Cyclic Groups

Recall: G a group, $H \subseteq G$ a subset. Then H is a subgroup provided

① for all $h_1, h_2 \in H$, $h_1 h_2 \in H$

② for all $h \in H$, $h^{-1} \in H$.

Examples $(\mathbb{C}, +)$ $\quad \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

$(\mathbb{C}^*, \cdot)$ $\quad \mathbb{R}_+ \leq \mathbb{R}^* \leq \mathbb{C}^*$

$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ $\quad \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ $\quad \mathbb{R}_+ = \{x > 0\} \subset \mathbb{R}$.

$GL(n, \mathbb{R}) = \{A \text{ } n \times n \text{ matrix with real entries} \mid \det A \neq 0\}$

$O(n) = \{A \in GL(n, \mathbb{R}) \mid A^T A = I\} \leq GL(n, \mathbb{R})$

Proposition Let G be a group and let $H_1 \leq G$, $H_2 \leq G$ be subgroups. Then $H_1 \cap H_2$ is a subgroup.

More generally, $\bigcap_{\alpha \in J} H_\alpha$ is a subgroup if

$\{H_\alpha\}_{\alpha \in J}$ is an indexed collection of subgroups ($H_\alpha \leq G$.)

Proof ① Suppose $h_1, h_2 \in \bigcap_\alpha H_\alpha$. Then $\forall \alpha$ $h_1 \in H_\alpha$ and $h_2 \in H_\alpha$ then since H_α is a subgroup, $\forall \alpha$ $h_1 h_2 \in H_\alpha$, so $h_1 h_2 \in \bigcap_\alpha H_\alpha$

② similar logic: $h \in \bigcap_\alpha H_\alpha \Rightarrow \forall \alpha \ h \in H_\alpha$

$\Rightarrow \forall \alpha \ h^{-1} \in H_\alpha \Rightarrow h^{-1} \in \bigcap_\alpha H_\alpha$.

Now suppose $A \subseteq G$, $A \neq \emptyset$ is any nonempty subset. A may not be a subgroup, but we would like to enlarge it so that it becomes a subgroup. We seek the minimal such enlargement.

<u>Definition</u>: <u>The subgroup generated by A</u> is

$$\langle A \rangle = \text{intersection of all subgroups } H \leq G \text{ that contain } A: A \subseteq H.$$

Because $\langle A \rangle$ is an intersection of subgroups, it is itself a subgroup. Also it is minimal in the sense that any subgroup that contains A must contain $\langle A \rangle$.

<u>Constructive approach</u> To construct $\langle A \rangle$, we start with all of the elements $a \in A$, and repeatedly take all possible products and inverses. We get

$$\langle A \rangle = \{ a_1^{e_1} a_2^{e_2} \cdots a_k^{e_k} \mid a_i \in A,\ e_i \in \{1,-1\} \}$$

e.g., if $a, b \in A$, then $aab^{-1}aba^{-1}bba^{-1} \in \langle A \rangle$

We can see directly that this is a subgroup:

$$(a_1^{e_1} a_2^{e_2} \cdots a_k^{e_k})(b_1^{f_1} \cdots b_\ell^{f_\ell}) = a_1^{e_1} \cdots a_k^{e_k} b_1^{f_1} \cdots b_\ell^{f_\ell} \in \langle A \rangle$$

$$(a_1^{e_1} a_2^{e_2} \cdots a_k^{e_k})^{-1} = a_k^{-e_k} a_{k-1}^{-e_{k-1}} \cdots a_1^{-e_1} \in \langle A \rangle$$

It is also clear that any subgroup that contains A must contain $a_1^{e_1} \cdots a_k^{e_k}$ for $a_i \in A$ $e_i \in \{1,-1\}$.

This justifies the equality of the two definitions.

Special case: $A = \{a\}$, a singleton set. Then we write

$$\langle a \rangle = \langle \{a\} \rangle = \{ a^k \mid k \in \mathbb{Z} \}$$

This is called <u>the subgroup generated by a</u>.

Here, $a^0 = e$, $a^k = \underbrace{a \cdot a \cdots a}_{k}$ for $k > 0$, and $a^{-k} = (a^k)^{-1}$ for $k > 0$

If G is a group, and $a \in G$, and $G = \langle a \rangle$, we say that G is a <u>cyclic group</u> (generated by a).

In general, if $a \in G$, then $\langle a \rangle \leq G$ is the <u>cyclic subgroup generated by a</u>.

<u>Examples</u> $G = (\mathbb{Z}, +)$ $d \in \mathbb{Z}$, $\langle d \rangle = \{ kd \mid k \in \mathbb{Z} \} = \langle -d \rangle$

$\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$, so $\mathbb{Z}$ is cyclic, generated by 1 (or -1).

$G = (\mathbb{Z}_n, +)$. $[d] \in \mathbb{Z}_n$, $\langle [d] \rangle = \{ [kd] \mid k \in \mathbb{Z} \}$

$\langle [1] \rangle = \mathbb{Z}_n$, so $\mathbb{Z}_n$ is cyclic. (Are there other generators?)

For a given group G, we can consider all subgroups H. Subgroups are partially ordered by inclusion, and any two subgroups H_1 H_2 have a "minimum" $H_1 \cap H_2$ as well as a maximum $\langle H_1 \cup H_2 \rangle$.
Thus the set of subgroups of G forms what is called a <u>lattice</u>.

