(g)|_W: W \to W$, $\rho(g)^{-1}|_W: W \to W$ $\Rightarrow \rho(g)^{-1} \circ \pi_1 \circ \rho(g)(x) \in W$ ✓
- π° is surjective: $\forall y \in W$, $\rho(g)^{-1} \circ \pi_1 \circ \rho(g)(y) = \rho(g)^{-1} \circ \rho(g)(y) = y$ ✓

Now, notice $\pi^\circ \circ \pi^\circ = \pi^\circ$ ($T^2 = T$) $\Rightarrow V = \operatorname{Im} \pi^\circ \oplus \operatorname{Ker} \pi^\circ$ ($\operatorname{Im} \pi^\circ = W$, $\operatorname{Ker} \pi^\circ = W^\circ$)

- π° is equivariant: $\forall g' \in G$, $\rho(g) \circ \pi^\circ = \pi^\circ \circ \rho(g)$ (we say π° here is G-invariant)

Thus, $\forall x \in V$, $\pi^\circ \circ \rho(g')(x) = \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} \circ \pi_1 \circ \rho(g)(\rho(g')(x)) = \rho(g')\pi^\circ(x)$ ($\rho(g')\rho(g')^{-1}\rho(g)^{-1} = \rho(g')\rho(gg')^{-1}$, $\rho(gg')(x)$)

- $W_0 = \operatorname{Ker} \pi_0$ is G-invariant: $\forall x \in W^\circ$, $\pi^\circ(\rho(g)(x)) = \rho(g)\pi^\circ(x) = \rho(g)(0) = 0 \Rightarrow \rho(g)(x) \in W$

REMARK

If $W \subset V$ is G-invariant, then $W^{\perp}$ (w.r.t. G-invariant positive definite Hermitian form) is also G-invariant

Indeed, $\forall x \in W^{\perp}, y \in W$, $\langle \rho(g)(x), y \rangle = \langle \rho(g)^{-1}\rho(g)(x), \rho(g)^{-1}y \rangle = \langle x, \rho(g^{-1})(y) \rangle = 0 \Rightarrow \rho(g)(x) \in W$ (since $\rho(g^{-1})(y) \in W$)

DEFINITION

$\rho: G \longrightarrow GL(V)$ is **irreducible** if ρ has no proper nontrivial **subrepresentations**

THEOREM 3

Each $\rho: G \longrightarrow GL(V)$ is a direct sum of **irreducible subrepresentations**

Proof

By induction on $\dim V$, $\dim V = 1 \Rightarrow \rho$ is irreducible

For $\dim V > 1$, if ρ is irreducible, then done

Otherwise, $\exists\, W, W^{\circ}$: G-invariant, s.t. $V = W \oplus W^{\circ}$ with $\dim W \geq 1$, $\dim W^{\circ} \geq 1$, i.e. $\rho = \rho^{W} \oplus \rho^{W^{\circ}}$. By induction hypothesis, OK ✓ (OK, OK (by induction hypothesis))

10-18-24 (WEEK 7)

SCHUR'S LEMMA

DEFINITION

Let $\rho: G \longrightarrow GL(V) \ni \rho(g)$

R ↘ ; $\downarrow S_\beta = \{e_i\}$

$GL_n(\mathbb{C}) \ni [\rho(g)]_\beta$

We define the trace function $\chi_\rho: G \longrightarrow \mathbb{C}$, $g \longmapsto \text{Trace}(R(g))$, which we define as the character of ρ

REMARK

(1) χ_ρ is independent of the choice of $\beta = \{e_i\}$ ($\text{Trace}(AB) = \text{Trace}(BA) \Rightarrow \text{Trace}(Q(AQ^{-1})) = \text{Trace}(AQ^{-1}Q) = \text{Trace}(A)$)
For another basis $\beta' = \{e_i'\}$, ρ associated with R', it is easy to see that $R'(g) = Q^{-1}R(g)Q$

(2) $\rho \cong \rho' \Rightarrow \chi_\rho \cong \chi_{\rho'}$

$V \xrightarrow{\rho(g)} V$; $T \downarrow S$; $V' \xrightarrow{\rho'(g)} V'$ $\Rightarrow \rho'(g) = T \circ \rho(g) \circ T^{-1}$

DEFINITION

- The degree of χ_ρ is defined to be the degree of ρ
- χ_ρ is called an irreducible character if ρ is irreducible

BASIC FACTS

1. $\chi_\rho(1) = \text{Trace}(I_n) = n$
2. χ_ρ is a class function, i.e. it is constant on each conjugacy class ($\chi_\rho(aga^{-1}) = \text{Trace}(R(aga^{-1})) = \text{Trace}(R(a)R(g)R(a)^{-1}) = \text{Trace}(R(g)) = \chi_\rho(g)$)
3. $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$: Assume that the eigenvalues of $R(g)$ are $\lambda_1, \dots, \lambda_n$, i.e. they satisfy $0 = \det(\lambda I_n - R(g))$
   Notice, this is the same as $0 = \det(\lambda(A^{-1} - \lambda^{-1} I_n)A) = \lambda^n \det(A^{-1} - \lambda^{-1} I_n)\det(A)$ ($\det(A) \neq 0$) $\Rightarrow \det(A^{-1} - \lambda^{-1} I_n) = 0$
   Then, the eigenvalues of $R(g)^{-1}$ are $\lambda_1^{-1}, \dots, \lambda_n^{-1}$
   $\because g^m = 1 \Rightarrow R(g)^m = I_n \Rightarrow |\lambda_i| = \lambda_i \overline{\lambda_i} = 1 \Rightarrow \lambda_i^{-1} = \overline{\lambda_i} \Rightarrow$ no repeated roots
4. $\chi_{\rho \oplus \rho'} = \chi_\rho + \chi_{\rho'}$: $\rho: G \to GL(V)$, $\rho': G \to GL(V')$ $\Rightarrow \rho \oplus \rho': G \longrightarrow GL(V \oplus V')$, $g \longmapsto \rho(g) \oplus \rho'(g)$ $\Leftrightarrow \begin{pmatrix} R(g) & 0 \\ 0 & R(g') \end{pmatrix}$
   $\therefore \text{Trace}(R \oplus R')(g) = \text{Trace}(R(g)) + \text{Trace}(R'(g))$
5. $\chi_{\rho \otimes \rho'} = \chi_\rho \cdot \chi_{\rho'}$: We define the tensor product as $\rho \otimes \rho': G \longrightarrow GL(V \otimes V')$
   $g \longmapsto \rho(g) \otimes \rho(g'): V \otimes V' \longrightarrow V \otimes V'$
   $e_p \otimes e_q' \longmapsto \rho(g)(e_p) \otimes \rho'(g)(e_q')$

   Now, for $g \in G$, $R(g) = (r_{ij})$, $R'(g) = (r_{ij}')$, we have
   $\rho(g) \otimes \rho(g')(e_p \otimes e_q') = \rho(g)(e_p) \otimes \rho(g')(e_q') = \sum_{i,j} r_{ip} r_{jq}' (e_i \otimes e_j')$
   $\Downarrow$
   $\chi_{\rho \otimes \rho'}(g) = \sum_{p,q} r_{pp} r_{qq}' = (r_{11} + \dots + r_{nn})(r_{11}' + \dots + r_{mm}') = \chi_\rho(g)\chi_{\rho'}(g)$

DEFINITION

Let $C(G, \mathbb{C})$ = the vector space of complex valued functions on G

$\cup$

$\mathcal{C}(G)$ = the vector space of complex valued class functions on G

REMARK

Assume that $\{c_1, \dots, c_k\}$ is the set of distinct conjugacy classes in G

By defining $f_i(c_j) := \delta_{ij}$, $\{f_1, \dots, f_k\}$ forms a basis for $\mathcal{C}(G)$ over $\mathbb{C}$

- $\forall f \in \mathcal{C}(G)$, say $f(c_i) = a_i$, then $f = \sum_{i=1}^{k} a_i f_i$ suffices
- When $\sum_{i=1}^{k} a_i f_i = 0$, for $x_j \in c_j$, $\forall j$, $0 = \sum_{i=1}^{k} a_i f_i(x_j) = a_j$

Hence, $\dim \mathcal{C}(G) = k$

DEFINITION

$\forall \varphi, \psi \in \mathcal{C}(G, \mathbb{C})$, we define $\langle \varphi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}$. This results in $\langle \cdot, \cdot \rangle$ being a positive-definite Hermitian form on $\mathcal{C}(G, \mathbb{C})$

SCHUR'S LEMMA

Let $\rho: G \to GL(V)$ and $\rho': G \to GL(V')$ to be two irreducible representations of G

Let $V \xrightarrow{T} V'$ be G-equivariant

$$\begin{array}{ccc} V & \xrightarrow{T} & V' \\ \downarrow \rho(g) & \circlearrowleft & \downarrow \rho'(g) \\ V & \xrightarrow{T} & V' \end{array}$$

Then, we have: (1) T is not an isomorphism $\Rightarrow T = 0$

(2) $V = V'$, $\rho = \rho' \Rightarrow T = \lambda 1_V$ for some $\lambda \in \mathbb{C}$

Proof

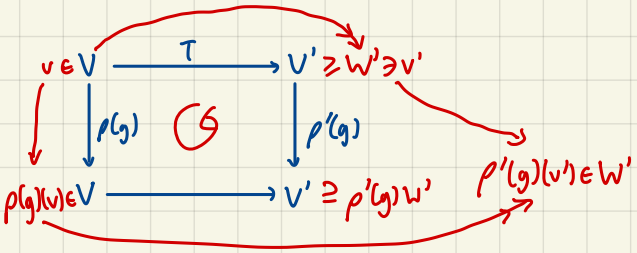
(1) Assume $T \neq 0$.

Let $W = \ker T$. Since T is G-equivariant, thus W is G-invariant

$\because \rho$ is irreducible $\therefore W = V$ or 0

($T = 0$ / T is 1-1)

Let $W' = \operatorname{Im} T$.



$\therefore W'$ is G-invariant $\Rightarrow W' = V'$ or 0

(T is onto / $T = 0$)

(Note: isomorphism = 1-1 + onto, so OK)

(2) Let λ be an eigenvalue of T, say $T(v) = \lambda v$ with $v \neq 0$.

Consider $T' = T - \lambda 1_V$

$\because 0 \neq v \in \ker T'$ $\therefore T'$ is not 1-1

Also, $\begin{array}{ccc} V & \xrightarrow{\lambda 1_V} & V \\ \downarrow \rho(g) & & \downarrow \rho'(g) \\ V & \xrightarrow{\lambda 1_V} & V \end{array}$, since $\rho(g)$ is $\mathbb{C}$-linear. Hence, T' is G-equivariant. By (1), $T' = 0$, i.e. $T = \lambda 1_V$

COROLLARY

For ρ, ρ' as above, let $L \in \operatorname{Hom}_{\mathbb{C}}(V, V')$ Define $T = \frac{1}{|G|} \sum_{g \in G} \rho'(g) \circ L \circ \rho(g)$. Then, ($\rho'(h)^{-1} \circ T \circ \rho(h) = T \ \forall h \in G$)

(1) T is not an isomorphism $\Rightarrow T = 0$

(2) $V = V'$, $\rho = \rho' \Rightarrow T = \lambda 1_V$ with $\lambda = \frac{\operatorname{Trace}(L)}{\dim V}$

Proof: $\lambda \dim V = \operatorname{Trace}(T) = \frac{1}{|G|} \sum_{g \in G} \operatorname{Trace}(\rho(g)^{-1} \circ L \circ \rho(g)) = \operatorname{Trace}(L)$

REMARK

Let $\begin{cases} \rho \xrightarrow{R} R : G \longrightarrow GL_n(\mathbb{C}) \\ \rho' \xrightarrow{R'} R' : G \longrightarrow GL_m(\mathbb{C}) \end{cases}$ and $\begin{cases} R(g) = (r_{ij}(g)) \\ R'(g) = (r'_{ij}(g)) \end{cases}$

Let L with $[L]_\rho^{\rho'} = (x_{\mu\nu}) \in M_{m\times n}(\mathbb{C})$

Then, T with $[T]_\rho^{\rho'} = (x^\circ_{tl})$ with $(x^\circ_{tl}) = \frac{1}{|G|}\sum_{g,i,j} r'_{tj}(g^{-1})\, x_{ji}\, r_{il}(g)$ ("$T = R' L R^{-1}$")

In the case of (1) in the corollary, $\frac{1}{|G|}\sum_{g,i,j} r'_{tj}(g^{-1})\, x_{ji}\, r_{il}(g) = 0$ (*) holds for any $(x_{ji}) \in M_{m\times n}(\mathbb{C})$, s.t. T is not zero

In the case of (2), $T = \lambda 1_V$, i.e. $x^\circ_{tl} = \lambda \delta_{tl}$ and $\lambda = \frac{1}{n}\sum_{i=1}^{n} x_{ii} = \frac{1}{n}\sum_{i,j} \delta_{ji}\, x_{ji}$, we thus have $x^\circ_{tl} \overset{\text{def}}{=} \frac{1}{|G|}\sum_{g,i,j} r_{tj}(g^{-1})\, x_{ji}\, r_{il}(g) \overset{\text{implication}}{=} \frac{1}{n}\sum_{i,j} \delta_{tl}\,\delta_{ji}\, x_{ji}$

Comparing coefficients of x_{ji} on both sides, thus $\frac{1}{|G|}\sum_{g\in G} r_{tj}(g^{-1})\, r_{il}(g) = \frac{1}{n}\delta_{ji}\,\delta_{tl}$ (☆)

PROPOSITION

(1) If χ_ρ is irreducible, then $\langle \chi_\rho, \chi_\rho \rangle = 1$, i.e. χ_ρ is of norm 1

(2) If two irreducible representations ρ, ρ' are not isomorphic, then $\langle \chi_\rho, \chi_{\rho'} \rangle = 0$, i.e. $\chi_\rho \perp \chi_{\rho'}$

Proof

(1) Let ρ be associated to R and $R(g) = (r_{ij}(g)) \in GL_n(\mathbb{C})$

Then, $\langle \chi_\rho, \chi_\rho \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_\rho(g)\overline{\chi_\rho(g)} = \frac{1}{|G|}\sum_{g\in G}\left(\sum_{i=1}^{n} r_{ii}(g)\right)\left(\sum_{j=1}^{n} r_{jj}(g')\right) = \sum_{i=1}^{n}\left(\frac{1}{n}\right) = 1$, where $\overline{\chi_\rho(g)} = \chi_\rho(g^{-1})$

(2) For ρ associated with R, $R(g) = (r_{ij}(g))$

ρ' associated with R' $R'(g) = (r_{\rho' ij}(g))$

(*) for $x_{ji} = 1$, $\langle \chi_\rho, \chi_{\rho'} \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_\rho(g)\overline{\chi_{\rho'}(g)} = \frac{1}{|G|}\sum_{g\in G}\left(\sum_{j=1}^{m} r'_{jj}(g^{-1})\right)\left(\sum_{i=1}^{n} r_{ii}(g)\right) = 0$ ↯ where $\overline{\chi_{\rho'}(g)} = \chi_{\rho'}(g^{-1})$

10-25-24 (WEEK 8)

ORTHOGONALITY

PROPOSITION 1

Let $\rho: G \to GL(V)$ and $\rho = \rho^{W_1} \oplus \dots \oplus \rho^{W_s}$, where $W_i \subseteq V$, $\rho_i := \rho^{W_i}$ is irreducible $\forall i$

If $\tilde{\rho}: G \to GL(W)$ is an irreducible representation then the number of ρ_i isomorphic to $\tilde{\rho}$ is equal to $\langle \chi_\rho, \chi_{\tilde{\rho}} \rangle$

Proof

We know $\chi_\rho = \chi_{\rho_1} + \dots + \chi_{\rho_s}$, so $\langle \chi_\rho, \chi_{\tilde{\rho}} \rangle = \sum_{i=1}^{s} \langle \chi_{\rho_i}, \chi_{\tilde{\rho}} \rangle$

Also if $\rho_i \cong \tilde{\rho}$ $(\chi_{\rho_i} = \chi_{\tilde{\rho}})$, then $\langle \chi_{\rho_i}, \chi_{\tilde{\rho}} \rangle = \langle \chi_{\rho_i}, \chi_{\rho_i} \rangle = 1$. Otherwise, $\langle \chi_{\rho_i}, \chi_{\tilde{\rho}} \rangle = 0$. □

OBSERVE

(1) If character $\chi_\rho = \chi_{\rho'}$, then $\rho \cong \rho'$

Proof

Write $\rho = \rho^{W_1} \oplus \dots \oplus \rho^{W_s}$, $\rho' = \rho^{W_1'} \oplus \dots \oplus \rho^{W_t'}$

For any irr rep $\tilde{\rho}: G \to GL(\tilde{W})$, $\#\rho^{W_i}$ isomorphic to $\tilde{\rho} = \#\rho^{W_i'}$ isomorphic to $\tilde{\rho}$ ✓

(2) If $\chi_1, \dots, \chi_\ell$ are distinct irr characters of G, then $\because \chi_1, \dots, \chi_\ell$ are orthonormal w.r.t. $\langle \cdot, \cdot \rangle$

$\therefore \chi_1, \dots, \chi_\ell$ are linearly independent over $\mathbb{C}$ in $\mathcal{C}(G)$

Also, $\because \dim_{\mathbb{C}} \mathcal{C}(G) = k = \#$distinct conjugacy classes in G $\therefore \ell \le k$

We conclude that there are at most k naturally non-isomorphic irr rep of G, say $\rho_1, \dots, \rho_\ell$, $\ell \le k$

For any $\rho: G \to GL(V)$, $\rho \cong \rho_1^{\oplus m_1} \oplus \dots \oplus \rho_\ell^{\oplus m_\ell}$ where $m_i := \langle \chi_\rho, \chi_{\rho_i} \rangle \in \mathbb{N}_0$ is known as the multiplicity of ρ_i

PROPOSITION 2

If $\rho: G \to GL(V)$, then $\langle \chi_\rho, \chi_\rho \rangle \in \mathbb{N}_0$ and "$\langle \chi_\rho, \chi_\rho \rangle = 1 \iff \rho$ is irr"

Proof

Write $\rho = \rho_1^{\oplus m_1} \oplus \dots \oplus \rho_\ell^{\oplus m_\ell}$, then $\chi_\rho = \sum_{i=1}^{\ell} m_i \chi_{\rho_i}$, so $\langle \chi_\rho, \chi_\rho \rangle = \sum_{i=1}^{\ell} m_i^2$

"$\Rightarrow$": $\langle \chi_\rho, \chi_\rho \rangle = \sum_{i=1}^{\ell} m_i^2 = 1 \Rightarrow \exists\, m_i = 1$ and $m_j = 0$ $\forall i \neq j$, i.e. $\rho \cong \rho_i$

THEOREM

$\ell = k$

Proof

Define $D = \langle \chi_1, \dots, \chi_\ell \rangle \subseteq \mathcal{C}(G)$ (Hope "$D = \mathcal{C}(G) \Rightarrow \dim D = \ell$, $\dim \mathcal{C}(G) = k$")

Then, $\mathcal{C}(G) = D \oplus D^\perp$

Claim: $D^\perp = 0$

Proof

For $\rho \in D^\perp$, we hope "$\rho(g) = 0$ $\forall g \in G$"

Notice, $\langle \varphi, \chi_i \rangle = 0$ $\forall i = 1, \dots, \ell \Rightarrow \langle \varphi, \chi_\rho \rangle = 0$ $\forall \rho: G \to GL(V)$.

Define $T_\rho \in \mathrm{Hom}_{\mathbb{C}}(V, V)$. By $T_\rho = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)}\, \rho(g) \Rightarrow \mathrm{Trace}(T_\rho) = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)}\, \chi_\rho(g) = \langle \varphi, \chi_\rho \rangle$

- T_ρ is G-equivariant ($\rho(G) \circ T = T \circ \rho(G)$) w.r.t. $\rho: G \to GL(V)$

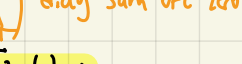
  Let $\{C_1, \dots, C_k\}$ be the set of conjugacy classes in G.

  $\forall h \in G$, $\rho(h)^{-1} \circ T_\rho \circ \rho(h) = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)}\, \rho(h)^{-1} \circ \rho(g) \circ \rho(h) = \frac{1}{|G|} \sum_{i=1}^{k} \overline{\varphi(g_i)} \sum_{g \in C_i} \rho(h^{-1}gh) = \frac{1}{|G|} \sum_{i=1}^{k} \overline{\varphi(g_i)} \sum_{g' \in C_i} \rho(g') = \frac{1}{|G|} \sum_{i=1}^{k} \sum_{g'' \in C_i} \overline{\varphi(g'')}\, \rho(g'') = T_\rho$

For $\rho = \rho_i$, by Schur's Lemma, $T_{\rho_i} = \lambda_i 1_{W_i}$, where $\rho_i: G \to GL(W_i)$

However, $\mathrm{Trace}(T_{\rho_i}) = 0 \Rightarrow \lambda_i = 0 \Rightarrow T_{\rho_i} = 0$

In general, $\rho \cong \rho_1^{\oplus m_1} \oplus \dots \oplus \rho_\ell^{\oplus m_\ell}$, so $T_{\rho_i} = 0$ $\forall i \Rightarrow T_\rho = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)}\, \rho(g) = 0$



diag sum of c zero

In particular, $\rho = \rho^{reg}: G \to GL(V)$ where $V = \bigoplus_{g\in G} \mathbb{C}e_g$

Then, $T_\rho = 0 \Rightarrow 0 = T_\rho(e_1) = \frac{1}{|G|}\sum_{g\in G} \overline{\varphi(g)}\,\rho(g)(e_1) \overset{=e_g}{\Rightarrow} \overline{\varphi(g)} = 0 \ \forall g \in G$, so $\varphi = 0$ in $\mathcal{C}(G)$ ○

PROPOSITION 2

Every irr rep $\rho_i: G \to GL(W_i)$ is contained in ρ^{reg} with multiplicity equal to $\dim W_i = m_i$:

In particular, $\bigoplus_{g\in G} \mathbb{C}e_g \cong (W_1 \oplus \dots \oplus W_1) \oplus \dots \oplus (W_k \oplus \dots \oplus W_k) \Rightarrow |G| = m_1^2 + \dots + m_k^2$
(m_1 times; m_k times)

Proof

Let $\chi^{reg} := \chi_{\rho^{reg}}$ and $\chi_i := \chi_{\rho_i}$, $i = 1, \dots, k$

Then, $\langle \chi^{reg}, \chi_i \rangle = \frac{1}{|G|}\sum_{g\in G} \chi^{reg}(g)\,\chi_i(g^{-1}) = \frac{1}{|G|}|G| m_i = m_i$

Note: $\chi^{reg}(g) = \mathrm{Tace}(\rho^{reg}(g)) = \begin{cases} |G|, & g = 1 \\ 0, & \text{otherwise} \end{cases}$, so $[\rho^{reg}(g)] = \begin{pmatrix} 0 & & \\ & \ddots & \\ & & 0 \end{pmatrix}$, for $g \neq 1$

EXAMPLE 1

For $G = C_n = \langle a \rangle$ with $a^n = 1$, we have $k = n$ (i.e. we have n representations)

$\rho_j: G \to \mathbb{C}^*$

$a \longmapsto \xi_j$ with $\xi_j^n = 1$ ($a^n = 1$), i.e. $\xi_j = e^{\frac{2\pi i}{n} j}$

Here, $\langle \chi_{\rho_j}, \chi_{\rho_j} \rangle = \frac{1}{n}\sum_{t=0}^{n-1} \chi_{\rho_j}(a^t)\,\overline{\chi_{\rho_j}(a^t)} = \frac{1}{n}\sum_{t=0}^{n-1} \xi_j^t \overline{\xi_j^t} \overset{=1}{=} \frac{1}{n}(n) = 1$

Also, $\langle \chi_{\rho_j}, \chi_{\rho_s} \rangle = \frac{1}{n}\sum_{t=0}^{n-1} e^{\frac{2\pi i}{n}(j-s)t} = 0$ ($j \neq s$)

EXAMPLE 2

For $G = S_3 = D_6$, we have 3 conjugacy classes $(1, (1\,2), (1\,2\,3))$

$\therefore 6 = 1^2 + 1^2 + 2^2$

The permutation representation, $V = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3$

$\rho: S_3 \longrightarrow \underset{\cong GL_3(\mathbb{C})}{GL(V)}$,

$1 \longmapsto I_3$, $\chi_\rho(1) = 3$

$2 \longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\chi_\rho((1\,2)) = 1$

$3 \longmapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, $\chi_\rho((1\,2\,3)) = 0$

$V = \mathbb{C}(e_1 \oplus e_2 \oplus e_3) \oplus W$ ($\mathbb{C}(e_1 \oplus e_2 \oplus e_3) = U$)

So, $\chi_\rho = \chi^U \oplus \chi^W$

$\begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix}$ (deduced)

This means, $\langle \chi^W, \chi^W \rangle = \frac{1}{6}(2^2 + 3(0)^2 + 2(-1)^2) = 1 \Rightarrow \rho^W$ is irr

Character Table:

classes	1	(1 2)	(1 2 3)
size	1	3	2
deg=1 χ_1	1	1	1
deg=1 χ_2	1	−1	1
deg=2 χ_3	2	0	−1

(χ_2 deduced from $\chi^{reg} = \chi_1 + \chi_2 + 2\chi_3 \Rightarrow \begin{pmatrix} 6 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 2\begin{pmatrix} 2 \\ -1 \end{pmatrix}$)

($\otimes$ increases size faster than $\oplus$)

Now, $\tilde{\rho} = \rho^W \otimes \rho^W \Rightarrow \chi_{\tilde{\rho}} = \chi_3 \cdot \chi_3 = \begin{pmatrix} 4 \\ 0 \end{pmatrix} \Rightarrow \langle \chi_{\tilde{\rho}}, \chi_1 \rangle = \frac{1}{6}(1(4\cdot 1) + 3(0\cdot 1) + 2(1\cdot 1)) = 1$

