Algebra Lec 10. Structure theorem of finite abelian group.

Fundamental Theorem of finitely generated abelian group

Thm. G. fin gen. ab. group

i.e. G: abelian. $G = \langle \text{finite set} \rangle$

$$\Rightarrow G = \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

$$\text{s.t.} \left\{ \begin{array}{ll} r \geq 0 & n_j \geq 2 \\ n_{i+1} \mid n_i & i = 1, 2, \ldots, s-1 \end{array} \right\} \Rightarrow \text{unique. determined.}$$

意思是一个群有唯一的分解与之对应

Rmk. modules over PID ring.

→ Jordan form
→ rat. can. form.
→ FTFGAB

Not Today

Finite abelian Group $\Rightarrow$ finitely gen. for $G = \langle G \rangle$

G: abelian. $|G| < \infty$

$|G| = p_1^{n_1} \cdots p_j^{n_j}$ (p_i distinct primes)

$$\text{By Sylow } \exists \; G_1 \trianglelefteq G \quad |G_1| = p_1^{n_1}$$

abelian

$$\vdots$$

$$G_j \trianglelefteq G \quad |G_j| = p_j^{n_j}$$

- $G_i \cdot G_j$ commutes $(i \neq j)$ (for G abelian)
- $G_{i+1} \cap (G_1 \cdots G_i) = \{0\}$ (for p_i distinct).

$$G_1 \times G_2 \times \cdots \times G_j \simeq G_1 \cdots G_j \; (\text{or written as } G_1 + G_2 + \cdots + G_j)$$

$$= G$$

$\Rightarrow$ Reduce the task to describe the structure of finite abelian p-groups

- A finite abelian p-group G

  has type $(p^{r_1} p^{r_2} \cdots p^{r_s})$, $r_1 \geq r_2 \geq \cdots \geq r_s$

  if $G \simeq \mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \cdots \times \mathbb{Z}_{p^{r_s}}$

eg. $|G| = 2^5 \cdot 3^2 \cdot 5^3$

$\Rightarrow G \simeq G_1 \times G_2 \times G_3$

if we have. $2^2 2^2 2^1 \quad 3^1 3^1 \quad 5^2 5^1$

纵左对齐

$$\begin{array}{ccc} n_1 & n_2 & n_3 \\ \begin{bmatrix} 2^2 \\ 3^1 \\ 5^2 \end{bmatrix} & \begin{bmatrix} 2^2 \\ 3^1 \\ 5^1 \end{bmatrix} & \begin{bmatrix} 2^1 \end{bmatrix} \end{array}$$

Rmk. * . A: finite abelian. p-group $0 \neq b \in A$ (order of $b = p^{\#}$).

Let k be an integer ≥ 0. s.t. $p^k \cdot b \neq 0$.

这里指 p^k 个 b 相加.
(abelian group 中用"+"比较多)

p^m = order (period) of $p^k \cdot b$

$\Rightarrow$ (order of b) $= p^{k+m}$

证. $p^{k+m} b = 0$.

if $p^n \cdot b = 0 \Rightarrow n > k$

and $n \geq k+m$. (otherwise if $n < k+m$

order of $p^k \cdot b < p^m$)

$\Rightarrow$ $k+m$ is the smallest

Thm. Every finite abelian p-group is isomorphism to a product of cyclic p-group. If its type is $(p^{r_1} \cdots p^{r_s})$ $r_1 \geq r_2 \geq \cdots \geq r_s$.

then. $(r_1, r_2, \cdots, r_s)$ is uniquely determined.

$|G| = p^{\#} \Rightarrow G \cong \mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \cdots \times \mathbb{Z}_{p^{r_s}}$

<u>pf.</u> <u>induction</u>.

Let $a_1 \in A$ be an element of max order in A

Assume A is not cyclic. (otherwise. done).

$A_1 = \langle a_1 \rangle$. $|\langle a_1 \rangle| = p^{r_1}$

<u>Lemma</u>. $\bar{b} \in A/A_1$. order of $\bar{b}$ in A/A_1 is p^r

$\Rightarrow$ $\exists$ representative $\underset{A}{\overset{\cap}{a}}$ of $\bar{b}$, which also has order $= p^k$ (in A)

<u>pf of Lemma</u>.

$$\begin{array}{ccc} A & \longrightarrow & A/A_1 \\ \cup & & \\ b & \longmapsto & \bar{b} \end{array}$$

order of $\bar{b} = p^r$.

i.e. $p^r b \in A_1$

i.e. $p^r \cdot b = n a_1$ for some integer n.

then. $|\bar{b}| = p^r \leq |b|$

- if $n = 0$. $\Rightarrow |b| = p^r = |\bar{b}|$ done
- if $n \neq 0$, $n = p^k \cdot \mu$. $(p, \mu) = 1$

$\Rightarrow p^r b = p^k \mu a_1$

because of $(p, \mu)=1$. we have μa_1 is also the gen of A_1

order of μa_1 is p^{r_1} so may assume. $k < r_1$. (if not. $p^k \mu a_1 = 0$)

Rmk(*1). $\Rightarrow$ $p^k \mu a_1$ order is $p^{r_1 - k}$

Rmk(*2) $\Rightarrow$ b has order $p^{r + r_1 - k}$ but. $\boxed{r + r_1 - k \leq r_1}$ for r_1 is max order

$\Rightarrow r \leq k$.

