Alg-20

01 April 2021 13:48

Alg-20

#4 p78 (a)

$t \in G_s$ — orbit of s

$G_s \subseteq S$

$\Rightarrow G_s = G_t$

Proof. $t \in G_s \Rightarrow t = gs$ for some $g \in G$

$G_t = G_{gs} = G_s$ as $G_g = G$ for $g \in G$.

Meeting on Friday, tomorrow at 1 pm.

Structure of finite abelian groups

Cyclic groups < finite / infinite

(1) Two cyclic groups of order n are iso $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

$W = \{z \in \mathbb{C} : z^N = 1\}$

$N > 1$ integer is a finite cyclic group

$= \{ e^{\frac{i2\pi k}{N}}, \ k = 0, 1, 2, \ldots, N-1 \}$

$= \langle e^{\frac{i2\pi}{N}} \rangle$

↑ generates

(2) A subgroup of a cyclic group is cyclic

(3) Homomorphic image of a cyclic group is cyclic.

However A & B are cyclic then $A \times B$ need not be cyclic

Ex $\mathbb{Z}_2 \times \mathbb{Z}_2$ is product of two cyclic groups, but $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

$2(a,b) = 0 \quad \forall (a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$

A is an abelian group

$n \in \mathbb{N}$ is an exponent of A iff $nx = 0 \quad \forall x \in A$.

Ex $\text{Exp}(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$

$m \in \mathbb{N}$, $f_m : A \to A$ defined by $f(a) = ma$. is a homo

...

$f_m(a) = ma$. is a homo

$\ker f_m \equiv A_m = \{a \in A : ma = f_m(a) = 0\}$

$\operatorname{Im} f_m = \{b \in A : b = f_m(a) \text{ for some } a \in A$
$= ma\}$

$= \{ma \in A : a \in A\}$

$= mA$

$A/A_m \cong mA$ abelian group

Def. $A_{tor} = \{a \in A : ma = 0 \text{ for some } m \in \mathbb{N}\}$

$|a| = m$ or $|a| \mid m$

Prop A_{tor} is a subgroup of A called the torsion subgroup.

Proof $a, b \in A_{tor} \Rightarrow ma = 0$
$nb = 0$
for some $m, n \in \mathbb{N}$

then $mn(a-b) = mna - mnb$
$= n(ma) - m(nb)$
$= 0 - 0$
$= 0$

$\Rightarrow a - b \in A_{tor}$

$\Rightarrow a-b \in A_{tor}$

Def. 1 If $A = A_{tor}$, we say that A is a torsion group

2. A is torsion free if $A_{tor} = \{0\}$

Ex 1. $\mathbb{Z} = A$ $\mathbb{Z}_{tor} = \{0\}$

So $\mathbb{Z}$ is torsion free

$A = \mathbb{Q}/\mathbb{Z}$ $(\mathbb{Q}/\mathbb{Z})_{tor} = A_{tor}$

$= \{\frac{p}{q} + \mathbb{Z} : \frac{p}{q} \in \mathbb{Q}\}$

$= \{\frac{m}{n} + \mathbb{Z} : n \neq 0\}$

$k\left(\frac{m}{n} + \mathbb{Z}\right) = 0_{\mathbb{Q}/\mathbb{Z}}$ the zero coset

$= \mathbb{Z}$

Take $k = n$, $n\left(\frac{m}{n} + \mathbb{Z}\right) = m + \mathbb{Z}$

$= \mathbb{Z}$, $m \in \mathbb{Z}$

$(\mathbb{Q}/\mathbb{Z})_t = \mathbb{Q}/\mathbb{Z}$., so $\mathbb{Q}/\mathbb{Z}$ is a torsion group

Def. A group G is called a p-group. p a prime, iff each $g \in G$, $|g| = p^r$ for some $r \geq 0$.

