Chapter 4: Cyclic Groups.

Def: A Group G is cyclic iff $\exists a \in G$, $G = \{a^n \mid n \in \mathbb{Z}\}$ and we write $G = \langle a \rangle$, a is called a generator for G.

exp1: $(\mathbb{Z}, +) = \langle 1 \rangle = \{\ldots, 1^{-2}, 1^{-1}, 1^{0}, 1^{1}, 1^{2}, 1^{3}, \ldots\}$

$= \{\ldots, -2, -1, 0, 1, 2, 3 \ldots\}$

Also $(\mathbb{Z}, +) = \langle -1 \rangle$.

RMK: if $a \in G$ is a generator than a^{-1} is also a generator.

---

exp 2: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} = \langle 1 \rangle = \langle 5 \rangle$

$\mathbb{Z}_{10} = \{0, 1, 2, \ldots\ldots 9\} = \langle 1 \rangle = \langle 9 \rangle = \langle 3 \rangle = \langle 7 \rangle$

$\langle 7 \rangle = \{0, 7, 4, 1, 8, 5, 2, 9, 6, 3\}$ generator (لانه يولد كل $\mathbb{Z}_{10}$)

not generator $\leftarrow \left\{ \begin{array}{l} \langle 5 \rangle = \{0, 5\} \\ \langle 4 \rangle = \{0, 4, 8, 2, 6\} \end{array} \right.$ cyclic subgroup of $\mathbb{Z}_{10}$

---

exp 3: $\mathbb{Z}_{12} = \langle 1 \rangle = \langle 11 \rangle = \langle 5 \rangle = \langle 7 \rangle$

---

exp 4: $(U(10), \otimes_{10}) = \{1, 3, 7, 9\}$

$\langle 3 \rangle$ and $\langle 7 \rangle$ generator for $U(10)$

$\langle 9 \rangle$ not generator for $U(10)$.

$\langle 3 \rangle = \{1, 3, 9, 7\} = \langle 7 \rangle = U(10)$

$\langle 9 \rangle = \{1, 9\} \neq U(10)$

$\langle 1 \rangle = \{1\} \neq U(10)$.

$\odot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	[illegible]	9	3
9	9	7	3	1

Thm 4.1 (criterion for $a^i = a^j$)

Let G be a group and let a belong to G. If a has infinite order then $a^i = a^j$ iff $i = j$.

If a has finite order, say, n then $\langle a \rangle = \{e, a, a^2, \dots a^{n-1}\}$ and $a^i = a^j$ iff n devides $i-j$.

$G = (\mathbb{R}, +)$ is not cyclic, $a = 2$, $|2| = \infty$

$G = (\mathbb{R}^*, \cdot)$ is not cyclic, $b = 5$, $|5| = \infty$

proof Thm :

$\Rightarrow$ suppose $a^m = a^n \Rightarrow \frac{a^m}{a^n} = e \Rightarrow a^{m-n} = e$

$\Rightarrow m-n = 0$ since $|a| = \infty$

$\Rightarrow m = n$

$\Leftarrow$ if $|a| = n$ spse $a^i = a^j \Rightarrow a^{i-j} = e$

$i-j = nq + r$

$\rightarrow a^{i-j} = a^{nq+r} = (a^n)^q a^r \quad 0 \leq r < n$

$= e\,(a)^r$

$= (a)^r = e$

So $r = 0 \Rightarrow n$ devides $i-j$.

exp: $|a| = 5$, $\langle a \rangle = ?$

$\langle a \rangle = \{e, a, a^2, a^3, a^4\}$

a^5, a^6, a^7, a^8, a^9

a^{10}

$a^4 = a^9$ $a^5 = a^{10} = e$

$a^3 = a^8$

$a^2 = a^7$

$a^1 = a^6$

$\rightarrow$ $|a| = 5 \mid 9-4$ divides

$|a| = 5 \mid 8-3$ حسب Thm 4 .

$|a| = 5 \mid 7-2$

$|a| = 5 \mid 6-1$

Corollary 1: For any group element a, $|a| = |\langle a \rangle|$. كتب مثال بعد ما شرح تحت .

Corollary 2: Let G be a group and let a be an element of order n in G. If $a^k = e$ then n divides k .

Thm 4.2: Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

مش مطلوب الاثبات .

