2.3 Cyclic Groups (page 57)

Thursday, October 12, 2023 11:00

Proposition 3:

Let G be a group $x \in G$

1) if $x^m = 1$ and $x^n = 1$ $m, n \in \mathbb{Z}$

Let $d = (m, n)$ then $x^d = 1$

2.) if $x^m = 1$ $\exists\, m \in \mathbb{Z}$

then $|x|$ divides m

Proposition 5:

Let G be a group $x \in G$

Let $a \in \mathbb{Z} - \{0\}$

if $|x| = \infty$ then $|x^a| = \infty$

if $x = n \in \mathbb{Z}^+$

then $x^a = \frac{n}{(n, a)}$

Think about what 5(2) says

in $\mathbb{Z}/6\mathbb{Z} = \langle \bar{1} \rangle$

What is the order of

$|3| = \frac{6}{\gcd(3,6)} = 2$

$|4| = \frac{6}{\gcd(6,4)} = 3$

$x^m \cdot x^n = 1$

$m = 2, \quad n = 1$

Proof

Let $d = \gcd(n, a)$

then $n = bd$

$a = cd$ for $a, b, c, d \in \mathbb{Z}$

$\Rightarrow b \in \mathbb{Z}^+$

by assumption $n \in \mathbb{Z}^+$

Since $n \in \mathbb{Z} - \{0\}$

$\Rightarrow c \neq 0$

$\gcd(b, c) = 1$

Let $k = |x^a|$

we need to show $k = \frac{n}{(n,a)} = b$

first $(x^a)^b = 1 \Rightarrow x^{ab} = x^{cb} = x^{nc}$

$= x^n = 1$

Since $b = \frac{n}{d}$ $\quad \therefore (x^n)^c = (1)^c = 1^c$

$a = cd$

$d = q_1 \cdot n + q_2 \cdot a$

$b = \frac{n}{q_1 \cdot n + q_2 \cdot a} = 1 = bs + ct$

So k ——— $\leq$ ——— b

k divides b

now it suffices to show

$b \mid k$

First consider $(x^a)^k = 1$

$x^{ak} = 1$

by 3(a)

n divides ak

$ak = nl$ for some $l \in \mathbb{Z}$

i.e.

$cdl = bdl$

so $ck = bl$

from $1 = |(x^c) = (x^b)|$

$\sqrt{}$

$x^a = (x^{sa+ta})$

$(x^a)^l = (x^{sal+tal}) = (x^b)^l$

Since $(b, c) = 1$

we have $1 = bs + ct$

$s, t \in \mathbb{Z}$

$k = bks + ctk = b(ks + tl)$

When are two cyclic groups isomorphic?

Any two cyclic groups are isomorphic iff the orders are the same

more specifically

if two cyclic groups by x and y are of order n

when the maps from $x^a \to y^a$

$\langle x \rangle \longrightarrow \langle y \rangle$

$x^k \longmapsto y^k$

is a well defined isomorphism

2.) if $\langle x \rangle$ is of infinite order

then $\ell : \mathbb{Z} \to \langle x \rangle$

$k \longmapsto x^k$

is a well defined isomorphism

When considering well-defined

Consider $x^a = x^b \quad a \neq b$

then $\ell(x^a) = \ell(x^b)$

$\Longrightarrow y^a = y^b$

for y is and x are of the order n

---

bijective

$\ell(x^a x^b) = \ell(x^a)\ell(x^b)$

and bijective isomorphism

$\ell(a+b) = \ell(a)\ell(b)$

Q66 What are the subgroups of a cyclic group?

List all of the distinct subgroups of $\mathbb{Z} = \langle 1 \rangle$

$\mathbb{Z} - \{x\} \quad x \in \mathbb{Z}$ | $\langle 0 \rangle$ $\quad 2\mathbb{Z} \hookrightarrow \langle 2 \rangle : 4$

List all the distinct subgroups of $\mathbb{Z}/6\mathbb{Z} = \langle T \rangle$

$\langle \bar{0} \rangle \quad \langle T \rangle = \langle \bar{5} \rangle$

$\| \qquad \|$

$\{\bar{0}\} \quad \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\langle \bar{2} \rangle = \langle \bar{4} \rangle \quad \langle \bar{3} \rangle$

$\{\bar{0}, \bar{2}, \bar{4}\} \quad \{\bar{0}, \bar{3}\}$

Theorem 7 Let $H = \langle x \rangle$

all subgroups of H are cyclic

if $K \leq H$

then either $K = \{\}$

or $K = \langle x^d \rangle$

where d is the smallest positive integer such that $x^d \in K$

$x \in K$

Suppose $|x| = \infty$ then for any two distinct nonnegative integers a and b

$\langle x^a \rangle \neq \langle x^b \rangle$ more over $\forall n \in \mathbb{Z}$

$\langle x^n \rangle = \langle x^{|n|} \rangle$

So the subgroups of H are bijective correspondence with non-negitive integers

3) Suppose $|x| = n \in \mathbb{Z}^+$

then for each positive integer a divides n

there exists a unique subgroup of H for order a

this group is $\langle x^d \rangle$,

where $d = \frac{n}{a}$

for any $m \in \mathbb{Z}$

$$\langle x^m \rangle = \langle x^{\gcd(n,m)} \rangle$$

Thus the groups of H

with positive distance of n.

Order

Let $K \leq (\mathbb{Z}, +)$

then either $K = \{0\}$

or K contains some

$a \neq \mathbb{Z} - \{0\}$

then K contains a

So K contains at least one positive integer

Let d be the smallest positive integer in K

$K = \langle d \rangle$

$\supseteq$ because K is a subgroup

$\subseteq$ if $a \in K$

$a = qd + r$

$1 \leq r \leq d-1$

$\Rightarrow$

$r = a - qd$

2.4 Subgroups generated by subsets of a group

Let G be a group and A be a subset of G.

Q What is the smallest subgroup of G containing A

all finite products of elements in A and their inverses

for $a, b \in A$

and $g \in G$ and $H \leq G$

$ab \in H$ s.t. $ab \in G$

$$\langle A \rangle = \{ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \mid n \in \mathbb{Z}_{>0},\ a_i \in A,\ \varepsilon_i \in \{1, -1\} \text{ for each } i \}$$

$\langle A \rangle$ = A

Alphabet $A = \{x_1, x_2, x_3, \ldots\}$

$n = 0$ empty word $= \lambda$

$n = 1$ $x_1, x_2, x_3, \ldots$

$x_1^{-1}, x_2^{-1}, x_3^{-1}$

$n = 2$ $x_1^2, x_2^2, \ldots x_n^2$

$x_1^{-2}, \ldots, x_n^{-2}$

$$(a_1^{\varepsilon_1} \ldots a_n^{\varepsilon_n})(b_1^{\delta_1} \ldots b_m^{\delta_m})^{-1}$$

$$= a_1^{\varepsilon_1} \ldots a_n^{\varepsilon_n} b_m^{-\delta_m} \ldots b_1^{-\delta_1}$$