Previously in Math 103a

Thm. G group, $a \in G$, $|a| = n$, then for $k > 0$

$$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$$

and $$|a^k| = \frac{n}{\gcd(n,k)} = |\langle a^{\gcd(n,k)} \rangle|$$

Ex. $G = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ addition mod n

What is $\langle k \rangle$? What is $|k|$?

Ans. To apply thm, express $k \in \mathbb{Z}_n$ as a^J for a generator $a \in \mathbb{Z}_n$.

Then $\langle k \rangle$ is a cyclic subgroup of order $\frac{n}{\gcd(J,n)}$. Take $a = 1$, which generates $\mathbb{Z}_n$.

Then $a^k = \underbrace{1 + \ldots + 1}_{k} = k$, i.e. $k = a^k$.

$\therefore \langle k \rangle$ is a cyclic group of order $\frac{n}{\gcd(n,k)}$

& $\langle k \rangle = \langle \gcd(n,k) \rangle$.

If $\gcd(n,k) = 1$, then $\langle k \rangle = \mathbb{Z}_n$.

Subgroups of a cyclic group

Ex. Find all subgroups of $\mathbb{Z}_{10}$. $10 = 2 \times 5$

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

By above, $\langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle = \mathbb{Z}_{10}$

$$|\langle 2 \rangle| = \frac{10}{\gcd(10,2)} = 5 = |\langle 4 \rangle| = |\langle 6 \rangle| = |\langle 8 \rangle|$$

$$\therefore \langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle$$

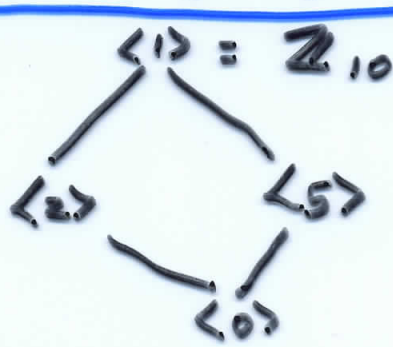
$$|\langle 5 \rangle| = \frac{10}{\gcd(10,5)}$$

Any other subgroups? No. subgroup containing both 2 & 5 is $\mathbb{Z}_{10}$

since $\gcd(2,5) = 1 \Rightarrow \exists\, s,t$

$2s + 5t = 1 \Rightarrow 1 \in$ subgroup

so every subgroup is cyclic.



subgroup lattice

Fundamental thm of cyclic groups, $G = \langle a \rangle$.

∎

Thm. (FTC G) $G = \langle a \rangle$, $|a| = n$

(1) Every subgroup of a cyclic group is cyclic. More precisely, if $H \subset G$ is a subgroup, then $\exists\, m$ s.t. $0 \le m < n$, $m \mid n$ & $H = \langle a^m \rangle$, $|H| = |a^m| = \frac{n}{\gcd(m,n)}$.

(2) If $k \mid n$, then $\exists!$ subgroup of order k, namely $\langle a^{n/k} \rangle$.

Ex. $\mathbb{Z}_{12}$ $\quad 12 = 2 \times 2 \times 3$

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

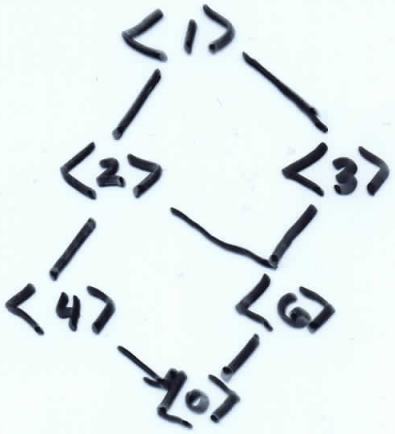
subgroup of order 2 $= \langle a^6 \rangle = \langle 6 \rangle$
" " " $3 = \langle a^4 \rangle = \langle 4 \rangle$
" " " $4 = \langle a^3 \rangle = \langle 3 \rangle$
" " " $6 = \langle a^2 \rangle = \langle 2 \rangle$

How about $\langle 9 \rangle$? $\gcd(12,3) = \gcd(12,9)$

so $\langle 9 \rangle = \langle 3 \rangle$

Similarly $\langle 10 \rangle = \langle 2 \rangle$, $\langle 8 \rangle = \langle 4 \rangle$

Lattice of subgroups



Pf of FTCG: If $H = \{e\}$, done.

