Subgroups

Subgroups of $\mathbb{Z}_4$. Seen: every element of a group generates a cyclic subgroup

$\langle [1] \rangle = \mathbb{Z}_4$ $\langle [3] \rangle = \mathbb{Z}_4$ $\langle [0] \rangle = \{[0]\}$

$\langle [2] \rangle = \{[2]_4, [0]_4\} \xrightarrow{\cong} \mathbb{Z}_2 = \{[0]_2, [1]_2\}$. by theorem 5.a

Could also have seen this by looking at Cayley Table.

Subgroup lattice of $\mathbb{Z}_4$

$\mathbb{Z}_4$
$\langle [2] \rangle \cong \mathbb{Z}_2$
$\{[0]\}$

are all subgroups.

Proposition 5.6. A subgroup of a cyclic group is cyclic.

proof: $G = \langle [x] \rangle$ [binary operation multiplication], and $H \leq G$.

1) $H = \{e\}$ is cyclic 2) $H \neq \{e\} \Rightarrow \exists m \in \mathbb{Z}$ s.t. $x^m \in H$.

S2) $\Rightarrow x^{-m} \in H$ hence we can assume $m > 0$.

Suppose m smallest positive integer s.t $x^m \in H$

i.e. $\forall k < m, k > 0 : x^k \notin H$.

Want to show $H = \langle x^m \rangle$. Pick $x^i \in H$ (by S2) assume $i > 0$).

Division algorithm: $i = mq + r$ $0 \leq r < m$ $x^i = x^{mq+r} = (x^m)^q \cdot x^r$

$(x^m)^{-q} x^i = x^r$ by assumption $x^i \in H$, $x^m \in H \Rightarrow$ S1) $(x^m)^q \in H$,

S2) $(x^m)^{-q} \in H \Rightarrow$ S1) $(x^m)^{-q} x^i = x^r \in H$

$x^r \in H$ with $0 \leq r < m$ minimal $\Rightarrow r = 0$.

$r = 0 \Rightarrow x^i = (x^m)^q$ $x^i \in \langle x^m \rangle$ $\forall x^i \in H \Rightarrow H \leq \langle x^m \rangle$ and $\langle x^m \rangle$ is smallest subgroup of G containing $x^m \Rightarrow H = \langle x^m \rangle$ is cyclic □.

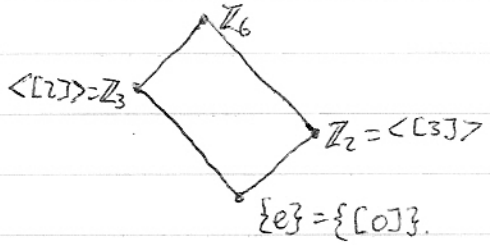
Corollary 5.7: finding all subgroups of a cyclic group reduces to determining orders of elements.

$G = \langle x \rangle$ $g \in G$ and $|g| = n \Rightarrow \langle g \rangle \cong \mathbb{Z}_n$.

$G = \mathbb{Z}_6$ $|[0]| = 1$ $|[1]| = |[5]| = 6$ $|[2]| = |[4]| = 3$ $|[3]| = 2$

$\{e\}$ $G \cong \mathbb{Z}_6$ $\mathbb{Z}_3 \cong \{[0], [2], [4]\}$ $\mathbb{Z}_2 \cong \{[0]_6, [3]_6\}$.

$\langle \langle [2] \rangle, \langle [3] \rangle \rangle = G$ $\langle [2] \rangle \cap \langle [3] \rangle = \{[0]\} = \{e\}$.



$\mathbb{Z}_5$ $|[0]| = 1$,

$|[1]| = |[2]| = |[3]| = |[4]| = 5$

only subgroups are $\mathbb{Z}_5$, $\{[0]\}$.

$G = \mathbb{Z}_{12}$ $|[0]| = 1$ $\{e\} = \{[0]\}$.

$|[1]| = |[5]| = |[7]| = |[11]| = 12$ $\langle [1] \rangle \cong \mathbb{Z}_{12}$

$|[2]| = |[10]| = 6$ $\langle [2] \rangle = \langle [10] \rangle \cong \mathbb{Z}_6$.

$|[3]| = |[9]| = 4$ $\langle [3] \rangle = \langle [9] \rangle \cong \mathbb{Z}_4$

$|[4]| = |[8]| = 3$ $\langle [4] \rangle \cong \mathbb{Z}_3$

$|[6]| = 2$ $\langle [6] \rangle \cong \mathbb{Z}_2$.

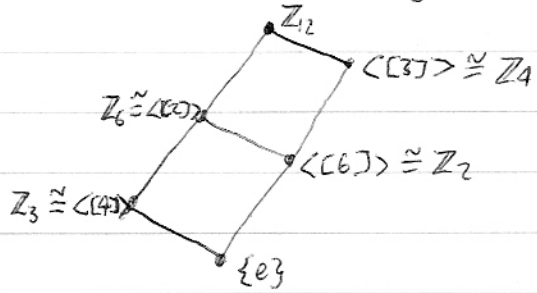
$\langle [4] \rangle \leq \langle [2] \rangle$ $\{[0], [4], [8]\} \leq \{[0], [2], \ldots, [10]\}$.

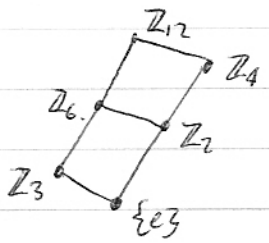
$\langle [6] \rangle \leq \langle [2] \rangle$

$\langle [6] \rangle \leq \langle [3] \rangle$ $\{[0], [6]\} \leq \{[0], [3], [6], [9]\}$.

$\langle [2] \rangle \cap \langle [3] \rangle = \{[0], [6]\} = \langle [6] \rangle$ rest intersects trivially.

$\langle [2] \rangle$ and $\langle [3] \rangle$ generate whole group.





Theorem: Let $n \in \mathbb{Z}$, $n > 0$. Then for each divisor d of n $\mathbb{Z}_n$ has a subgroup of order d. (Later show (Lagrange) these are all subgroups of $\mathbb{Z}_n$).

Proof: Let $k = \frac{n}{d}$. Then $|[k]_n| = d$.