We can visualize the subgroup lattice using a diagram

$$S_3 = \{ e, (12), (13), (23), (123), (132) \}$$

$$\begin{tikzcd}
 & & S_3 \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle (12) \rangle \arrow[drr, dash] & \langle (13) \rangle \arrow[dr, dash] & \langle (23) \rangle \arrow[d, dash] & \langle (123) \rangle = \langle (132) \rangle \arrow[dl, dash] \\
 & & \{e\} &
\end{tikzcd}$$

Let G be a group, and let $a \in G$. Then $\langle a \rangle$ is either finite or infinite. If $\langle a \rangle$ is finite, the number of elements in this set is called the <u>order of a</u>

$$o(a) = |\langle a \rangle|$$

If $\langle a \rangle$ is infinite we say the order of a is infinite and write $o(a) = \infty$.

Recall two groups G, H are <u>isomorphic</u> if there is a bijective function $\varphi : G \to H$ with $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. We write $G \cong H$ to mean G and H are isomorphic.

<u>Proposition</u> (Classification of cyclic groups)
Let G be a group and $a \in G$.
(i) if $o(a) = \infty$, then $\langle a \rangle \cong \mathbb{Z}$
(ii) if $o(a) = n \in \mathbb{N}$, then $\langle a \rangle \cong \mathbb{Z}_n$.

<u>Proof</u>: Two cases: either all powers a^k are distinct elements of G, or else there are $k \neq l$ with $a^k = a^l$ in G.

If all powers a^k are distinct, then $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ is infinite, so $o(a) = \infty$. In this case, we define

$\varphi : \mathbb{Z} \to \langle a \rangle$ by $\varphi(k) = a^k$

φ is surjective: every element of $\langle a \rangle$ is a^k for some $k \in \mathbb{Z}$.
φ is injective: if not, then $a^k = a^l$ for $k \neq l$, which we're assuming doesn't happen

Lastly $\varphi(k+l) = a^{k+l} = a^k a^l = \varphi(k)\varphi(l)$
so φ is an isomorphism, and $\langle a \rangle \cong \mathbb{Z}$. ✓

If two powers a^k and a^l are equal for $k < l$, we deduce

$$a^k = a^l \Rightarrow (a^k)^{-1} a^k = (a^k)^{-1} a^l \Rightarrow e = a^{l-k}$$

Thus there is a positive power of a that equals e.
Let n be the least positive integer with $a^n = e$.
We claim $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

First: $e, a, a^2, \ldots, a^{n-1}$ are all distinct (Exercise 2.2.9)
For any $k \in \mathbb{Z}$, write $k = qn + r$ with $0 \leq r \leq n-1$.
Then $a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$.

So <u>any</u> power of a is equal to some element of the set $\{e, a, a^2, \ldots, a^{n-1}\}$.

Define $\varphi : \mathbb{Z}_n \to \langle a \rangle$ by $\varphi([k]) = a^k$.
Well defined since $k \equiv k' \bmod n$ implies $k' = k + qn$ so

$$a^{k'} = a^k (a^n)^q = a^k e^q = a^k.$$

Since
$\mathbb{Z}_n = \{[0],[1],\dots,[n-1]\}$, φ is bijective, and
$\varphi([k]+[\ell]) = \varphi([k+\ell]) = a^{k+\ell} = a^k a^\ell = \varphi([k])\varphi([\ell])$.
so φ is an isomorphism. $\mathbb{Z}_n \cong \langle a \rangle$. ☒

Now consider the subgroups of $\mathbb{Z}$.

<u>Proposition</u>: If $H \leq \mathbb{Z}$ is a subgroup, then either $H = \{0\}$ there is a unique $d \in \mathbb{N}$ such that $H = \langle d \rangle$.

<u>Proof</u>: If $H \neq \{0\}$, there is some $k \in H$ $k \neq 0$. Then $-k \in H$ also. Either k or $-k$ is positive, so H contains a positive number. Let $d \in \mathbb{N} \cap H$ be the least positive number in H. Then $\langle d \rangle \subseteq H$.
We claim $H \subseteq \langle d \rangle$ as well.
Take $k \in H$. Write $k = qd + r$ $\quad 0 \leq r < d$
If $r \neq 0$, then $k - qd = r \in H$ is a positive number less than d, contradicting the assumed minimality of d.
So $r = 0$ and $k = qd$ for some $q \in \mathbb{Z}$. Thus $k \in \langle d \rangle$.
So $H \subseteq \langle d \rangle$ and we conclude $H = \langle d \rangle$.

For uniqueness, observe that $\langle d_1 \rangle = \langle d_2 \rangle$ implies $d_1 \mid d_2$ and $d_2 \mid d_1$, so $d_1 = \pm d_2$. If $d_1, d_2 \in \mathbb{N}$, this forces $d_1 = d_2$.

<u>Proposition</u> In $(\mathbb{Z},+)$, $\langle d_1 \rangle \leq \langle d_2 \rangle \iff d_2 \mid d_1$.

<u>Proof</u>: $\langle d_1 \rangle \leq \langle d_2 \rangle \iff d_1 \in \langle d_2 \rangle \iff d_1 = k d_2$ for some $k \in \mathbb{Z}$
$\iff d_2 \mid d_1$