$\langle \chi_{\tilde{\rho}}, \chi_2 \rangle = \frac{1}{6}(1(4\cdot 1) + 3(0\cdot -1) + 2(1\cdot 1)) = 1$

$\langle \chi_{\tilde{\rho}}, \chi_3 \rangle = \frac{1}{6}(1(4\cdot 2) + 3(0\cdot 0) + 2(1\cdot -1)) = 1$

} that's the point of a tensor

10-30-24 (WEEK 9)

DIVISIBILITY

GOAL

$m_i \mid |G|$, i.e. $\frac{|G|}{m_i} \in \mathbb{Z}$

DEFINITION

Let R be a ring s.t. $\mathbb{Z} \subseteq R$

For $a \in R$, a is said to be an **algebraic integer** if $\exists$ monic polynomial $f(x) \in \mathbb{Z}[x]$, s.t. $f(a)=0$ (or a is **integral** over $\mathbb{Z}$)

Then, $\mathbb{Z}(a) = \{f(a) \mid f(x) \in \mathbb{Z}[x]\}$

FACT

a is integral over $\mathbb{Z} \Rightarrow \mathbb{Z}[a]$ is a finitely generated $\mathbb{Z}$-module

Proof

Assume that $a^n + r_{n-1}a^{n-1} + \dots + r_1 a + r_0 = 0$ with $r_i \in \mathbb{Z}$

Then $a^n = -r_{n-1}a^{n-1} - \dots - r_0$, so $\mathbb{Z}[a] = \langle 1, a, a^2, \dots, a^{n-1} \rangle_{\mathbb{Z}}$

KEY PROPOSITION

Let $a \in R$. TFAE

(1) a is integral over $\mathbb{Z}$

(2) $\mathbb{Z}[a]$ is a finitely generated $\mathbb{Z}$-module

(3) $\mathbb{Z}[a] \subseteq S \subseteq R$ (subring), s.t. S is a f.g. $\mathbb{Z}$-module (Convenient to be used)

(4) There exists a faithful $\mathbb{Z}[a]$-module M which is f.g. as a $\mathbb{Z}$-module (Convenient to prove)

Proof

(1) $\Rightarrow$ (2): OK

(2) $\Rightarrow$ (3): $S = \mathbb{Z}[a]$

(3) $\Rightarrow$ (4): $M = S$ ($\because \mathbb{Z}[a] \subseteq M$ $\therefore M$ is a $\mathbb{Z}[a]$-module)

Faithful: if $f(a)M = 0$, then $1 \in M = S$ module, so $f(a) \cdot 1 = f(a) = 0$

(4) $\Rightarrow$ (1): Let $M = \langle v_1, \dots, v_m \rangle_{\mathbb{Z}}$

$\because \mathbb{Z}[a] \times M \longrightarrow M$

$(a, v_i) \longmapsto a v_i$

$\therefore$ We can write $a v_i = \sum_{j=1}^{m} r_{ij} v_j$ $\forall i$ (★)

Rewriting (★), we have $\sum_{j=1}^{m} (r_{ij} - a\delta_{ij}) v_j = 0$ $\forall i$, which in matrix form is:

$$A := \begin{pmatrix} r_{11}-a & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22}-a & \cdots & r_{2m} \\ \vdots & & & \\ r_{m1} & \cdots & & r_{mm}-a \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} = 0$$

Thus, $(\mathrm{adj}\, A) A \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = 0 \Rightarrow (\det A) v_i = 0$ $\forall i \Rightarrow (\det A) M = 0 \Rightarrow \det A = 0$ (Faithful)

COROLLARY 1

Let $a_1, \dots, a_n$ be integral elements in R over $\mathbb{Z}$. Then the ring $\mathbb{Z}[a_1, \dots, a_n]$ is a f.g. $\mathbb{Z}$-module

Proof

By induction on n,

- $n=1$: OK (from above)
- $n>1$: Observe that $\mathbb{Z}[a_1, \dots, a_n] = \mathbb{Z}[a_1, \dots, a_{n-1}][a_n]$

$\because$ By induction hypothesis, $\mathbb{Z}[a_1, \dots, a_{n-1}] = \langle g_1, \dots, g_\ell \rangle$ and $\mathbb{Z}[a_1, \dots, a_n] = \langle f_1, \dots, f_m \rangle$ ($\because a_n$ is integral $\mathbb{Z}[a_1, \dots, a_{n-1}]$)

$\therefore \forall F \in \mathbb{Z}[a_1, \dots, a_n]$, $F = h_1 f_1 + \dots + h_m f_m$ where $h_i \in \mathbb{Z}[a_1, \dots, a_{n-1}]$ ($h_i = \sum_{j=1}^{\ell} r_{ij} g_j$) $\Rightarrow F = (\sum_{i,j} r_{ij} g_j) f_1 + \dots$

Thus, $\mathbb{Z}[a_1, \dots, a_n] = \langle g_j f_i \mid {\scriptstyle j=1,\dots,\ell \atop i=1,\dots,m} \rangle_{\mathbb{Z}}$

COROLLARY 2

$a,b \in R$ are integral over $\mathbb{Z} \Rightarrow a+b$, ab are integral over $\mathbb{Z}$

Proof

By corollary 1, $\mathbb{Z}[a,b]$ is a f.g. $\mathbb{Z}$-module. And $\mathbb{Z}[a+b] \subseteq \mathbb{Z}[a,b] \subset R$ (or $a-b, ab$) $\Rightarrow$ By key prop, $a+b$ is integral over $\mathbb{Z}$

THEOREM

$\forall i = 1, \dots, k$, $m_i \mid |G|$

Proof

For $\rho = \rho_i$ (W_i), $\chi = \chi_i$, $T = \sum_{g \in C_j} \rho(g) = \frac{|C_j| \chi(g_0)}{m_i} I_{m_i}$ ($W_i \to W_i$) $\forall g_0 \in C_j$

Observe that $\forall h \in G$, $\rho(h)^{-1} \circ T \circ \rho(h) = \sum_{g \in C_j} \rho(h^{-1}gh) = \sum_{g' \in C_j} \rho(g') = T$ $\Rightarrow$ (Schur's Lemma) T is G-equivariant, W_i is irreducible, $T = \lambda I_{m_i}$ for some $\lambda \in \mathbb{C}$

And $m_i \lambda = \text{Trace}(T) = \sum_{g \in C_j} \chi(g) = \chi(g_0)|C_j|$ for any $g_0 \in C_j$ $\Rightarrow \lambda = \frac{|C_j| \chi(g_0)}{m_i}$

Now, claim $\lambda_\mu(C_j) := \frac{|C_j| \chi_\mu(g_0)}{m_\mu}$ for $g_0 \in C_j$ is an algebraic integer

Notice, $\mathbb{Z}[\lambda_\mu(C_j)] \subseteq \mathbb{Z}[\lambda_\mu(C_1), \dots, \lambda_\mu(C_k)] = \langle \lambda_\mu(C_1), \dots, \lambda_\mu(C_k) \rangle_{\mathbb{Z}}$ ✓ $(\lambda_\mu(C_i)\lambda_\mu(C_\ell) = \sum_{t=1}^{k} a_{t} \lambda_\mu(C_t))$

For $g \in C_\ell$, $a_{i,j,\ell} = \#$ of $\{(g_i, g_j) \in C_i \times C_j\} \in \mathbb{N}_0$

Claim: $\lambda_\mu(C_i)\lambda_\mu(C_j) = \sum_{\ell=1}^{k} a_{i,j,\ell} \lambda_\mu(C_\ell)$ $\forall i, j, \mu$

Proof

Let $\rho = \rho_\mu$.

$\lambda_\mu(C_i)\lambda_\mu(C_j) I_{m_\mu} = (\lambda_\mu(C_i) I_{m_\mu})(\lambda_\mu(C_j) I_{m_\mu}) = \sum_{g \in C_i} \rho(g) \sum_{h \in C_j} \rho(h) = \sum_{g \in C_i, h \in C_j} \rho(gh) = \sum_{\ell=1}^{k} \sum_{g \in C_\ell} a_{i,j,\ell} \rho(g') = \sum_{\ell=1}^{k} a_{i,j,\ell} \sum_{g' \in C_\ell} \rho(g') = \sum_{\ell=1}^{k} a_{i,j,\ell} \lambda_\mu(C_\ell) I_{m_\mu}$

Hence, $\mathbb{Z}[\lambda_\mu(C_1), \dots, \lambda_\mu(C_k)] = \langle 1, \lambda_\mu(C_1), \dots, \lambda_\mu(C_k) \rangle_{\mathbb{Z}}$ $\Rightarrow$ By key prop (3), $\lambda_\mu(C_j)$ is integral over $\mathbb{Z}$

Now, notice $\frac{|G|}{m_i} = \frac{|G|}{m_i}(\chi_i, \chi_i) = \frac{1}{m_i} \sum_{g \in G} \chi_i(g)\chi_i(g^{-1}) = \frac{1}{m_i} \sum_{j=1}^{k} \chi_i(g_j) \sum_{g \in C_j} \chi_i(g^{-1}) = \sum_{i=1}^{k} \frac{|C_j| \chi_i(g_j)}{m_i} \chi_i(g_j^{-1})$ for $g_j \in C_j$ $\Rightarrow$ MUST BE AN INTEGER

($\frac{|C_j|\chi_i(g_j)}{m_i} = \lambda_i(C_j)$; $\chi_i(g_j^{-1})$ = sum of roots of unity is also an integer)

EXAMPLE

$G = D_8 = \langle r, s \mid r^4 = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$

$|G| = 8$, $srs^{-1}r^{-1} = r^{-2}$, $sr^2s^{-1}r^{-2} = 1$, $sr^3s^{-1}r^{-3} = r^{-3}r^{-3} = r^{-2} \Rightarrow [G,G] = \langle r^2 \rangle$

$\therefore |G/[G,G]| = 4$

$\| $

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{C}^\times$

$(\bar{1}, \bar{0}) \longmapsto \pm 1$ $\Rightarrow 8 = |G| = (-1)^2 + (-1)^2 + 1^2 + 1^2 + 2^2$

$(\bar{0}, \bar{1}) \longmapsto \pm 1$

Classes	1	s	r	r^2	rs	
Sizes	1	2	2	1	2	
χ_1	1	1	1	1	1	deg = 1
χ_2	1	-1	-1	1	1	deg = 1
χ_3	1	1	-1	1	-1	deg = 1
χ_4	1	-1	1	1	-1	deg = 1
χ_5	2	0	0	-2	0	deg = 2 $(\chi_5, \chi_5) = 1$

Let ρ_5 (geometric representation):

$s \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$r \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$r^2 \longmapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$rs \longmapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

11-1-24 (WEEK 9)

APPLICATIONS

EXAMPLE 1

$G = S_4 \Rightarrow |G| = 24$

$\because S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$: abelian $\therefore [G,G] \leq A_4$

$\because S_4/V_4$ is not abelian (and $[G,G] \leq A_4$) $\therefore [G,G] = A_4$

$\therefore G/[G,G] \cong \mathbb{Z}/2\mathbb{Z} \Rightarrow$ # rep deg 1 = 2

Permutation Representation

$\rho: S_4 \longrightarrow GL(V)$

$1 \longmapsto V$

$(12) \longmapsto \begin{pmatrix} 0 & 1 & \cdots \\ \vdots & & \end{pmatrix}$

$V = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3 \oplus \mathbb{C}e_4$

$\chi_\rho = (4,2,1,0,0) \Rightarrow V = \mathbb{C}(e_1+e_2+e_3+e_4) \oplus W \Rightarrow \chi^W = (3,1,0,-1,-1)$, where $\langle \chi_W, \chi_W \rangle = \frac{1}{24}(1\cdot 3^2 + 6\cdot 1^2 + 8\cdot 0^2 + 6(-1)^2 + 3(-1)^2) = 1$

(!! $\cup$ $e_1+e_2+e_3+e_4$)

Character Table:

Classes	1	(12)	(123)	(1234)	(12)(34)
Size	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

Notice, $24 = 1^2+1^2+2^2+3^2+3^2$

$\chi^{reg} = (24,0,0,0,0) = \chi_1 + \chi_2 + 2\chi_3 + 3\chi_4 + 3\chi_5$ (coef: deg)

(Permutation Representation) ($\rho_2 \otimes \rho^W$)

EXAMPLE 2

$G = A_4 \Rightarrow |G| = 12$

$A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z} \Rightarrow [A_4,A_4] \leq V_4$

$A_4/\langle (12)(34) \rangle$ is not abelian

$\Rightarrow [A_4,A_4] = V_4$, so $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{C}^\times$, where $x^3-1=0 \Rightarrow x = 1, \omega, \omega^2$

Character Table

Classes	1	(123)	(213)	(12)(34)	
Size	1	4	4	3	
χ_1	1	1	1	1	(must have)
χ_2	1	ω	ω^2	1	(roots of unity if cannot 1,-1,1,...,1 end on 1)
χ_3	1	ω^2	ω	1	
χ_4	3	0	0	-1	(deduced from χ_{reg})

EXAMPLE 3

$G = S_5$ $\quad 120 = 1^2+1^2+4^2+4^2+5^2+5^2+6^2$ (remaining, so act on deg 6)

Classes	1	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
Size	1	10	20	30	24	15	20
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	5	-1	-1	1	0	1	-1
χ_6	5	1	-1	-1	0	1	1
χ_7	6	0	0	0	1	-2	0

$\hookrightarrow (120,0,0,0,0,0,0) = \chi_1 + \chi_2 + 4\chi_3 + 4\chi_4 + 5\chi_5 + 5\chi_6 + 6\chi_7$

Permutation Representation $\Rightarrow$ deg 4

$\chi_\rho = (5,3,2,1,0,1,0)$

$\chi^W = (4,2,1,0,-1,0,-1) \Rightarrow \langle \chi^W, \chi^W \rangle = 1$

$\chi_\rho \chi^W = (4,-2,1,0,-1,0,1)$

Action (deg 6)

$(1+5k)|24 \Rightarrow n_5 = 6$. Let $X = Syl_5(6) = \{P_1, P_2, P_3, P_4, P_5, P_6\}$

($P_1 = \langle (12345) \rangle$, $P_2 = \langle (12453) \rangle$, $P_3 = \langle (12543) \rangle$, $P_4 = \langle (12354) \rangle$, $P_5 = \langle (12435) \rangle$, $P_6 = \langle (12534) \rangle$)

$S_5 \times X \longrightarrow X$

$(\sigma, P_i) \longmapsto \sigma P_i \sigma^{-1}$

$\frac{|S_5|}{|N_{S_5}(P_1)|} = 6$ ($N_{S_5}(P_1) = \langle (1\,2\,3\,4\,5), (2\,3\,4\,5) \rangle$)

$S_5 \times V \longrightarrow V$

$(\sigma, e_i) \longmapsto e_j$ if $\sigma P_i \sigma^{-1} = P_j$

$\Psi: S_5 \longrightarrow GL(V)$, $\sigma \longmapsto$ "$\sigma: e_i \mapsto e_j$"

For $\sigma P_i \sigma^{-1} = P_i$,

Notice, $\chi_4(\sigma) = \#P_i$ normalizing $\sigma \Rightarrow \chi_4 = (6,0,0,2,1,2,0)$

$\chi_{\omega'} = (5,-1,-1,1,0,1,-1) \Rightarrow \langle \chi_{\omega'}, \chi_{\omega'} \rangle = 1$

PRODUCT OF GROUPS

Let $\rho: G \to GL(V)$ and $\rho': G' \to GL(V')$. Then, $\rho \oplus \rho': G \times G' \to GL(V \oplus V')$ works, but is not irreducible $(V \oplus \langle 0 \rangle, \langle 0 \rangle \oplus V')$

We can consider: $\rho \otimes \rho': G \times G' \longrightarrow GL(V \otimes V')$

$(s, s') \longmapsto \rho(s) \otimes \rho'(s') : V \otimes V' \longrightarrow V \otimes V'$

$v \otimes v' \longmapsto \rho(s)(v) \otimes \rho(s)(v')$

PROPOSITION

(1) If ρ, ρ' are irreducible, then $\rho \otimes \rho'$ is irreducible

(2) Every irr rep of $G \times G'$ is iso to some $\rho \otimes \rho'$

Proof

(1) $\langle \chi_\rho, \chi_\rho \rangle = 1 \Rightarrow \frac{1}{|G|} \sum_{s \in G} \chi_\rho(s) \overline{\chi_\rho(s)} = \frac{1}{|G|} \sum_{s \in G} |\chi_\rho(s)|^2 = 1$

$\langle \chi_{\rho'}, \chi_{\rho'} \rangle = 1 \Rightarrow \frac{1}{|G|} \sum_{s' \in G} |\chi_{\rho'}(s')|^2 = 1$

Multiplying the above, we get $\frac{1}{|G||G|} \left(\sum_{s \in G} |\chi_\rho(s)|^2 \right) \left(\sum_{s' \in G} |\chi_{\rho'}(s')|^2 \right) = \frac{1}{|G \times G|} \sum_{s, s' \in (G, G')} |\chi_\rho(s) \chi_{\rho'}(s')|^2 = \frac{1}{|G \times G'|} \sum_{s, s' \in (G, G')} |\chi_{\rho \otimes \rho'}(s \otimes s')|^2 = 1$

(2) Let $\{\rho_1, \dots, \rho_k\}$ and $\{\rho_1', \dots, \rho_{k'}'\}$ be the set of distinct irr rep of G and G' respectively.

Write $\chi_i = \chi_{\rho_i}$, $\chi_j' = \chi_{\rho_j'}$.

Claim: $\mathcal{C}(G \times G') = \langle \chi_{\rho_i \otimes \rho_j'} \mid i = 1, \dots, k,\ j = 1, \dots, k' \rangle_{\mathbb{C}}$ (ii ⊕)

Proof

Let $f \in \oplus^\perp$. By def, $\langle f, \chi_{\rho_i \otimes \rho_j'} \rangle = 0 \ \forall i, j \Rightarrow \frac{1}{|G \times G'|} \sum_{(s,s') \in (G,G')} f(s,s') \overline{\chi_i(s) \chi_j'(s')} = 0$

In particular, $\forall i = 1, \dots, k$, $\frac{1}{|G|} \sum_{s' \in G} \left(\frac{1}{|G|} \sum_{s \in G} (f(s,s') \overline{\chi_i(s)}) \right) \overline{\chi_j'(s')} = 0 \ \forall j = 1, \dots, k' \Rightarrow \left\langle \frac{1}{|G|} \sum_{s \in G} f(s, \cdot) \overline{\chi_i(s)}, \chi_j' \right\rangle = 0 \ \forall j$ $\left(\sum_{s \in G} f(s, \cdot) \overline{\chi_i(s)} = 0 \ \forall i \text{ too} \right)$

$\therefore f(\cdot, s') \in \langle \chi_1, \dots, \chi_k \rangle^{\perp_{\mathcal{C}(G)}} = 0$

$\therefore f(s, s') = 0 \ \forall s \in G, s' \in G'$ □

EXAMPLE (why this idea cannot extend to semidirect product)

For $A_3 \leq S_3$, $A_3 = [S_3, S_3]$

$\rho: A_3 \longrightarrow \mathbb{C}^\times$

$1 \longmapsto 1$

$(123) \longmapsto \omega$

$(132) \longmapsto \omega^2$

$\tilde{\rho}: G \to \mathbb{C}^\times$?

DEFINITION (turning groups into rings)

$\mathbb{C}[G] := \left\{ \sum_{s \in G} r_s s \mid r_s \in \mathbb{C} \right\}$ and $\sum_{s \in G} r_s s = \sum_{s \in G} r_s' s \Leftrightarrow r_s = r_s' \ \forall s \in G$, we define:

↳ Addition: $\sum_{s \in G} r_s s + \sum_{s \in G} r_s' s = \sum_{s \in G} (r_s + r_s') s$

↳ Multiplication: $\left(\sum_{s \in G} r_s s \right) \left(\sum_{s \in G} r_s' s \right) := \sum_{s \in G} \left(\sum_{rr' = s} r_r r_{r'}' \right) s$ (satisfies dist prop)

This is called an **algebra**

FACTS

(1) $\{V: a\ \mathbb{C}[G]\ module\} \leftrightarrow \{\rho: G \to GL(V)\}$

$\mathbb{C}[G] \times V \longrightarrow V \Rightarrow \mathbb{C} \times V \to V \Rightarrow V$: $\mathbb{C}$-vector space

$s \mapsto \tilde{\rho}(s): x \mapsto \varphi(s, x)$

ring homo $\tilde{\rho}: \mathbb{C}[G] \to End(V) \Rightarrow \rho = \tilde{\rho}|_G : G \to End(V)$

- $\forall s \in G$, $\rho(s)$ is $\mathbb{C}$-linear: $\forall r \in \mathbb{C}, x \in V$, $\rho(s)(rx) = \tilde{\rho}(s)(\varphi(r,x)) = \varphi(s, \varphi(r,x)) = \varphi(\underline{sr}, x) = \varphi(r, \varphi(s,x)) = \varphi(r, \rho(s)(x)) = r\rho(s)(x)$ (module; $rs (: r \in \mathbb{C})$)
- $\forall s \in G$, $\rho(s)$ is invertible: $\rho(s)\rho(s^{-1}) = \rho(s \cdot s^{-1}) = \rho(1) = Id_V \Rightarrow \rho(s)^{-1} = \rho(s^{-1})$

$\therefore$ "$\to$" is done. "$\leftarrow$" can be done with extension by linearity with $\mathbb{C}[G] \times V \longrightarrow V$, $(\sum r_s s, x) \longmapsto \sum r_s \rho(s)(x)$

EXTENSIONS OF LINEAR REPRESENTATIONS

$\rho : H \to GL(V)$ associates $V : \mathbb{C}[H] \subseteq \mathbb{C}[G]$ module $\Rightarrow \mathbb{C}[G] : \mathbb{C}[H]$ module
$V : \mathbb{C}[H]$ module
$\Rightarrow {}^{(g \otimes v)}\mathbb{C}[G]_{\mathbb{C}[H]} \otimes V$ (which is a $\mathbb{C}[G]$-module)

Then, $\tilde{\rho} : G \to GL(\tilde{V})$, where $\tilde{V} = {}^{\mathbb{C}[G]}\mathbb{C}_{[H]} \otimes V$ for $G = K \rtimes H$, H is abelian or cyclic $\Rightarrow$ recover G

11-6-24 (WEEK 10)

EXTENSIONS OF ABELIAN GROUPS

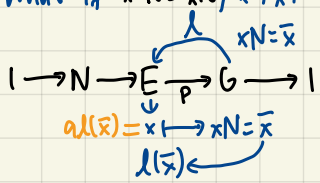
RECALL

If a group E contains a normal subgroup N and $E/N \cong G$, then we call E an **extension of N by G**, denoted by
$1 \hookrightarrow N \to E \overset{p}{\twoheadrightarrow} G \to 1$

When N and G are given, how do we obtain all extensions of N by G?

EXPERIMENTATION

What if $x'N = xN$, $x' \neq x$?



