Groups + Subgroups (Examples!)

Recall: A group is a set G w/ assoc. bin op $\cdot : G \times G \to G$ s.t.
(i) $\exists$ identity $e \in G$
(ii) $\forall g \in G \ \exists g^{-1} \in G$ s.t. $g \cdot g^{-1} = e = g^{-1} \cdot g$

A **Subgroup** of G is a subset $H \subseteq G$ s.t. $(H, \cdot|_{H \times H})$ is a group. Write $H \leq G$.

This means (i) $H \neq \emptyset$ ($e \in H$),
(ii) for any $h, h' \in H$, $h \cdot h'$ (which a priori is in G) is in H,
(iii) for any $h \in H$, h^{-1} (which a priori is in G) is in H.

Prop (3.4.12 in notes) if G is finite, suffices to check (i) and (ii).

(Boring)
Ex. For any group G, $e \leq G$ and $G \leq G$.

Ex. For $\mathbb{Z}/p\mathbb{Z}$, p prime, these are the only subgps!

Ex. Groups / subgroups of matrices

Consider $GL_n(\mathbb{R}) = \{ \text{invertible } (n \times n)\text{-matrices w/ entries in } \mathbb{R} \}$, which is a group under mtx mult.

This group is **non**-Abelian for $n \geq 2$:

e.g.
$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

Note! $GL_n(\mathbb{R}) \hookrightarrow \mathbb{R}^{n \times n}$ as a set but not as a group!
($GL_n(\mathbb{R})$: non-Abelian; $\mathbb{R}^{n \times n}$: Abelian)

Important subgroups

(1) $\mathrm{Diag}_n(\mathbb{R}) = \{ \text{diagonal } (n \times n)\text{-matrices} \} \leq GL_n(\mathbb{R})$

Pf/ (i) $e = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \in \mathrm{Diag}_n(\mathbb{R})$

(ii) if $A = \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}$ and $B = \begin{bmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{bmatrix}$, then $AB = \begin{bmatrix} a_1 b_1 & & 0 \\ & \ddots & \\ 0 & & a_n b_n \end{bmatrix} \in \mathrm{Diag}_n(\mathbb{R})$.

(iii) for A as above, $A^{-1} = \begin{bmatrix} a_1^{-1} & & 0 \\ & \ddots & \\ 0 & & a_n^{-1} \end{bmatrix} \in \mathrm{Diag}_n(\mathbb{R})$.

Hence $\mathrm{Diag}_n(\mathbb{R}) \leq GL_n(\mathbb{R})$. Note that (ii) shows $\mathrm{Diag}_n(\mathbb{R})$ is Abelian (since $\cdot$ in $\mathbb{R}$ is commutative).

(2) $SL_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) \mid \det A = 1 \} \leq GL_n(\mathbb{R})$

Pf/ (i) $I_n \in SL_n(\mathbb{R})$.

(ii) if $A, B \in SL_n(\mathbb{R})$, then $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$ so $AB \in SL_n(\mathbb{R})$.

(iii) Similarly, for $A \in SL_n(\mathbb{R})$, we know $A^{-1} \in GL_n(\mathbb{R})$. But

$$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}) = 1 \cdot \det(A^{-1})$$

So $A^{-1} \in SL_n(\mathbb{R})$ as well.

Ex. (Exc 1.1 from HW5) If G is a group, then $\Delta = \{(g,g) \mid g \in G\} \leq G \times G$. ($(g_1,g_2)\cdot(g_1',g_2') = (g_1g_1', g_2g_2')$)

Pf/ Note $\Delta \subseteq G \times G$ so just need to check (i), (ii), (iii).

(i) The identity is $(e,e) \in \Delta$

(ii) For $g, g' \in G$, $(g,g)\cdot(g',g') = (gg', gg') \in \Delta$

(iii) For $g \in G$, we know $g^{-1} \in G$ and hence by (ii)

$$(g,g)\cdot(g^{-1},g^{-1}) = (e,e)$$

so $(g,g)^{-1} = (g^{-1}, g^{-1}) \in \Delta$.

Generators + Order of Elements

Recall:
- For $g \in G$, the order of g is the smallest $k \in \mathbb{N}_{>0}$ s.t. $g^k = g \cdots g = e$. Write $o(g) = k$. (or $|g|$ or $\operatorname{ord}(g)$)
- If such k DNE, set $o(g) = \infty$.
- The subgp gen'd by $g \in G$ is $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{e, g, g^2, g^3, \dots\} \leq G$.
- If $o(g) < \infty$, $\langle g \rangle = \{e, g, g^2, \dots, g^{o(g)}\}$.
- If $G = \langle g \rangle$, G is cyclic and g is a generator.