Def A is an abelian group $p \in \mathbb{N}$ is prime

$A(p) = \{a \in A : |a| = p^r$. for some $r \geq 0\}$

$A(p)$ is a subgroup of A & is called a p-primary subgp of A, $A(p) \leq A_{tor}$

Proof $b, a \in A(p)$, $|a| = p^r$

$|b| = p^s$

$p^{r+s}(a-b) = p^s(p^r a) - p^r(p^s a)$

$= 0 - 0 = 0$

$\Rightarrow |a-b| \mid p^{r+s}$

$$|a-b| = p^k, \quad 0 \le k \le r+s$$

If A is finite abelian then $A(p)$ is a p-group

$$|A(p)| = p^r \text{ for some } r \ge 0$$

Ex $A = \mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$

find $A(p)$, $p = 2, 3, 5, 7, 11$

$$A(2) = \{a \in \mathbb{Z}_{12} : 2^r a = 0 \text{ for } r \ge 0\}$$

$$= \{0, 6, 3, 9\} \quad |A(2)| = 2^2$$

$$A(3) = \{a \in \mathbb{Z}_{12} : 3^r a = 0 \text{ for } r \ge 0\}$$

$$= \{0, 4, \ldots, 8\}$$

$$|A(3)| = 3$$

$$A(p) = \{0\} \text{ for } p = 5, 7, 11$$

$A(p) = \{0\}$ for all p.

Thm A is an abelian group of exp n. Assume $n = mm'$, $(m, m') = 1$

Then $A = A_m \oplus A_{m'}$ where

$A_r = \{a \in A : ra = 0\}$

Proof. To show each $a \in A$

$\exists\ b \in A_m,\ c \in A_{m'}$

s.t. $\boxed{a = b + c}$ and

$A_m \cap A_{m'} = \{0\}$

$(m, m') = 1 \Rightarrow \exists\ x, y \in \mathbb{Z}$

s.t. $1 = xm + ym'$

$a = 1 \cdot a = (xm)a + ym'a$

$= b + c$, $b = ym'a$

$c = xma$

$b \in A_m$ as $mb = m(ym'a)$

$= y(mm'a)$

$= y(na)$

$= y0$

$= 0$

Similarly $m'c = m'(xma)$

$(m'm)a)$

summary $nc = m'(xma)$

$= x(m'ma)$

$= x(na)$

$= 0$

Suppose $b \in A_m \cap A_{m'}$

then $b = 1b = (xm + ym')b$

$= x(mb) + y(m'b)$

$= 0 + 0 = 0$

$\Rightarrow b = 0$

thus $A = A_m \oplus A_{m'}$

(2) Thm. A is abelian of exp n. $n = p_1^{r_1} \cdots p_k^{r_k}$

Then $A = \bigoplus_{i=1}^{k} A(p_i)$ where $p_1 \cdots p_k$ are distinct $r_i \geq 1$

(This theorem is called the primary decomposition Thm)

(3) A is finite abelian, $|A| = n$

$n = p_1^{r_1} \cdots p_k^{r_k}$ where $p_1 \cdots p_k$ are dist.

(3) A is finite abelian

$= p_1^{r_1} \cdots p_k^{r_k}$ $\quad p_1 \cdots p_k$ are distinct.

$r_i \geq 1, \; i = 1 \cdots k.$

$$A = \bigoplus_{i=1}^{k} A(p_i), \quad |A(p_i)| = p_i^{r_i}$$

Note $|A| = n$. & A is abelian

Then the p-primary part $A(p)$ of A is a p-group, $|A(p)| = p^r$

Finite abelian p-group. A is an abelian groups of order $|A| = p^r$ for some $r \geq 1$.

