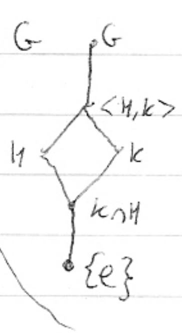
Subgroups.

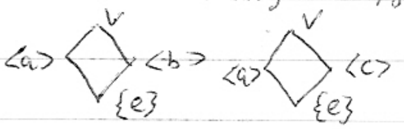
~~Definition 4.12~~ Example 4.11 ($K, H \leq G$ $\quad K \cap H \leq G \quad \langle H, K \rangle \leq G$



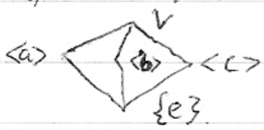
$V = \{e, a, b, c \mid a^2 = b^2 = c^2 = e\}$ $\quad \langle a \rangle = \{e, a\}$.

G generated by a, b; b, c; a, c (2 elements)

$\langle a \rangle \cap \langle b \rangle = \{e\}$ $\quad \langle a, b \rangle = G$ $\quad$ Same for a, c and b, c.



full subgroup diagram:



Definition 4.12: $a \in G$. We say a has finite order if $\exists n \in \mathbb{N}$ s.t. $a^n = e$.

If further $\forall m$ with $0 \leq m < n$ $a^m \neq e$ we say a has order n.

If a has not finite order, we say it has infinite order

order a is n: $|a| = n$ $\quad (\mathrm{ord}(a) = n)$ $\quad$ order a is ∞: $|a| = \infty$.

Remark: · G finite $\Rightarrow \forall a \in G$ $\; |a| < \infty$ i.e. $\exists n$ s.t. $a^n = e$

· Converse not true: $\exists$ infinite groups in which all elements have finite order, $\exists$ finitely generated example

· $|a| = n$, $a^0, a^1, \ldots, a^{n-1}$ are all distinct $a^i = a^j \Rightarrow a^{j-i} = e \Rightarrow j - i = 0$.

Examples 4.13 a) $(\mathbb{Z}, +)$ $\quad |0| = 1$ $\quad \forall x \neq 0$ $|x| = \infty$

b) $(\mathbb{Q}^*, \cdot)$ $\quad |1| = 1$ $(e = 1)$ $\quad |-1| = 2$ $(-1)^2 = 1 = e$ $\quad \forall x \neq \pm \Rightarrow |x| = \infty$

c) $(\mathbb{Z}_4, +)$ $\quad |[0]| = 1$; $|[1]| = |[3]| = 4$ $\quad |[2]| = 2$.

d) $V = \{e, a, b, c \mid a^2 = b^2 = c^2 = e\}$ $\quad |a| = |b| = |c| = 2$ $\quad |e| = 1$

(V has no element of order 4 $\Rightarrow$ cannot be 'essentially' the same as $\mathbb{Z}_4$).

e) $D_3 = \{e, r, r^2, s, rs, r^2 s\}$ $\quad |s| = |rs| = |r^2 s| = 2$ $\quad |r| = |r^2| = 3$.

f) $\mathbb{Z}_6$ $\quad |[1]| = 6 = |[5]|$ $\quad$ Hence D_3 cannot be the same as $\mathbb{Z}_6$ – D_3 has no element of order 6.

g). Theorem 3.13 $\quad \pi \in S_n$ $\quad |\pi| = \mathrm{lcm}\{$lengths of cycles in disjoint cycle decomposition of $\pi\}$.

e.g. $|(12)(3456)| = 4$ $\quad |(12)(345)| = 6$

Example 4.14: What is the largest possible order of an element in ~~S8~~ S_8?

$|S_8| = 8!$

$\pi \in S_8$ $\quad \pi = \pi_1 \pi_2 \ldots \pi_l$ $\quad \pi_i$ disjoint cycles $i = 1, \ldots, l$.

Length $\pi_i = k_i$ $\quad 8 = \sum_{i=1}^{l} k_i$ (including 1-cycles).

Which positive integers k_i adding up to 8 have largest lcm?

$8 = 1 + \ldots + 1$ lcm $= 1$ $\quad 8 = 8$ lcm $= 8$ $\quad 8 = 7 + 1$ lcm $= 7$ $\quad 8 = 2 + 4 + 2$ lcm $= 4$.

$8 = 5 + 3$ lcm $= 15$ $\quad 8 = 5 + 2 + 1$ lcm $= 10$ $\quad 8 = 4 + 3 + 1$ lcm $= 12$.

$\Rightarrow$ largest possible order is 15 $\quad$ e.g. $\pi = (1\,2\,3\,4\,5)(6\,7\,8)$.

Proposition 4.15. a) An element $a \in G$ of order n generates a cyclic subgroup of order n.

b). Conversely, every cyclic subgroup $H \leq G$ with $|H| = n$ is generated by an element of order n.

a) Done - see remark after 4.12.

$H = \{a^m \mid m \in \mathbb{Z}\} = \langle a \rangle$ 4.6. pick $a^m \in H$. Division Algorithm $m = q \cdot n + r$

$0 \leq r < n$ $\quad a^m = a^{qn+r} = (a^n)^q a^r = ea^r$ $\quad H = \{e, a, \ldots, a^{n-1}\} \Rightarrow |H| = n$.

b) Definition of a cyclic subgroup.

CHAPTER 5 - CYCLIC GROUPS

What does it mean for two groups to be 'essentially' the same.

1) Cayley-Tables essentially only 1 group of order 3, 2 groups of order 4.

$\mathbb{Z}_6$ and D_5 are NOT the same.

essentially $\sim$ 'up to renaming of elements etc they have the same structure'.

Definition 5.1 Let $(G, *)$ and $(H, \circ)$ be two groups. An isomorphism from G to H is a bijection $\varphi: G \to H$ satisfying $\varphi(a * b) = \varphi(a) \circ \varphi(b)$ $\forall a, b \in G$.

We say G and H are isomorphic $G \cong H$.

Remark:
- Isomorphic groups have same order (φ bijection).
- Groups of the same order need not be isomorphic e.g. $\mathbb{Z}_6 \ncong D_5$.
- $D_3 \cong S_3$ explicit isomorphism
- $D_3 \ncong \mathbb{Z}_6$ need a test.