We get $xN = l(\bar{x})N \Rightarrow l(\bar{x})^{-1}x = a \in N \Rightarrow x = a\,l(\bar{x})$

If $a\,l(\bar{x}) = b\,l(\bar{y})$ in E, $p(a\,l(\bar{x})) = p(b\,l(\bar{y})) \Rightarrow p(a)\,p(l(\bar{x})) = p(b)\,p(l(\bar{y})) \Rightarrow \bar{1}(\bar{x}) = \bar{1}(\bar{y}) \Rightarrow \bar{x} = \bar{y} \Rightarrow a = b$ (unique!) (Kernel)

For two distinct $a\,l(\bar{x})$, $b\,l(\bar{y})$, $(a\,l(\bar{x}))(b\,l(\bar{y})) = a\,(l(\bar{x})\,b\,l(\bar{x})^{-1})\,l(\bar{x})\,l(\bar{y})$ ($l(\bar{x})\,b\,l(\bar{x})^{-1} \in N$)

We have $p(l(\bar{x})\,l(\bar{y})) = p(l(\bar{x}\bar{y})) = \bar{x}\bar{y} \Rightarrow l(\bar{x})\,l(\bar{y}) = f(\bar{x},\bar{y})\,l(\bar{x}\bar{y})$ ($f(\bar{x},\bar{y}) \in N$)

DEFINITION

$1 \to N \to E \overset{p}{\underset{l}{\rightleftarrows}} G \to 1$ has a **lifting** if $p \circ l = \mathrm{id}_G$ and $l(1) = 1$

PROPOSITION 1

(1) $\forall \bar{x} \in G$, $\theta_{\bar{x}} : N \to N$, $a \mapsto l(\bar{x})\,a\,l(\bar{x})^{-1}$ is **indep of choice of N**

Proof

Suppose $l' : G \to E$ is another lifting $\because l(\bar{x})N = l'(\bar{x})N$ $\therefore l(\bar{x})^{-1}l'(\bar{x}) = b \in N$, i.e. $l'(\bar{x}) = l(\bar{x})$

$\forall a \in N$, $l'(\bar{x})\,a\,l'(\bar{x})^{-1} = (l(\bar{x})b)\,a\,(l(\bar{x})b)^{-1} = l(\bar{x})\,bb^{-1}a\,l(\bar{x})^{-1} = l(\bar{x})\,a\,l(\bar{x})^{-1}$

(2) $\theta : G \to \mathrm{Aut}(N)$, $\bar{x} \mapsto \theta_{\bar{x}}$ is a **group homo**

Proof

$\theta_{\bar{x}\bar{y}}(a) = l(\bar{x}\bar{y})\,a\,l(\bar{x}\bar{y})^{-1}$

$\theta_{\bar{x}} \circ \theta_{\bar{y}}(a) = l(\bar{x})\,l(\bar{y})\,a\,l(\bar{y})^{-1}l(\bar{x})^{-1}$

$l(\bar{x}\bar{y})$ and $l(\bar{x})l(\bar{y})$ are both liftings of $\bar{x}\bar{y} \Rightarrow \theta_{\bar{x}\bar{y}} = \theta_{\bar{x}} \circ \theta_{\bar{y}} \Rightarrow G \curvearrowright N$

DEFINITION

An extension $1 \to N \to E \overset{p}{\to} G \to 1$ **splits** if $\exists$ a lifting l that is a group homo of $G \to E$

PROPOSITION 2

TFAE

(1) $1 \to N \to E \overset{p}{\to} G \to 1$ splits

(2) $\exists$ a subgroup $K \leq E$, s.t. $K \cong G$ and $K \cap N = \{1\}$, $KN = E \Rightarrow E$ is a **semidirect product** of N by G

Proof

"(1) $\Rightarrow$ (2)": Let $K = \mathrm{Im}\, l \leq E$ since l is group homo

- $l : G \xrightarrow{\sim} K$: If $l(\bar{x}) = l(\bar{y})$, then $pl(\bar{x}) = pl(\bar{y}) \Rightarrow \bar{x} = \bar{y} \Rightarrow 1\text{-}1 \Rightarrow$ onto $\Rightarrow$ isom ($\because$ homo)

- $E = KN$: $\forall x \in E$, $\bar{x} := p(x)$, $y = l(\bar{x}) \in K$, and $p(x) = p(y) \Rightarrow y^{-1}x \in \ker p = N$, say $y^{-1}x = a \in N \Rightarrow x = ya$
- $K \cap N = \{1\}$: $k \in K \cap N \Rightarrow a = l(\bar{x}) \Rightarrow \bar{1} = p(a) = p\,l(\bar{x}) = \bar{x} \Rightarrow a = l(\bar{x}) = l(\bar{1}) = 1$

"(2) ⇒ (1)":
- $p|_K : K \to G$ is an isom
  - ↳ onto: $p(K) \overset{\text{by proj def}}{=} p(KN) = p(E) = G$ ✓
  - ↳ 1-1: $\ker(p|_K) = N \cap K = \{1\}$ ✓
- $l := (p|_K)^{-1}$

REMARK (reverse order from before)

In this case, $E = N \times_\theta G$ via $\theta : G \to \mathrm{Aut}(N) \Rightarrow (a, \bar{x}) \cdot (b, \bar{y}) = (a(\theta(\bar{x})(b)), \bar{x}\bar{y})$ ($\theta(\bar{x})(b) \in N$) (Just redefining old concepts / semidirect product)

DEFINITION

Given $1 \to N \to E \xrightarrow{p} G \to 1$ and lifting $l : G \to E$, a **factor set** is a function $f : G \times G \to N$, s.t. $\forall \bar{x}, \bar{y} \in G$, $l(\bar{x})l(\bar{y}) = f(\bar{x}, \bar{y})\, l(\bar{x}\bar{y})$ ($f(\bar{x}, \bar{y}) \in N$)

PROPOSITION 3

Let $1 \to N \to E \xrightarrow{p} G \to 1$ and $l : G \to E$ be a lifting. If $f : G \times G \to N$ is its corresponding **factor set**, then

(1) $\forall \bar{x}, \bar{y} \in G$, $f(\bar{1}, \bar{y}) = 1 = f(\bar{y}, \bar{1})$

$l(\bar{1})l(\bar{y}) = 1 \cdot l(\bar{1} \cdot \bar{y}) = l(\bar{y})$

(2) **Cocycle Identity**: $\forall \bar{x}, \bar{y}, \bar{z} \in G$, $f(\bar{x}, \bar{y})\, f(\bar{x}\bar{y}, \bar{z}) = \theta_{\bar{x}}(f(\bar{y}, \bar{z}))\, f(\bar{x}, \bar{y}\bar{z})$

Proof

By associativity, $(l(\bar{x})l(\bar{y}))\,l(\bar{z}) = f(\bar{x}, \bar{y})\, l(\bar{x}\bar{y})\, l(\bar{z}) = f(\bar{x}, \bar{y}) f(\bar{x}\bar{y}, \bar{z})\, l(\bar{x}\bar{y}\bar{z})$

$l(\bar{x})(l(\bar{y})l(\bar{z})) = l(\bar{x})\, f(\bar{y}, \bar{z})\, l(\bar{y}\bar{z}) = l(\bar{x}) f(\bar{y}, \bar{z}) l(\bar{x})^{-1} l(\bar{x})\, l(\bar{y}\bar{z}) = \theta_{\bar{x}}(f(\bar{y}, \bar{z}))\, f(\bar{x}, \bar{y}\bar{z})\, l(\bar{x}\bar{y}\bar{z})$ ✓

THEOREM 1

Let $\sigma : G \to \mathrm{Aut}(N)$ be a group homo and $f : G \times G \to N$ satisfy (1) and (2)

($\bar{x} \mapsto \sigma_{\bar{x}}$)

Then, $\exists\ 1 \to N \to E \xrightarrow{p} G \to 1$ and a lifting $l : G \to E$, s.t. $\theta = \sigma$ (conjugation given by lifting) and f is the corresponding factor set

Proof

Define $E = N \times G$ equipped with the operation $(a, \bar{x}) \cdot (b, \bar{y}) = (a\sigma_{\bar{x}}(b)\, f(\bar{x}, \bar{y}), \bar{x}\bar{y})$ (need a factor set for this generalization)

- Associativity: $((a, \bar{x}) \cdot (b, \bar{y})) \cdot (c, \bar{z}) = (a\sigma_{\bar{x}}(b)\, f(\bar{x}, \bar{y}), \bar{x}\bar{y}) \cdot (c, \bar{z}) = ((a\sigma_{\bar{x}}(b)\, f(\bar{x}, \bar{y}))\, \sigma_{\bar{x}\bar{y}}(c)\, f(\bar{x}\bar{y}, \bar{z}), \bar{x}\bar{y}\bar{z})$

  $= (a\sigma_{\bar{x}}(b)\, \sigma_{\bar{x}\bar{y}}(c)\, f(\bar{x}, \bar{y})\, f(\bar{x}\bar{y}, \bar{z}), \bar{x}\bar{y}\bar{z})$ (abelian)

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

  $(a, \bar{x}) \cdot ((b, \bar{y}) \cdot (c, \bar{z})) = (a, \bar{x}) \cdot (b\sigma_{\bar{y}}(c) f(\bar{y}, \bar{z}), \bar{y}\bar{z}) = (a\sigma_{\bar{x}}(b\sigma_{\bar{y}}(c) f(\bar{y}, \bar{z}))\, f(\bar{x}, \bar{y}\bar{z}), \bar{x}\bar{y}\bar{z})$

  $= (a\sigma_{\bar{x}}(b)\sigma_{\bar{x}}\sigma_{\bar{y}}(c)\sigma_{\bar{x}}(f(\bar{y}, \bar{z}))\, f(\bar{x}, \bar{y}\bar{z}), \bar{x}\bar{y}\bar{z})$ ✓
- Identity $= (\bar{1}, \bar{1})$
- $(a, \bar{x})^{-1} = (\sigma_{\bar{x}^{-1}}(a^{-1} f(\bar{x}, \bar{x}^{-1})^{-1}), \bar{x}^{-1})$
- $p : E \to G$ is a group homo by def, $(a, \bar{x}) \mapsto \bar{x}$
- $i : N \to E$ is a group homo: $(a, 1)(b, 1) = (a\sigma_1(b) f(1, 1), 1) = (ab, 1)$, $a \mapsto (a, 1)$

$\Rightarrow \ker p = \mathrm{Im}\, i$ because $1 \to N \xrightarrow{i} E \xrightarrow{p} G \to 1$

Now, for the lifting, let $l(\bar{x}) = (1, \bar{x})$

$\Rightarrow \theta_{\bar{x}}(a) = l(\bar{x})(a, 1)\, l(\bar{x})^{-1} = (1, \bar{x})(a, 1)(\sigma_{\bar{x}^{-1}}(f(\bar{x}, \bar{x}^{-1})^{-1}), \bar{x}^{-1}) = (\sigma_{\bar{x}}(a)\, f(\bar{x}, \bar{1}), \bar{x})(\sigma_{\bar{x}^{-1}}(f(\bar{x}, \bar{x}^{-1})^{-1}), \bar{x}^{-1})$ ($f(\bar{x}, \bar{1}) = 1$)

$= (\sigma_{\bar{x}}(a)\, \sigma_{\bar{x}}(\sigma_{\bar{x}^{-1}}(f(\bar{x}, \bar{x}^{-1})^{-1}))\, f(\bar{x}, \bar{x}^{-1}), 1) = (\sigma_{\bar{x}}(a), 1)$, so "$\sigma$ is the same as θ"

- $l : G \to E$, $\bar{x} \mapsto (1, \bar{x})$: $l(\bar{x})l(\bar{y})l(\bar{x}\bar{y})^{-1} = (1, \bar{x})(1, \bar{y})(1, \bar{x}\bar{y})^{-1} = (f(\bar{x}, \bar{y}), \bar{x}\bar{y})(\sigma_{(\bar{x}\bar{y})^{-1}}(f(\bar{x}\bar{y}, (\bar{x}\bar{y})^{-1})^{-1}), (\bar{x}\bar{y})^{-1})$

$= (f(\bar{x}, \bar{y})\, \sigma_{\bar{x}\bar{y}}\sigma_{(\bar{x}\bar{y})^{-1}}(f(\bar{x}\bar{y}, (\bar{x}\bar{y})^{-1})^{-1})\, f(\bar{x}\bar{y}, (\bar{x}\bar{y})^{-1}), 1) = (f(\bar{x}, \bar{y}), 1) \Rightarrow f$ is a factor set

$\therefore$ We proved that with (1), (2), we can create an extension.

PROPOSITION 4

Let $1 \to N \to E \underset{\ell, \ell'}{\overset{\rho}{\rightleftarrows}} G \to 1$ and ℓ corr to f, ℓ' corr to f'. Then $\exists\, h: G \to N$ with $h(1)=1$ and $\forall \bar{x}, \bar{y} \in G$,

$\ell'(\bar{x})\ell'(\bar{y})\ell'(\bar{x}\bar{y})^{-1}$

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

$[\ell(\bar{x})\ell(\bar{y})\ell(\bar{x}\bar{y})^{-1}]^{-1}$

Proof

For $\bar{x} \in G$, $\exists\, h(\bar{x}) \in N$ (i.e. $\in N$), s.t. $\ell'(\bar{x}) = h(\bar{x})\ell(\bar{x})$

Then, $f'(\bar{x},\bar{y})\ell'(\bar{x}\bar{y}) = \ell'(\bar{x})\ell'(\bar{y}) = h(\bar{x})\ell(\bar{x})h(\bar{y})\ell(\bar{y}) = h(\bar{x})\ell(\bar{x})h(\bar{y})\ell(\bar{x})^{-1}\ell(\bar{x})\ell(\bar{y}) = h(\bar{x})h(\bar{y})\ell(\bar{x})\ell(\bar{y}) = h(\bar{x})h(\bar{y}) f(\bar{x},\bar{y})\ell(\bar{x}\bar{y})$

$= f'(\bar{x},\bar{y})h(\bar{x}\bar{y})\ell(\bar{x}\bar{y})$

DEFINITION

Two extensions $1 \to N \to E \to G \to 1$, $1 \to N \to E' \to G \to 1$ are equivalent if $\exists\, E \overset{\varphi}{\underset{\sim}{\to}} E'$, s.t.

$$\begin{array}{ccccccccc} 1 & \to & N & \to & E & \to & G & \to & 1 \\ & & \downarrow 1_N & & \downarrow \varphi & & \downarrow 1_N & & \\ 1 & \to & N & \to & E' & \to & G & \to & 1 \end{array}$$

This happens iff $\exists\, \ell: G \to E$, $\ell': G \to E'$, s.t. they are f, f' factor sets respectively if $f - f' \in B^2(G,N)$

DEFINITION

- $Z^2(G,N)$ = the abelian group of all $f: G \times G \to N$ satisfying (1) and (2) ("cocycle")
- $B^2(G,N)$ = the abelian group of all $h: G \to N$ with $h(1)=1$ and $f(\bar{x},\bar{y}) = \bar{x}h(\bar{y})\, h(\bar{x}\bar{y})^{-1} h(\bar{x})$ ("coboundary")

11-8-24 (WEEK 10)

FIRST AND SECOND GROUP COHOMOLOGY

Let N be an abelian group and G be any group with a group homo $\sigma: G \to \mathrm{Aut}(N)$

group action from homo: $u \mapsto \sigma_u : N \to N$ ($\because G \curvearrowright N$, $u \in G, a \in N \Rightarrow u \cdot a$)

Define $e(G,N) := \{$equivalence classes of extensions of N by $G\}$

$H^2(G,N) := \dfrac{Z^2(G,N) := \{f: G\times G \to N \mid f(1,v) = 0 = f(u,1)$ and $f(u,v) + f(uv,w) = uf(v,w) + f(u,vw)\ \forall u,v,w \in G\}}{B^2(G,N) := \{f: G\times G \to N \mid \exists h: G \to N$ with $h(1)=0$, s.t. $f(u,v) = uh(v) - h(uv) + h(u)\ \forall u,v \in G\}}$

(2-cocycle; cocycle identity; 2-coboundary; use pointwise adding)

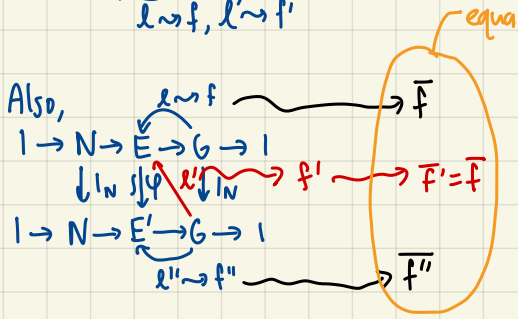
MAIN RESULT

$\exists$ 1-1 correspondence of $e(G,N) \longleftrightarrow H^2(G,N)$

Proof

"$\to$": $[1 \to N \to E \xrightarrow{\ell} G \to 1] \longmapsto \bar{f} = \bar{f'}$

$\ell \rightsquigarrow f$, $\ell' \rightsquigarrow f'$



$f'(u,v)\,\ell'(uv) = \ell'(u)\,\ell'(v)$ (apply $\varphi^{-1}(\ell''(uv))$, $\varphi^{-1}(\ell''(u))$, $\varphi^{-1}(\ell''(v))$) $\xrightarrow{\text{applying } \varphi}$ $\varphi(f'(u,v)) = f''(u,v)$ ($\in N$, "$f''(u,v)$") $\Rightarrow \bar{f} = \bar{f'} = \bar{f''}$ ✓

$f''(u,v)\,\ell''(uv) = \ell''(u)\,\ell''(v)$

"$B^2 \le Z^2$":
- $f(u,1) = u\cdot h(1) - h(u\cdot 1) + h(u) = 0$
- $uf(v) - h(uv) + h(u) + uvh(w) - h(uvw) + h(uv)$
  $uvh(w) - h(vw) + h(v) + uh(vw) - h(uvw) + h(u)$ ✓

"$\leftarrow$": $[1 \to N \to E(N,G,f,\sigma) \to G \to 1] \longleftarrow \bar{f}$

$(a,u)\cdot(b,v) = (a\sigma_u(b)f(u,v), uv)$

- "$\bar{f} = \bar{f'}$": $E(N,G,f,\sigma) \xrightarrow{\simeq} E(N,G,f',\sigma)$

  $f(u,v)f'(u,v)^{-1} = \sigma_u(h(v))h(uv)^{-1}h(u)$

  $(a,u) \longmapsto (ah(u), u)$ ← 1-1 and onto

  $(a,u) \longmapsto (ah(u), v)$, $(b,v) \longmapsto (bh(u), v)$ MULTIPLY

  LHS $= (a\sigma_u(b)f(u,v)h(uv), uv)$

  RHS $= (ah(u)\sigma_u(bh(v))f'(u,v), uv)$

$\ell \rightsquigarrow f$

$[1 \to N \to E \to G \to 1] \longmapsto \bar{f} \longmapsto [1 \to N \to E(N,G,f,\sigma) \to G \to 1] = [1 \to N \to E \to G \to 1]$ ✓

$\bar{f} \mapsto [1 \to N \to E(N,G,f,\sigma) \to G \to 1] \mapsto \bar{f'}$ ✓ ($(1,u) \leftarrow u$)

$[1 \to N \to N \rtimes_\sigma G \to G \to 1] \longmapsto \bar{1}$ ✓ (by def) ($1 \mapsto (1,1)$)

DEFINITION

- $\varphi \in \mathrm{Aut}(E)$ stabilizes $1 \to N \to E \to G \to 1$: if $1 \to N \to E \to G \to 1$ with $\downarrow 1_N$, $\downarrow \varphi$, $\downarrow 1_G$, $1 \to N \to E \to G \to 1$
- $\mathrm{Stab}_E(G,N) = \{$stabilizing automorphisms$\} \le \mathrm{Aut}(E)$ ($\varphi \in \mathrm{Stab}_E(N,G) \Rightarrow \varphi(\ell(u)) = d(u)\ell(u)\ \forall u \in G$, $d: G \to N$, so $f: G\times G \to N \rightsquigarrow H^2$, $d: G \to N \rightsquigarrow H$)

DEFINITION

A derivation is a function $d: G \to N$, s.t. $d(uv) = ud(v) + d(u)\ \forall u,v \in G$

We say $D(G,N) = \{$derivations $: G \to N\}$ (pointwise addition)

THEOREM

Let $1\to N\to E\to G\to 1$ with $\theta=\sigma$. Then, $\exists$ group iso, s.t. $\mathrm{Stab}_E(G,N)\cong \mathrm{Der}(G,N)$

Proof

Let $\varphi\in \mathrm{Stab}_E(G,N)$ and fix $\ell: G\to E$

Then, $\varphi(a\ell(u)) = a\varphi(\ell(u)) = ad(u)\ell(u)$ for some $d: G\to N$

For another $\ell': G\to E$, say $\ell'(u)=g(u)\ell(u)$, say $d'(u)\ell'(u)$ ($g(u)\in N$)

$\Rightarrow$ We have $d'(u) = \varphi(\ell'(u))(\ell'(u))^{-1} = \varphi(g(u)\ell(u))(g(u)\ell(u))^{-1} = g(u)d(u)\ell(u)\ell(u)^{-1}g(u)^{-1} = d(u)$ $\therefore$ Said d is unique

"$d\in \mathrm{Der}(G,N)$": Notice, $d(uv) = \varphi(\ell(uv))\ell(uv)^{-1} = \varphi(f(u,v)^{-1}\ell(u)\ell(v))\ell(v)^{-1}\ell(u)^{-1}f(u,v)) = f(u,v)^{-1}d(u)\ell(u)d(v)\ell(u)^{-1}\ell(u)\ell(v)\ell(u)^{-1}f(u,v)$ ($u\,d(v)\in N$)

$= d(u)(u\,d(v))$

"$\leftarrow$": For $d\in \mathrm{Der}(G,N)$, define $\varphi(a\ell(u)) := ad(u)\ell(u)$. We prove "$\varphi(a\ell(u)b\ell(v)) = \varphi(a\ell(u))\varphi(b\ell(v))$"

$a\ell(u)b\ell(u)^{-1}\ell(u)\ell(v) = a(ub)f(u,v)\ell(uv)$ ($a(ub)f(u,v)\ell(uv)$) $= a(ub)f(u,v)\,d(uv)\ell(uv)$ ✓

Group homo: $\varphi_2\varphi_1(a\ell(u)) = \varphi_2(ad_1(u)\ell(u)) = a\,d_1(u)d_2(u)\ell(u) = (ad_1(u)\ell(u))(ad_2(u)\ell(u)) = \varphi_1(a\ell(u))\varphi_2(a\ell(u))$ (abelian, so addition)

DEFINITION

$\mathrm{Inn}_E(G,N) = \{\varphi\in \mathrm{Stab}_E(G,N) \mid \varphi: \underset{x\mapsto a_0xa_0^{-1}}{E\to E}$ for some $a_0\in N\}$ (principal)

$\mathrm{PDer}(G,N) = \{d\in \mathrm{Der}(G,N) \mid d(u) = ua_1 - a_1$ for some $a_1\in N\}$ ($d(uv) = u\,d(v)\,d(u)$ ✓)

$H^1(G,N) := \mathrm{Der}(G,N)/\mathrm{PDer}(G,N)$

Notice,

$\mathrm{Inn}_E(G,N) \xrightarrow{\ \simeq\ } \mathrm{PDer}(G,N)$

$\varphi \overset{\sim a_0}{\mapsto} a_1 := a a_0^{-1}$ ($\varphi(a\ell(u)) = a_0(a\ell(u))a_0^{-1} = a(a_0\ell(u)a_0^{-1}) = aa_0\ell(u)a_0^{-1}\ell(u)^{-1}\ell(u) = a\,a_0(ua_0^{-1})\ell(u)$)

GOAL

To uncover $H^1(G,N)$, $H^2(G,N)$

We know abelian N can be seen as a $\mathbb{Z}$-module

$\mathbb{Z}[G] = \{\sum_{\text{finite}} a_i g_i \mid a_i\in\mathbb{Z}, g_i\in G\}$ is lin indep over $\mathbb{Z}$

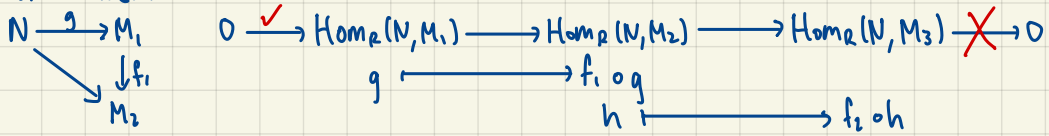
Notice, $G\curvearrowright N \longleftrightarrow N: \mathbb{Z}[G]$-module

DEFINITION

For R-modules M_1, M_2, M_3, $0\to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3\to 0$ is exact if f_1 is 1-1, f_2 is onto, and $\mathrm{Im}\,f_1 = \ker f_2$. In other words, $M_3\cong M_2/M_1$.

