Cyclic Subgroups

Theorem

Let G be a group and $a \in G$:

$$\langle a \rangle \leq G$$

Proof

Assume $x \in \langle a \rangle$
$\exists\, n \in \mathbb{Z}, x = a^n$
But by closure, $a^n = x \in G$
$\langle a \rangle \subseteq G$
$\langle a \rangle$ is a group under the induced operation of G.
$\therefore \langle a \rangle \leq G$

Corollary

Let G be a group and $a \in G$:

$\langle a \rangle$ is the smallest subgroup of G containing a.

Proof

Assume $H \leq G$ such that $a \in H$
$\langle a \rangle \leq H$
$\forall\, H \leq G, \langle a \rangle \leq H$
$\therefore \langle a \rangle$ is the smallest subgroup of G containing a.

Definition

Let G be a group and $a \in G$. $\langle a \rangle$ is called the *cyclic subgroup* of G generated by a.

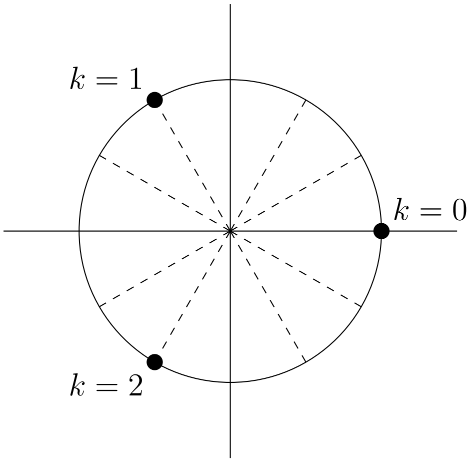
The *order* of a is given by $|\langle a \rangle|$.

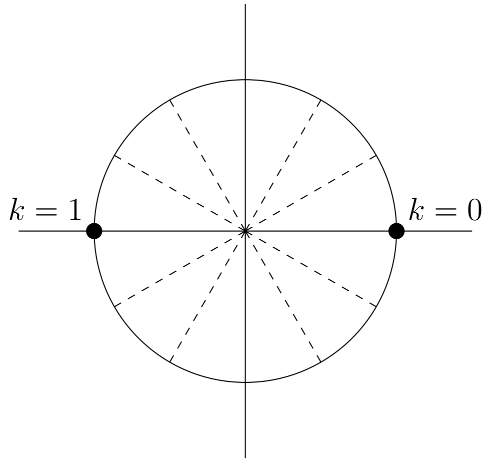
Example

$U_{12} = \{e^{i\frac{2\pi k}{12}} \mid 0 \leq k < 12\}$

Let $a = e^{i\frac{2\pi 8}{12}} = e^{i\frac{4\pi}{3}}$
$\langle a \rangle = \{1, e^{i\frac{4\pi}{3}}, e^{i\frac{8\pi}{3}}\} = U_3$
$U_3 \leq U_{12}$

Let $a = e^{i\frac{2\pi 6}{12}} = e^{i\pi} = -1$
$\langle a \rangle = \{1, -1\}$
$U_2 \leq U_{12}$





Theorem

Let G be a group:

G has no proper, non-trivial subgroups $\implies G$ is cyclic.

Proof

Assume G has no proper, non-trivial subgroups
Assume $a \in G$
$\langle a \rangle \leq G$
But $\langle a \rangle$ is neither trivial nor proper, so $\langle a \rangle = G$
$\therefore G$ is cyclic

Theorem

Let G be cyclic. $\forall\, H \leq G, H$ is cyclic.

Proof

$\{e\} \leq G$, so AWLOG that $H \leq G$ is non-trivial
Let $H' = \mathbb{Z}_n$ or $H' = \mathbb{Z}$
$H \simeq H'$
Let $S = \{a \in H' \mid a \in \mathbb{Z}^+\}$
$1 \in S$, so $S \neq \emptyset$
Let $h = \min H'$
Assume $k \in H', k \leq h$
By the division algorithm: $k = qh + r$ such that $q, r \in \mathbb{Z}$ and $0 \leq r < h$
$r = k - qh \in H'$
But by the minimality of $h, r = 0$
$k = qh$
$H' = \langle h \rangle$
H' is cyclic
$\therefore H$ is cyclic.

Theorem

Let $G = \langle a \rangle$. Let $a^h, a^k \in G$ and $d = (h, k)$:

$$H = \left\{ \left(a^h\right)^n \left(a^k\right)^m \mid n, m \in \mathbb{Z} \right\} = \left\langle a^d \right\rangle \leq G$$

Proof

$G \simeq \mathbb{Z}_n$ or $G \simeq \mathbb{Z}$, so let G' be the appropriate one
Let $H' = \{mh + nk \mid m, n \in \mathbb{Z}\}$
$H \simeq H'$
Assume $x, y \in H'$
$\exists\, m_1, n_1 \in \mathbb{Z}, x = m_1 h + n_1 k$
$\exists\, m_2, n_2 \in \mathbb{Z}, y = m_2 h + n_2 k$
$-y = -m_2 h - n_2 k \in G'$
$x - y = (m_1 - m_2)h + (n_1 - n_2)k \in H'$
So, by the subgroup test, $H' \leq G'$
$\therefore H \leq G$

But also, $\exists\, c \in \mathbb{Z}, x = m_1 h + n_1 k = c(h, k) = cd$
So, $H' = \langle d \rangle$
$\therefore H = \left\langle a^d \right\rangle$

Corollary

Let $G = \langle a \rangle$. Let $a^h, a^k \in G$ and $d = (h, k)$. $\left\langle a^d \right\rangle$ is the smallest subgroup of G containing a^h and a^k.

Proof

$G \simeq \mathbb{Z}_n$ or $G \simeq \mathbb{Z}$, so let G' be the appropriate one
Assume $H \leq G'$
Assume $h, k \in H$
$\langle d \rangle = \{mh + nk \mid m, n \in \mathbb{Z}\} \leq H$
Thus, $d \in H$
$h = 1 \cdot h + 0 \cdot k \in \langle d \rangle$
$k = 0 \cdot h + 1 \cdot k \in \langle d \rangle$
But $\langle d \rangle$ is the smallest subgroup of H containing d
So $\langle d \rangle$ is also the smallest subgroup of H containing h and k
But since $H \leq G'$, $\langle d \rangle$ is the smallest subgroup of G' containing h and k
$\therefore \left\langle a^d \right\rangle$ is the smallest subgroup of G containing a^h and a^k.

Example

$9, 15 \in \mathbb{Z}_{24}$ and $(9, 15) = 3$

$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}$

$\langle 3 \rangle$ is the smallest subgroup of $\mathbb{Z}_{24}$ containing 9 and 15