Ex. For $n \in \mathbb{Z}$, $\langle n \rangle = \{0, n, 2n, 3n, \dots, kn, \dots, -kn, \dots, -2n, -n\} \leq (\mathbb{Z}, +)$

In particular, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. (Note generators are not unique! $\langle g \rangle = \langle g^{-1} \rangle$)

Ex For $G = (\mathbb{Z}/n\mathbb{Z}, +)$, can we write $\mathbb{Z}/n\mathbb{Z} = \langle g \rangle$ for some $g \in \{0,1,\dots,n-1\}$?

Observation: Since $|\mathbb{Z}/n\mathbb{Z}| = n$, need $o(g) = n$. In fact this is iff!

Claim $\mathbb{Z}/n\mathbb{Z} = \langle g \rangle$ iff $o(g) = n$.

Pf/ Write $\langle g \rangle = \{e, g, g^2, \dots, g^{o(g)}\}$. Note that $|\langle g \rangle| = o(g)$. Thus if $\mathbb{Z}/n\mathbb{Z} = \langle g \rangle$ then $n = |\mathbb{Z}/n\mathbb{Z}| = |\langle g \rangle| = o(g)$. ($\Leftarrow$) If $o(g) = n$, then have a bijection $\langle g \rangle \to \mathbb{Z}/n\mathbb{Z}$ by $g^k \mapsto k$ $(0 \leq k < n)$.

Claim This is an isomorphism of groups (Hint: $g^k \cdot g^{k'} = g^{k+k'} \mapsto k + k'$).

In fact, $o(g) = n \iff \gcd(g,n) = 1$. (Exc.)

Thm Let $|G| = n$ w/ $G = \langle g \rangle$. Then $G \cong \mathbb{Z}/n\mathbb{Z}$ and

- $G = \langle g^k \rangle \iff \gcd(k,n) = 1$.
- if $H \leq G$, then $H = \langle g^d \rangle$ for some $d \mid n$. (Note $|H| \mid |G|$)

- For each $d|n$, $\exists!$ subgp $H \leq G$ w/ $|H| = d$, specifically $H = \langle g^{\frac{n}{d}} \rangle$

This is very abstract. Let's look at specific examples.

Ex. $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\} = \langle 1 \rangle = \langle 2 \rangle$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{0, 1, 2\}$

$\langle 2 \rangle = \{0, 2, 4 \equiv_3 1\}$

This shows $\{\text{subgps of } \mathbb{Z}/3\mathbb{Z}\} = \{e = \langle 0 \rangle, \mathbb{Z}/3\mathbb{Z}\}$! (This is true for $\mathbb{Z}/p\mathbb{Z}$, p prime)

Ex. $\mathbb{Z}/6\mathbb{Z} = \{0, 1, \ldots, 5\}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \mathbb{Z}/6\mathbb{Z}$

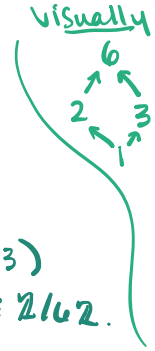
$\langle 2 \rangle = \{0, 2, 4\}$ $(\cong \mathbb{Z}/3\mathbb{Z}, \ o(2) = 6/2 = 3)$

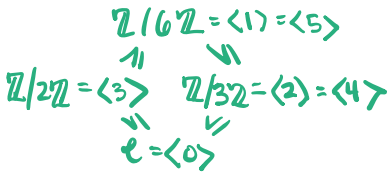
$4 \equiv -2$ $\langle 3 \rangle = \{0, 3\}$ $(\cong \mathbb{Z}/2\mathbb{Z}, \ o(3) = 6/3 = 2)$

$\langle 4 \rangle = \{0, 4, 8 \equiv 2\}$ $(\cong \mathbb{Z}/3\mathbb{Z}, \ o(4) = 6/4 = 3)$

$\langle 5 \rangle = \{0, 5, 10 \equiv 4, 15 \equiv 3, 20 \equiv 2, 25 \equiv 1\} \cong \mathbb{Z}/6\mathbb{Z}$.

Visually





~ break ~

Important defn (for the problems): For non-empty $X \subseteq G$, define $\langle X \rangle \leq G$ to be the smallest subgroup containing X. This means: (i) $X \subseteq \langle X \rangle$

(ii) $\langle X \rangle \leq G$

(iii) if H satisfies (i) and (ii), then $\langle X \rangle \subseteq H$.

Group work: Highlight: $\frac{1}{n} \leq$ taste $\leq n$ importance of boardwork

(1) Prove if G is finite, then $H \leq G \iff H \neq \emptyset$ and $h, h' \in H \Rightarrow h \cdot h' \in H$.

(2) Determine the groups G s.t.

(a) $\{(g, g^{-1}) \mid g \in G\} \leq G$

(b) $\text{Cube}(G) = \{g^3 \mid g \in G\} \leq G$

(c) $\langle S \rangle = e$ for $S = \{x^{-1}y^{-1}xy \mid x, y \in G\}$

(3) Let $X \subseteq G$ non-empty and show $\langle X \rangle = \bigcap_{\substack{X \subseteq H \\ H \leq G}} H$.