4.2 (in notes)

$$(G, \underline{\cdot}_G, e_G) \to (H, \underline{\cdot}_H, e_H)$$

Def: Let G, H be groups.

A function $f: G \to H$ is

called a homomorphism if,

$\forall\, x, x' \in G$, (1) $f(x \cdot x') = f(x) \cdot f(x')$.

($x \cdot x'$: G; $f(x) \cdot f(x')$: H)

Remark: If $f: G \to H$ is a homomorphism then automatically

(2) $f(e_G) = e_H$: $\forall\, x \in G$

$f(x)^{-1}$ / $f(x) = f(e \cdot x) = f(e) \cdot f(x)$

$\Rightarrow \quad e_H = f(e_G)$.

(3) $\forall x \in G$, $f(x^{-1}) = f(x)^{-1}$:

$f(x)^{-1} / e_H = f(e_G) = f(x x^{-1}) = f(x) f(x^{-1})$.

$\Rightarrow \quad f(x)^{-1} = f(x)^{-1} f(x) \cdot f(x^{-1})$

$\Rightarrow f(x)^{-1} = f(x^{-1})$.

Example: Let $f: \mathbb{Z}_+ \to \mathbb{Z}_n$ ($+ \bmod n$)

be $f(x) = x \pmod n$.

Then f is a homomorphism:

$$f(x+y) = (x+y) \pmod n$$

$$\overset{\vee}{=} f(x) + f(y) \pmod n$$

$$= \big(x \pmod n + y \pmod n\big) \pmod n$$

Example: Let $m, n \in \mathbb{N}$

and $f : \mathbb{Z}_{nm} \longrightarrow \mathbb{Z}_n$

be $f(x) = x \pmod n$.

To see that f is a homomorphism

write
$$(*) \begin{cases} x = nq_1 + r_1 \\ y = nq_2 + r_2 \\ x+y = nq_3 + r_3 . \end{cases}$$

$$f(x) = r_1 \qquad f(y) = r_2$$

$$f(x+y) = r_3 .$$

$$(**)\begin{cases} f(x)+f(y) = r_1 + r_2 . \\ f(x+y) = r_3 \end{cases}$$

$$(*) \Rightarrow \quad r_1 + nq_1 + r_2 + nq_2 = r_3 + nq_3 .$$

$$\Rightarrow \quad r_1 + r_2 = r_3 \pmod n$$

$$\Rightarrow \quad f(x) + f(y) = f(x+y).$$

Example: $\mathbb{Z}_{nm+1} \longrightarrow \mathbb{Z}_n$

given by $x \longmapsto x \pmod n$.

Exercise: show that this is not a homomorphism.

~~Not~~ Term: $\forall$ gps G, H we have the trivial homomorphism

$$G \longrightarrow H$$
$$x \longmapsto e_H .$$

$$x \longrightarrow e_H$$
$$x \cdot x' \longmapsto e_H \qquad e_H \cdot e_H = e_H$$

$x \mapsto e_H$ $\quad x \longmapsto e_H$

Claim: There is no non-trivial homomorphism $\mathbb{Z}_n \to \mathbb{Z}$.

pf: If there was such

$$f : \mathbb{Z}_n \xrightarrow{\text{mod } n} \mathbb{Z}$$

then $\forall\, 0 \neq x \in \mathbb{Z}_n$

$$nx := \underbrace{x + x + \dots + x}_{n \text{ times}} = 0 \in \mathbb{Z}_n$$

$$0 = f(0) = f(\underbrace{x + x + \dots + x}_{n\text{-times}}) = \underbrace{f(x) + \dots + f(x)}_{n\text{-times}}$$

$$= n \cdot f(x) \in \mathbb{Z}$$

so

$$f(x) = 0.$$

Example: Suppose G is abelian and $H \leq G$.

Then $q : G \to G/H = \{xH \mid x \in G\}$

$$q(x) = xH.$$

q is a homomorphism:

$$q(x \cdot x') = q(x) \cdot q(x')$$

$$x \cdot x' \cdot H = xH \cdot x'H = x \cdot x'H$$

Note also that the inclusion

- $H \hookrightarrow G$ is a gp homomorphism.