OBSERVE

For R-module N:



($0\to\mathbb{Z}\xrightarrow{2}\mathbb{Z}\to\mathbb{Z}/2\mathbb{Z}\to 0$ is counterexample)

11-13-24 (WEEK 11)

Hom AND ⊗ FUNCTORS

DEFINITION

A category C consists of 3 elements: (1) a class of objects $\leftarrow Obj(C)$
(2) $A, B \in Obj(C)$, a set of morphisms from A to $B \leftarrow Mor(A, B)$
(3) A law of contraposition: $Mor(A,B) \times Mor(B,C) \longrightarrow Mor(A,C)$, $(f, g) \longmapsto gf$

satisfying ① $Mor(A_1, B_1) \cap Mor(A_2, B_2) = \emptyset$ unless $A_1 = A_2$, $B_1 = B_2$
② $f \in Mor(A,B)$, $g \in Mor(B,C)$, $h \in Mor(C,D)$, $h(gf) = (hg)f$
③ $\forall A \in Obj(C)$, $\exists 1_A \in Mor(A,A)$, s.t. $f \circ id_A = f$, $id_A \circ g = g$

EXAMPLES

- A: The category of groups
- R: A ring $\Rightarrow {}_R\mathcal{M}$: The category of left R-modules, $\mathcal{M}_R$: The category of right R-modules

DEFINITION

For two categories C, D, a covariant functor $F: C \to D$: $\cdot \forall A \in Obj(C), \exists F(A) \in Obj(D)$

$A \xrightarrow{f} B$, $F(A) \xrightarrow{F(f)} F(B)$

$\cdot \forall f \in Mor(A,B)\ \exists F(f) \in Mor(F(A), F(B))$, s.t. (1) $F(gf) = F(g)F(f)$
(2) $F(id_A) = id_{F(A)}\ \forall A \in Obj(C)$

For a contravariant functor, we have $F(gf) = F(f)F(g)$ where $A \xrightarrow{f} B$, $F(B) \xrightarrow{F(f)} F(A)$

With Hom, $M_1 \xrightarrow{f} M_2$

$Hom(N, M_1) \longrightarrow Hom(N, M_2)$, $h \longmapsto f \circ h$

$Hom(M_2, N) \longrightarrow Hom(M_1, N)$

R-MODULES

For R-modules ${}_R\mathcal{M}$, for $M, N \in {}_R\mathcal{M} \Rightarrow Hom_R(M,N) \in A$ (abelian group) via $(f+g)(x) := f(x) + g(x)$

When R is a commutative ring, we have $Hom_R(M,N) \in {}_R\mathcal{M}$: For $a \in R$, $(af)(x) := f(ax)$

↳ $(af)(x+y) = f(a(x+y)) = f(ax+ay) = f(ax) + f(ay) = (af)(x) + (af)(y) = (af)(x+y)$ ✓
↳ $(af)(bx) = f(a(bx)) = f(b(ax)) = bf(ax) = b(af)(x)$ (Commutative ring only)
↳ $a(f+g)(x) = (af+ag)(x)$
↳ $(a+b)f = af+bf$
↳ $(ab)f(x) = f((ab)(x)) = (bf)(ax) = a(bf)(x)$ (Commutative ring only)

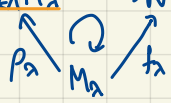
When R is non-commutative, $(rx)s = r(xs)$

- For $M \in {}_R\mathcal{M}_S$, $N \in \mathcal{M}_R$, $Hom_R(M,N) \in {}_S\mathcal{M}$ (and $M \in \mathcal{M}_S$, $N \in {}_R\mathcal{M}_S \Rightarrow Hom_S(M,N) \in {}_R\mathcal{M}$)
  $\forall s \in S$, $f \in Hom_R(M,N)$, $(sf)(x) := f(xs)$ (Doing what we did above but for non-commutative ring)
  ↳ $(sf)(rx) = f((rx)s) = f(r(xs)) = rf(xs) = r(sf)(x)$
  ↳ $(s_1 s_2)f(x) = f(x(s_1 s_2)) = f((xs_1)s_2) = (s_2 f)(xs_1) = s_1(s_2 f)(x)$
- For $M \in {}_R\mathcal{M}_S$, $N \in {}_S\mathcal{M}$, $Hom_S(M,N) \in \mathcal{M}_R$
  $\forall r \in R$, $g \in Hom_S(M,N)$, $(gr)(x) = g(rx)$

DIRECT SUM

Given a family of $\{M_\lambda \mid \lambda \in \Lambda\}$ in ${}_R\mathcal{M}$, the direct sum $\coprod_{\lambda\in\Lambda} M_\lambda$ (or $\bigoplus_{\lambda\in\Lambda}$, no relations in M_λ) of $\{M_\lambda \mid \lambda\in\Lambda\}$ is an R-module with injection $\rho_\lambda : M_\lambda \longrightarrow \coprod_{\lambda\in\Lambda} M_\lambda$, s.t. $\forall N \in {}_R\mathcal{M}$ with R-module homo with $f_\lambda : M_\lambda \longrightarrow N$ $\forall \lambda \in \Lambda$

$\exists!$ R-module homo $\varphi : \coprod_{\lambda\in\Lambda} M_\lambda \longrightarrow N$ (Free of relation too)



PROPOSITION

$\coprod_{\lambda\in\Lambda} M_\lambda$ exists and is **unique** up to isom

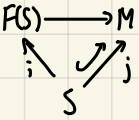
Proof

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

- $(x_\lambda)_{\lambda\in\Lambda} + (y_\lambda)_{\lambda\in\Lambda} = (x_\lambda + y_\lambda)_{\lambda\in\Lambda}$, $a(x_\lambda)_{\lambda\in\Lambda} := a(x_\lambda)_{\lambda\in\Lambda}$
- $\rho_\lambda : M_\lambda \longrightarrow \coprod_{\lambda} M_\lambda$
  $x_\lambda \longmapsto (y_{\lambda'})_{\lambda'\in\Lambda}$ with $y_\lambda = x_\lambda$, $y_{\lambda'} = 0$ $\forall \lambda' \neq \lambda$
- Given $f_\lambda : M_\lambda \longrightarrow N$, define
  $\varphi : \coprod_{\lambda\in\Lambda} M_\lambda \longrightarrow N$
  $(x_\lambda)_{\lambda\in\Lambda} \longmapsto \sum_{\lambda\in\Lambda} f_\lambda(x_\lambda)$ (finite sum)

DEFINITION

An R-module $F(S)$ is said to be free on $S \neq \emptyset$ if $\exists$ a map $i : S \to F(S)$, s.t. $\forall j : S \longrightarrow M \in {}_R\mathcal{M}$ (↪ $j(x_\lambda) \in M$), $\exists!$ R-module homo $\varphi : F(S) \longrightarrow M$



PROPOSITION

$F(S)$ exists and is unique up to isom

Proof

Let $S = \{x_\lambda : \lambda \in \Lambda\}$. Consider $M_\lambda = Rx_\lambda \cong R$ as a cyclic R-module ($rx_\lambda = 0 \Rightarrow r = 0$). Then, $M_\lambda \longrightarrow F(S) = \coprod_{\lambda\in\Lambda} M_\lambda$

We have $f_\lambda : M_\lambda \longrightarrow M$

$x_\lambda \longmapsto j(x_\lambda)$

$rx_\lambda \longmapsto rj(x_\lambda)$ □

TENSOR PRODUCT

DEFINITION

For $M \in \mathcal{M}_R$, $N \in {}_R\mathcal{M}$, additive $G \in \mathcal{A}$ (abelian group of $\mathrm{Hom}_R(M,N)$)

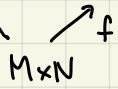
An **R-biadditive** function is a function $f : M \times N \longrightarrow G$, s.t.

(1) $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$
(2) $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$
(3) $f(x, ry) = f(rx, y)$ $(r \in R)$

} "Bilinear" over RING not FIELD

DEFINITION

A tensor product of M and N is an **abelian group** $M \otimes_R N$ with an R-biadditive function $h : M \times N \longrightarrow M \otimes_R N$, s.t. $\forall G \in \mathcal{A}$ and $\forall$ R-biadditive functions $f : M \times N \longrightarrow G$, $\exists!$ $\mathbb{Z}$-module homo $\tilde{f} : M \otimes_R N \longrightarrow G$ (def prop makes $\otimes$ have smth like universal-biadditivity)



THEOREM

$M\otimes_R N$ exists and is unique up to isom

Proof

- Let F be the free $\mathbb{Z}$-module on $M\times N$, i.e. $F=\coprod_{(x,y)\in M\times N}\mathbb{Z}(x,y)$
- Define $I=\left\langle \begin{matrix}(x_1+x_2,y)-(x_1,y)-(x_2,y)\\ (x,y_1+y_2)-(x,y_1)-(x,y_2)\\ (x,ry)-(xr,y)\end{matrix} \;\middle|\; \begin{matrix}x_1,x_2,x\in M\\ y_1,y_2,y\in N\\ r\in R\end{matrix}\right\rangle_{\mathbb{Z}}$ and $M\otimes_R N := F/I$ $\quad x\otimes y \leftarrow (x,y)+I$ $\quad \left(\begin{matrix}(x_1+x_2)\otimes y = x_1\otimes y + x_2\otimes y\\ \text{etc}\end{matrix}\right)$
- Define $h: M\times N \longrightarrow M\otimes_R y$ is additive (OK, we quotient I)
  $(x,y)\longmapsto x\otimes y$
- Universal Property: $M\times N \xhookrightarrow{i} F \xrightarrow{p} F/I = M\otimes_R N$
  R-biadditive $\rightarrow f: M\times N\to G$; $\exists! \tilde f: F\to G$ (universal property of F); $\exists \bar f: M\otimes_R N\to G$ by factor thm since $I\subseteq \ker \tilde f$. (f is R-biadditive)

REMARK

1. This yields $\{$R-biadditive function $f: M\times N\to G\}\longleftrightarrow\{\mathbb{Z}$-module homo $M\otimes_R N\longrightarrow G\}$
2. Can we define left R- $\otimes$ left R- ? No.
   $(a_1a_2)(x\otimes y) = a_1(a_2x)\otimes y = (a_2x)\otimes(a_1y) = x\otimes(\underline{a_2a_1})y$
   $\shortparallel$
   $x\otimes(\underline{a_1a_2})y$
3. Is $M\otimes_R N$ an R-module? No. $a(x\otimes y):=(xa)\otimes y = x\otimes(ay) \Rightarrow (a_1a_2)(x\otimes y) = a_1(a_2(x\otimes y)) = (xa_2)\otimes(a_1y) = x\otimes \underline{a_2}(a_1y)$
   $\shortparallel$
   $x\otimes(\underline{a_1a_2})y$

EXAMPLE

For $M\in {}_R\mathcal{M}_S$, $N\in {}_S\mathcal{M} \Rightarrow M\otimes_S N\in {}_R\mathcal{M}$

(HW Question)

MORE REMARKS

- $g: M\longrightarrow M'$: right R-module homo
  $h: N\longrightarrow N'$: left R-module homo
  $\Rightarrow g\otimes h: M\otimes N\longrightarrow M'\otimes N$ is a group homo
  $x\otimes y\longmapsto g(x)\otimes h(y)$

  Proof

  $f: M\times N\longrightarrow M'\otimes N'$
  $(x,y)\longmapsto g(x)\otimes h(y)$ $\leftarrow$ R-biadditive
  $\exists!\,\bar f: M\otimes N\longrightarrow M'\otimes N'$
  $x\otimes y\longmapsto g(x)\otimes h(y)$
- Let $f: R\to S$ be a ring homo. Then S is an R-module: $R\times S\longrightarrow S$ and for $M\in {}_R\mathcal{M}$, $S\otimes_R M\in {}_S\mathcal{M}$ $(S\in {}_S\mathcal{M}_R,\ S\otimes_R M\in {}_S\mathcal{M})$
  $(r,s)\longmapsto f(r)s$
- $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}/n\mathbb{Z}=0$ since $q\otimes\bar a = (\frac{q}{n}\cdot n)\otimes\bar a = \frac{q}{n}\otimes \underset{\overset{\shortparallel}{0}}{n\bar a} = 0$ $(a\otimes 0 = a\otimes 0 + a\otimes 0 \because 0=0+0)$
  This means, for $G\cong \mathbb{Z}/d_1\mathbb{Z}\oplus\mathbb{Z}/d_2\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/d_n\mathbb{Z}\oplus\mathbb{Z}^s$, by doing $\mathbb{Q}\otimes_{\mathbb{Z}} G$, we can isolate $\mathbb{Z}^s$ (logic for finding totient)

11-15-24 (WEEK 11)

SPECIAL MODULES FOR Hom AND ⊗

Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ be exact in ${}_R\mathcal{M}$

For $M, N \in {}_R\mathcal{M}$, $0 \to \mathrm{Hom}_R(M, M_1) \xrightarrow{\bar{\alpha}} \mathrm{Hom}_R(M, M_2) \xrightarrow{\bar{\beta}} \mathrm{Hom}_R(M, M_3)$ ← $\mathrm{Hom}_R(M, \cdot)$ preserves left-exactness

$f \longmapsto \alpha \circ f$

$0 \to \mathrm{Hom}_R(N, M_3) \xrightarrow{\bar{\beta}} \mathrm{Hom}_R(N, M_2) \xrightarrow{\bar{\alpha}} \mathrm{Hom}_R(N, M_1)$ ← $\mathrm{Hom}_R(\cdot, N)$ preserves left-exactness

$g \longmapsto g \circ \beta$

↑ Not onto: $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$

$N = \mathbb{Z} \Rightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$

$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$, $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \ni 1_{\mathbb{Z}}$

Img $= n\mathbb{Z}$, say $f(a) = n$, but $f(\frac{a}{2}) + f(\frac{a}{2}) = n$

$\therefore f(a) = 0$ ($\because n = 0$)

For $M \in \mathcal{M}_R$, $M \otimes_R M_1 \xrightarrow{1_M \otimes \alpha} M \otimes_R M_2 \xrightarrow{1_M \otimes \beta} M \otimes M_3 \to 0$

Why surjective but not 1-1:

$0 \to \mathbb{Z}^2 \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

$M = \mathbb{Z}/2\mathbb{Z} \Rightarrow \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \xrightarrow{!\otimes 2} \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}$

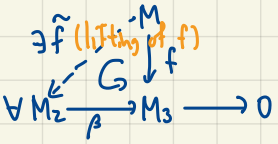
$\bar{1} \otimes 1 \longmapsto \bar{1} \otimes 2 = \bar{1} \otimes 1 = \bar{0} \otimes 1 = 0$

DEFINITION

- $M \in {}_R\mathcal{M}$ is **projective** if $\mathrm{Hom}(M, \cdot)$ preserves right-exactness (it already has left-exactness)
- $N \in {}_R\mathcal{M}$ is **injective** if $\mathrm{Hom}(\cdot, N)$ preserves right-exactness (it already has left-exactness)
- $M \in \mathcal{M}_R$ is **flat** if $M \otimes \cdot$ preserves left-exactness

FACTS

1. M is projective $\iff$

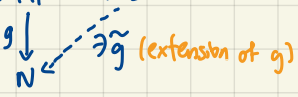


Proof

$\mathrm{Hom}(M, M_2) \longrightarrow \mathrm{Hom}(M, M_3)$

$\exists \tilde{f}$ s.t. $f = \beta \circ \tilde{f}$

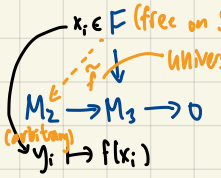
2. N is injective $\iff$



3. free ⇒ projective (free module)

⇓

flat



(projective)

$M_1 \otimes (\coprod_{i \in \Lambda} R x_i)$ ($\because M_1 \otimes_R R \cong M_1$ since M_1 is an R-module)

R

$\| \cong$

$\coprod_{i \in \Lambda} M_{1,i}$ ($M_{1,i} = M_1$)

$0 \to M_1 \to M_2 \not\Rightarrow 0 \to M_1 \otimes F \longrightarrow M_2 \otimes F$

$\coprod_{i \in \Lambda} R x_i$

⇓

$0 \to \coprod_{i \in \Lambda} M_{1,i} \to \coprod_{i \in \Lambda} M_{2,i}$, so $0 \to M_1 \otimes F \Rightarrow M_2 \otimes F$ ($\therefore$ flat)

GOAL

- $\forall M \in_R \mathfrak{M}$, $F(S) \to M \to 0$ (free ⇒ proj)
  - $e_i \mapsto x_i$, $\langle x_i \mid i \in \Lambda \rangle_R$
  - ↑ generating set $S = \{x_i \mid i \in \Lambda\}$
- $\forall M \in_R \mathfrak{M}$, $\exists N$: injective s.t. $0 \to M \to N$

BAER'S CRITERION

N is injective $\Leftrightarrow$ $0 \to I \to R$, $f \downarrow$, $\exists h : I \to N$

Proof

"⇒": ok (special case)

"⇐": Given $0 \to M_1 \to M_2$, $g \downarrow N$, consider $S = \{(M, \rho) \mid M_1 \subset M \subset M_2,\ \rho \text{ extends } g\} \neq \emptyset$ ($\rho \in \mathrm{Hom}_R(M, N)$; (M, g))

Define partial order as $(M, \rho) < (M', \rho') \Rightarrow M \subset M'$, ρ' extends ρ

Let $\{(M_i', \rho_i) \mid i \in \Lambda\}$ be a chain in S. Let $(\bigcup_{i \in \Lambda} M_i', \rho')$ be a least upper bound ($\rho'|_{M_i'} = \rho_i$; can be used all the time to extend)

By Zorn's Lemma, $\exists$ a max element $(M^*, \mu) \in S$

Claim: $M^* = M_2$

Proof

Otherwise, $\exists x \in M_2 \setminus M^*$. Let $M' = M^* + Rx$

Let ideal $I = \{r \in R \mid rx \in M^*\}$. Define $f : I \to N$, $r \mapsto \mu(rx)$

$R \downarrow \exists f'$ by assumption; $0 \leftarrow I$

Define $\mu' : M' \to N$, $z + rx \mapsto \mu(z) + f'(r)$ (well-def: $z + rx = z' + r'x \Rightarrow \mu(z) + f'(r) = \mu(z') + f'(r')$)

Then, $(M^*, \mu) \lneq (M', \mu')$ ↯

DEFINITION

N is divisible if $\forall x \in M$, $r \in R \setminus \{0\}$, $\exists y \in M$, s.t. $x = ry$, i.e. $\forall r \in R \setminus \{0\}$, $rM = M$

KEY PROPOSITION

(1) Every injective module N over an integral domain is divisible

(2) Every divisible module N over a PID R is injective

Proof

(1) For $x_0 \in N$, $r_0 \in R \setminus \{0\}$, $0 \to Rr_0 \to R$, $y_0 := h(1) \Rightarrow r_0 y_0 = r_0 h(1) = h(r_0) = x_0$

$rr_0 \downarrow$, $f \downarrow$, $\exists h$; $r_0 x_0 \in N$, r_0

(2) For $0 \to I = \langle r_0 \rangle \to R$, $\exists$ s.t. $r_0 y_0 = x_0$

$\exists y_0 \in N$; $x_0 \in N$, $\exists y_0$; $r_0 y_0$

MAIN THEOREM

$\forall M \in {}_R\mathcal{M}$, $\exists N \in {}_R\mathcal{M}$: injective, s.t. $M \hookrightarrow N$

Proof

- $R=\mathbb{Z}$: Let $M=\langle x_i \mid i\in\Lambda\rangle_{\mathbb{Z}}$ and F be $\mathbb{Z}$-free on $\{x_i \mid i\in\Lambda\}$ ($F=\bigoplus_{i\in\Lambda}\mathbb{Z}e_i$)

  $0 \to \ker f \to F \xrightarrow{f} M \to 0 \Rightarrow M = F/\ker f$

  ($e_i \mapsto x_i$)

  (Notice $\mathbb{Q}$ is injective, and divisible: $n\mathbb{Q}=\mathbb{Q}$, $n\in\mathbb{Z}$)

  Let $F'=\bigoplus_{i\in\Lambda}\mathbb{Q}e_i \Rightarrow F\subset F'$ and F' is a divisible $\mathbb{Z}$-module $\Rightarrow F'/\ker f$ ($nF'/\ker f = F'/\ker f$)

  Hence, $M\cong F/\ker f \subseteq F'/\ker f$ ← divisible ⇒ injective

- General R: As above, $M \hookrightarrow N_0$: injective $\mathbb{Z}$-module (abelian group)

  Write $N=\mathrm{Hom}_{\mathbb{Z}}(R,N_0)$, which is an R-module

  Claim: N is injective

  Proof

  Given $0\to M_1 \to M_2$ in ${}_R\mathcal{M}$ (as $\mathbb{Z}$), define $f': M_1 \to M_0$, $x \mapsto f(x)$ which is a $\mathbb{Z}$-module homo ($\in \mathrm{Hom}_{\mathbb{Z}}(R,N_0)$)

  f ↓, h (want to find): $M_2 \to N$

  $N \ni h(z): R \to N_0$, $r \mapsto h'(rz)$ ← cannot be $rh'(z)$

  $\therefore \exists h': M_2 \to N_0$, s.t. $h'|_{M_1} = f'$

  $h(z) \in \mathrm{Hom}_{\mathbb{Z}}(R,N_0)$, $h \in \mathrm{Hom}_R(M_2,N)$, $h|_{M_1} = f \leftarrow h'|_{M_1} = f'$

Finally, $\mathrm{Hom}_R(R,M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R,M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R,N_0)$ ($f \mapsto x$)

$\wr\wr$ $\qquad$ $\wr\wr$

$x \in M \longrightarrow N$

IMPORTANT PROPOSITION

(1) TFAE: (a) M is projective

(b) $\forall\ 0\to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M \to 0$ split exact

(c) $\exists M'$, s.t. $M\oplus M' \cong F$: free

Proof

"(a)⇒(b)":

$\exists\beta'$: $M_2 \xrightarrow{\beta} M \to 0$, $M \xrightarrow{\beta'} M_2$, $M \xrightarrow{id_M} M$

"(b)⇒(c)": $\exists F$: free, s.t. $F \xrightarrow{f} M \to 0 \Rightarrow 0 \to \ker f \to F \to M \to 0$

$\Rightarrow M \oplus \ker f \cong F$

"(c)⇒(a)": $0 \to M' \to F \xrightarrow{\beta} M \to 0$

$\exists r$: $F \to M_2$, $\exists\beta'$: $M \to F$, f: $F \to M_3$, $M_2 \xrightarrow{\beta} M \to M_3 \to 0$

(2) TFAE (a) M is injective

(b) $\forall\ 0\to M \to M_2 \xrightarrow{\alpha} M_3 \to 0$ split exact

Proof

"(a)⇒(b)": (red) $\quad id_M$: $M \to M$, $\exists\alpha'$: $M \to M_2$

"(b)⇒(a)": $\exists N$: injective, s.t. $0 \to M \xrightarrow{i} N$ (Full would be $0 \to M \xrightarrow{i} N \xrightarrow{\rho} \mathrm{coker}\, i \to 0$, $\mathrm{coker}\, i = N/\mathrm{Im}\, i$)

($\exists i'$: $N \to M$)

for $0 \to M_1 \xrightarrow{\alpha} M_2$

f ↓, h: $M_1 \to M$, $i'\circ h'$: $M_2 \to M$, $\exists h'$: $M_2 \to N$

$h\circ\alpha = i'\circ h'\circ\alpha = i'\circ f' = i'\circ i\circ f = f$ ($i'\circ i = id$)

11-20-24 (WEEK 12)

HOMOLOGY FUNCTOR

QUESTION

How do we study a general R-module M?

STRATEGY

$0 \to \underline{\ker \pi_1} \xrightarrow{i_1} F_1 \xrightarrow{\pi_1} M \to 0$

$\ker \pi_1 = K_1$

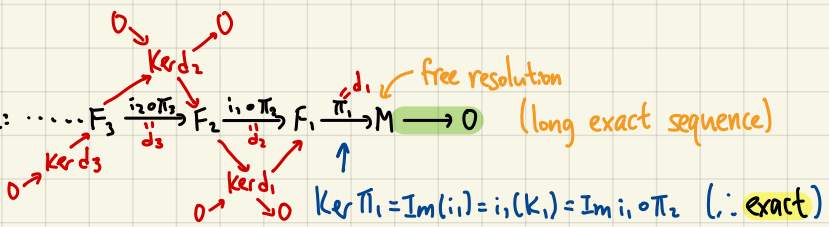
$\Downarrow$

$0 \to K_2 \xrightarrow{i_2} F_2 \xrightarrow{\pi_2} K_1 \to 0$

$\Downarrow$

$0 \to K_3 \xrightarrow{i_3} F_3 \xrightarrow{\pi_3} K_2 \to 0$

gets smaller and smaller



We denote: $\cdots\cdots F_3 \xrightarrow{i_2\circ\pi_2 = d_3} F_2 \xrightarrow{i_1\circ\pi_1 = d_2} F_1 \xrightarrow{\pi_1 = d_1} M \longrightarrow 0$ (long exact sequence)

$\ker \pi_1 = \mathrm{Im}(i_1) = i_1(K_1) = \mathrm{Im}\, i_1 \circ \pi_2$ (∴ exact)

$0 \to M \xrightarrow{i} N_1 \xrightarrow{p_1} Q_1 \to 0$

$\Downarrow$

$0 \to Q_1 \xrightarrow{i_2} N_2 \xrightarrow{p_2} Q_2 \to 0$

$\Downarrow$

$\vdots$

We join and get another exact sequence (injective resolution). $0 \longrightarrow M \xrightarrow{i_1} N_1 \xrightarrow{i_2\circ p_1} N_2 \xrightarrow{i_3\circ p_2} N_3 \to \cdots$

So, if we are given a (need not exact) sequence: $\cdots\cdots \underline{C_3 \xrightarrow{d_3} C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} M \longrightarrow 0}$ satisfying $d_i \circ d_{i+1} = 0 \Rightarrow \mathrm{Im}\, d_{i+1} \subseteq \ker d_i$

Here, we get:

$0 \to \mathrm{Im}\, d_1 \to M \to M/\mathrm{Im}\, d_1 \to 0$

$0 \to \ker d_1 \to C_1 \xrightarrow{d_1} \mathrm{Im}\, d_1 \to 0$

$0 \to \ker d_2 \to C_2 \xrightarrow{d_2} \mathrm{Im}\, d_2 \to 0$

So we must choose different short exact sequences to keep distinctiveness

$0 \to \ker d_1/\mathrm{Im}\, d_2 \to C_1/\mathrm{Im}\, d_2 \xrightarrow{d_1} \underbrace{\mathrm{Im}\, d_1}_{\text{"}\mathrm{Im}\, d_1/\mathrm{Im}\, d_2\text{"}} \to 0$

$0 \to \ker d_2/\mathrm{Im}\, d_3 \to C_2/\mathrm{Im}\, d_3 \xrightarrow{d_2} \mathrm{Im}\, d_2 \to 0$

If we are given a sequence $\underline{0 \to M \xrightarrow{d_1} C^1 \xrightarrow{d_2} C^2 \xrightarrow{d_3} C^3 \to \cdots}$ with $d_{i+1} \circ d_i = 0 \Rightarrow \mathrm{Im}\, d_i \subseteq \ker d_{i+1}$, so similar to above but we consider $\ker d_{i+1}/\mathrm{Im}\, d_i$

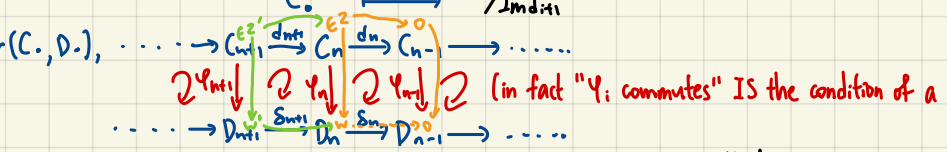
DEFINITION

- Chain complex $\mathrm{Com}_*(_R\mathrm{M})$: Obj: $C_\cdot: \cdots\cdots C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} \cdots\cdots \xrightarrow{d_1} C_0 \longrightarrow 0$, s.t. $d_i \circ d_{i+1} = 0\ \forall i$ ($\Rightarrow \mathrm{Im}\, d_{i+1} \subseteq \ker d_i$)

  We associate the functor $H_i : \mathrm{Com}_*(_R\mathrm{M}) \longrightarrow {}_R\mathrm{M}$ and call it the ith homology functor

  $C_\cdot \longmapsto \ker d_i/\mathrm{Im}\, d_{i+1}$

  For $\varphi \in \mathrm{Mor}(C_\cdot, D_\cdot)$,



  (in fact "φ_i commutes" IS the condition of a valid map)

  $\varphi_n(\ker d_n) \subseteq \ker \delta_n$, $\varphi_n(\mathrm{Im}\, d_{n+1}) \subseteq \mathrm{Im}\, \delta_{n+1} \Rightarrow$ Well-defined $H_\cdot(\varphi_n): H_n(C) = \ker d_n/\mathrm{Im}\, d_{n+1} \longrightarrow \ker \delta_n/\mathrm{Im}\, \delta_{n+1} = H_n(D)$

  (can not write $C_\cdot$)

- Co-chain complex $\mathrm{Com}^*(_R\mathrm{M})$: Obj: $C^\cdot: 0 \longrightarrow C^0 \xrightarrow{d_1} C^1 \xrightarrow{d_2} C^2 \to \cdots$, s.t. $d_{i+1} \circ d_i = 0\ \forall i$ ($\Rightarrow \mathrm{Im}\, d_i \subseteq \ker d_{i+1}$)

