<u>Last time:</u> A homomorphism $f: H \to G$ is a map between groups that preserves multiplication.

<u>We showed:</u> If $f: H \to G$ is a homomorphism then

(i) $f(e_H) = e_G$

(ii) $f(h^{-1}) = (f(h))^{-1}$

(iii) $f(H) = \{f(h) \mid h \in H\}$ is a subgroup of G.

We defined, for $g \in G$
$$g^n = \begin{cases} \underbrace{g \cdots g}_{n} & \text{if } n > 0 \\ e & \text{if } n = 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{|n|} & \text{if } n < 0 \end{cases}$$

We showed. $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$ is a subgroup of G

It is the image of the homomorphism $f: \mathbb{Z} \to G$, $f(n) = g^n$.

<u>Lemma 12.1</u> Let $\{H_\alpha\}_{\alpha \in A}$ be a collection of subgroups of G. Then $\bigcap_{\alpha \in A} H_\alpha$ is a subgroup of G.

<u>Proof</u> Suppose $a, b \in \bigcap_{\alpha \in A} H_\alpha$. Then $a, b \in H_\alpha$ $\forall \alpha$.

Since H_α is a subgroup, $ab^{-1} \in H_\alpha$ for all α.

$\Rightarrow ab^{-1} \in \bigcap_{\alpha \in A} H_\alpha$

$\Rightarrow \bigcap_{\alpha \in A} H_\alpha$ is a subgroup of G

<u>Application</u> Suppose G is a group and $U \subseteq G$ a subset. Then
$$\langle U \rangle = \bigcap_{\substack{H < G \\ U \subseteq H}} H$$
is a subgroup of G by 12.1.

<u>Note</u> If $K \leq G$ is any subgroup containing U
$$\langle U \rangle = \bigcap_{\substack{H < G \\ U \subseteq H}} H \subseteq K$$
$\therefore$ $\langle U \rangle$ is the smallest subgroup containing U

__Definition__ A set $U \subseteq G$ __generates__ the group G if $\langle U \rangle = G$.

__Ex__ If $U = \{g\}$ and $\langle U \rangle = G$, G is a cyclic group.

__Ex__ S_3 is generated by $\{(12), (23)\}$.

We'll prove later:

S_n is generated by the set of 2-cycles.

__Lemma 12.2__ All subgroups of $\mathbb{Z}$ are cyclic:
If H is a subgroup of $\mathbb{Z}$ then $H = k\mathbb{Z} \equiv \langle k \rangle$ for some $k \geq 0$.
(compare with 2.2.21a of Goodman)

__Proof__ If $H = \{0\}$, then $H = \langle 0 \rangle$.
Suppose $H \neq \{0\}$.
Consider $S = \{n \in H \mid n > 0\}$. __Claim 1__ $S \neq \emptyset$.

__Proof__ Since $H \neq \{0\}$, $\exists\, \ell \in H$ st $\ell \neq 0$. If $\ell > 0$, $\ell \in S$ and $S \neq \emptyset$.
If $\ell < 0$, $-\ell \in H$ since H is a subgroup. $S \neq \emptyset$ since $-\ell \in S$.

By well-ordering S has the smallest element, call it d

__Claim 2__ $H = d\mathbb{Z}$.

__Proof of claim 2__ Given $a \in H \leq \mathbb{Z}$, $\exists\, q, r \in \mathbb{Z}$ s.t.

$$a = q \cdot d + r \quad \text{and} \quad 0 \leq r < d.$$

Since $d \in H$ and H is a subgroup, $q \cdot d = \text{“}d^{q}\text{”} \in H$

$\Rightarrow r = a - q \cdot d \in H$. Since $r < \min S$, $r = 0$.

$\therefore\ a = q \cdot d$ for some $q \in \mathbb{Z}$

$\Rightarrow H \subseteq d\mathbb{Z}$.

Since $d \in H$, $d\mathbb{Z} \subseteq H$. $\therefore\ H = d\mathbb{Z}$. $\square$

Definition A homomorphism $f: H \to G$ between two groups is an **isomorphism** if f is 1-1 and onto.

