

Recap

- subgroup of a group $(G, *)$: subset $H \subset G$
s.t. $e \in H$, $a, b \in H \Rightarrow a * b, a^{-1} \in H$

"subsystem of $(G, *)$ "

- cyclic subgroup $\langle a \rangle \subset G$ for $a \in G$

$$\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \} = \{ \underbrace{a * \dots * a}_{n \text{ times}}, e, \underbrace{a^{-1} * \dots * a^{-1}}_{n \text{ times}} \mid n = 1, 2, \dots \}$$

§ 6 Cyclic groups

Suppose $\langle a \rangle = G$ happens for some $a \in G$

i.e. any $b \in G$ is of the form $b = a^n$

then we say a is a generator of G

G is a cyclic group

Rem In this case we have an isomorphism ϕ

from $(\mathbb{Z}, +)$ or $(\mathbb{Z}_m, +)$ to G given by $\phi(n) = a^n$

(see last time)

Q. what are subgroups of a cyclic group?

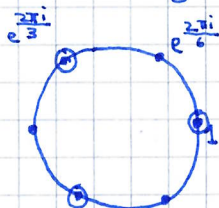
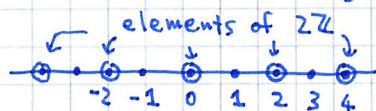
Ex. if $G = \mathbb{Z}$ and k is an integer,

$H = k\mathbb{Z} = \{ kn \mid n \in \mathbb{Z} \}$ is a subgroup

$$km + kn = k(m+n), \quad -km = k(-m), \quad 0 = k \cdot 0$$

Ex. similar const. for $G = \mathbb{Z}_m$: $H = k\mathbb{Z}_m$

Obs. these subgroups are again cyclic: $k\mathbb{Z} = \langle k \rangle$



generator of H =
elem $a \in H$ which is
"closest" to e

Thm 6.6 Suppose $G (= (G, *))$ is a cyclic group

If $H \subset G$ is a subgroup, then H is also cyclic

(with a different generator)

Proof Fix a generator $a \in G$ for $G : \langle a \rangle = G$

Take a subgroup $H \subset G$

Step 0 if $H = \{e\}$ then $H = \langle e \rangle$ and we are done

Suppose H is bigger than $\{e\}$

Step 1 take the smallest positive int. m s.t. $a^m \in H$

this makes sense : $a^n \in H \Rightarrow a^{-n} = (a^n)^{-1} \in H$

Claim $H = \langle a^m \rangle$ (hence cyclic)

we want $b \in H \Rightarrow b = (a^m)^k = a^{mk}$ for some $k \in \mathbb{Z}$

Step 2 write $b = a^n$ (possible by $b \in H \subset G = \langle a \rangle$)

and write $n = mq + r$ $r = 0, 1, \dots, m-1$

Step 3 $a^r \in H$

combine $a^n \in H$ and $a^{-mq} = (a^{-m})^q = (a^m)^{-1})^q \in H$

($a^r = a^n a^{-mq}$ from $r = n - mq$)

Step 4 r must be 0

use the minimality of m $\square$

For finite cyclic groups

suppose G is a cyclic group with n elements

(so $(\mathbb{Z}_n, +)$ is isom. to G) with generator a

Q. what can we say about $|H|$ for subgroups $H \subset G$?

Q. what are the other generators of G ?

Ex. $G = \mathbb{Z}_{12}$ $a = 1$ is a generator

other generators : 5, 7, 11

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\} = \langle 10 \rangle$ 6 elements

$\langle 4 \rangle = \{0, 4, 8\} = \langle 8 \rangle$ 3 elements

$\langle 6 \rangle = \{0, 6\}$ 2 elems. $\langle 0 \rangle = \{0\}$ 1 elem.

$\langle 3 \rangle = \{0, 3, 6, 9\} = \langle 9 \rangle$ 4 elements

$H = \langle a^k \rangle$ has $\frac{12}{\gcd(12, k)}$ elements, $\langle a^k \rangle = G \Leftrightarrow k \& 12$ coprime

$$\langle a^k \rangle = \langle a^j \rangle \Leftrightarrow \gcd(12, k) = \gcd(12, j)$$

↑ greatest common divisor

This can be generalized to arbitrary cyclic groups
(replace 12 by $n = |G|$; Thm 6.14)

§7 Generating sets, Cayley graphs

G : group

$S \subset G$: subset (we don't assume S is a subgroup)

Def. The subgroup of G generated by S is the

subset $H = \{ \text{all possible products of the form} \\ a_1 a_2 \dots a_k \mid k = 0, 1, \dots \\ \text{rem. } k = 0 \rightarrow \text{interpret as } e \\ \text{ } \uparrow \text{ } a_i \text{ or } a_i^{-1} \in S \}$

(cf. Def 7.5 & Thm 7.6)

If the above H agrees with G , we say S
generates G or S is a generating (sub)set of G

Ex. $\mathbb{Z}^2 = \{(m, n) \mid m, n \in \mathbb{Z}\}$ with $+$

$S = \{(1, 0), (0, 1)\}$ is a generating subset

Cayley digraph

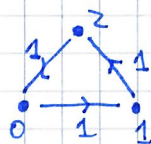
suppose G is a group, $S \subset G$ generates G

consider a graph ~~with~~ defined as

- vertex set = G
- for each vertex $x \in G$ and $a \in S$, there is
an oriented edge from x to $y = xa$
with label a



Ex. $G = \mathbb{Z}_3$, $S = \{1\}$



Ex. $G = \mathbb{Z}^2$, $S = \{a, b\}$ with $a = \begin{pmatrix} 1, 0 \\ 0, 0 \end{pmatrix}$, $b = (0, 1)$