  Functor $H^i : \mathrm{Com}^*(_R\mathrm{M}) \longrightarrow {}_R\mathrm{M}$

  $C^\cdot \longmapsto \ker d_{i+1}/\mathrm{Im}\, d_i$

  $\varphi \in \mathrm{Mor}(C^\cdot, D^\cdot)$, $H^\cdot(\varphi_n): H^n(C) = \ker d_{n+1}/\mathrm{Im}\, d_n \longrightarrow \ker \delta_{n+1}/\mathrm{Im}\, \delta_n = H^n(D)$

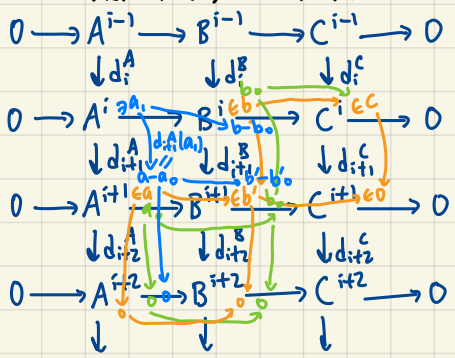
(Long exact sequence)

- $0 \to A^\cdot \xrightarrow{\varphi} B^\cdot \xrightarrow{\psi} C^\cdot \to 0$ is exact in f if $0 \to A^n \xrightarrow{\varphi_n} B^n \xrightarrow{\psi_n} C^n \to 0$ is exact $\forall n$

$\Rightarrow \exists$ coshan $0 \to H^0(A) \xrightarrow{H^0(\varphi)} H^0(B) \xrightarrow{H^0(\psi)} H^0(C) \xrightarrow{\delta_0} H^1(A) \to H^1(B) \to H^1(C) \xrightarrow{\delta_1} H^2(A) \to \cdots$, where δ_i are ith connecting homomorphisms $\hookrightarrow H^i(C) \xrightarrow{\delta_i} H^{i+1}(A)$

SNAKE LEMMA

$\ker d_{i+1}^C / \mathrm{Im} d_i^C = H^i(C) \xrightarrow{\delta_i} H^{i+1}(A) = \ker d_{i+2}^A / \mathrm{Im} d_{i+1}^A$



STATEMENT (This is the real lemma, not the diagram above)

$0 \to M_1 \to M_2 \to M_3 \to 0$ exact

$\downarrow f_1 \quad \downarrow f_2 \quad \downarrow f_3$

$0 \to N_1 \to N_2 \to N_3 \to 0$ exact

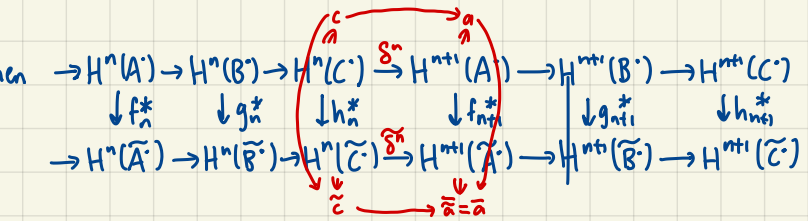
$\Rightarrow 0 \to \ker f_1 \to \ker f_2 \to \ker f_3 \to \underbrace{\mathrm{coker} f_1}_{N_1/\mathrm{Im} f_1} \to \mathrm{coker} f_2 \to \mathrm{coker} f_3 \to 0$

(Use same logic as the short $\Rightarrow$ long exact sequence for co-chain complex)

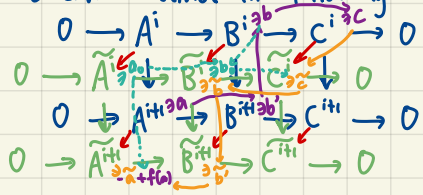
NATURALITY OF δ

If $0 \to A^\cdot \to B^\cdot \to C^\cdot \to 0$ exact, then $\to H^n(A^\cdot) \to H^n(B^\cdot) \to H^n(C^\cdot) \xrightarrow{\delta^n} H^{n+1}(A^\cdot) \to H^{n+1}(B^\cdot) \to H^{n+1}(C^\cdot)$

$0 \to \tilde{A}^\cdot \to \tilde{B}^\cdot \to \tilde{C}^\cdot \to 0$ exact $\to H^n(\tilde{A}^\cdot) \to H^n(\tilde{B}^\cdot) \to H^n(\tilde{C}^\cdot) \xrightarrow{\tilde{\delta}^n} H^{n+1}(\tilde{A}^\cdot) \to H^{n+1}(\tilde{B}^\cdot) \to H^{n+1}(\tilde{C}^\cdot)$



We can constract the following



DEFINITION

- $f: C_\cdot \to \tilde{C}_\cdot$ is said to be null homotopy if $\exists\, S_n: C_n \to \tilde{C}_{n+1}$, s.t. $f_n = \tilde{d}_{n+1} S_n + S_{n-1} d_n \ \forall n$

$\cdots \to C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \to \cdots$

$\downarrow f_{n+1} \quad \swarrow S_n \quad \downarrow f_n \quad \swarrow S_{n-1} \quad \downarrow f_{n-1}$

$\cdots \to \tilde{C}_{n+1} \xrightarrow{\tilde{d}_{n+1}} \tilde{C}_n \xrightarrow{\tilde{d}_n} \tilde{C}_{n-1} \to \cdots$

$\rightsquigarrow H_\cdot(f): H_n(C) = \ker d_n / \mathrm{Im} d_{n+1} \to H_n(\tilde{C}) = \ker \tilde{d}_n / \mathrm{Im} \tilde{d}_{n+1}$, so $f_n(z) = \tilde{d}_{n+1} S_n(z) + S_{n-1} d_n(z)$

$z \mapsto 0 \quad \tilde{d}_{n+1}(S_n(z))$

- $f, g: C_\cdot \to \tilde{C}_\cdot$ are homotopic if $f-g$ is null homotopy, i.e. $H_\cdot(f) = H_\cdot(g)$

Thus, to study $_R\mathcal{M} \rightsquigarrow$ to study $\mathrm{Com}_*({}_R\mathcal{M}) \rightsquigarrow$ to study $\mathcal{K}({}_R\mathcal{M})$ (=: the homotopy category of ${}_R\mathcal{M}$)

Notice, $\mathrm{Obj}(\mathcal{K}({}_R\mathcal{M})) = \mathrm{Obj}(\mathrm{Com}_*({}_R\mathcal{M}))$

$\mathrm{Mor}_{\mathcal{K}({}_R\mathcal{M})}(C_\cdot, D_\cdot) = \mathrm{Mor}_{\mathrm{Com}_*({}_R\mathcal{M})}(C_\cdot, D_\cdot) \,/$ homotopy equivalence relations

11-22-24 (WEEK 12)

Ext

DEFINITION

Let $M \in_R m$. $\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$, where P_i is projective $\forall i$

Let $N \in_R m$. $0 \to \mathrm{Hom}_R(M,N) \xrightarrow{\bar{\varepsilon}} \mathrm{Hom}_R(P_0,N) \xrightarrow{\bar{d}_1} \mathrm{Hom}_R(P_1,N) \xrightarrow{\bar{d}_2} \mathrm{Hom}_R(P_2,N) \to \cdots$, $\bar{d}_{i+1} \circ \bar{d}_i = 0$, is a cochain complex of abelian groups.

We define $\forall n \geq 1$, $\mathrm{Ext}^n_R(M,N) := \ker \bar{d}_{i+1} / \mathrm{Im}\, \bar{d}_i$ and $\mathrm{Ext}^0_R := \ker \bar{d}_1 = \mathrm{Im}\, \bar{\varepsilon} = \mathrm{Hom}_R(M,N)$ (Actually, $H^2(G,N) = \mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z},N)$)

THEOREM (Comparison)

Given a projective resolution $\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$

$\quad \downarrow \exists f_2 \quad \downarrow \exists f_1 \quad \downarrow \exists f_0 \quad \downarrow f$

and an exact sequence $\cdots \to C_2 \xrightarrow{d_2'} C_1 \xrightarrow{d_1'} C_0 \xrightarrow{\varepsilon'} N \to 0$

$\Rightarrow \exists f_i : P_i \to C_i$ s.t. $\{f_i\}$ forms a chain map making the completed diagram commute

Then, any two such chain maps are homotopic

Proof

Existence: By induction on n, $n=0$, $P_0 \xrightarrow{\varepsilon} M \to 0$

by projectivity of $P_0 \to \exists f_0 \downarrow$, $f_0 \varepsilon \downarrow f$

$C_0 \to N \to 0$

For $n>0$, consider $\to P_n \xrightarrow{d_n} P_{n-1} \xrightarrow{d_{n-1}} P_{n-2} \to \cdots$

$\downarrow f_{n-1} \quad \downarrow f_{n-2}$

$\to C_n \xrightarrow{d_n'} C_{n-1} \xrightarrow{d_{n-1}'} C_{n-2} \to \cdots$

Claim: $\mathrm{Im}(f_{n-1} d_n) \subseteq \mathrm{Im} d_n' = \ker d_{n-1}' \Rightarrow$

Proof

$d_{n-1}'(f_{n-1} d_n) = (f_{n-2} d_{n-1}) d_n = 0$

P_n, $\exists ? \swarrow$, $\downarrow f_{n-1} d_n$

$C_n \twoheadrightarrow \mathrm{Im} d_n' \to 0$

Uniqueness: for another chain map $\{g_i : P_i \to C_i\}$, we construct a homotopy (up to homotopy)

$\to P_1 \to P_0 \to 0$, $s_{-1} := 0$

$\to C_1 \to C_0 \to 0$

By induction on n,

$P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1}$

$\downarrow s_n = ? \quad \downarrow g_n - f_n \quad \downarrow s_{n-1}$

$C_{n+1} \xrightarrow{d_{n+1}'} C_n \xrightarrow{d_n'} C_{n-1}$

Claim: $\mathrm{Im}(g_n - f_n - s_{n-1} d_n) \subseteq \underbrace{\mathrm{Im} d_{n+1}'}_{\ker d_n'} \Longrightarrow$

Proof

$d_n'(g_n - f_n - s_{n-1} d_n) = d_n' g_n - d_n' f_n - d_n' s_{n-1} d_n$

$= g_{n-1} d_n - f_{n-1} d_n - (g_{n-1} - f_{n-1} - s_{n-2} d_{n-1}) d_n$

P_n, $\exists s_n \swarrow$, $\downarrow g_n - f_n - s_{n-1} d_n$

$C_{n+1} \xrightarrow{d_{n+1}'} \mathrm{Im} d_{n+1}' \to 0$

THEOREM (Independency of the choice of projective resolutions)

Proof

(1) Consider two projective resolutions $M, \tilde{M}$, $\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$

$\downarrow \exists f_2 - g_2 \quad \downarrow \exists f_1 - g_1 \quad \downarrow \exists f_0 - g_0 \quad \downarrow f$

$\cdots \to \tilde{P}_2 \xrightarrow{d_2'} \tilde{P}_1 \xrightarrow{d_1'} \tilde{P}_0 \xrightarrow{\varepsilon'} \tilde{M} \to 0$

Apply Ham, then we have:

$0 \to \mathrm{Hom}_R(M,N) \xrightarrow{\bar{\varepsilon}} \mathrm{Hom}_R(P_0,N) \xrightarrow{\bar{d}_1} \mathrm{Hom}_R(P_1,N) \xrightarrow{\bar{d}_2} \cdots$

$\uparrow \bar{f} \quad \bar{s}_{-1} = 0 \quad \uparrow \exists \bar{f}_0 \quad \bar{s}_0 \quad \uparrow \exists \bar{f}_1$

$0 \to \mathrm{Hom}_R(\tilde{M},N) \xrightarrow{\bar{\varepsilon}'} \mathrm{Hom}_R(\tilde{P}_0,N) \xrightarrow{\bar{d}_1'} \mathrm{Hom}_R(\tilde{P}_1,N) \xrightarrow{\bar{d}_2'} \cdots$

$\hookrightarrow \bar{f}^* : \mathrm{Ext}^i_R(\tilde{M},N) \to \mathrm{Ext}^i_R(M,N)$

If $\exists \{g_i\}$ instead of $\{f_i\}$, since $\{f_i\}$ and $\{g_i\}$ are homotopic, thus $\{\bar{f}_i\}$ and $\{\bar{g}_i\}$ are homotopic, so $\bar{f}^* = \bar{g}^*$

(2) $f=Id$, $\tilde{M}=M$ in (1)

$\cdots\to P_2\to P_1\to P_0\to M\to 0$

$\downarrow g_2 \quad \downarrow g_1 \quad \downarrow g_0 \quad \downarrow id_M$

$\cdots\to \tilde{P}_2\to \tilde{P}_1\to \tilde{P}_0\to M\to 0$ (id$_{P_2}$, id$_{P_1}$, id$_{P_0}$)

$\downarrow f_2 \quad \downarrow f_1 \quad \downarrow f_0 \quad \downarrow id_M$

$\cdots\to P_2\to P_1\to P_0\to M\to 0$

$\Rightarrow \bar{g}_n^* \bar{f}_n^* : Ext_R^n(M,N)\to Ext_R^n(M,N)$ (where $\bar{f}_n^*$: ${}^{P}Ext_R^n(M,N)\to {}^{\tilde{P}}Ext_R^n(M,N)$, $\bar{g}_n^*$ the reverse)

$\Rightarrow$ any two $\bar{f}^*$ are isomorphic (can pick any P)

$(Id)^* = Id$

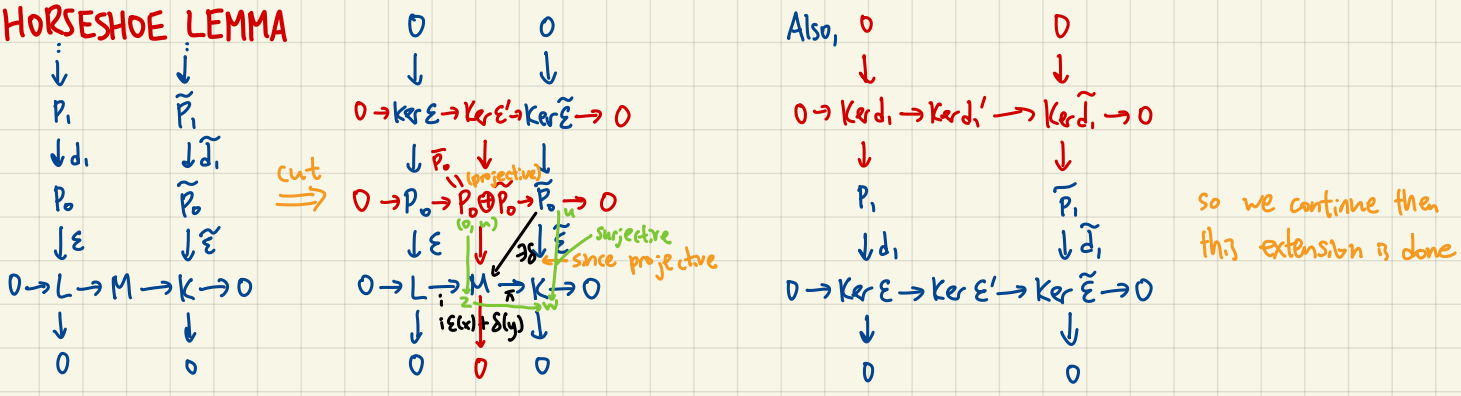
THEOREM (Long exact sequence for Ext) $H^0(Hom(P_\cdot,N))$ $H^1(Hom(P_\cdot,N))$ $H^1(Hom(\tilde{P}_\cdot,N))$

$0\to L\to M\to K\to 0 \rightsquigarrow 0\to Hom(K,N)\to Hom(M,N)\to Hom(L,N)\to Ext^1(K,N)\to Ext^1(M,N)\to \cdots\to 0$

Proof

We choose $\cdots\to P_2\to P_1\to P_0\to L\to 0$ (L's projective resolution) and $\cdots\to \tilde{P}_2\to \tilde{P}_1\to \tilde{P}_0\to K\to 0$

HORSESHOE LEMMA



By Horseshoe lemma, $\exists \cdots\to \bar{P}_2\to \bar{P}_1\to \bar{P}_0\to M\to 0$

Then, taking Hom,

$0\leftarrow Hom_R(P_1,N)\leftarrow Hom_R(\bar{P}_1,N)\leftarrow Hom_R(\bar{P}_2,N)\leftarrow 0$

$0\leftarrow Hom_R(P_0,N)\leftarrow Hom_R(\bar{P}_0,N)\leftarrow Hom_R(\tilde{P}_0,N)\leftarrow 0$ ($\bar{P}_0\oplus\tilde{P}_0$, so it is $\uparrow Hom_R(P_0,N)\oplus Hom_R(\tilde{P}_0,N)$, i.e. it is still exact)

$\rightsquigarrow$ Short exact sequence in $Com_{\mathbb{Z}}^{\geq}(A)$ (abelian group not module)

$\Downarrow$

long exact sequence in Homology objects

DEFINITIONS

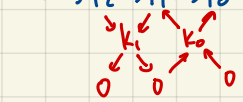
$Ext_{inj}^i(M,N) \leftarrow 0\to N\xrightarrow{\beta} I^\cdot$ is an injective resolution, define $H^i(Hom(M,I^\cdot)) = Ext_{inj}^i(M,N)$ (using inj/proj's exactness preservation)

Similarly, we can define $Ext_{proj}(M,N)$ for a projective resolution $P^\cdot\xrightarrow{\alpha} M\to 0$, define $H^i(Hom(P^\cdot,N)) = Ext_{proj}^i(M,N)$

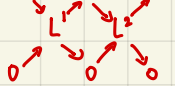
THEOREM (Equivalence of two definitions $Ext_{inj}^i(M,N) = Ext_{proj}^i(M,N)$)

Proof

- M: proj $\Rightarrow Ext_{proj}^n(M,N)=0$ $\forall n>0$ $\forall N\in_R M: \to 0\to 0\to M\xrightarrow{id} M\to 0$ (proj resolution of M)
- N: inj $\Rightarrow Ext_{inj}^n(M,N)=0$ $\forall n>0$ $\forall M\in_R m: 0\to N\to N\to 0\to 0\to \cdots$
- $\cdots\to P_2\to P_1\to P_0\to M\to 0$



$0\to N\to I^0\to I^1\to I^2\to \cdots$



For $0 \to K_0 \to P_0 \to M \to 0$, $0 \to N \to I^0 \to L' \to 0$,

$$\begin{array}{ccccccccccc}
0 & & 0 & & 0 & & & & & & \\
\downarrow & & \downarrow & & \downarrow & & & & & & \\
0 \to \mathrm{Hom}(M,N) & \to & \mathrm{Hom}(M,I^0) & \xrightarrow{\varphi} & \mathrm{Hom}(M,L') & \to & \mathrm{Ext}^1_{inj}(M,N) & \to & \mathrm{Ext}^1_{inj}(M,I^0) & \xleftarrow{inj} & 0 \\
\downarrow & & \downarrow & & \downarrow & & \| & & & & \\
0 \to \mathrm{Hom}(P_0,N) & \to & \mathrm{Hom}(P_0,I^0) & \xrightarrow{\sigma} & \mathrm{Hom}(P_0,L') & \to & 0 & & & & \\
\downarrow & & \downarrow & & \downarrow & \nwarrow proj & & & & & \\
0 \to \mathrm{Hom}(K_0,N) & \to & \mathrm{Hom}(P_0,I^0) & \to & \mathrm{Hom}(K_0,L') & \to & \mathrm{Ext}^1_{inj}(K_0,N) & \to & 0 & & \\
\downarrow \alpha & \cong \mathrm{coker}\,\alpha & \downarrow \beta & & \downarrow \gamma & & \cong \mathrm{coker}\,\gamma & & & & \\
0 \to \mathrm{Ext}^1_{proj}(M,N) & \to & 0 & \to & \mathrm{Ext}^1_{proj}(M,L') & \to & 0 & & & &
\end{array}$$

$\mathrm{coker}\,\sigma = \mathrm{Ext}^1_{proj}(M,N)$

By Snake lemma for α, β, γ, $\mathrm{Hom}(M,I^0) \xrightarrow{\varphi} \mathrm{Hom}(M,L') \to \mathrm{coker}\,\alpha \to 0$

$\mathrm{coker}\,\varphi \cong \mathrm{Ext}^1_{inj}(M,N)$

Also, $\mathrm{Im}\,\gamma = \gamma(\mathrm{Hom}(P_0,L')) = \gamma_\sigma(\mathrm{Hom}(P_0,I^0))$

$\mathrm{Im}\,\tau = \tau(\mathrm{Hom}(K_0,I^0)) = \tau_\beta(\mathrm{Hom}(P_0,I^0))$

$\Rightarrow \mathrm{coker}\,\tau \cong \mathrm{coker}\,\gamma$

$\mathrm{Ext}^1_{inj}(K_0,N) \cong \mathrm{Ext}^1_{proj}(M,L')$

OBSERVE

$I^{n-1} \xrightarrow{d_n} I^n \xrightarrow{d_{n+1}} \cdots$

$0 \to L^{n-1} \to$ an inj resolution of L^{n-1} $\to \mathrm{Ext}^1_{inj}(M,L^{n-1}) \cong \ker \overline{d_{n+1}} / \mathrm{Im}\,\overline{d_n} = \mathrm{Ext}^n_{inj}(M,N)$

Similarly, $\mathrm{Ext}^n_{proj}(M,L^{n-1}) \cong \mathrm{Ext}^1_{proj}(K_{n-1},N)$

$\therefore$ In conclusion, $\mathrm{Ext}^n_{inj}(M,N) \cong \mathrm{Ext}^1_{inj}(M,L^{n-1}) \cong \mathrm{Ext}^1_{proj}(K_0,L^{n-2}) \cong \mathrm{Ext}^1(K_1,L^{n-3}) \cong \cdots \cong \mathrm{Ext}^1(K_{n-1},L^0) \cong \mathrm{Ext}^n_{proj}(M,N)$

11-27-24 (WEEK 13)

Tor

RECALL

- $M \in {}_R\mathcal{M}$ is flat if $0 \to M_1 \to M_2$ in ${}_R\mathcal{M} \Rightarrow 0 \to M \otimes_R M_1 \to M \otimes_R M_2$ is exact in A
- $M \in \mathcal{M}_R$ is flat if $0 \to M_1 \to M_2$ in $\mathcal{M}_R \Rightarrow 0 \to M_1 \otimes_R M \to M_2 \otimes_R M$ is exact in A

PROPOSITION 1

Projective $\Rightarrow$ flat

Proof

Claim: $\bigoplus_{i \in \Lambda} M_i$ is flat $\Leftrightarrow M_i$ is flat $\forall i$

Proof

Given $0 \to N_1 \to N_2$ in ${}_R\mathcal{M}$, by def,

$$\begin{array}{ccc} (\bigoplus_{i\in\Lambda} M_i) \otimes N_1 & \longrightarrow & (\bigoplus_{i\in\Lambda} M_i) \otimes N_2 \text{ is injective} \\ \| & & \| \\ \bigoplus_{i\in\Lambda} (M_i \otimes N_1) & \longrightarrow & \bigoplus_{i\in\Lambda} (M_i \otimes N_2) \text{ is injective } \forall i \end{array}$$

DEFINITION

Let $P_\cdot \to M \to 0$ be a projective resolution in $\mathcal{M}_R$ and $N \in {}_R\mathcal{M}$, define ${}^R\mathrm{Tor}_n(M,N) := H_n(P_\cdot \otimes N)$ $\forall n > 0$ and ${}^R\mathrm{Tor}_0(M,N) := M \otimes_R N$

Let $Q_\cdot \to N \to 0$ be a projective resolution in ${}_R\mathcal{M}$ and $M \in \mathcal{M}_R$, define ${}^L\mathrm{Tor}_n(M,N) := H_n(M \otimes Q_\cdot)$ $\forall n > 0$ and ${}^L\mathrm{Tor}_0(M,N) := M \otimes_R N$

FACT

Given a flat U, $\mathrm{Tor}_n(U,N) = 0$ $\forall n > 0$, say U is $\cdots \to F_1 \to F_0 \to N \to 0$

Proof

We can "cut" U into many short exact sequences:

$$0 \to K_0 \to \overset{\text{free}}{F_0} \to N \to 0 \implies 0 \to U \otimes K_0 \to U \otimes F_0 \to U \otimes N \to 0$$

$$0 \to K_1 \to F_1 \to K_0 \to 0 \implies 0 \to U \otimes K_1 \to U \otimes F_1 \to U \otimes K_0 \to 0$$

Then we combine the short exact sequences again to form $\cdots \to U \otimes F_1 \to U \otimes F_0 \to U \otimes N \to 0$ which is exact

$\therefore$ In other words, $H_n(U \otimes F_\cdot) = 0$ $\forall n > 0$. $\square$

REMARK

By applying Hom (Hom$(M, \cdot)$) instead of $\otimes$, we can similarly get for all projective M, $\mathrm{Ext}^n(M,N) = 0$ $\forall n > 0$

PROPOSITION 2

Given $0 \to L \to M \to K \to 0$ in $\mathcal{M}_R$ and $N \in {}_R\mathcal{M}$, then $\exists$ a long exact sequence

$$\cdots \to \mathrm{Tor}_1(L,N) \to \mathrm{Tor}_1(M,N) \to \mathrm{Tor}_1(K,N) \to L \otimes N \to M \otimes N \to K \otimes N \to 0$$

$$H_1(P_L \otimes N) \quad H_1(P_M \otimes N) \quad H_1(P_K \otimes N) \qquad\qquad H_0(P_K \otimes N)$$

THEOREM (Tor for flat resolutions)

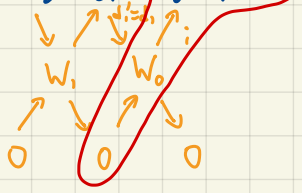
Let $U_\cdot \to M \to 0$ be a flat resolution of M in $\mathcal{M}_R$, then $\mathrm{Tor}_n(M,N) \cong H_n(U_\cdot \otimes N)$ $\forall n \geq 0$.