$y \longmapsto y$

Example: $\rightarrow G \times H = \{(x,y) \mid \begin{matrix} x \in G \\ y \in H \end{matrix}\}$

$$G \times \{e_H\} = \{(x, e_H) \mid x \in G\}$$

$\hookrightarrow$

$G \longrightarrow G \times \{e_H\} \hookrightarrow G \times H$ $\quad G \rightarrow G \times H$

$x \longmapsto (x, e_H) \hookrightarrow G \times H$

Obs: If $f : G \rightarrow H$, $g : H \rightarrow k$ are gp homomorphisms, then

$g \circ f : G \rightarrow k$ is a homomorphism.

homomorphism.

if $x, x' \in G$

$$(g \circ f)(x \cdot x') = g(f(x \cdot x'))$$

$$= g(f(x) \cdot f(x')) = g(f(x)) \cdot g(f(x'))$$

$$= (g \circ f)(x) \cdot (g \circ f)(x').$$

Recall: $n\mathbb{Z} \leq \mathbb{Z}$

$$\| \{ na \mid a \in \mathbb{Z} \}$$

$$\mathbb{Z}/n\mathbb{Z} = \{ x + n\mathbb{Z} \mid x \in \mathbb{Z} \}$$

$$= \{ 0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z} \}$$

$$(x + n\mathbb{Z}) + (y + n\mathbb{Z})$$

$$= (x+y) \pmod n + n\mathbb{Z}$$

"$=$" $\mathbb{Z}_n$

Def: A homomorphism of gps

$f: G \to H$ is called an isomorphism if it is bijective.

$f: G \xrightarrow{\cong} H \quad (G \cong H)$

Intuition

$G = \{x_1, x_2, x_3\}$

$H = \{f(x_1), f(x_2), f(x_3)\}$

	x_1	x_2	x_3
x_1	x_1x_1	x_1x_2	x_1x_3
x_2	x_2x_1	x_2x_2	x_2x_3
x_3	x_3x_1	x_3x_2	x_3x_3

	$f(x_1)$	$f(x_2)$	$f(x_3)$
$f(x_1)$	$f(x_1)\cdot f(x_1)$ $f(x_1 \cdot x_1)$	$f(x_1x_2)$	$f(x_1x_3)$
$f(x_2)$	$f(x_2x_1)$	$f(x_2x_2)$	$f(x_2x_3)$
$f(x_3$	$f(x_3x_1)$	$f(x_3x_2)$	$f(x_3x_3)$

$\{0+n\mathbb{Z}, \cdots, (n-1)+n\mathbb{Z}\}$

Example: $f: \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}_n$

$\{0, \cdots, n-1\}$

$$x + n\mathbb{Z} \longmapsto x$$

Then f is a homomorphism

$$(x + n\mathbb{Z}) + (y + n\mathbb{Z})$$

$$= (x+y) \pmod n + n\mathbb{Z}$$

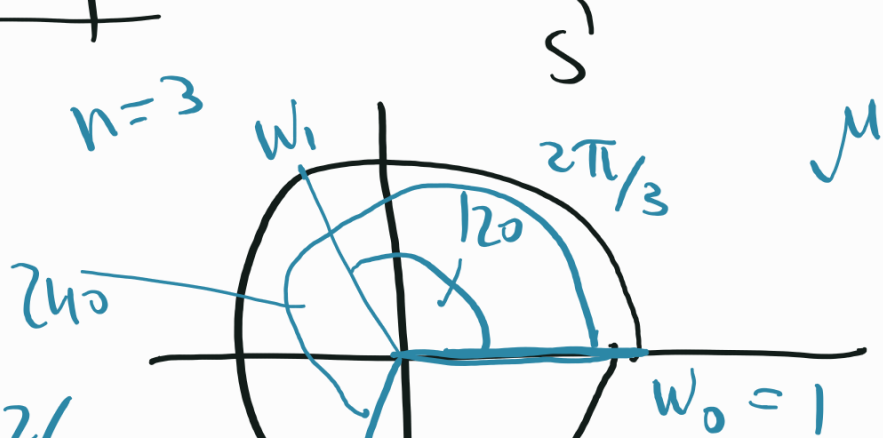
$$\longmapsto (x+y) \pmod n$$

$$= x \pmod n + y \pmod n$$

f is clearly bijective

$$\Rightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

Example: Recall $\mathbb{C}^*$



$\mu_n(\mathbb{C}) = \{x \in \mathbb{C} \mid x^n = 1\}$

Fix n:

