Last time: A (left) action of a group G on a set X is a map $G \times X \to X$, $(g, x) \mapsto g \cdot x$ so that

i) $e_G \cdot x = x \quad \forall x \in X$

ii) $a \cdot (b \cdot x) = (ab) \cdot x \quad \forall a, b \in G \quad \forall x \in X$.

An **orbit** through $x_0 \in X$ is the set

$$G \cdot x_0 = \{ g \cdot x_0 \mid g \in G \}$$

Theorem 7.1 Let $G \times X \to X$ be an action. Then $\{G \cdot x\}_{x \in X}$ is a partition of X.

Corollary 8.1 Let $G \times X \to X$ be an action, $x, y \in X$. Then

$$G \cdot x \cap G \cdot y \neq \emptyset \iff G \cdot x = G \cdot y$$
$$\iff x \in G \cdot y$$
$$\iff x = g \cdot y \text{ for some } g \in G.$$

Proof (Easy (?) exercise.

Definition Let H be a subgroup of a group G.
The **right coset** of $g \in G$ is the set $Hg := \{ hg \mid h \in H \}$

Note H acts on G by multiplication on the left: $H \times G \to H$, $(h, g) \mapsto hg$
and Hg = orbit of g for this action.

Therefore

right cosets of H partition G: $G = \bigcup_{g \in G} Hg$

and

$$Hg_1 \cap Hg_2 \neq \emptyset \iff Hg_1 = Hg_2$$
$$\iff g_1 \in Hg_2$$
$$\iff g_1 = hg_2 \text{ for some } h \in H.$$
$$\iff g_1 g_2^{-1} \in H$$

Ex $G = \mathbb{Z}$, $n \in \mathbb{N}$, $n > 0$. Then $H = n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
The right cosets of $H = n\mathbb{Z}$ are

$n\mathbb{Z}$ $(= H)$, $n\mathbb{Z} + 1$, $n\mathbb{Z} + 2$, ... $n\mathbb{Z} + (n-1)$.

Note: The right cosets of H are equivalence classes for the equivalence relation $\sim$ on G defined by

$$g_1 \sim g_2 \iff g_1 g_2^{-1} \in H.$$

Ex $H = n\mathbb{Z} \leq \mathbb{Z} = G$. $\quad k \sim \ell \iff k - \ell \in n\mathbb{Z} \quad (\iff n \mid (k-\ell))$

Notation $H \backslash G = \{ Hg \mid g \in G \}$ the set of right cosets of H, the subgroup H of G.

Ex $\quad n\mathbb{Z} \backslash \mathbb{Z} = \mathbb{Z}_n$

HW $\Rightarrow \quad \mathbb{Z} \backslash \mathbb{R} = \{ \mathbb{Z} + x \mid x \in \mathbb{R} \}$, a partition of $\mathbb{R}$.

Remark Left cosets of a subgroup H of G are defined similarly

A left coset of H is

$$gH = \{ gh \mid g \in G \}.$$

Left cosets are orbits of the (left) action of H on G

$$H \times G \to G, \quad (h, g) \mapsto gh^{-1}$$

Note the map $\text{inv}: H \to H$, $\text{inv}(h) = h^{-1}$, is a bijection (since $(h^{-1})^{-1} = h$, ie $\text{inv} \circ \text{inv} = \text{id}_H$)

Hence

$$gH = \{ gh \mid h \in H \} = \{ gk^{-1} \mid k \in H \} = H \cdot g$$

So left cosets also partition G.

Theorem 8.3 Let $f: G \to H$ be a homomorphism, $K = \ker f$.

Then $\bar{f}: K \backslash G \to H$, $\bar{f}(Kg) = f(g)$

is a well-defined injective map.

< we'll use this result and its variants throughout the semester >

Proof We need to check: (i) $Ka = Kb \Rightarrow (f(a) =) \bar{f}(Ka) = \bar{f}(Kb) \; (= f(b))$

(ii) if $\bar{f}(Ka) = \bar{f}(Kb)$ then $Ka = Kb$

Suppose $Ka = Kb$. Then $a = kb$ for some $k \in K = \ker f$.
$\Rightarrow f(a) = f(kb) = f(k) f(b) = e_H \cdot f(b) = f(b)$.
This proves (i).