$\Rightarrow p^r (b - p^{k-r} \mu a_1) = 0$ let. $b - p^{k-r} \mu a_1 = a$.

then we have. $p^r \cdot a = 0$

and $\bar{a} = \bar{b}$

now we only have (order of $a \leq p^r$)

if not eq $p^{\#} (b - p^{k-r} \underset{\substack{\cap \\ A_1}}{\mu a_1}) = 0$

$\Rightarrow |\bar{b}| < r$ $*$ $\square$

---

now. $\underline{\text{assume}}$ $A/A_1 \overset{f}{\cong} \bar{A}_2 \times \bar{A}_3 \times \cdots \times \bar{A}_s$ by induction

a product of cyclic groups

of order $p^{r_2}, \ldots, p^{r_s}$

$r_2 \geq r_3 \geq \cdots \geq r_s$

$$A/A_1 \xrightarrow[\sim]{f} \bar{A}_2 \times \cdots \times \bar{A}_s$$

$$\bar{a}_2 \longmapsto (1, 0, \ldots, 0) \qquad |\bar{a}_2| = p^{r_2}$$

$$\vdots \qquad\qquad\qquad \vdots$$

$$\bar{a}_s \longmapsto (0, 0, \ldots, 1) \qquad |\bar{a}_s| = p^{r_s}$$

use Lemma. $\exists\, a_2, \ldots, a_s$ is representative of $\bar{a}_i$ in A.

with the same order as $\bar{a}_i$

$$\langle a_i \rangle = A_i \leq A$$

Claim. A is direct product of $A_1, \ldots, A_s$

let $x \in A$.

$$\bar{x} = m_2 \bar{a}_2 + m_3 \bar{a}_3 + \cdots + m_s \bar{a}_s$$

$$\Rightarrow \quad x - m_2 a_2 - m_3 a_3 - \cdots - m_s a_s \in A_1$$

$$\exists\, m_1 \qquad x = m_1 a_1 + m_2 a_2 + \cdots + m_s a_s$$

$$\therefore \boxed{A = A_1 + A_2 + \cdots + A_s} \qquad (1)$$

Now. suppose $m_i < p^{r_i}$

$$0 = m_1 a_1 + m_2 a_2 + \cdots + m_s a_s$$

take bar

$$0 = m_2 \bar{a}_2 + \cdots + m_s \bar{a}_s$$

send to RHS by f

$$m_2 = m_3 = \cdots = m_s = 0$$

$\therefore m_1 = 0 \quad \Rightarrow \quad A_1 \cap (A_2 \cdots A_s) = \{0\}.$

同理. $\boxed{A_{i+1} \cap (A_1 A_2 \cdots A_i) = \{0\}}$ (2)

and. $\boxed{A_i \cdot A_j \text{ commutes}}$ (3)

$$\Rightarrow A \simeq A_1 \times A_2 \times \cdots \times A_s$$
$$\parallel$$
$$A_1 + A_2 + \cdots + A_s$$

$\square$ (存在性).

唯一性 $\quad (p^{r_1} \cdots p^{r_s}) \quad (p^{m_1} \cdots p^{m_k})$

then pA (every element add itself p times.)

is also abelian p-group

and $pA \leq A$

type of pA is $(p^{r_1-1} \cdots p^{r_s-1})$ or $(p^{m_1-1} \cdots p^{m_k-1})$

By induction $(r_1-1, \cdots, r_s-1)$ consisting of integer ≥ 1 are uniquely determined.

Then we may have the condition as

$$(p^{r_1} p^{r_2} \cdots p^{r_n} \overbrace{p \cdots p}^{\nu \text{ times}})$$

or $(p^{r_1} p^{r_2} \cdots p^{r_n} \overbrace{p \cdots p}^{\mu \text{ times}})$ using the order of $A \Rightarrow \nu = \mu$

$\blacksquare$

Eg. G. group $|G| = 8$

① abelian. $\mathbb{Z}_8$. $\mathbb{Z}_4 \times \mathbb{Z}_2$. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

② nonabelian. if all element's order is 2, then is abelian $\times$

$ab = ba$

we consider $aba^{-1}b^{-1}$

$= abab$

$= (ab)^2$

$= e$. ✓

if have one element's order is 8 $\Rightarrow \mathbb{Z}_8$ $\times$

then. $\exists x \in G$ $|x| = 4$.

$\langle x \rangle \trianglelefteq G$. $y \in G - \langle x \rangle$

why normal? use Lagrange.

$\therefore \langle x, y \rangle = G$

$\Rightarrow y \langle x \rangle y^{-1} = \langle x \rangle$

if $gH \neq H$ then $H \neq Hg$ and $Hg = gH$

then $yxy^{-1} = x$ or $yxy^{-1} = x^3$

$yxy^{-1} = x \Rightarrow$ commute $\Rightarrow$ abelian $\times$

$yxy^{-1} = x^3 \Rightarrow$

- $|y| = 2$: $yx = x^3 y = x^{-1} y$, $x^4 = 1$ — D_8
- $|y| = 4$: $yx = x^3 y$ — Q_8