$G = \mathbb{Z}_{12}$, $a = 2$, $|a| = 6$, $k = 3$

$\rightarrow \langle a^k \rangle = \langle 2^3 \rangle = \langle 6 \rangle = \{0, 12\}$

$= 2^{g.c.d(6,3)} = 2^3 = \langle 6 \rangle = \{0, 6\}$

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

cyclic

Corollary 1 : orders of elements in Finite cyclic group

If a finite cyclic group, the order of an element divides the order of the group. يكون من قواسم العدد

exp: if G cyclic, $|G| = 24$

If $|G| = 18$, $G = \langle a \rangle$, $b \in G$ $\rightarrow |b| = 1, 9, 18$ $a \in G \rightarrow |a| = 1, 2, 3, 4, 6, 8, 12, 24$

Corollary 2 : Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$.

القاسم المشترك الأكبر

let $|a| = n$, Then $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n, i) = \gcd(n, j)$. and $|a^i| = |a^j|$ iff $\gcd(n, i) = \gcd(n, j)$.

exp $|a| = 12 \Longrightarrow |a^3| = |a^9| = \frac{12}{3} = 4$ By Thm 4.2

$|a^5| = |a^7| = |a^{11}| = \frac{12}{(12,5)} = \frac{12}{1} = 12$ By Thm 4.2

---

* If $|G| = \langle a \rangle$ of order 24

generators of G are $a, a^5, a^7, a^{11}, a^{13}, a^{17}, a^{19}, a^{23}$.

- $|a^5| = \frac{24}{g.c.d(5, 24)} = \frac{24}{1} = 24$

- $|a^6| = \frac{24}{g.c.d(6, 24)} = \frac{24}{6} = 4 \rightarrow \langle a^6 \rangle = \{e, a^6, a^{12}, a^{18}\}$.

- $|a^{15}| = \frac{24}{g.c.d(12, 15)} = \frac{24}{3} = 8 \rightarrow \langle a^{15} \rangle = \{e, a^{15}, a^6, a^{21}, a^{12}, a^3, a^{18}, a^9\}$.

Corollary 3 : Generators of Finite cyclic Groups.

Let $|a| = n$ Then $\langle a \rangle = \langle a^j \rangle$ iff $\gcd(n,j) = 1$ and $|a| = |\langle a^j \rangle|$ iff $\gcd(n,j) = 1$. $a^j = \frac{n}{\gcd(n,j)}$

Corollary 4 : Generators of $\mathbb{Z}_n$:

An integer K in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $\gcd(n,K) = 1$.

$\langle 1 \rangle$, $|1| = n$, $1^K = K$ is a generator iff $\frac{n}{(n,K)} = \frac{n}{1} = n$

* Find all generators of $\mathbb{Z}_{12}$: 1, 5, 7, 11

of cyclic subgroup 2

$\mathbb{Z}_{12} \rightarrow$ Find $\langle \overset{a}{2} \rangle = \{0, 2, 4, 6, 8, 10\}$ $\rightarrow$ cyclic subgroup of $\mathbb{Z}_{12}$ $\rightarrow$ generator $= \{a^1, a^5\}$ $= \{2, 10\}$

$\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$

* Consider $G = \mathbb{Z}_{24}$

1. Find all other generators : 1, 5, 7, 11, 13, 17, 19, 23
2. Find the cyclic subgroup generatared by 3 : $\boxed{\{0, 3, 6, 9, 12, 15, 18, 21\}}$, $|\langle 3 \rangle| = 8$
3. Find $|3^2| = |6| = \frac{8}{g.c.d(2,8)} = \frac{8}{2} = 4 \rightarrow \langle 3^2 \rangle = \langle 6 \rangle = \{0, 6, 12, 18\}$

$\rightarrow$ other generators $= 3, 3^3, 3^5, 3^7 = 3, 9, 15, 21$.

Classification of subgroups of cyclic groups.

The next theorem tells us how many subgroups a finite cyclic group has and how to find them.

Thm 4.3: Fundamental Theorem of cyclic groups:

*every subgroups of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$ then the order of any subgroup of $\langle a\rangle$ is a divisor of n, and for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order K — namely, $\langle a^{\frac{n}{k}}\rangle$ $\langle a^{\frac{1}{k}}\rangle$

proof *: let $G = \langle a\rangle$, let $H \leq G \Rightarrow$ either $H = \{e\}$ then $H = \langle e\rangle$

OR $H \neq \{e\} \rightarrow H = \{e, b, c, \ldots\}$, $b = a^s$, $c = a^t$

let s be the smallest s.t $b = a^s \in H$ then $H = \langle b\rangle$

then if $c = a^k \in H \Rightarrow K = sq + r$

$\Rightarrow a^k = c = (a^s)^q \cdot a^r$ $\quad 0 \leq r < s$.

$\underbrace{a^k}_{\in H} \cdot \underbrace{(a^s)^{-q}}_{b \in H} = a^r \in H$

So $r = 0 \Rightarrow K = sq$

$a^k = (a^s)^q = b^q$.