$\mathbb{Z}_p$, $\mathbb{Z}_{p^2}$ are p-group abelian

$\mathbb{Z}_{p^r}$ is a p-group

Thm 4. Every finite abelian

(i) p-group A is isomorphic to

$$A \simeq \coprod_{i=1}^{k} \mathbb{Z}_{p^{r_i}} \text{ where } r_1 \geq r_2 \geq \cdots \geq r_k \geq 1$$

$$\simeq \coprod_{i=1}^{\ell} \mathbb{Z}_{p^{m_i}} \qquad m_1 \geq \cdots \geq m_\ell \geq 1$$

(ii) If $A \simeq \prod_{j=1}^{\ell} \mathbb{Z}_{p^{m_j}}$, $m_1 \geq \cdots \geq m_\ell \geq 1$

then $\ell = k$ & $m_i = r_i$

We say A is of type $(p^{r_1}, \ldots p^{r_k})$

$r_1 \ldots r_k$ are called the invariants of A whose A is a finite p-group

---

1- $A = \mathbb{Z}_2 \times \mathbb{Z}_2$ is of type $(2,2)$

2- $A = \mathbb{Z}_p \times \mathbb{Z}_p$ is of type (p,p)

From $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$

if $(m,n) = 1$

Proof: Need Chinese remainded Thm. #5 P14 of Lang

$\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if $(m,n)=1$

$(m,n)=1$, Then the eqns $x = r \bmod m$, $x = s \bmod n$

$\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if $(m,n)=1$

Show a cool $k \in \mathbb{Z}$.

Proof $f : \mathbb{Z} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$

$= \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$f(k) = (k+m\mathbb{Z},\ k+n\mathbb{Z})$

Now f is a homo

$f(k+l) = (k+l+m\mathbb{Z},\ k+l+n\mathbb{Z})$

$= (k+m\mathbb{Z}+l+m\mathbb{Z},\ k+n\mathbb{Z}+l+n\mathbb{Z})$

def of $+$ in the coordin

$= (k+m\mathbb{Z}, k+m\mathbb{Z}) + (l+m\mathbb{Z}, l+n\mathbb{Z})$

$= f(k) + f(l)$

So f is a homo

Suppose $k \in \ker f \leq \mathbb{Z}$

$f(k) = 0_{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}}$.

$(k+m\mathbb{Z}, k+n\mathbb{Z}) = (m\mathbb{Z}, n\mathbb{Z})$

$k+m\mathbb{Z} = m\mathbb{Z}$, $k+n\mathbb{Z} = n\mathbb{Z}$

$k \in m\mathbb{Z}$, $k \in n\mathbb{Z}$.

$k \in m\mathbb{Z}$, $k =$

$k = mp$, $k = nq$

$m \mid k$ and $n \mid k$. , $(m,n) = 1$

$\Rightarrow mn \mid k$.

$1 = rm + ns$

$k = rmk + nsk$

$= kmnq + nsmp$

$= (kq + sp)mn$

$\Rightarrow mn \mid k$

$k \in mn\mathbb{Z}$.

$\ker f = mn\mathbb{Z}$.

$f(\mathbb{Z}) \overset{\text{onto}}{=} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$\subseteq$

Suppose $(x,y) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$x = r + m\mathbb{Z}$. $y = s + n\mathbb{Z}$.

To find k s.t. $f(k) = (x,y)$

$(k + m\mathbb{Z}, k + n\mathbb{Z}) = (r + m\mathbb{Z}, s + n\mathbb{Z})$

$k+m\mathbb{Z} = r+m\mathbb{Z}$, $k+n\mathbb{Z} = s+n\mathbb{Z}$

$k - r = 0 \bmod m$

$k = r \bmod m$
$k = s \bmod n$ }

To find k. Now $1 = pm + qn$ for some $p, q \in \mathbb{Z}$.

Take $k = pms + qnr$

To show $k = r \bmod m$.

$$k = pms + qnr$$
$$= pms + (1 - pm)r$$
$$= pms + r - pmr$$
$$k - r = pm(s - r)$$
$$= m(ps - pr)$$
$$k - r = 0 \bmod m$$
$$k = r \bmod m$$

$$k = (1 - qn)s + qnr$$
$$k - s = qn(r - s) = n(qr - qs)$$

$\Rightarrow k = s \bmod n$.

$(3,7)=1$, find sol of

$x = 4 \bmod 3$

$x = 6 \bmod 7$.