(1) Show H is cyclic. $G = \{e, a, a^2, \ldots, a^{n-1}\}$,

Let $m > 0$ be smallest with $a^m \in H$.

(Every element of H is of form a^k, some k)

If $a^l \in H$, use division algorithm:

$$l = qm + r, \quad 0 \le r < m$$

Then $a^l = (a^m)^q a^r$

$\therefore a^r = a^l (a^{mq})^{-1} \in H$ (since $a^l \in H$ & $a^{mq} \in H$)

since $r < m$, must have $r = 0$

$\therefore a^l = (a^m)^q \in \langle a^m \rangle$

Hence $\langle a^m \rangle = H$, i.e. H is cyclic.

Already know $|a^m| = \dfrac{n}{\gcd(m,n)}$

$|H|$

Since $|a^{\gcd(m,n)}| = \dfrac{n}{\gcd(m,n)}$, it follows that $\langle a^m \rangle = \langle a^{\gcd(m,n)} \rangle$. Since

$m \le \gcd(m,n) \le m$, it follows that

why? → $m = \gcd(m,n)$ i.e. $m \mid n$.

(2) Suppose $k \mid n$. Put $H = \langle a^{n/k} \rangle$

Then $|a^{n/k}| = k$ (check it!)

Q: How many elements of order k are in a cyclic group of order n?

Euler phi function φ, defined by

$$\varphi(1) = 1, \quad \varphi(n) = \#\{m > 0 : m < n \text{ and } \gcd(m,n) = 1\}$$

In a cyclic group of order n, there are $\varphi(n)$ elements of order n.

Reason: Let $G = \langle a \rangle$. Then $|a^m| = \frac{n}{\gcd(n,m)}$

i.e. $|a^m| = n \iff \gcd(m,n) = 1$

Ex. $n = 30 = 2 \times 3 \times 5$

1, 7, 11, 13, 17, 19, 23, 28 coprime to 30

$\varphi(30) = 8$ 8 elements of order 30 in $\mathbb{Z}_n$.

Ex $n = 10$ 1, 3, ~~5~~, 7, 9 coprime to 10

$\varphi(10) = 4$

Thm If G is cyclic & $|G| = n$, suppose $d > 0$ & $d \mid n$. Then there are $\varphi(d)$ elements of order d in G.

Note: if $d \nmid n$, there are no elements of order d in G.

Pf of Thm. Already proved there is a unique subgroup of order d, if $d \mid n$. Call this subgroup $\langle a \rangle$ (so that $|a| = d$). If $a^m \in \langle a \rangle$ is an element of order d, then $\gcd(m, d) = 1$

$\therefore$ $\exists$ $\varphi(d)$ elements of order d in $\langle a \rangle$.

Can G have any other elements of order d? If $b \in G$ & $|b| = d$, then $|\langle b \rangle| = d$. $\therefore \langle b \rangle = \langle a \rangle$ (since there is only 1 subgroup of a given order in a cyclic group)

$\therefore$ $b \in \langle a \rangle$ //

Ex. Find the order of all elements in the group $\mathbb{Z}_{10}$. $10 = 5 * 2$

Possible orders: 1, 2, 5, 10

Order 10 : $\{1, 3, 7, 9\}$ $\varphi(10) = 4$

Order 5 start with $2 = \frac{10}{5}$

$\{2, 4, 6, 8\}$ $\varphi(5) = 4$

$\uparrow$

$a \; a^2 \; a^3 \; a^4$

Order 2 $\{5\}$ $\varphi(2) = 1$

Order 1 $\{0\}$

total of 10 elements

Next: Isomorphisms (chapter 6)

Q: When are 2 groups the "same"?

Def: Let $G, \bar{G}$ groups

A bijection $\varphi: G \longrightarrow \bar{G}$ is an isomorphism if $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall\, a, b \in G$.

If such a φ exists, we say G and $\bar{G}$ are isomorphic.