So $H = \langle b\rangle$.

second part:

Corollary : subgroups of $\mathbb{Z}_n$:

For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. Moreover, these are the only subgroups of $\mathbb{Z}_n$.

$\mathbb{Z}_{20} = \langle 1 \rangle$ $\quad\quad$ $\underbrace{1, 2, 4, 5, 10, 20}$ subgroup.

$\langle 0 \rangle$ of order 1

$\langle 10 \rangle$ of order 2

$\langle 5 \rangle$ of order 4

$\langle 4 \rangle$ of order 5

$\langle 2 \rangle$ of order 10

$\langle 1 \rangle$ of order 20

Thm 4.4 : Number of elements of each order in a cyclic group :

If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$. $\quad$ if n is prime $\rightarrow \phi(d) = n-1$.

2 $\quad \phi(2) = 1$

3 $\quad \phi(3) = 2$

4 $\quad \phi(4) = 2$

5 $\quad \phi(5) = 4$ $\{1, 2, 3, 4\}$

6 $\quad \phi(6) = 2 = \{1, 5\}$

7 $\quad \phi(7) = 6$

8 $\quad \phi(8) = 4 = \{1, 3, 5, 7\}$

Corollary: Number of elements of order d in a Finite group.

In a Finite group, the number of elements of order d is divisible by $\phi(d)$.

Summary:

- Definition of cyclic groups:

① let G be a group with operation $(\cdot)$

Pick $x \in G$

What's the smallest subgroup of G that contains x?

$$\langle x \rangle = \{ \ldots\ldots, x^{-4}, x^{-3}, x^{-2}, x^{-1}, \underset{e}{1}, x, x^2, x^3, x^4, \ldots \}$$

$=$ Group generated by x.

→ If $G = \langle x \rangle$ for some x, then we call G a cyclic group.

② let H be a group with operation $(+)$

pick $y \in H$

→ Group generated by y = smallest subgroup of H containing y.

$$\langle y \rangle = \{ \ldots\ldots, -3y, -2y, -y, \underset{e}{0}, y, 2y, 3y, \ldots \}$$

→ If $H = \langle y \rangle$ for some y, then we call H a cyclic group.

- Finite cyclic groups:

Group: G = integers mod n under addition

Elements: $\{0, 1, 2, \dots, n-1\}$

G is cyclic: $G = \langle 1 \rangle$.

$-2, -1, 0, 1, 2, \dots n-1, n, n+1, n+2 \dots 2n-1, 2n$

$n-2 \quad n-1 \quad \underbrace{0 \quad 1 \quad 2 \quad n-1} \quad \underbrace{0 \quad 1 \quad 2 \quad n-1} \quad 0 \dots$

$n \equiv 0 \pmod n$

$n+1 \equiv 1 \pmod n$

$n+2 \equiv 2 \pmod n$

$n+3 \equiv 3 \pmod n$

$-1 \equiv n-1 \pmod n$

$-2 \equiv n-2 \pmod n$

$-3 \equiv n-3 \pmod n$

⋮

Note: two type of cyclic groups:

1. Infinite: $\mathbb{Z}, +$
2. Finite: $\mathbb{Z}/n\mathbb{Z}, +$ — $\mathbb{Z}/n\mathbb{Z}$: integers mod n.

---

exp: Consider the group $\mathbb{Z}_6$: under addition.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

→ Consider the cyclic subgroups of $\mathbb{Z}_6$: Mod 6 مع

$\langle 1 \rangle = \{1, 1, 1, 1, 1, 1\} = \{1, \overset{1+1}{2}, \overset{2+1}{3}, \overset{3+1}{4}, \overset{4+1}{5}, \overset{5+1}{6 \pmod 6}\} = \{1, 2, 3, 4, 5, 0\}$

$\langle 2 \rangle = \{2, 2, 2, 2, 2, 2\} = \{2, \underset{2+2}{4}, \underset{4+2}{6 \bmod 6}, \underset{6+2}{8 \bmod 6}, 10 \bmod 6, 12 \bmod 6\} = \{2, 4, 0\}$

$\langle 3 \rangle = \{3, 0\}$

$\langle 4 \rangle = \{4, 2, 0\}$

$\langle 5 \rangle = \{5, 4, \underset{3+5}{3}, 2, 1, 0\}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle$ and $\langle 5 \rangle$ generator to $\mathbb{Z}_6$. $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$

→ every cyclic group is Abelian. proof خ الها

→ Not All abelian is cyclic.

$U(10)$ is cyclic and Abelian.

$U(12)$ is Abelian but not cyclic.