So $f(\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

By 1st iso thm

$$\mathbb{Z}/\ker f \simeq \mathrm{Im}\, f$$

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

or $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$

provided $(m,n)=1$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \not\simeq \mathbb{Z}_4 = \mathbb{Z}_2$$

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$$

Thm. A is a finite abelian p-group & $|A| = p^n$. Then these

(assemble)

& $|A| = p^n$. Then there are $p(n)$ distinct (not isomorphic) groups of the form $\prod_{i=1}^{k} \mathbb{Z}_{p^{r_i}}$

where $r_1 \geq \cdots \geq r_k \geq 1$

and $p(n) = \#$ of possibilities of n

$= r_1 + r_2 + \cdots + r_k$.

and $r_1 \geq r_2 \geq \cdots \geq r_k$.

$$|A| = p^n, \quad \left|\prod_{i=1}^{k} \mathbb{Z}_{p^{r_i}}\right| = \prod_{i=1}^{k} \left|\mathbb{Z}_{p^{r_i}}\right| = \prod_{i=1}^{k} p^{r_i} = p^{r_1 + \cdots + r_k}$$

$$n = r_1 + r_2 + \cdots + r_k.$$

Ex A is abelian group of order

$4 = 2^2$

$$A \cong \prod_{i=1}^{k} \mathbb{Z}_{2^{r_i}} \qquad r_1 \geq r_2 \geq \cdots \geq r_k \geq 1$$

& $r_1 + r_2 + \cdots + r_k = 2$.

$2 = 1+1$, 2

$2 = 1+1$, 2

Those two abelian groups of order 4. They are

$$A \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

or

$$\mathbb{Z}_4$$

2 Find all abelian groups A of order $16 = 2^4$

Here $p=2$, $n=4$ partitions of 4

$p(4) =$ # of partitions $(r_1 \cdots r_k)$

$r_1 \geq \cdots \geq r_k \geq 1$

and $r_1 + \cdots + r_k = 4$

$4 = 1+1+1+1$

$= 1+1+2$

$= 1+3$

4

and $2+2$

$$A \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_9^2$$

$\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2^2$

$\cong \mathbb{Z}_2^2 \times \mathbb{Z}_2^2$

$\cong \mathbb{Z}_2 \times \mathbb{Z}_2^3$

$\cong \mathbb{Z}_2^4$

Ex Find upto isomorphism all abelian groups of order (a) 12, (b) 15, (c) 30, (d) 72.

(a) $|A| = 12 = 2^2 \cdot 3$

$A = A(2) \oplus A(3)$, $|A(2)| = 2^2$, $|A(3)| = 3$

$A(3) = \mathbb{Z}_3$

$A(2) = \mathbb{Z}_2 \times \mathbb{Z}_2$

$\cong \mathbb{Z}_4$

$A \cong \mathbb{Z}_4 \times \mathbb{Z}_3$

$\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$

(b) $|A| = 15 = 3 \cdot 5$

$A \simeq A(3) \oplus A(5)$

$\mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$

(c) $|A| = 30 = 2 \cdot 3 \cdot 5$

$A \simeq A(2) \oplus A(3) \oplus A(5)$

$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

$\simeq \mathbb{Z}_6 \times \mathbb{Z}_5$

$\simeq \mathbb{Z}_{30}$

(d) $|A| = 72 = 2^3 \cdot 3^2$

$A = A(2) \oplus A(3)$

$|A(2)| = 2^3$, $|A(3)| = 3^2$

$2 = 1+1$

~ 2

$3 = 1+1+1$

$= 1+2$

$= 3$

$A(2) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

$\sim \mathbb{Z} \times \mathbb{Z}_2$ and $A(3) \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$

$\therefore \mathbb{Z}_2$

$\mathbb{Z}_2 \times \mathbb{Z}_2$ $\mathbb{Z}_3^2$

$\mathbb{Z}_2^3$

$A \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3^2$

$\mathbb{Z}_2 \times \mathbb{Z}_2^2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{Z}_2 \times \mathbb{Z}_2^2 \times \mathbb{Z}_3^2$

$\mathbb{Z}_2^3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{12}^2$

$\mathbb{Z}_2^3 \times \mathbb{Z}_3^2$