$$\Rightarrow w_k = \cos\left(2\pi k/n\right) + i\sin\left(2\pi k/n\right)$$

$$\mu_n(\mathbb{C}) = \{w_0, \dots, w_{n-1}\}.$$

obs: $\forall\, 0 \le k, k' \le n-1$

$$(*)\quad w_k \cdot w_{k'} = \mathrm{cis}\left(2\pi k/n\right) \cdot \mathrm{cis}\left(2\pi k'/n\right)$$

$$= \mathrm{cis}\left(2\pi(k+k')/n\right).$$

Define $f : \mathbb{Z}_{n,\,+_{\bmod n}} \longrightarrow \mu_n(\mathbb{C})$,

$$k \longmapsto w_k.$$

Claim: f is an iso.

Exercise: $f(k +_{\bmod n} k') = f(k)\cdot f(k')$

Rem:

(1) $id_G : G \to G$ is an iso.

$$id_G(x \cdot x') = x \cdot x' =$$

$id_G(x) \cdot id_G(x')$.

(2) $\mathbb{Z}_{nm} \xrightarrow{f} \mathbb{Z}_n$

$x \longmapsto x \pmod n$

$f(x +_{\mod nm} y) \overset{?}{=} f(x) +_{(\mod n)} f(y)$

$x + y = nm \cdot q_3 + r_3$

$x = n \cdot q_1 + r_1$

$y = n \cdot q_2 + r_2$

$f(x +_{\mod nm} y) = f(r_3) = r_3 \pmod n$

$f(x) = r_1$

$f(y) = r_2$

$r_1 + r_2 = r_3 \pmod n$

- $\mathbb{Z}_{nm+1} \xrightarrow{f} \mathbb{Z}_n$

$x \longmapsto x \pmod n$

is not a homomorphism

Prop: if $f: G \to H$ is an iso then so is $f^{-1}: H \to G$.

Proof: Recall the def'n of f^{-1}:

if $y \in H$, since f is bijective $\exists!\ x \in G$ s.th $f(x) = y$.

Then $f^{-1}(y) = x$.

We saw that f^{-1} is bijective.

Left to check: f^{-1} is a gp homomorphism. Let $y, y' \in H$.

Then $\exists!\ x \in G$ s.th $f(x) = y$ ($x = f^{-1}(y)$) and $\exists!\ x' \in G$ s.th $f(x') = y'$ ($x' = f^{-1}(y')$).

Since f is a homomorphism,

$f(\quad) \quad f(x) \cdot f(x') = y \cdot y'$

$f(x \cdot x') = f(x) \cdot f(x') = y \cdot y'$

$\Rightarrow f^{-1}(y \cdot y') = x \cdot x' = f^{-1}(y) \cdot f^{-1}(y')$

Notation: $G \cong H$

Exercise: $H = \{0, 5\} \leq \mathbb{Z}_{10}$

show $\mathbb{Z}_{10}/H \cong \mathbb{Z}_5$.

Def: Let $f : G \to H$ be a homomorphism. (1) The kernel of f is

$$G \geq \ker(f) := \{ x \in G \mid f(x) = e_H \}.$$

(2) The image of f is

$$H \geq Im(f) = \{ f(x) \mid x \in G \}$$

Lemma: (1) $\ker(f) \leq G$

(2) $\mathrm{Im}(f) \leq H$.