Suppose $\bar{f}(Ka) = \bar{f}(Kb)$, ie $f(a) = f(b)$. Then
$e_H = f(a)(f(b))^{-1} = f(ab^{-1}) \Rightarrow kb = ab^{-1} \in \ker f = K$
$\Rightarrow a = kb$ for some $k \in K$. $\Rightarrow Ka = Kb$. □

Recall For any group G and for any element $a \in G$ we have a homomorphism $f: \mathbb{Z} \to G$, $f(n) = a^n$.
$\operatorname{im} f = \langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$.
Hence if f is injective, $f: \mathbb{Z} \to \langle a \rangle$ is an isomorphism.
[Recall that this happens iff $a^n = e_G \Rightarrow n = 0$]

Thm 8.4 Suppose G is a group, $a \in G$ and $f: \mathbb{Z} \to \langle a \rangle$ is not injective (ie $\exists\, l, m \in \mathbb{Z}$, $l \neq m$ with $a^l = a^m$).
Then $\langle a \rangle$ is isomorphic to $(\mathbb{Z}_n, +, 0)$. Moreover
$$n = \min \{ m \in \mathbb{Z} \mid m > 0,\ a^m = e_G \}.$$

Definition Let G be a group, $a \in G$. The order of a is defined to be the size of the subgroup $\langle a \rangle$. That is
$$\operatorname{order}(a) = |\langle a \rangle| = \begin{cases} \infty & \text{if } n \mapsto a^n \text{ is injective} \\ n = \min \{ m \in \mathbb{Z} \mid m > 0,\ a^m = e \} & \text{if } n \mapsto a^n \text{ is not injective} \end{cases}.$$

To prove theorem 8.4 we need

Lemma 8.5 Let H be a subgroup of $(\mathbb{Z}, +, 0)$. Then
$H = n\mathbb{Z}$ for some $n \geq 0$.

Proof If $H = \{0\}$, let $n = 0$

Suppose $H \neq \{0\}$. Then $\exists h \in H$ s.t. $h \neq 0$.

Since H is a subgroup, "h^{-1}" $= -h \in H$ as well.

Hence $|h| \in H$.

In particular $S := \{m \in H \mid m > 0\} \neq \emptyset$.

By the well-ordering principle $\exists n \in S$ s.t. $n = \min S$

We now argue that $H = n\mathbb{Z}$.

Note that since $n \in S \subseteq H$, $n\mathbb{Z} = \langle n \rangle \subseteq H$.

Now suppose $h \in H$. By the division algorithm $\exists q, r \in \mathbb{Z}$ s.t.

$h = qn + r$ and $0 \leq r < n$.

Since $h, n \in H$, $r = h - qn \in H$

Since $r < n = \min S$, $r \notin S$. $\Rightarrow r = 0$.

$\Rightarrow h = qn \in n\mathbb{Z}$.

Since h is arbitrary, $H \subseteq n\mathbb{Z}$. Since $n\mathbb{Z} \subset H$,

$\therefore H = n\mathbb{Z}$ □

Proof of 8.4

Since $f: \mathbb{Z} \to G$, $f(m) = a^m$ is not injective. $K = \ker f \neq \{0\}$.

By 8.5, $K = n\mathbb{Z}$ for $n = \min\{m \in \mathbb{Z} \mid m > 0, a^m = e_G\}$

By 8.3 $\bar{f}: n\mathbb{Z} \setminus \mathbb{Z} \to \langle a \rangle$, $\bar{f}(n\mathbb{Z} + \ell) = f(\ell) = a^\ell$

is a well-defined injective map. It's also onto, hence

$\bar{f}: n\mathbb{Z} \setminus \mathbb{Z} \to \langle a \rangle$ is a bijection.

Remains to check that $\bar{f}$ is a homomorphism, ie

$$\bar{f}([k] + [\ell]) = \bar{f}([k]) \cdot \bar{f}([\ell])$$

(where $[k] = n\mathbb{Z} + k$, $[\ell] = n\mathbb{Z} + \ell$ etc)

Now $\bar{f}([k] + [\ell]) = \bar{f}([k + \ell]) = f(k + \ell) = f(k) f(\ell)$

$= \bar{f}([k]) \cdot \bar{f}([\ell])$

f is a homomorphism!

$\therefore \bar{f}: \mathbb{Z}_n \equiv n\mathbb{Z} \setminus \mathbb{Z} \to \langle a \rangle$ is a bijective homomorphism,

hence an isomorphism.

More examples of groups:

Example $O(n) = \{ A \in M_n(\mathbb{R}) \mid A^T A = I \}$ the orthogonal group.

$O(n)$ is a subgroup of $GL(n, \mathbb{R})$.

check $\forall A \in O(n)$ $\quad 1 = \det I = \det A^T A = \det A^T \det A = (\det A)^2$

$\Rightarrow \det A = \pm 1$ and A is invertible.

$\Rightarrow A^{-1} = I A^{-1} = (A^T A) A^{-1} = A^T$

$(\Rightarrow I = A A^{-1} = A A^T.)$

Also, $\forall A, B \in O(n)$

$(AB^{-1})^T (AB^{-1}) = (A B^T)^T (A B^T) = (B^T)^T A^T A B^T$

$= B I B^T = B B^T = I.$

$\therefore$ $O(n)$ is a subgroup of $GL(n, \mathbb{R})$ by the subgroup test:

$(O(n) \neq \emptyset$ and $\forall A, B \in O(n)$, $AB^{-1} \in O(n))$