Proof

- $n=0$: $\because U_1 \otimes N \xrightarrow{d_1 \otimes 1} U_0 \otimes N \to M \otimes N \to 0$ is exact $\Rightarrow U_1 \otimes N \to U_0 \otimes N \to 0$ is a chain complex (not exact)

  $\therefore H_0(U_0 \otimes N) = U_0 \otimes N / \mathrm{Im} d_1 \otimes 1 \cong M \otimes N = \mathrm{Tor}_0(M,N)$ ("mini" exact sequence)

- $n=1$: $\to U_2 \xrightarrow{d_2} U_1 \xrightarrow{d_1} U_0 \to M \to 0$



Then, we have $0 \to \mathrm{Tor}_2(M,N) \to \mathrm{Tor}_1(W_0,N) \to \mathrm{Tor}_1(U_0,N) \to \mathrm{Tor}_1(M,N) \to W_0 \otimes N \xrightarrow{i\otimes 1} U_0 \otimes N \to M \otimes N \to 0$ ($\mathrm{Tor}_1(U_0,N) = 0$ (∵ flat), $\mathrm{Tor}_1(M,N) = \ker(i\otimes 1)$)

$\hookrightarrow U_2 \otimes N \xrightarrow{d_2\otimes 1} U_1 \otimes N \xrightarrow{d_1\otimes 1} U_0 \otimes N$ where $H_1(U_\cdot \otimes N) = \ker d_1\otimes 1 / \mathrm{Im} d_2 \otimes 1$

$d_1' \otimes 1$, $i \otimes 1$, $\overline{d_1 \otimes 1}$

$W_0 \otimes N \xleftarrow{\cong} U_1 \otimes N / \mathrm{Im} d_2 \otimes 1$

$W_0 \otimes N \to 0$

└ Im is always 2 arrows away (just a pattern I observed lol)

KEY!!

But this also means $\ker i\otimes 1 = \ker d_1 \otimes 1 = \ker d_1 \otimes 1 / \mathrm{Im} d_2 \otimes 1 = H_1(U_\cdot \otimes N)$ where $\ker i \otimes 1 = \mathrm{Tor}_1(M,N)$

KEY! Use the "diff" property of Tor! (Not rigorously saying it but that's the idea)

- $n=2$: $\mathrm{Tor}_2(M,N) = \mathrm{Tor}_1(W_0,N) \cong H_1(U_{W_0} \otimes N) = H_2(U_M \otimes N)$

$\cdots \to U_1 \to U_0 \to M \to 0$

W_0

$0 \quad 0$

By induction, we can decrease the degree by 1 every time, so $\mathrm{Tor}_n(M,N) = H_n(U_\cdot \otimes N)$!

COROLLARY

Let $A \in \mathcal{A} = {}_{\mathbb{Z}}\mathcal{M}$. Then, $\mathrm{Tor}_1(\mathbb{Q}/\mathbb{Z}, A) = t(A)$ ← the torsion part of A and also $\mathrm{Tor}_n(\mathbb{Q}/\mathbb{Z}, A) = 0 \ \forall n \geq 2$

Proof

We have the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, and $\mathbb{Q}$ is a flat $\mathbb{Z}$-module

Thus, $0 \to A_1 \xrightarrow{\delta} A_2 \Rightarrow 0 \to \mathbb{Q} \otimes_{\mathbb{Z}} A_1 \xrightarrow{1\otimes\delta} \mathbb{Q} \otimes_{\mathbb{Z}} A_2$

REMARK

What is $\mathbb{Q} \otimes_{\mathbb{Z}} A$?

Each element is $\mathbb{Q} \otimes_{\mathbb{Z}} A \Rightarrow \sum_{i=1}^n \frac{a_i}{b_i} \otimes x_i = \sum_{i=1}^n \frac{1}{b_i} \otimes a_i x_i = \sum_{i=1}^n \frac{\overline{b_i}}{b} \otimes a_i x_i = \sum_{i=1}^n \frac{1}{b} \otimes \overline{b_i} a_i x_i = \frac{1}{b} \otimes \sum_{i=1}^n \overline{b_i} a_i x_i$

(We define $b = b_1 \cdots b_n$, $\overline{b_i} = b_1 \cdots \widehat{b_i} \cdots b_n$)

Notice, $\frac{1}{a} \otimes x + \frac{1}{b} \otimes y = \frac{b}{ab} \otimes x + \frac{a}{ab} \otimes y = \frac{1}{ab} \otimes (bx + ay)$, and also $\frac{1}{a} \otimes x = \frac{1}{b} \otimes 0 \Rightarrow bx = 0$ (∵ $\frac{1}{a} = \frac{b}{ab}$)

Here, $\mathbb{Q} \otimes_{\mathbb{Z}} A_1 \xrightarrow{1\otimes\delta} \mathbb{Q} \otimes_{\mathbb{Z}} A_2$

$\frac{1}{a} \otimes x \longmapsto \frac{1}{a} \otimes \delta(x) = \frac{1}{b} \otimes 0 \Rightarrow b\delta(x) = 0 \Rightarrow bx = 0 \Rightarrow \frac{1}{a} \otimes x = 0$

PROPOSITION 3

TFAE

(1) M is a flat left R-module

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

(3) $\forall 0 \to I \to R$: exact $\Rightarrow 0 \to I \otimes M \to R \otimes M$: exact (kind of like Baer's criterion)

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

Proof

(2)⇔(3): For $0 \to I \to R \to R/I \to 0$, we form the long exact sequence $\mathrm{Tor}_1(R,M) \to \mathrm{Tor}_1(R/I, M) \to I \otimes M \to R \otimes M \to 0$ ($\mathrm{Tor}_1(R,M) = 0$)

(1)⇔(4): $\forall 0 \to N' \to N$: exact, we have $\mathrm{Hom}_R(N, M^*) \to \mathrm{Hom}_R(N', M^*)$

$\| \qquad\qquad \| \cong$

$\mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z}) \qquad \| \cong$

$\| \cong$

$\mathrm{Hom}_R(N \otimes M, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_R(N' \otimes M, \mathbb{Q}/\mathbb{Z})$

$\| \qquad\qquad \|$

$(N \otimes M)^* \longrightarrow (N' \otimes M)^*$

FACT

$A^* = 0 \Leftrightarrow A = 0$, $0 \to B \to C \Leftrightarrow C^* \to B^* \to 0$

Proof

"$A^* = 0 \Leftrightarrow A = 0$": "⇐": OK

"⇒": If $\exists\, 0 \neq a \in A$, then $0 \to \langle a \rangle \to A$, $a \mapsto \frac{1}{\operatorname{ord}(a)} \in \mathbb{Q}/\mathbb{Z}$ (or $\frac{1}{2}$ if undef), f inj, $\exists \tilde{f} \neq 0 \Rightarrow A^* \neq 0$ ⨯

"$0 \to B \to C \Leftrightarrow C^* \to B^* \to 0$": $0 \to \ker f \to B \xrightarrow{f} C \Rightarrow C^* \xrightarrow{f^*} B^* \to (\ker f)^* = \operatorname{coker} f^* \to 0$

$\therefore \ker f = 0 \Leftrightarrow \operatorname{coker} f^* = (\ker f)^* = 0$

Now, M^* is injective $\Leftrightarrow \operatorname{Hom}_R(N, M^*) \to \operatorname{Hom}_R(N', M^*) \to 0$, where $\operatorname{Hom}_R(N, M^*) = (N \otimes M)^*$ and $\operatorname{Hom}_R(N', M^*) = (N' \otimes M)^*$

$\Leftrightarrow 0 \to N \otimes M \to N' \otimes M$

"(4) ⇔ (3)": By Baer's criterion, M^* is injective $\Leftrightarrow \operatorname{Hom}_R(R, M^*) \to \operatorname{Hom}_R(I, M^*) \to 0 \ \forall I \subseteq R$, where $\operatorname{Hom}_R(R, M^*) = (R \otimes M)^*$ and $\operatorname{Hom}_R(I, M^*) = (I \otimes M)^*$

$\Leftrightarrow 0 \to I \otimes M \to R \otimes M \ \forall I \subseteq R$

EXAMPLES

$R = \mathbb{Z}$, $M = \mathbb{Z}/m\mathbb{Z}$, $m \geq 0$: $\operatorname{Ext}^0(\mathbb{Z}/m\mathbb{Z}, N) \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) = \{a \in N \mid ma = 0\} = {}_mN$ $(t(N) = \operatorname{Tor}_1(\mathbb{Q}/\mathbb{Z}, N)$, $a \in N$, $\exists n \in \mathbb{N}$, s.t. $na = 0)$

$\bar{1} \mapsto 0$

Then, we create the exact sequence $0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$ ($\mathbb{Z}$ → 0 (deg 0))

$0 \to \operatorname{Hom}(\mathbb{Z}, N) \xrightarrow{\bar{m}} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \to 0$, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \cong N$

$\therefore \operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) \cong N/mN$, $\operatorname{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) = 0 \ \forall n \geq 2$

$R = \mathbb{Z}/m\mathbb{Z}$, $M = \mathbb{Z}/d\mathbb{Z}$, $d \mid m$: $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ is homo $\Rightarrow \mathbb{Z}/d\mathbb{Z}$ is a $\mathbb{Z}/m\mathbb{Z}$-module

Free resolution: $\cdots \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{\times d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{\times \frac{m}{d}} \mathbb{Z}/m\mathbb{Z} \xrightarrow{\times m} \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \to 0$ (doesn't stop)

$\operatorname{Ext}^0_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, N) \cong \operatorname{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, N) = \{a \in N \mid \frac{m}{d} a = 0\} = {}_{\frac{m}{d}}N$

$\operatorname{Ext}^n_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, N) \cong {}_{\frac{m}{d}}N/{}_dN$ for odd n, $N/N \cong 0$ for even n

11-29-24 (WEEK 13)

BAR RESOLUTION

RECALL

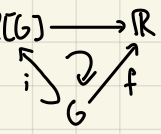
The group ring of G is $\mathbb{Z}[G] := \{\sum_{g\in G} a_g g \mid (a_g)_{g\in G} \in \bigoplus_{g\in G}\mathbb{Z}\}$ under where $(\sum_{g\in G} a_g g)(\sum_{g\in G} b_g g) = \sum_{g\in G}\sum_{h\in G} a_h b_{h^{-1}g}\, g$

EXAMPLES

1. $G=\{1\} \Rightarrow \mathbb{Z}[G]\cong\mathbb{Z}$
2. $G=\langle x\rangle\cong\mathbb{Z} \Rightarrow \mathbb{Z}[G]\cong\mathbb{Z}[x,x^{-1}]$
3. $G=\langle a\rangle\cong\mathbb{Z}/n\mathbb{Z} \Rightarrow \mathbb{Z}[G]\cong \mathbb{Z}[x]/\langle x^n-1\rangle$ (quotient from the "mod")
4. $G=S_3 \Rightarrow \mathbb{Z}[G]\cong\mathbb{Z}\oplus\mathbb{Z}\sigma\oplus\mathbb{Z}\tau\oplus\mathbb{Z}\sigma^2\oplus\mathbb{Z}\sigma\tau\oplus\mathbb{Z}\sigma^2\tau$ (cannot write it in a prettier way)

UNIVERSAL PROPERTY (for $\mathbb{Z}[G]$, $i: G\hookrightarrow\mathbb{Z}[G]$)

$\forall$ ring R and $\forall f: G\longrightarrow R^\times$ group homo, then $\exists$ ring homo $\varphi:\mathbb{Z}[G]\longrightarrow R$



RECALL

Given $N\in A$ and $G\curvearrowright N \Rightarrow N$ is a left $\mathbb{Z}[G]$-module

NOTE

Given $N\in_{\mathbb{Z}[G]}\mathcal{M}$, $N\times G\longrightarrow N$ (already can $G\times N$!) we have $N\curvearrowleft G$, so $N=\mathrm{Inv}(N)$ is a right $\mathbb{Z}[G]$-module ("involution" means this kind of inverse action)

$(a,g)\longmapsto g^{-1}a$

DEFINITION

$\forall N, M\in_{\mathbb{Z}[G]}\mathcal{M}$, define $N\otimes_G M := \mathrm{Inv}(N)\otimes_{\mathbb{Z}[G]} M \in\mathbb{Z}\mathcal{M}$ (Intuition: $ga\otimes b = ag^{-1}\otimes b = a\otimes g^{-1}b$)

define $\mathrm{Hom}_G(N,M) := \mathrm{Hom}_{\mathbb{Z}[G]}(N,M)\in\mathbb{Z}\mathcal{M}$

CONVENTION

- $\mathbb{Z}$ can be regarded as a trivial $\mathbb{Z}[G]$-module: $G\times\mathbb{Z}\longrightarrow\mathbb{Z}$, $(g,n)\mapsto n$
- $\mathbb{Z}[G]$ is a $\mathbb{Z}[G]$-$\mathbb{Z}[G]$ bimodule

DEFINITION

Given $G\curvearrowright N$, $N\in_{\mathbb{Z}[G]}\mathcal{M}$, the invariants of N are $N^G := \{a\in N \mid g\cdot a = a\ \forall g\in G\}\in\mathbb{Z}\mathcal{M}$

We can also define the coinvariants (kind of like "dual") of N are $N_G := N/\langle ga-a \mid g\in G, a\in N\rangle$ (We forcefully cause $g\bar{a}=\bar{a}$)

FACT

- $N^G\xrightarrow{\sim}\mathrm{Hom}_G(\mathbb{Z},N)$ (extension of $N\cong\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},N)\cong\mathrm{Hom}_G(G,N)$ idea)

  $a\longmapsto\sigma_a: 1\longmapsto a$

  $\hookrightarrow \sigma_a(g\cdot 1)=\sigma_a(1)=a$, but $g\sigma_a(1)=ga$, so $ga=a$ (because of Hom), i.e. N^G!
- $N_G\cong N\otimes_G\mathbb{Z}$

  $\bar{a}\longmapsto a\otimes 1$ (Using $\bar{\varphi}$)

  We construct the above with $\varphi: N\longrightarrow N\otimes_G\mathbb{Z}$, $a\mapsto a\otimes 1$

  Claim: $\langle ga-a \mid g\in G, a\in N\rangle\subseteq\ker\varphi$

  Proof

  $\varphi(ga-a)=(ga-a)\otimes 1 = ga\otimes 1 - a\otimes 1 = a\otimes g^{-1}1 - a\otimes 1 = a\otimes 1 - a\otimes 1 = 0$ ✓

We know φ is onto with $\sum_{i=1}^{s} a_i \otimes n_i = \sum_{i=1}^{s} (n_i a_i \otimes 1) = (\sum_{i=1}^{s} n_i a_i) \otimes 1$

To construct φ^{-1}, define $\psi : N \times \mathbb{Z} \longrightarrow N_G$ as a **bad additive map**
$(a, n) \longmapsto \overline{na}$ (so (a, g^n), (ag, n) map to the same thing $\Rightarrow \overline{ng^{-1}a} = \overline{na}$, i.e. $n(\overline{g^{-1}a} - \overline{a}) = \overline{0} \in N_G$)

EXAMPLES

1. $|G| < \infty$, $(\mathbb{Z}[G])_G \cong \mathbb{Z}$

   Proof

   Let $G = \{g_1, \dots, g_s\}$, then $\forall \sum_{i=1}^{s} a_i g_i \in (\mathbb{Z}[G])_G$, $g_j(\sum_{i=1}^{s} a_i g_i) = \sum_{i=1}^{s} a_i g_j g_i$ (which equals 1 as we defined.)

   $\sum_{i=1}^{s} a_i g_i$ — elements in the form $a_j g_j$

   $a_i g_j g_i = a_1 g_j \Rightarrow a_i = a_1 \ \forall i = 2, \dots, s$, i.e. $\sum_{i=1}^{s} a_i g_i = a_1 \sum_{i=1}^{s} g_i$ (since it has "g_j" at the end, it must be equal to "g_j" on the LHS, so $a_j g_j = a_1 g_j$)

   $\therefore (\mathbb{Z}[G])_G \cong \langle \sum_{i=1}^{s} g_i \rangle_{\mathbb{Z}} \cong \mathbb{Z}$ ($\mathbb{Z} = \langle 1 \rangle_{\mathbb{Z}}$, so just map $\sum_{i=1}^{s} g_i \longmapsto 1$)

2. $|G| = \infty$, $(\mathbb{Z}[G])_G = \{0\}$

   $\forall \sum_{i=1}^{s} a_i g_i$ with $\{g_1, \dots, g_s\} \in G$ (assume none equal), then $\exists g \in G$, s.t. $gg_1 \notin \{g_1, \dots, g_s\}$

   Then, $g(\sum_{i=1}^{s} a_i g_i) = \sum_{i=1}^{s} a_i g g_i$, but gg_i does not appear in LHS $\forall i \Rightarrow a_i = 0 \ \forall i$

   $\sum_{i=1}^{s} a_i g_i$

3. $(\mathbb{Z}[G])_G \cong \mathbb{Z}(G) \otimes_{\mathbb{Z}(G)} \mathbb{Z} \cong \mathbb{Z}$

THE BAR RESOLUTION OF $\mathbb{Z}$

We consider $B(G): \cdots \to B_2 \xrightarrow{d_2} B_1 \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ in $\mathbb{Z}[G]$-$\mathbf{m}$

↳ $B_0 = \mathbb{Z}[G][\,]$ (rank 1), $\varepsilon : [\,] \longmapsto 1 \Rightarrow \varepsilon((\sum_{\text{finite}} \lambda_g g)[\,]) = (\sum_{\text{finite}} \lambda_g g)(1) = \sum_{\text{finite}} \lambda_g$ ($\varepsilon([\,]) = 1$; extend by linearity)

↳ $B_n = \bigoplus_{x_i \in G} \mathbb{Z}(G)[x_1 | x_2 | \cdots | x_n]$ (kind of like $G^{\oplus n}$)

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

EXAMPLE

We know $d_1[x] = x[\,] - [\,]$, $d_2[x|y] = x[y] - [xy] + [x]$ (coboundary), $d_3[x|y|z] = x[y|z] - [xy|z] + [x|yz] - [x|y]$ (factor set)

"$\varepsilon d_1 = 0$": $\varepsilon d_1[x] = \varepsilon(x[\,] - [\,]) = x - 1$????

"$d_n d_{n+1} = 0$": $d_n d_{n+1}[x_1 | \cdots | x_{n+1}] = d_n(x_1[x_2 | \cdots | x_{n+1}]) + \sum_{i=1}^{n} (-1)^i d_n([x_1 | \cdots | x_i x_{i+1} | \cdots | x_{n+1}]) + (-1)^{n+1} d_n([x_1 | \cdots | x_n])$

$= x_1 x_2 [x_3 | \cdots | x_{n+1}] + \sum_{i=1}^{n-1} (-1)^i x_1 [x_2 | \cdots | x_i x_{i+1} | \cdots | x_{n+1}] + (-1)^n x_1 [x_2 | \cdots | x_n]$

$+ \sum_{i=1}^{n} (-1)^i$

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

Continue at home

THE HOMOGENOUS RESOLUTION OF $\mathbb{Z}$

We consider $P(G): \cdots \to P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon'} \mathbb{Z} \to 0$

↳ $P_n = \bigoplus_{x_i \in G} \mathbb{Z}(x_0, \dots, x_n)$; $G \curvearrowright P_n$ by $x(x_0, \dots, x_n) = (xx_0, \dots, xx_n)$ so we rewrite $P_n = \bigoplus_{x_i \in G} \mathbb{Z}(G)(1, x_1, \dots, x_n)$

↳ $\varepsilon' : (x) \longmapsto 1$

↳ $\partial_n : (x_0, \dots, x_n) \longmapsto \sum_{i=0}^{n} (-1)^i (x_0, \dots, \hat{x}_i, \dots, x_n) \Rightarrow \partial_n \partial_{n+1} = 0$

$P(G) \cong B(G)$

Construct the chain map:

$$\begin{array}{ccccccccccc}
\cdots & \to & P_{n+1} & \xrightarrow{\partial_{n+1}} & P_n & \xrightarrow{\partial_n} & P_{n-1} & \to \cdots \to & P_0 & \xrightarrow{\varepsilon'} & \mathbb{Z} \to 0 \\
 & & \downarrow \tau_{n+1} & & \downarrow \tau_n & & \downarrow \tau_{n-1} & & \downarrow \tau_0 & & \downarrow \mathrm{id} \\
\cdots & \to & B_{n+1} & \xrightarrow{d_{n+1}} & B_n & \xrightarrow{d_n} & B_{n-1} & \to \cdots \to & B_0 & \xrightarrow{\varepsilon} & \mathbb{Z} \to 0
\end{array}$$

(τ_n: $(x_0, x_1, \dots, x_n) \longmapsto [x_0 | x_0^{-1}x_1 | x_1^{-1}x_2 | \cdots | x_{n-1}^{-1}x_n]$; τ_n^{-1}: $x_0[x_0^{-1}x_1 | x_1^{-1}x_2 | \cdots | x_{n-1}^{-1}x_n] \longmapsto (x_0, x_1, \dots, x_n)$)

Check $(x_0, x_1, \dots, x_n) \longrightarrow x \curvearrowright (x_0, x_1, \dots, x_n) = (xx_0, xx_1, \dots, xx_n)$

↓ ↓ Prove this holds

$x_0[x_0^{-1}x_1 | x_1^{-1}x_2 | \cdots | x_{n-1}^{-1}x_n] \longmapsto x \curvearrowright x_0[x_0^{-1}x_1 | x_1^{-1}x_2 | \cdots | x_{n-1}^{-1}x_n]$

P(G) IS EXACT

Define $s_{-1}: \mathbb{Z} \to P_0$, $1 \mapsto (1)$; $s_n: P_n \longrightarrow P_{n+1}$, $(x_0, \dots, x_n) \longmapsto (1, x_0, \dots, x_n)$

Now, we prove 1_{P_n} on $P(G)$ via s_n to $P(G)$

Then, we have $1_{P_n} = s_{n-1} \circ \partial_n + \partial_{n+1} \circ s_n$. That is, $id: P(G) \to P(G)$ and $0: P(G) \to P(G)$ are homotopic $\Rightarrow H_n(P(G)) = 0 \ \forall n$

In other words, $\ker \partial_n(P(G)) = \operatorname{Im} \partial_{n+1}(P(G))$, so $P(G)$ is exact, then as $P(G) \cong B(G)$, $B(G)$ is also exact

NORMALIZED BAR RESOLUTION OF $\mathbb{Z}$ (Quotienting to make $[x|1] = 0$, $[1|y] = 0$ like factor set)

We define the following: $\cdots \to B_2^* \xrightarrow{d_2^*} B_1^* \xrightarrow{d_1^*} B_0^* \xrightarrow{\varepsilon} \mathbb{Z} \to 0$

↳ Define $U_n = \bigoplus_{x_i \in G, \exists x_i = 1} \mathbb{Z}[G][x_1|\cdots|x_n]$, $B_n^* := B_n / U_n \cong \bigoplus_{x \in G} \bigoplus_{x_i \neq 1} \mathbb{Z}[G][x_1|\cdots|x_n]$

↳ Define $d_n^*: [x_1|\cdots|x_n] + U_n \longmapsto d_n([x_1|\cdots|x_n]) + U_{n-1}$ (Note: $d_n(U_n) \subseteq U_{n-1}$)

$B^*(G)$ IS EXACT (We can't define $P^*(G)$ but we can use homotopy)

Define $t_n: B_n \to B_{n+1}$ by $t_n = \tau_{n+1} \circ s_n \circ \tau_n^{-1}$ ($\mathbb{Z}$-module homo) and of course the associated $t_n^*: B_n^* \to B_{n+1}^*$, (Note: $t_n(U_n) \subseteq U_{n-1}$)

Then, we get it is a homotopy with $1_{B_n^*} = d_{n+1}^* t_n^* + t_{n-1}^* d_n^* \Rightarrow B^*(G)$ is exact

(Upcoming we want $H^2(G, N) = \operatorname{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, N)$)

12-4-24 (WEEK 14)

LOW-DIMENSIONAL COHOMOLOGY

RECALL

The normalized Bar resolution: $\cdots \to B_2^* \xrightarrow{d_2^*} B_1^* \xrightarrow{d_1^*} B_0^* \xrightarrow{\varepsilon^*} \mathbb{Z} \to 0$ and its corresponding $\mathrm{Hom}_{\mathbb{Z}[G]}(B_0^*, N) \xrightarrow{\overline{d_1^*}} \mathrm{Hom}_{\mathbb{Z}[G]}(B_1^*, N) \xrightarrow{\overline{d_2^*}} \mathrm{Hom}_{\mathbb{Z}[G]}(B_2^*, N) \xrightarrow{\overline{d_3^*}} \cdots$