Proof: (1) $e \in \ker(f)$

if $x, y \in \ker(f)$ then

$$f(x) = e, \quad f(y) = e$$

$$f(xy) = f(x) \cdot f(y) = e$$

$$\Rightarrow x \cdot y \in \ker(f)$$

if $x \in G$, $f(x^{-1}) = f(x)^{-1}$

So if $x \in \ker(f)$ $f(x^{-1}) = e^{-1} = e$

So $x^{-1} \in \ker(f)$.

(2) suppose $\alpha, \beta \in \mathrm{Im}(f) \subseteq H$

then $\exists\ x, y \in G$ s.t.h

$$\alpha = f(x) \quad \beta = f(y).$$

$$\Rightarrow \alpha \cdot \beta = f(x) \cdot f(y) = f(xy)$$

so $\alpha \cdot \beta \in \mathrm{Im}(f)$.

Also $e \in \mathrm{Im}(f)$

and if $a = f(x) \in \mathrm{Im}$

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

so $a^{-1} \in \mathrm{Im}(f)$. //

Thm (The first isomorphism thm)

Let $f: G \to H$ be a homomorphism of abelian gps and denote $k = \ker(f)$.

Then $G/k \cong \mathrm{Im}(f) \leq H$

Proof: Define

$$f': G/k \to \mathrm{Im}(f)$$

$$G/k = \{xk \mid x \in G\}$$

by $f'(xk) := f(x) \left(\in \mathrm{Im}(f)\right)$

To check that f' is well-defined, suppose $xk = yk$.

Then $xy^{-1} \in k = \ker(f)$.

so $f(xy^{-1}) = e$

$\Leftrightarrow$ $f(x) \cdot f(y)^{-1} = e$

$\Leftrightarrow$ $f(x) = f(y)$.

$\Leftrightarrow$ $f'(xk) = f'(yk)$

so f' is well-defined.

f' is a homomorphism:

$=$

$f' : G/k \longrightarrow Im(f)$

$=$

$xk \longmapsto f(x)$

$xk \longmapsto f(x)$

$\cdot \longrightarrow f(x \cdot x') = f(x) \cdot f(x')$

$x'k \longmapsto f(x')$

Remains to show that f' is bijective.

surj: if $a \in Im(f)$

then $a = f(x)$ for

some $x \in G$ and then

$\bar{f}(xk) = f(x) = a.$

inj: If $\bar{f}(xk) = \bar{f}(yk)$

then $f(x) = f(y)$

$\Leftrightarrow f(xy^{-1}) = e$

$\Leftrightarrow xy^{-1} \in \ker(f) = k$

$\Leftrightarrow xk = yk.$ //

Examples:

$x \mapsto x \pmod n$

(1) $f: \mathbb{Z} \to \mathbb{Z}_n$

$$\ker(f) = \{ x \in \mathbb{Z} \mid x \pmod n = 0 \}$$

$$= n\mathbb{Z}$$

$$\text{Im}(f) = \{ f(x) \mid x \in \mathbb{Z} \}$$

$$= \mathbb{Z}_n$$

$$\Rightarrow \quad \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

(2) Let $f : \mathbb{Z}_{10} \to \mathbb{Z}_2$

be $f(x) = x \pmod 2$.

$$\ker(f) = \{ x \in \mathbb{Z}_{10} \mid x \pmod 2 = 0 \}$$

$$= \{ 0, 2, 4, 6, 8 \} = k$$

$$\text{Im}(f) = \mathbb{Z}_2$$

$$\Rightarrow \quad \mathbb{Z}_{10}/k \cong \mathbb{Z}_2$$

$$k \leq \mathbb{Z}_{10}$$

note: $k \cong \mathbb{Z}_5$

$g : \mathbb{Z}_5 \longrightarrow k$

$g(x) = 2x.$

check g is iso.

"$\mathbb{Z}_{10}/\mathbb{Z}_5 \cong \mathbb{Z}_2$"

(3) $H \leq G$

$q : G \longrightarrow G/H$

$x \longmapsto xH$

$\ker(q) = \{ x \in G \mid q(x) = eH \}$

$\Rightarrow \ker(q) = H.$