Recall

Group G is cyclic iff

$\exists a \in G \quad \langle a \rangle = G$

$\{a^n \mid n \in \mathbb{Z}\}$

Every cyclic group is abelian

If G is finite $G \simeq \mathbb{Z}_n$

" " infinite $G \simeq \mathbb{Z}$

For $\mathbb{Z}_n$: any elem $\mathbb{Z}_n^*$ s.t. $\gcd(m,n)=1$
is a generator of $\mathbb{Z}_n$

any elem s.t. $\gcd(m,n) \neq 1$
generates a nontrivial proper
subgroup of $\mathbb{Z}_n$

For $\mathbb{Z}$: nontrivial proper subgroups of $\mathbb{Z}$
are of the form

$n\mathbb{Z} = \langle n \rangle = \{k \cdot n \mid k \in \mathbb{Z}\}$ for $n \geq 2$

$= \{0, n, -n, 2n, -2n, \dots\}$

Generating Sets and Cayley Digraphs

Let G be a group

Let $S = \{a, b\}$

The subgroups of G generated by S

$$\langle S \rangle$$

contains all finite <u>products</u> of integral powers of a + b

<u>Ex</u>

$a, a^2, a^{-2}, \ldots$

$b, b^2, b^{-2}, \ldots$

$ab, ab^2, aba^2, a^{-1}b^3a^{-2}b^4, \ldots$

are elems of $\langle S \rangle$

In general if S is a finite subset of G s.t. $\langle S \rangle = G$ then G is finitely generated

Definition

G is a **finitely generated group** iff
$\exists S \subseteq G$, S-finite s.t. $\langle S \rangle = G$
the set is called the generating set

Note: Every cyclic group is finitely generated
The converse is <u>not</u> true

Recall

let S_i be a set for $i \in I$ s.t. $S_i \subseteq U$

$$\bigcap_{i \in I} S_i = \{ x \mid x \in S_i \text{ for all } i \in I \}$$

is a set

$$\bigcap S_i \subseteq U$$

Theorem

The intersection of subgroups H_i of a group G for $i \in I$ is a subgroup of G

Proof

Notice $\bigcap_{i \in I} H_i \subseteq G$ s.t.

1) $\forall m, n \in \bigcap_{i \in I} H_i$, $h_1 \cdot h_2 \in \bigcap_{i \in I} H_i$

bcs $h_1 \cdot h_2 \in \bigcap H_i \Rightarrow \forall i \in I, h_1, h_2 \in H_i$

since $\forall i \in I$, $H_i \leq G$,

$h_1, h_2 \in H_i \Rightarrow h_1 \cdot h_2 \in G$

2) Since $\forall i \in I$, $H_i \leq G$ we have

$e \in H_i$ for all $i \in I$

then $e \in \bigcap_{i \in I} H_i$ [each subgroup contains the identity]

3) let $h \in \bigcap_{i \in I} H_i$ then

$\forall i \in I$, $h \in H_i$ since

$\forall i \in I,\ H_i \leq G \quad h^{-1} \in H_i$ so

$$h^{-1} \in \bigcap_{i \in I} H_i$$ [subgroup containing h must contain its inverse]

If $S \subseteq G$ is a subset of each H_i

$\bigcap_{i \in I} H_i$ is the smallest subgroup of G that contains S, that is,

if $G' \leq G$ that contains S, then

$$\bigcap_{i \in I} H_i \leq G'$$

Theorem

If G is a group and $a_i \in G$ the subgroup H of G generated by $\{a_i \mid i \in I\}$ has the elements that are finite products of integral powers of a_i's, where the powers of a fixed a_i may occur several times in the product

Proof

Let K be set of all finite products of powers of a_i

Then $K \subseteq H$, Notice

1) Since a product of 2 elems of K that are finite products of powers of a_i is a finite product of powers of a_i's, the product belongs to K

[closure]

2) The identity is $a_i^0 \in K$ for $i \in I$

3) The inverse of an elem in K is a finite product of integral powers of a_i's, hence it is an elem of K

Ex/ $(a_1^2 a_2^{-3} a_3^4)^{-1} = a_3^{-4} a_2^3 a_1^{-2}$

Thus $K \leq H$

Since H is smallest subgroup containing $\{a_i \mid i \in I\}$, we have $K = H$

Notice:

If S is a generating set of a group G then $S' \subseteq G$ s.t. $S \subseteq S'$ then S' also generates S

Cayley Digraphs

Illustrates structure of finitely generated groups wrt their generating set

It's a directed graph w/

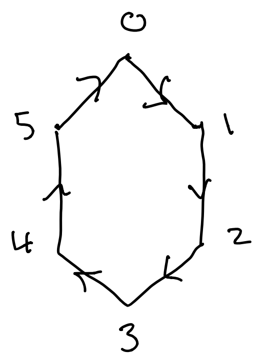
- vertices as elems of a group
- edges as generators of a group

Moreover if a generator is its own inverse ($a^{-1} = a$), it is repr. as a line

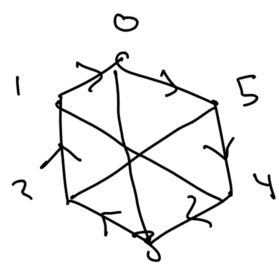
Ex Cayley Digraph for $(\mathbb{Z}_6, +_6)$ wrt following generating sets

$S = \{1\}$ $\quad$ $S = \{5, 3\}$ $\quad$ $S = \{2, 3\}$

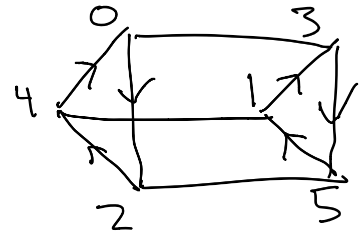
$\xrightarrow{1}$ $\quad$ $5 \rightarrow$ $\quad$ $2 \rightarrow$



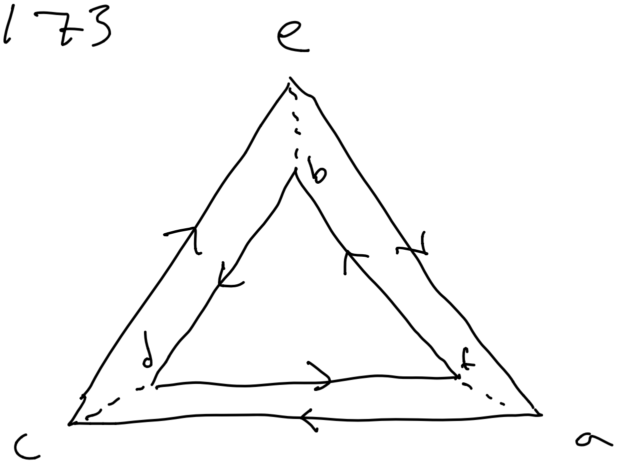
3 —

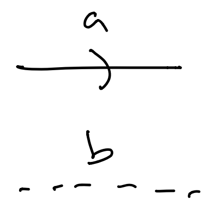


3 —



Ex 10/23





$b^{-1} = b$

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	c	f	e	b	d
b	b	d	e	f	a	c
c	c					
d	d					
f	f					

Start @ identity and follow shortest paths to elem

$a * a = c$

$a * b = f$

$$a * c = a * a * a = e$$
$$a * d = a * (b * a) = a * b * a = b$$