1. $\mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, N) = \mathrm{Ker}\overline{d_3^*}/\mathrm{Im}\overline{d_2^*} = H^2(G, N)$
   - $f \in \mathrm{Ker}\overline{d_3^*}$, i.e. $\overline{d_3^*}(f) = 0$ ($= f \circ d_3^*$) $\Rightarrow f \cdot \overline{d_3^*}[x|y|z] = f(x[y|z]) - f([xy]|z] + f([x|yz]) - f([x|y]) = 0$
     $B_2^* \to N$; d_3^*: $f([x|1]) = 0$, $f([1|y]) = 0$ (since it is normalized); $f: G \times G \to N$ is a factor set
     So, $Z^2(G, N) = \mathrm{Ker}\, d_3^* = \mathrm{Hom}_{\mathbb{Z}[G]}(B_2^*, N)$
   - $f \in \mathrm{Im}\overline{d_2^*}$, say $f = \overline{d_2^*}(h) = h \circ d_2^* \Rightarrow f([x|y]) = h \circ d_2^*([x|y]) = h(x[y]) - h([xy]) + h([x]) = xh[y] - h[xy] + h[y]$
     $\Downarrow$
     $f \in B^2(G, N)$
     So, $\mathrm{Im}\overline{d_2^*} = B^2(G, N)$
2. $\mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, N) := \mathrm{Ker}\overline{d_2^*}/\mathrm{Im}\overline{d_1^*} \cong \mathrm{Der}(G, N)/\mathrm{PDer}(G, N) = H^1(G, N)$
   - $g \in \mathrm{Ker}\overline{d_2^*} \subseteq \mathrm{Hom}_{\mathbb{Z}[G]}(B_1^*, N) \Rightarrow g \circ d_2 = 0$
     $\forall x, y \in G$, $g \circ d_2([x|y]) = g(x[y]) - [xy] + [x]) = 0 \Rightarrow xg([y]) - g([xy]) + g([x]) = 0$
     $\Downarrow$
     Associate $g \rightsquigarrow d: G \to N$ by $d(x) = g([x]) \Rightarrow d(xy) = xd(y) + d(x) \Rightarrow x \in \mathrm{Der}(G, N)$
   - $d \in \mathrm{Der}(G, N)$, define $g \in \mathrm{Hom}_{\mathbb{Z}[G]}(B_1^*, N)$ by $g([x]) = d(x) \Rightarrow g \in \mathrm{Ker}\overline{d_2^*}$
   - Let $t \in \mathrm{Hom}(B_0^*, N)$, say $t([\,]) = a_0 \in N$, then $\mathrm{PDer}(G, N)$: $\overline{d_1^*}(t)([x]) = t \circ d_1([x]) = t(x[\,] - [\,]) = xt([\,]) - t([\,]) = xa_0 - a_0$
   - Let $p \in \mathrm{PDer}(G, N)$, say $p(x) = xb_0 - b_0$ for some $b_0 \in N$. Define $s: B_0 \to N$, $[\,] \mapsto b_0$ $\Rightarrow p = \overline{d_1^*}(s) \in \mathrm{Im}\overline{d_1^*}$
3. $\mathrm{Ext}^0_{\mathbb{Z}[G]}(\mathbb{Z}, N) := \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, N) = \mathrm{Hom}_G(\mathbb{Z}, N) \cong N^G$

APPLICATION

Let $N = C_4$, $G = C_2 \Rightarrow 0 \to N \to E \to G \to 1$

Consider addition for N, $N = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, and multiplication for G, $G = \langle t \rangle$

Step 1: Find all $\sigma: G \to \mathrm{Aut}(N)$
- $t \mapsto \mathrm{id}$ ← $G \curvearrowright N$ trivially
- $t \mapsto \sigma(t): \bar{1} \mapsto -\bar{1}$ ← non-trivial

Step 2: For each σ, compute $H^2(G, N) = \mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, N)$

In general, if G is cyclic of order n, say $G = \langle t \rangle$, i.e. $t^n = 1 \Rightarrow (t-1)(\underbrace{t^{n-1} + t^{n-2} + \ldots + t + 1}_{u \in \mathbb{Z}[G]}) = 0$

We get $\cdots \to \mathbb{Z}[G] \xrightarrow{u} \mathbb{Z}[G] \xrightarrow{t-1} \mathbb{Z}[G] \xrightarrow{u} \mathbb{Z}[G] \xrightarrow{t-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$

($\sum_{i=0}^{n-1} a_i t^i$; $\sum a_g g$; $\sum a_g$)

Rough Work:
- $\mathrm{Ker}\varepsilon = \{\sum_{i=0}^{n-1} a_i t^i \mid \sum_{i=0}^{n-1} a_i = 0\} = \sum_{i=0}^{n-1} a_i t^i - \sum_{i=0}^{n-1} a_i = \sum_{i=0}^{n-1} a_i (t-1) = (t-1)$ ★
- $\mathrm{Im}(t-1) \ni (t-1)(\sum_{i=0}^{n-1} a_i t^i) = \sum_{i=0}^{n-1} a_i t^{i+1} - \sum_{i=0}^{n-1} a_i t^i = \ldots \in ((t-1)(\quad)) = 0$
- $\mathrm{Ker}(t-1) \ni \sum_{i=0}^{n-1} a_i t^i = a_0(\sum_{i=0}^{n-1}) = a_0 u$, also $(t-1)(\sum_{i=0}^{n-1} a_i t^i) = 0 \Rightarrow a_{n-1} - a_0 = 0 \Rightarrow a_0 = a_i\ \forall i$
- $\mathrm{Ker}\, u \ni \sum_{i=0}^{n-1} a_i t^i \Rightarrow (t^{n-1} + t^{n-2} + \ldots + t + 1)(a_{n-1}t^{n-1} + \ldots + a_1 t + a_0) = 0 \Rightarrow$ constant term $a_{n-1} + \ldots + a_2 + a_1 + a_0$, i.e. $(t-1) \mid \sum_{i=0}^{n-1} a_i t^i$

$\Rightarrow$ We know the sequence is like: $0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, N) \xrightarrow{\bar{\varepsilon}} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], N) \xrightarrow{\overline{(t-1)}} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], N) \xrightarrow{\bar{u}} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], N) \xrightarrow{\overline{(t-1)}} \cdots$

Hence, $H^2(G, N) = \mathrm{Ker}\overline{(t-1)}/\mathrm{Im}\bar{u} = \mathrm{Im}\bar{\varepsilon}/\mathrm{Im}\bar{u} = \mathrm{Hom}_G(\mathbb{Z}, N)/\mathrm{Im}\bar{u} = \frac{N^G}{uN}$

Case 2.1: $G \curvearrowright N$ trivially

Then, $H^2(G, N) = N^G/uN = N/2N \cong \frac{\mathbb{Z}/4\mathbb{Z}}{2\mathbb{Z}/4\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$

($u = t+1$, $a \in N \Rightarrow ua = 2a$)

Case 2.2: Otherwise

Then, $H^2(G, N) = \{\bar{0}, \bar{2}\}/\{\bar{0}\} \cong \mathbb{Z}/2\mathbb{Z}$

($u = t+1$, $a \in N$, $-ua = 0$)

Step 3: Determine all extensions up to equivalence

For $f \in Z^2(G,N)$, $x,y,z \in G$, $xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0 \Rightarrow G = \{1, t\}$, $f(1,t) = f(t,1) = f(1,1) = 0$, $tf(t,t) - f(t,t) = 0$

$\therefore$ There are four possible factor sets we denote by $f_i(t,t) := \bar{i}$, $i = 0,1,2,3$

Case 3.1: $G \curvearrowright N$ trivially

$f \in B^2(G,N)$, $\exists\ h: G \to N$ s.t. $f(x,y) = xh(y) - h(xy) + h(x) \Rightarrow f(t,t) = h(t) + h(t) = 2h(t)$

$h: 1 \mapsto 0,\ t \mapsto \bar{0}$

So, $B^2(G,N) = \{f_0, f_2\}$, and thus $H^2(G,N) = \{\bar{f}_0, \bar{f}_1\}$

That is, $\exists$ two extensions E_{f_0}, E_{f_1}, so consider the following:

$0 \to N \to E_{f_0} \to G \to 1$

$(a,x)(b,y) = (a + xb + f_0(x,y), xy) = (a+b, xy)$

($a \in N$, $x \in G$, $b \in N$)

So, $E_{f_0} \cong N \times G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$0 \to N \to E_{f_1} \to G \to 1$

$(a,x)(b,y) = (a + xb + f_1(x,y), xy)$
$(b,y)(a,x) = (a + b + f_1(y,x), yx)$ $\Rightarrow E_{f_1}$ is abelian, so $(1,t)^2 = (3,1_G)$, $(1,t)^4 = (2,1_G)$, $(1,t)^8 = (0,1_G) \Rightarrow \mathrm{ord}((1,t)) = 8$ so $E_{f_1} \cong \mathbb{Z}/8\mathbb{Z}$

Case 3.2: Otherwise

We know $tf(t,t) = f(t,t) \Rightarrow 2f(t,t) = 0$, so $Z^2(G,N) = \{f_0, f_2\}$ and $B^2(G,N) = \{0\} \Rightarrow H^2(G,N) = \{f_0, f_2\}$

$0 \to N \to E_{f_0} \to G \to 1$

$(a,x)(b,y) = (a + xb + f_0(x,y), xy)$ ← in this case. If it's 0 then it's semidirect product

$r = (\bar{1}, 1_G)$, $s = (\bar{1}, t)$

Here, $E_{f_0} = \langle r, s \mid r^4 = (0,1_G),\ s^2 = (0,1_G),\ srs = s^{-1} \rangle \cong D_8$

Now, for E_{f_2}, we know $(a,x)(b,y) = (a + xb + 2, xy)$, $w = (1,1_G)$, $v = (1,t)$

$\therefore E_{f_2} = \langle w, v \mid w^4 = (0,1_G),\ w^2 = v^2,\ vwv^{-1} = w^{-1} \rangle \cong Q_8$

REMARK

If $|E| = 8$ and $\nexists\ a \in E$ with $\mathrm{ord}(a) = 4$, then $\mathrm{ord}(a) = 2\ \forall a \Rightarrow E \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

HOMOLOGY, NOT COHOMOLOGY

DEFINITION

$IG = \ker \varepsilon = \{\sum a_g g \in \mathbb{Z}[G] \mid \sum a_g = 0\} \Rightarrow \mathbb{Z}[G]/IG \cong \mathbb{Z}$ via $\mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$

- $IG = \langle g - 1 \mid g \neq 1 \in G \rangle_{\mathbb{Z}}$: $\sum a_g g \in \ker \varepsilon = IG \Leftrightarrow \sum a_g = 0 \Leftrightarrow \sum a_g g = \sum a_g g - \sum a_g = \sum a_g (g-1) \in \langle g-1 \mid g \in G \rangle_{\mathbb{Z}}$
- $0 \to IG \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ ($\leadsto - \otimes_{\mathbb{Z}[G]} \mathbb{Z}$)

  free $\Rightarrow$ flat, middle of short exact sequences are always free

  $\Rightarrow \mathrm{Tor}_1(\mathbb{Z}[G], \mathbb{Z}) \to \mathrm{Tor}_1(\mathbb{Z}, \mathbb{Z}) \to IG \otimes_{\mathbb{Z}[G]} \mathbb{Z} \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} \mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z} \to 0$

  ($IG \otimes_{\mathbb{Z}[G]} \mathbb{Z} = H_1$)

  $\sum a_g g \otimes n = 1 \otimes (\sum a_g g) n = 1 \otimes \sum a_g n$ (! over $\mathbb{Z}[G]$) ||| so this is an identity map

  $1 \otimes \mathbb{Z}$, "$\sum a_g g \otimes n$" $\mapsto \sum a_g \otimes n = 1 \otimes \sum a_g n$
- Define $H_1(G,N) = \mathrm{Tor}_1(\mathbb{Z}, N)$

In this case, $H_1(G,\mathbb{Z}) \cong IG \otimes_{\mathbb{Z}[G]} \mathbb{Z} \cong IG \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]/IG \cong IG/(IG)^2$ ($R/I \otimes M \cong M/IM$)

- $G/[G,G] \cong IG/(IG)^2$: $\exists$ group homo (by univ prop of $\mathbb{Z}$-modules) $\psi: IG \to G/[G,G]$, $g - 1 \mapsto \bar{g}$

  ($\bar{\psi}: IG/(IG)^2 \to G/[G,G]$, $\overline{g-1} \mapsto \bar{g}$)

Claim: $(IG)^2 \subseteq \ker \psi$

Proof

$u = (\sum m_i (x_i - 1))(\sum n_j (y_j - 1)) = \sum m_i n_j (x_i - 1)(y_j - 1) = \sum m_i y_j (x_i y_j - 1) - (x_i - 1) - (y_j - 1))$

$\therefore \psi(u) = \prod_{i,j} (x_i y_j x_i^{-1} y_j^{-1})^{m_i n_j} = 0$

Now, we find the inverse.

$\varphi: G \longrightarrow IG/(IG)^2$

$g \longmapsto (g-1)+(IG)^2$

$\Rightarrow \varphi$ is a group homo: $\varphi(g_1g_2) = (g_1g_2-1)+(IG)^2 = \underbrace{(g_1-1)(g_2-1)}_{\in (IG)^2} + (g_1-1)+(g_2-1)+(IG)^2 = \overline{g_1-1}+\overline{g_2-1} = \varphi(g_1)+\varphi(g_2)$

$\because G/\ker\varphi \hookrightarrow \underbrace{IG/(IG)^2}_{\text{abelian}}$ $\therefore [G,G] \subseteq \ker\varphi$, i.e. $\exists\ G/[G,G] \longrightarrow IG/(IG)^2$

$\bar{g} \longmapsto \overline{g-1}$

We call this $G/[G,G] \xrightarrow{\simeq} \underbrace{IG/(IG)^2}_{H_1(G,\mathbb{Z})}$ the abelianization of G

EXAMPLE

G is abelian, $H_1(G,\mathbb{Z}) = G$. Now if G is NOT abelian, we can still do abelianization. For example, for $n \geq 2$, $H_1(S_n,\mathbb{Z}) \cong S_n/(S_n,S_n) \cong S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ ($[S_n,S_n]=1$ for abelian)

12-6-24 (WEEK 14)

INDUCED REPRESENTATIONS

RECALL

(1) $\{V: \text{a } \mathbb{C}[G]\text{-module}\} \longleftrightarrow \{\rho: G \to GL(V)\}$

(2) $\{W \subset V: \mathbb{C}[G]\text{-module}\} \longleftrightarrow \{W \subset V: G\text{-invariant representation}\}$

(3) V is a simple $\mathbb{C}[G]$-module $\Leftrightarrow \rho$ is irreducible (simple: its only submodules are 0 and V)

(4) ρ and ρ' are isomorphic $\Leftrightarrow V \cong V'$ (isom as a $\mathbb{C}[G]$-module)

REMARK

$\mathbb{C}[G]$ can be regarded as a $\mathbb{C}[G]$-module $\Rightarrow$ associates with a regular representation of G

↳ We know that by seeing $\mathbb{C}[G]$ as $\bigoplus_{g \in G} \mathbb{C}e_g$

↳ $\exists$ $\mathbb{C}[G]$-module isom $\mathbb{C}[G] \cong W_1 \oplus \dots \oplus W_k$ where $W_1, \dots, W_k$ are simple $\Rightarrow \mathbb{C}[G]$ is said to be semi-simple

GOAL

To obtain a representation of G from the representation of its subgroups

NOTE

It may not be possible to extend a representation ψ of $H \leq G$ to a representation ρ of G in a way s.t. $\rho|_H = \psi$

Example: $\psi: A_3 \to \mathbb{C}^*$, however, when we extend to S_3, $\forall \tau: S_3 \to \mathbb{C}^*$ abelian $\Rightarrow [S_3, S_3] \leq \ker \tau \Rightarrow A_3 \leq \ker \tau$

$1 \mapsto 1$

$(123) \mapsto \omega$

$(132) \mapsto \omega^2$

Thus, $(12)3) \mapsto 1$, so we cannot extend ψ to τ ↛

DEFINITION

Let $H \leq G$ and V be a $\mathbb{C}[H]$-module via $\psi: H \to GL(V)$. The $\mathbb{C}[G]$-module $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ is called the induced module denoted by $\mathrm{Ind}_H^G(V)$.

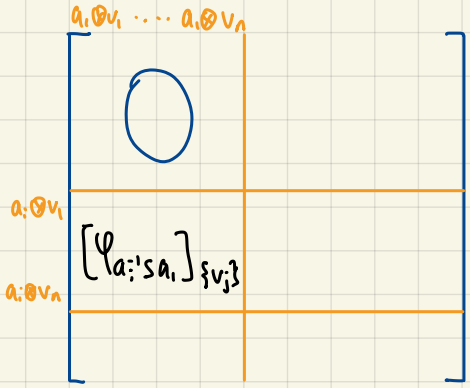
($\mathbb{C}[G]$, $\mathbb{C}[H]$ bimodule, since $\mathbb{C}[H] \hookrightarrow \mathbb{C}[G]$)

Then, $\rho: G \to GL(\mathrm{Ind}_H^G(V))$ is called the induced representation and χ_ρ is called the induced character, denoted by $\mathrm{Ind}_H^G(\chi_\psi)$

MISSION

To understand $\mathrm{Ind}_H^G(V)$, we need:

- $\{a_1H, \dots, a_mH\}$: the set of distinct left cosets of H in G, where $m = [G:H]$
  $\dim V = n \Rightarrow$ associated with a basis for V
- As a $\mathbb{C}$-vector space, $\mathbb{C}[G] = \mathbb{C}[\bigcup_{i=1}^m a_iH] = a_1\mathbb{C}[H] \oplus \dots \oplus a_m\mathbb{C}[H]$, as a free right $\mathbb{C}[H]$-module
  Now, consider $\mathbb{C}[H] \otimes \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V = a_1\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V \oplus \dots \oplus a_m\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V = (a_1 \otimes V) \oplus \dots \oplus (a_m \otimes V) \Rightarrow$ right $\mathbb{C}[H]$-module structure is absorbed by left $\mathbb{C}[H]$-module structure
  In other words, $\dim W = nm$
- $\{a_i \otimes v_j\}_{i=1,\dots,m;\ v=1,\dots,n}$ forms a basis for W in $\mathbb{C}$, where we arrange the order like $\{\underbrace{a_1 \otimes v_1}_{e_1}, \dots, \underbrace{a_1 \otimes v_n}_{e_n}, \dots, a_m \otimes v_1, \dots, a_m \otimes v_n\}$
- For $s \in G$, $\rho_s(a_i \otimes v_j) = sa_i \otimes v_j$. Notice, $sa_i \in G = \bigcup_{i=1}^m a_iH$, so say $s = a_ih$, so $\rho_s(a_i \otimes v_j) = a_ih \otimes v_j = a_i \otimes hv_j = a_i \otimes \psi_h(v_j)$
  $\therefore$ We know the representation looks like so: (Since $h = a_i^{-1}sa_i$, thus it equals $a_i \otimes \psi_{a_i^{-1}sa_i}(v_j)$)



IN GENERAL

$$[\beta_s]_{\{e_i\}} = \begin{pmatrix} [\psi_{a_i^{-1}sa_i}]_{n\times n} & & \\ \vdots & & \\ [\psi_{a_i^{-1}sa_1}]_{n\times n} & \cdots & [\psi_{a_i^{-1}sa_j}]_{n\times n} \cdots \\ \vdots & & \\ [\psi_{a_m^{-1}sa_1}]_{n\times n} & & \end{pmatrix}$$

, where we denote $\psi_{a_i^{-1}sa_j} := 0 \ \forall a_i^{-1}sa_j \notin H$

- Character: $\mathrm{Ind}_H^G(\chi_\psi)(s) = \sum_{i=1}^m \chi_\psi(a_i^{-1}sa_i)$ where $\chi_\psi(a_i^{-1}sa_i) := 0$ if $a_i^{-1}sa_i \notin H$

OBSERVE $G = a_1H \cup \dots \cup a_mH$, $\forall a \in G$, $h \in H$, say $h = a_i h$, $a^{-1}sa = h^{-1}(a_i^{-1}sa_i)h$. As χ_ψ is a class function, $\chi_\psi(a^{-1}sa) = \chi_\psi(a_i^{-1}sa_i)$

Hence, $\mathrm{Ind}_H^G(\chi_\psi)(s) = \frac{1}{|H|}\sum_{a\in G}\chi_\psi(a^{-1}sa)$, which is what we call the **reciprocity formula**

↳ Since $a \in a_iH$, counting a once counts a_i $|H|$ times

EXAMPLES

1. If s is not conjugate to some element of H in G, then $\mathrm{Ind}_H^G(\chi_\psi)(s) = 0$
   In particular, if $H \trianglelefteq G$, then $\mathrm{Ind}_H^G(\chi_\psi)|_{G\setminus H} = 0$
2. For $G = D_{12} = \langle r, s \mid r^6 = 1, s^2 = 1, srs^{-1} = r^{-1}\rangle$, we pick a subset to form $H = \{1, s, r^3, \underbrace{sr^3}_{r^3s}\} \cong V_4$ hence $G = H \cup rH \cup r^2H$

   We get $\psi: H \longrightarrow GL_2(\mathbb{C})$
   $1 \longmapsto \begin{pmatrix}1 & \\ & 1\end{pmatrix}$
   $s \longmapsto \begin{pmatrix}-1 & \\ & 1\end{pmatrix} = A$
   $r^3 \longmapsto \begin{pmatrix}1 & \\ & -1\end{pmatrix} = B$
   $sr^3 \longmapsto \begin{pmatrix}-1 & \\ & -1\end{pmatrix} = C$

   Thus, $\dim = 2(3) = 6$, where $e_1 = 1\otimes v_1$, $e_2 = 1\otimes v_2$, $e_3 = r\otimes v_1$, $e_4 = r\otimes v_2$, $e_5 = r^2\otimes v_1$, $e_6 = r^2\otimes v_2$

   $$[\rho_r]_{\{e_i\}} = \left(\begin{array}{c|c|c} 0 & 0 & B \\ \hline I_2 & 0 & 0 \\ \hline 0 & I_2 & 0 \end{array}\right)$$

   $\rho_r(1\otimes v_i) = r\otimes v_i$
   $\rho_r(r\otimes v_i) = r^2\otimes v_i$
   $\rho_r(r^2\otimes v_i) = r^3\otimes v_i$, associated with B, notice $r^3 \neq 1$!!

   ↖ first row cuz $1 = r^0$ is the RHS of $\otimes$

   Now, $[\rho_s]_{\{e_i\}} = \left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline 0 & 0 & C \\ \hline 0 & C & 0 \end{array}\right)$

   $\rho_s(1\otimes v_i) = s\otimes v_i = 1\otimes sv_i \Rightarrow$ associated with A
   $\rho_s(r\otimes v_i) = sr\otimes v_i$. Notice, $sr = r^{-1}s = \underline{r^2(r^3s)}$, so $\rho_s(r\otimes v_i) = r^2\otimes \underbrace{(r^3s)}_{=sr^3}v_i \Rightarrow$ associated with C
   $\rho_s(r^2\otimes v_i) = sr^2\otimes v_i = r\otimes \underline{(r^3s)}\,v_i \Rightarrow$ associated with C

   ↖ last row cuz r^2 is the LHS of $\otimes$

PROPOSITION (Considering Ind_H^G as an operator)

($\mathrm{Ind}_H^G(\chi_\psi)(s) = \frac{1}{|H|}\sum_{a\in G}\chi_\psi(a^{-1}sa)$)

(1) $\mathrm{Ind}_H^G(\chi_\psi + \chi_{\psi'}) = \mathrm{Ind}_H^G(\chi_\psi) + \mathrm{Ind}_H^G(\chi_{\psi'})$ by the reciprocity formula $\Rightarrow$ It is additive

(2) **Transitivity**: If $H \le K \le G$, $\psi: H \to GL(V)$, then $\mathbb{C}[G]\otimes_{\mathbb{C}[K]}(\mathbb{C}[K]\otimes_{\mathbb{C}[H]}V) \cong \mathbb{C}[G]\otimes_{\mathbb{C}[H]}V$

We deduce: $\begin{cases} \mathrm{Ind}_K^G(\mathrm{Ind}_H^K(V)) \cong \mathrm{Ind}_H^G(V) \\ \mathrm{Ind}_K^G(\mathrm{Ind}_H^K(\chi_\psi)) = \mathrm{Ind}_H^G(\chi_\psi) \end{cases}$: $LHS(s) = \frac{1}{|K|}\sum_{a\in G}\mathrm{Ind}_H^K(\chi_\psi)(as^{-1}a) = \frac{1}{|K|}\frac{1}{|H|}\sum_{a\in G}\sum_{c\in K}\chi_\psi(cab)^{-1}s(cab)$

$= \frac{1}{|H|}\frac{1}{|K|}\sum_{b\in K}\sum_{c\in G}\chi_\psi(c^{-1}sc) = RHS(s)$ ✓

↳ ab is like $c \in G$ since b is fixed

(3) **FROBENIUS RECIPROCITY** If $g \in \mathcal{C}(H)$, $h \in \mathcal{C}(G)$, then $\langle g, \mathrm{Res}\, f\rangle_{\mathcal{C}(H)} = \langle \mathrm{Ind}\, g, f\rangle_{\mathcal{C}(G)}$

where $\mathcal{C}(G) \ni f$ (Ind ↑, Res ↓) $g \in \mathcal{C}(H) \ni f|_H$

$\mathrm{Ind}(g)(s) = \frac{1}{|H|}\sum_{a\in G, as^{-1}a\in H} g(a^{-1}sa)$

Proof

Claim: If $\begin{cases}\rho: G \to GL(W) \\ \rho': G \to GL(W')\end{cases}$, then $\langle \chi_\rho, \chi_{\rho'}\rangle = \dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}[G]}(W, W')$

Proof

Write $\begin{cases}\rho = \rho_1^{\oplus m_1}\oplus\dots\oplus\rho_k^{\oplus m_k} \\ \rho' = \rho_1^{\oplus m_1'}\oplus\dots\oplus\rho_k^{\oplus m_k'}\end{cases} m_i \ge 0 \iff \begin{cases} W \cong W_1^{\oplus m_1}\oplus\dots\oplus W_k^{\oplus m_k} \\ W' \cong W_1^{\oplus m_1'}\oplus\dots\oplus W_k^{\oplus m_k'}\end{cases} \iff \begin{cases}\chi_\rho = m_1\chi_1 + \dots + m_k\chi_k \\ \chi_{\rho'} = m_1'\chi_1 + \dots + m_k'\chi_k\end{cases}$

Now, the **orthogonality** of $\{\chi_i\}$ implies that $\langle \chi_\rho, \chi_{\rho'}\rangle = \sum_{i,j} m_i m_j' \langle \chi_i, \chi_j\rangle = \sum_{i=1}^k m_i m_i'$

Schur's lemma implies that $\mathrm{Hom}_{\mathbb{C}[G]}(W, W') \cong \bigoplus_{i,j}\mathrm{Hom}_{\mathbb{C}[G]}(W_i, W_j)^{\oplus m_i m_j'}$, where $\mathrm{Hom}_{\mathbb{C}[G]}(W_i, W_j) = \begin{cases} 0 & i \neq j \\ \mathbb{C}\cdot 1_{\mathbb{C}[G]} \cong \mathbb{C} & i = j\end{cases}$

↳ $\dim_{\mathbb{C}} LHS = \sum_{i=1}^k m_i m_i'$ ✓

Now, back to original proof:

let $\mathcal{C}(G) = \langle \chi_{\rho_1}, \dots, \chi_{\rho_k}\rangle_{\mathbb{C}}$, $\mathcal{C}(H) = \langle \chi_{\psi_1}, \dots, \chi_{\psi_\ell}\rangle_{\mathbb{C}}$. By (1), we can assume that $g = \chi_\psi$, $\psi: H \to GL(V)$: irr
$f = \chi_\rho$, $\rho: G \to GL(V)$: irr

Should be $\mathbb{C}[G]$ from above, but the only domain here is $\mathbb{C}[H]$, so it applies

Thus, $\langle \chi_\psi, \mathrm{Res}\,\chi_\rho \rangle = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[H]}(V, W)$

$\langle \mathrm{Ind}\,\chi_\psi, \chi_\rho \rangle = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V, W) = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[H]}(V, W)$

$\cong \mathrm{Hom}_{\mathbb{C}[H]}(V, \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], W))$

W

Hence, it is proved. □

12-11-24 (WEEK 15)

MOCKEY'S CRITERION

EXAMPLES

1. $G=S_3$, $H=C_2=\langle(12)\rangle$, $\varphi: H \longrightarrow \mathbb{C}^*$ ($GL_2(\mathbb{C}) \curvearrowright V \supset \langle 1\rangle_{\mathbb{C}}$), $[G:H]=3$, $|G|=1^2+1^2+2^2$

$1 \longmapsto 1$

$(12) \longmapsto -1$

$G = H \cup (123)H \cup (132)H$

$W = \mathrm{Ind}_{H=1}^{G}(V) = \langle id\otimes 1, (123)\otimes 1, (132)\otimes 1\rangle_{\mathbb{C}}$ associates a ρ.