Remark Suppose $f: H \to G$ is an isomorphism. Then, since f is 1-1 and onto, it has an inverse $h: G \to H$
(so that $h(f(h)) = h \ \forall h \in H$, and $f(h(g)) = g \ \forall g \in G$)

Claim h is also a homomorphism.

Proof We need to check: $\forall a, b \in G$ $h(ab) = h(a)\,h(b)$.
Now since f is onto, $a = f(x)$, $b = f(y)$ for some $x, y \in G$.
$\Rightarrow$ In fact $x = f^{-1}(a) = h(a)$ and $y = f^{-1}(b) = h(b)$.

Now

$$\begin{aligned} h(ab) &= h(f(x)\,f(y)) = h(f(xy)) \quad (f \text{ is a homomorphism}) \\ &= xy \qquad (h = f^{-1}) \\ &= h(a)\,h(b) \end{aligned}$$

$\square$

Definition Let $f: H \to G$ be a homomorphism.
The **kernel** of f is the set

$$\ker f = \{ h \in H \mid f(h) = e_G \}.$$

Proposition 12.3 Let $f: H \to G$ be a homomorphism. Then

$$f(a) = f(b) \iff ab^{-1} \in \ker f$$

Proof

$$\begin{aligned} f(a) = f(b) &\iff f(a)\big(f(b)\big)^{-1} = e_G \\ &\iff f(a)\,f(b^{-1}) = e_G \\ &\iff f(ab^{-1}) = e_G \\ &\iff ab^{-1} \in \ker f. \end{aligned}$$

Corollary 12.4 (compare with 2.4.16 in Goodman)
A homomorphism $f: H \to G$ is 1-1 $\iff$ $\ker f = \{e_H\}$.

Remark $e_H \in \ker f$ since $f(e_H) = e_G$. In fact we'll see soon $\ker f$ is a subgroup of H.

Proof ($\Rightarrow$) Suppose f is 1-1, $a \in \ker f$. Then $f(a) = e_G = f(e_H)$
Since f is 1-1, $a = e_H$. $\Rightarrow$ $\ker f = \{e_H\}$.

($\Leftarrow$) Suppose $\ker f = \{e_H\}$ $a, b \in H$ and $f(a) = f(b)$.

Then (by 12.3) $ab^{-1} \in \ker f = \{e_H\}$. $\Rightarrow ab^{-1} = e_H \Rightarrow a = b$

$\therefore$ f is 1-1. $\square$

Ex $\pi : \mathbb{Z} \to \mathbb{Z}_n$ is a homomorphism. $\ker \pi = \{k \in \mathbb{Z} \mid [k] = [0]\} = n\mathbb{Z} \neq \{0\}$

π is not 1-1.

$f : \mathbb{R} \to \mathbb{R}^\times$ $f(x) = e^x$

$\ker f = \{x \mid e^x = 1\} = \{0\}$. f is 1-1.

Lemma 12.5 Let $f : H \to G$ be a homomorphism. Then

(i) $\ker f$ is a subgroup of H

(ii) $\forall a \in H$ $\forall x \in \ker f$ $axa^{-1} \in \ker f$.

Proof (i) $\forall x, y \in \ker f$, $f(xy^{-1}) = f(x)(f(y))^{-1} = e_G \cdot e_G^{-1} = e_G$

$\Rightarrow xy^{-1} \in \ker f$. $\Rightarrow$ $\ker f$ is a subgroup.

$\forall x \in \ker f$ $\forall a \in H$

$f(axa^{-1}) = f(a) f(x) f(a^{-1}) = f(a) e_G (f(a))^{-1} = f(a) f(a)^{-1} = e_G$.

$\Rightarrow axa^{-1} \in \ker f$.

Definition A subgroup K of a group G is *normal* if $\forall x \in K$ $\forall g \in G$ $gxg^{-1} \in K$

Ex Any subgroup of $\mathbb{Z}$ is normal. $\langle (12) \rangle \in S_3$ is *not* normal.