χ_ρ: $id \longmapsto \begin{pmatrix}1&0\\0&1\end{pmatrix} \rightsquigarrow 3$

$(12) \longmapsto \begin{pmatrix}-1&0\\0&-1\end{pmatrix} \rightsquigarrow -1$

$(12)(id\otimes 1) = id\otimes(12)1 = id\otimes(-1) = -(id\otimes 1)$

$(12)((123)\otimes 1) = (132)(12)\otimes 1 = (132)(id\otimes(12)1) = -(132)(id\otimes 1)$

$(132) \longmapsto \begin{pmatrix}\omega&0\\0&\omega^2\end{pmatrix} \rightsquigarrow 0$

So, $\chi_{\rho_1}: G \longrightarrow \mathbb{C}^*$, $\chi_{\rho_2}: G \longrightarrow \mathbb{C}^* \Rightarrow \chi_\rho = \chi_{\rho_1} + \chi_{\rho_2}$, $\rho \cong \rho_1 \oplus \rho_2$

	1	(12)	(123)
$1 \longmapsto$	1	-1	1
χ_{ρ_2}	2	0	-1

2) $G=Q_8$, $H=\langle i\rangle \cong \mathbb{Z}/4\mathbb{Z}$, $H \lhd G$, $\varphi: H \longrightarrow \mathbb{C}^*$, $i \longmapsto \sqrt{-1}$

Representatives: We know $G = Hj \cup H = \langle 1\otimes 1, j\otimes 1\rangle$ associates a ρ

Character Table:

	1	-1	$\{i,-i\}$	$\{j,-j\}$	$\{k,-k\}$
χ_ρ	2	-2	0	0	0
	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$	$\begin{pmatrix}\sqrt{-1}&0\\0&-\sqrt{-1}\end{pmatrix}$	$\begin{pmatrix}0&-1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&-\sqrt{-1}\\-\sqrt{-1}&0\end{pmatrix}$

$i(1\otimes 1) = i\otimes 1 = 1\otimes i1 = \sqrt{-1}(1\otimes 1)$

$i(j\otimes 1) = -j(i\otimes 1) = -j(1\otimes i(1)) = -\sqrt{-1}(j\otimes 1)$

$k(1\otimes 1) = -j(i\otimes 1)$, $k(j\otimes 1) = -i(1\otimes 1)$

$j(1\otimes 1) = j\otimes 1$ $j(j\otimes 1) = -1(1\otimes 1)$

$\therefore$ Inner product $= 1$ $\therefore$ It is irreducible

DEFINITION

Given $K, H \leq G$, the (K,H) double cosets of G are $\{KaH \mid a\in G\}$

↳ If $\exists c \in KaH \cap KbH$, say $c = k_1ah_1 = k_2bh_2$, then $a = k_1^{-1}k_2bh_2h_1^{-1} \Rightarrow KaH \subseteq KbH$, by symmetry, $KbH \subseteq KaH$ too, so $KaH = KbH$

↳ We can find a subset $S \subseteq G$, s.t. $\{KaH \mid a\in S\}$ is the set of distinct double cosets of G and $G = \dot{\bigcup}_{a\in S} KaH$ ($\bigsqcup_{a\in S} KaH$)

↳ Determine $|KaH|$: Let $b, b' \in Ka$, say $b = ka$, $b' = k'a$, then $bH = b'H \Leftrightarrow b^{-1}b' = a^{-1}k'a \in H \Leftrightarrow k^{-1}k' \in aHa^{-1} \cap K$

$\therefore$ There are a total of $[K : aHa^{-1}\cap K]$ left cosets of H in KaH, i.e. $|KaH| = |H|[K:(aHa^{-1})\cap K]$

Define $H_a = (aHa^{-1}) \cap K$

PROPOSITION

Let $\varphi: H \to GL(V)$ and $W = \mathbb{C}[G]\otimes_{\mathbb{C}[H]} V$, then $\mathrm{Res}_K \mathrm{Ind}_H^G(V) \cong \bigoplus_{a\in S} \mathrm{Ind}_{H_a}^K(V_a)$ where $\varphi_a: H_a \longrightarrow GL(V)$ ← We say V here as V_a

($a^{-1}sa \in H \Rightarrow s \longmapsto \varphi(a^{-1}sa)$)

Proof

$W = \mathbb{C}[G]\otimes_{\mathbb{C}[H]} V = \mathbb{C}[\bigsqcup_{a\in S} KaH] \otimes_{\mathbb{C}[H]} V = (\bigoplus_{a\in S} \underbrace{\mathbb{C}[KaH]) \otimes_{\mathbb{C}[H]} V}_{W(a)}$

(Not a ring, $(k_1ah_1)(k_2ah_2) \notin KaH$)

Claim: $W(a) \cong \mathbb{C}[K]\otimes_{\mathbb{C}[H_a]} V_a$ ($\mathbb{C}[K]$-module isom)

Proof

- $a\otimes V$ is a $\mathbb{C}[H_a]$-module: $\forall r \in H_a$, say $r = aha^{-1} \in K$, $\forall v\in V$, $r(a\otimes v) = ra\otimes v = ah\otimes v = a\otimes hv = a\otimes v'$, $v'\in V \Rightarrow r(a\otimes V) = a\otimes V$ ($ra = ah$)
- $V_a \cong a\otimes V$: $V_a \longrightarrow a\otimes V$, $\forall r \in H_a$, say $r = aha^{-1} \in K$, $\varphi_a(r)v = \varphi(a^{-1}ra)v = \varphi(h)v$, notice also $r(a\otimes v) = a\otimes hv$

($\mathbb{C}[H_a]$-module isom) $v \longmapsto a\otimes v$

$r \overset{h}{\longmapsto} r(a\otimes v) = a\otimes hv$

- $\mathbb{C}[KaH]\otimes_{\mathbb{C}[H]} V = \mathbb{C}[K]a\otimes V = \mathbb{C}[K]\otimes_{\mathbb{C}[H_a]} V_a = \mathrm{Ind}_{H_a}^{K}(V_a)$ ($H_a \le K$)

MOCKEY'S CRITERION

Consider the case of $K=H$ and $H_a=(aHa^{-1})\cap H$, $\varphi: H\to GL(V)$, $\varphi_a: H_a \longrightarrow GL(V)$, $aha^{-1}\longmapsto \varphi(h)$

Then, $W=\mathrm{Ind}_H^G(V)$ is irreducible $\Leftrightarrow$ (1) φ is irr

(2) $\forall a\in G\backslash H$, φ_a and $\mathrm{Res}_{H_a}(\varphi_a)$ are disjoint, i.e. $\langle \chi_{\varphi_a}, \chi_{\mathrm{Res}_{H_a}(\varphi)}\rangle = 0$

Proof

$\langle \mathrm{Ind}_H^G(\chi_\varphi), \mathrm{Ind}_H^G(\chi_\varphi)\rangle_{cG} \overset{\text{Frobenius}}{=} \langle \chi_\varphi, \mathrm{Res}_H \mathrm{Ind}_H^G(\chi_\varphi)\rangle = \langle \chi_\varphi, \sum_{a\in S} \mathrm{Ind}_{H_a}^H(\chi_{\varphi_a})\rangle = \sum_{a\in S}\langle \chi_\varphi, \mathrm{Ind}_{H_a}^H(\varphi_a)\rangle = \sum_{a\in S}\langle \mathrm{Res}_{H_a}\chi_\varphi, \chi_{\varphi_a}\rangle$

($H\backslash G/H$ ($KaH \Rightarrow$ rep. $K\backslash a/H$); $s\in H_a$, LHS $= \chi_\varphi(s)$, RHS $= \chi_\varphi(a^{-1}sa)$)

Now, W is irr $\Leftrightarrow$ LHS $=1 \Leftrightarrow \langle \chi_\varphi, \chi_\varphi\rangle = 1$, $\langle \mathrm{Res}_{H_a}\chi_\varphi, \chi_{\varphi_a}\rangle = 0$ $\forall a\neq 1$ □

COROLLARY

$H\lhd G$, $\varphi: H\longrightarrow GL(V)$, then W is irr $\Leftrightarrow$ φ is irr, $\varphi \not\cong \varphi_a$ $\forall a\neq 1$

Proof

$H\lhd G \Rightarrow \forall a\in G$, $H_a = H$. So, $\mathrm{Res}_{H_a} V = V$, i.e. (2) $\Leftrightarrow \varphi\not\cong\varphi_a$

EXAMPLES

1. $G=S_5$, $H=A_5$, $\chi_\varphi: A_5 \longrightarrow \mathbb{C}$ ($(12345)\longmapsto z_1$, $(12354)\longmapsto z_2$) $\Rightarrow \mathrm{Ind}_{A_5}^{S_5}\varphi$ is irr (for $a=(12)\notin A_5$, $\varphi_a((12345)) = \varphi((12354)) \neq \varphi((12345))$)

2. $G=SL_2(\mathbb{F}_p)$, $H=\{\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix} \mid a\in\mathbb{F}_p^\times, b\in\mathbb{F}_p\}$, $\omega: \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ group homo $\Rightarrow$ associates $\varphi: H\longrightarrow \mathbb{C}^\times$, $\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix}\longmapsto \omega(a)$

- $|GL_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$, $|SL_2(\mathbb{F}_p)| = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1)$, $|H| = p(p-1)$

  For $A\in H$, $|HAH| = |H| = p(p-1)$

  $A\notin H$, $|HAH| = |H|[H:(AHA^{-1})\cap H]$

  ↳ Have $A=\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0\end{pmatrix}$, $A^{-1} = \begin{pmatrix} d_0 & -b_0 \\ -c_0 & a_0\end{pmatrix}$ ($a_0^{-1}=d_0$), then $AHA^{-1} = \begin{pmatrix} a_0 & b_0 \\ c_0a_0 & b_0d_0\end{pmatrix}\begin{pmatrix} a & b \\ 0 & d\end{pmatrix}\begin{pmatrix} d_0 & -b_0 \\ -c_0 & a_0\end{pmatrix} = \begin{pmatrix} \star_1 & \star_2 \\ c_0da-c_0^2b-c_0d_0d & \star_3\end{pmatrix}$

  ($\star_1 = a_0d_0 - c_0(a_0b+b_0d) = d(a_0d_0-c_0b_0) = d$)

  If $c_0da - c_0^2b - c_0d_0d = 0$, then since $c_0\neq 0$, thus $d_0a - c_0b - d_0d = 0 \Rightarrow d_0(a-d) = c_0b \leftarrow b$ is determined by a and d

  $\therefore |(AHA^{-1})\cap H| = p-1$, thus $|HAH| = p^2(p-1)$

  However, $p(p-1) + p^2(p-1) = p(p-1)(1+p) \Rightarrow |S|=2$, so $S=\{\underset{=I}{\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}}, \underset{=S}{\begin{pmatrix} 1 & 0 \\ 0 & -1\end{pmatrix}}\}$

- $H_I = H$, $H_S = H\cap SHS^{-1} = \{\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix} \mid a\in\mathbb{F}_p^\times\}$

  $\begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix}\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix}\begin{pmatrix} -b & a \\ -a^{-1} & 0\end{pmatrix} = \begin{pmatrix} a^{-1} & 0 \\ -b & a\end{pmatrix}$

- $\mathrm{Res}_{H_S}\varphi: \begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}\mapsto \omega(a)$
- $\varphi_S: H_S\longrightarrow \mathbb{C}$, $\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}\mapsto \varphi(\begin{pmatrix} a^{-1} & 0 \\ 0 & a\end{pmatrix}) = \omega(a^{-1})$

$\mathrm{Ind}_H^G(\varphi)$ is irr $\Leftrightarrow \omega^2\neq 1$ ($\omega(a)\neq\omega(a^{-1})$)

12-13-24 (WEEK 15)

GOOD ENDING

Consider the representations of $G = A \rtimes H$, $A \trianglelefteq G$, A is abelian

RECALL

Any irr rep of abelian A is of degree 1, since $\rho: A \longrightarrow \underset{\parallel}{GL_1(\mathbb{C})} \overset{\mathbb{C}^\vee}{\underset{\parallel}{\mathbb{C}^*}} \Rightarrow \chi_\rho = \rho$

Let $\mathcal{X} = \mathrm{Hom}(A, \mathbb{C}^*)$ be the group ("+") of irr characters of A

Define $G \times \mathcal{X} \longrightarrow \mathcal{X}$
$(s, \chi) \longmapsto \chi_s : A \longrightarrow \mathbb{C}^*$, $a \longmapsto \chi(s^{-1}as)$

($\chi_s(ab) = \chi(s^{-1}abs) = \chi(s^{-1}as\, s^{-1}bs) = \chi_s(a)\chi_s(b) \Rightarrow$ group homo)

Note $\forall\, s = \overset{A}{b}\overset{H}{h}$, $\chi_s(a) = \chi(s^{-1}as) = \chi(h^{-1}\underline{b^{-1}abh}) = \chi(h^{-1}ah) = \chi_h(a) \Rightarrow H \times \mathcal{X} \longrightarrow \mathcal{X}$
($b^{-1}abh = a$)

Let $\{H\chi_1, \dots, H\chi_k\}$ be the set of distinct orbits in $\mathcal{X}$ under H and $|H\chi_i| = \frac{|H|}{|H_i|}$ where $H \supseteq H_i := \mathrm{stab}\,\chi_i = \{h \in H \mid \underline{h\chi_i = \chi_i}\}$ (i.e. $\chi_i(h^{-1}ah) = \chi_i(a)$)

Only care about a

Define $G_i = AH_i \leq G$ and $\tilde{\chi}_i(\underset{\in}{a}\overset{H_i}{h}) = \chi_i(a)$ ($\tilde{\chi}_i(gh)\tilde{\chi}_i(g'h') = \tilde{\chi}_i(aha'h^{-1}hh') = \chi_i(aha'h^{-1}) = \chi_i(a)\chi_i(ha'h^{-1}) = \chi_i(a)\chi_i(\overset{H_i}{h^{-1}}(a')) = \chi_i(aa')$)
$\Rightarrow \tilde{\chi}_i : G_i \longrightarrow \mathbb{C}^*$ is a character

Only care about h

Let $\rho : H_i \longrightarrow GL(V_i)$ be an irr rep $\Rightarrow \tilde{\rho} : G_i \longrightarrow GL(V_i)$, $ah \longmapsto \rho(h)$ ($\tilde{\rho}[(ah)(a'h')] = \tilde{\rho}[a(h'a'h^{-1})hh'] = \rho(hh') = \rho(h)\rho(h') = \tilde{\rho}(ah)\tilde{\rho}(a'h')$)

CLAIM

$\tilde{\rho}$ is also irr (Proof: If $\exists\, W_i \subsetneq V_i$ s.t. W_i is G_i-invar, then by def of $\tilde{\rho}$, W_i is H_i-invar $\nrightarrow$)

We can conclude that $\tilde{\chi}_i \otimes \tilde{\rho}$ is also an irr rep of G_i $\rightsquigarrow \tilde{\chi}_i \otimes \tilde{\rho} : G_i \longrightarrow GL(\mathbb{C} \otimes_{\mathbb{C}} V_i) = GL(V_i)$
↳ Irr because $\langle \tilde{\chi}_i \otimes \tilde{\rho}, \tilde{\chi}_i \otimes \tilde{\rho} \rangle = \frac{1}{|G_i|}\sum_{g \in G_i} \tilde{\chi}_i(g)\tilde{\rho}(g)\overline{\tilde{\chi}_i(g)}\,\overline{\tilde{\rho}(g)} = \frac{1}{|G_i|}\sum_{g \in G_i} \tilde{\chi}_i(g)\tilde{\chi}_i(g)^{-1}\tilde{\rho}(g)\tilde{\rho}(g)^{-1}$

DEFINITION

Define $\theta_{i,\rho} = \mathrm{Ind}_{G_i}^{G}(\tilde{\chi}_i \otimes \tilde{\rho})$

MAIN THEOREM

(a) $\theta_{i,\rho}$ is irr

Proof

By Mackey's criterion, it suffices to show that $\forall s \in G \setminus G_i$, $\langle (\tilde{\chi}_i \otimes \tilde{\rho}), \mathrm{Res}_{(G_i)_s}(\tilde{\chi}_i \otimes \tilde{\rho})\rangle_{(G_i)_s} = 0$ ($(G_i)_s = sG_is^{-1} \cap G_i$)

Claim: The restriction of these two rep for A are disjoint

Proof

$\forall\, a \in A$, $(\tilde{\chi}_i \otimes \tilde{\rho})_s(a) = \tilde{\chi}_i \otimes \tilde{\rho}(\underset{\in a}{sas^{-1}}) = \chi_i(sas^{-1}) \otimes \rho(1) = (\chi_i)_s(a) \otimes \rho(1)$
$\mathrm{Res}_{(G_i)_s}(\tilde{\chi}_i \otimes \tilde{\rho})(a) = \chi_i(a) \otimes \rho(1)$

Since $s \notin G_i$, $(\chi_i)_s \neq \chi_i \Rightarrow$ they are disjoint

(b) If $\theta_{i,\rho} \cong \theta_{i',\rho'}$, then $i = i'$ and $\rho \cong \rho'$

Proof

- $\mathrm{Res}_A\, \theta_{i,\rho}$ can be split into a sum of irr rep in $\mathcal{X} = \mathrm{Hom}(A, \mathbb{C}^*)$: $\mathrm{Ind}_{G_i}^{G}(\chi_i \otimes \tilde{\rho})(a) \overset{(\star)}{=} \frac{1}{|G_i|}\sum_{s \in G} \underset{\in}{\chi_i(s^{-1}as)}\,\chi_{\tilde{\rho}}(s^{-1}as)$ which only involves characters in the orbit $H\chi_i$ of χ_i; ($\overset{H_i}{h}$: $(\chi_i)_h(a) = \chi_i(a)$, $\chi_{\tilde{\rho}}(1) = \dim V_i$)
- Let $\theta_{i,\rho} : G \longrightarrow GL(W)$. Define $W_i := \{x \in W \mid \theta_{i,\rho}(a)x = \chi_i(a)x\ \ \forall a \in A\}$ (eigenvector)
  ↳ $\dim W_i = \dim V_i$: $\because h \in H_i$, $(\chi_i)_h = \chi_i$ $\therefore$ There are $|AH_i| = |G_i|$ elements in G which contributes $(\chi_i)_h(a)\chi_{\tilde{\rho}}(1) = \chi_i(a)\chi_{\tilde{\rho}}(1)$ in $(\star)$
  After multiplying $\frac{1}{|G_i|}$, $\exists$ exactly $\dim V_i$ irr. components isomorphic to χ_i, i.e. $\theta_{i,\rho}|_A \cong \chi_i^{\oplus \dim V_i} \oplus \dots$

By def, W_i is the rep space of $\chi_i^{\oplus \dim V_i} \Rightarrow \dim W_i = \dim V_i$

↪ W_i is stable under H_i, i.e. $\theta_{i,\rho}(h)\, x \in W_i$: $\theta_{i,\rho}(a)(\theta_{i,\rho}(h)x) = \theta_{i,\rho}(ah)x = \theta_{i,\rho}(h)\,\theta_{i,\rho}(h^{-1}ah)\,x = \theta_{i,\rho}(h)\,\chi_i(h^{-1}ah)\,x$ ($\chi_i(a)$)

$= \chi_i(a)(\theta_{i,\rho}(h)x)$

($h \in H_i$, $x \in W_i$)

- $\mathrm{Res}_{H_i}\theta_{i,\rho} : H_i \longrightarrow GL(W_i)$
  $\|$
  $\rho \quad : H_i \longrightarrow GL(V_i)$

Claim: If $\langle v_1, \dots, v_n\rangle_{\mathbb{C}} = V_i$, then $\langle 1 \otimes v_1, \dots, 1 \otimes v_n\rangle_{\mathbb{C}} = W_i$ ($\mathbb{C}G$)

Proof

Since $\theta_{i,\rho}(a)(i \otimes v_j) = a \otimes v_j = 1 \otimes av_j = 1 \otimes (a \cdot 1)v_j = 1 \otimes \chi_i(a)\rho(1)v_j = \chi_i(a)(1 \otimes v_j) \Rightarrow 1 \otimes v_j \in W_i\ \forall j$ ($a \in A$)

And "$1 \otimes v_1, \dots, 1 \otimes v_n$" are lin indep over $\mathbb{C}$" + "$\dim W_i = n$" $\Rightarrow \{1 \otimes v_1, \dots, 1 \otimes v_n\}$ is a basis for W_i

$\forall h \in H_i$, $\theta_{i,\rho}(h)(1 \otimes v_j) = h \otimes v_j = 1 \otimes hv_j = 1 \otimes \chi_i(1)\rho(h)v_j = 1 \otimes \rho(h)v_j$ via the isom $W_i \xrightarrow{\sim} W_i$, $\theta_{i,\rho}|_{H_i} \cong \rho$

$1 \otimes v_j \longmapsto v_j$

(c) Let $\sigma : G \to GL(U)$ be an irr rep of G. Then, $\sigma \cong \theta_{i,\rho}$

Proof

Write $\sigma|_A \cong \chi_1^{\oplus r_1} \oplus \dots \oplus \chi_m^{\oplus r_m}$ with $r_1, \dots, r_m \in \mathbb{Z}^{>0}$, $\chi_1, \dots, \chi_m \in X$ (distinct)

Then, $U \cong U_1 \oplus \dots \oplus U_m$, $\dim U_i = r_i$

($\mathbb{C}[A]$-module isom)

NOTE

$\forall a \in A, v_j \in U_j$, $\sigma(a)v_j = \chi_j(a)v_j$

$\forall s \in G$, $\sigma(a)\sigma(s)v_j = \sigma(s)\sigma(s^{-1}as)v_j = \sigma_s(\chi_j)(a)v_j = (\chi_j)_s(a)(\sigma(s)v_j) \Rightarrow \sigma(s) : U_j \to U_j$ ($= : \chi_{i,j}$)

$\therefore$ We conclude that if $\chi_i \in H\chi_i$ and thus $H\chi_i = H\chi_i$, we rename $H_i := \mathrm{stab}\,\chi_i$, $\chi_i := \chi_i$, then $\sigma(h)^{H_i} : U_i \to U$, i.e. $\sigma|_{H_i} : H_i \longrightarrow GL(U_i)$

Let $\bar{U}$ be an irr $\mathbb{C}(H_i)$-submodule of U_i and $\rho : H_i \to GL(\bar{U})$ be the corresponding rep of H_i

Now, consider $(\sigma|_{G_i})^{\bar{U}} : G_i \longrightarrow GL(\bar{U})$. Note, $\sigma(ah)v = \sigma(a)\sigma(h)v = \chi_i(a)\rho(h)v = (\tilde{\chi}_i \otimes \tilde{\rho})(ah)v$

($G_i = AH_i$; $a \in A$, $h \in H_i$, $v \in \bar{U}$; $\theta_{i,\rho}$)

$\therefore \mathrm{Res}_{G_i}\sigma$ contains $\tilde{\chi}_i \otimes \tilde{\rho}$ at least once, i.e. $1 \le \langle \mathrm{Res}_{G_i}\sigma, \tilde{\chi}_i \otimes \tilde{\rho}\rangle_{G_i} = \langle \sigma, \mathrm{Ind}_{G_i}^{G}\, \tilde{\chi}_i \otimes \tilde{\rho}\rangle_G \Rightarrow \sigma$ occurs at least once in $\theta_{i,\rho}$

$\because \sigma$ is irr $\therefore \sigma \cong \theta_{i,\rho}$