Previously in Math 103a

The first isomorphism theorem (but not the last)

Thm $G, \bar{G}$ groups, $\varphi : G \to \bar{G}$ homomorphism. Then $G/\ker\varphi \approx \varphi(G)$,

with isomorphism ψ given by $\psi(g \operatorname{Ker}\varphi) = \varphi(g)$.

Pf: Check first that ψ is well-defined, i.e. if $g_1 \operatorname{Ker}\varphi = g_2 \operatorname{Ker}\varphi$, then $\varphi(g_1) = \varphi(g_2)$.

True! We proved these are equiv.

ψ 1-1 : true since these are equiv. ✓

ψ onto : true since $\varphi(g) = \psi(g \operatorname{Ker}\varphi)$ $\forall g \in G$

Preserves operations: OK since

$$\psi(g_1 \operatorname{Ker}\varphi \cdot g_2 \operatorname{Ker}\varphi) \underset{\substack{\uparrow \\ \text{multiplication} \\ \text{in } G/\ker\varphi}}{=} \psi(g_1 g_2 \operatorname{Ker}\varphi) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$
$$= \psi(g_1 \operatorname{Ker}\varphi)\psi(g_2 \operatorname{Ker}\varphi)$$

Ex $\mathbb{R} \longrightarrow$ unit circle in $\mathbb{R}^2$ with multipl. given by

$\theta \longmapsto (\cos 2\pi\theta, \sin 2\pi\theta)$

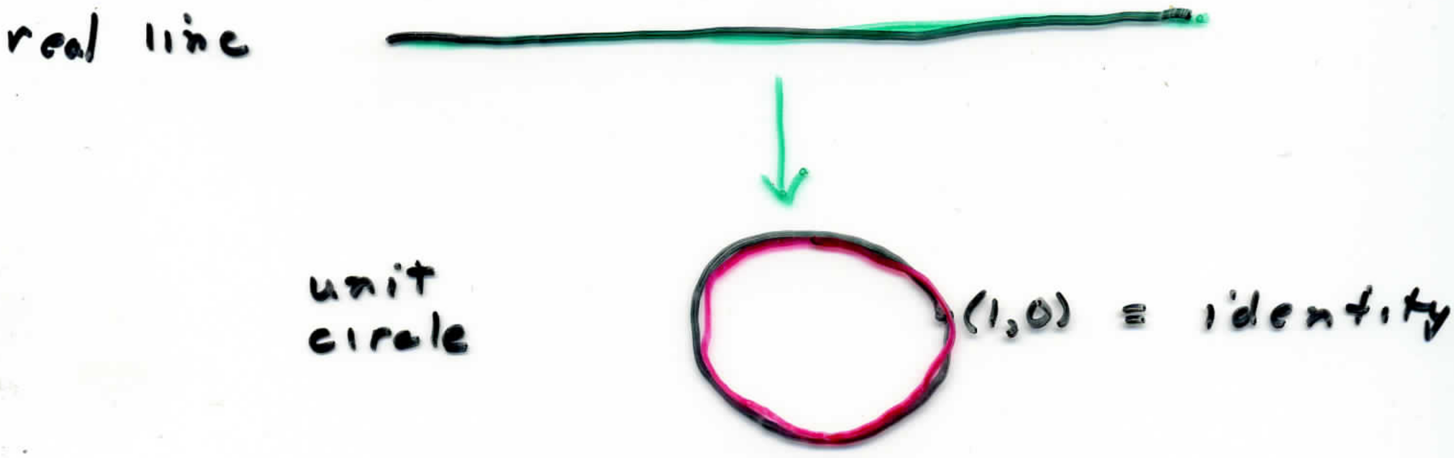
$\ker\varphi = \mathbb{Z}$

$(\cos\theta, \sin\theta)(\cos\theta', \sin\theta')$
$= (\cos(\theta+\theta'), \sin(\theta+\theta'))$

In complex notation
$(e^{i\theta})(e^{i\theta'}) = e^{i(\theta+\theta')}$

$\mathbb{R}/\mathbb{Z} \cong$ unit circle in $\mathbb{R}^2$

by first isomorphism Thm



Line wraps around circle ∞ often.

Thm (Normal subgroups are kernels).

$N \subset G$ normal. Then

$N = \ker \varphi \qquad \varphi : G \longrightarrow \bar{G} = G/N$

given by $\varphi(g) = gN$.

Note: φ is called the natural projection of G onto G/N.

Pf. Same argument as before: φ is 1-1, onto & preserves operations

Uses: $\varphi(g_1) = \varphi(g_2) \Longleftrightarrow g_1 N = g_2 N$

since $N = \ker \varphi$. //

Important: Recall $|\varphi(g)|$ divides $|g|$

Since $|g| \mid |G| \qquad |\varphi(g)|$ divides $|G|$

$\forall\, g \in G$

this is very useful for determining homomorphisms of finite groups.

Ex 1. Is there a homomorphism φ from $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ to $\mathbb{Z}_8$ which is onto?

Ans: No. Take $3 \in \mathbb{Z}_8$. $|3| = 8$ (since 3 & 8 are coprime). If $\phi(a,b) = 3$, $a,b \in \mathbb{Z}_4$, then $|3| = 8$ divides $|(a,b)|$. Since $|(a,b)| = \text{lcm}(|a|,|b|)$ & $|a| \leq 4$, $|b| \leq 4$, this is impossible.

Ex 2. Is there a homormorphism φ from $\mathbb{Z}_{16}$ onto $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

Ans. No, since $\mathbb{Z}_{16}$ cyclic $\Rightarrow \varphi(\mathbb{Z}_{16})$ cyclic, so $\varphi(\mathbb{Z}_{16})$ cannot be $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ for any homomorphism φ.
[$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not cyclic since every $(a,b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ except identity has $|(a,b)| = 2$]

Ex 3. Is there a homomorphism from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_8$?

No If $\varphi(n) = 3 \in \mathbb{Z}_8$, then $8 \mid |n|$

Since $|n| = 1$ or 2 or 4 or 5 or 10 or 20, impossible!

$G, \bar{G}$ finite groups

Ex 4. If $\varphi : G \to \bar{G}$ is a homomorphism onto and if $y \in \bar{G}$ with $|y| = k$, then show $\exists\, x \in G$ with $|x| = k$.

Note: This does not mean that $\exists\, x$, $|x| = k$ & $\varphi(x) = y$.

Ans. Choose $a \in G$ with $\varphi(a) = y$. Then $k \mid |a|$. Since $|a| = |\langle a \rangle|$, k divides $|\langle a \rangle|$. Since $\langle a \rangle$ is cyclic & $k \mid \langle a \rangle$, there is a cyclic subgroup of order $k \subset \langle a \rangle$.

$\therefore\ \exists\, j$ s.t. $|a^j| = k$. (Note: $a^j \in \langle a \rangle \subset G$.)

What value can be taken for j?

Recall: $\mathrm{Inn}(G)$ = group of inner automorphisms of G

Fix $a \in G$, the $g \longmapsto aga^{-1}$ is called an inner automorphism, φ_a

$\varphi_a = \text{identity} \iff aga^{-1} = g \quad \forall\, g \in G$

i.e. $a \in Z(G)$ center of G.

Then

Thm $G/Z(G) \approx \mathrm{Inn}(G)$

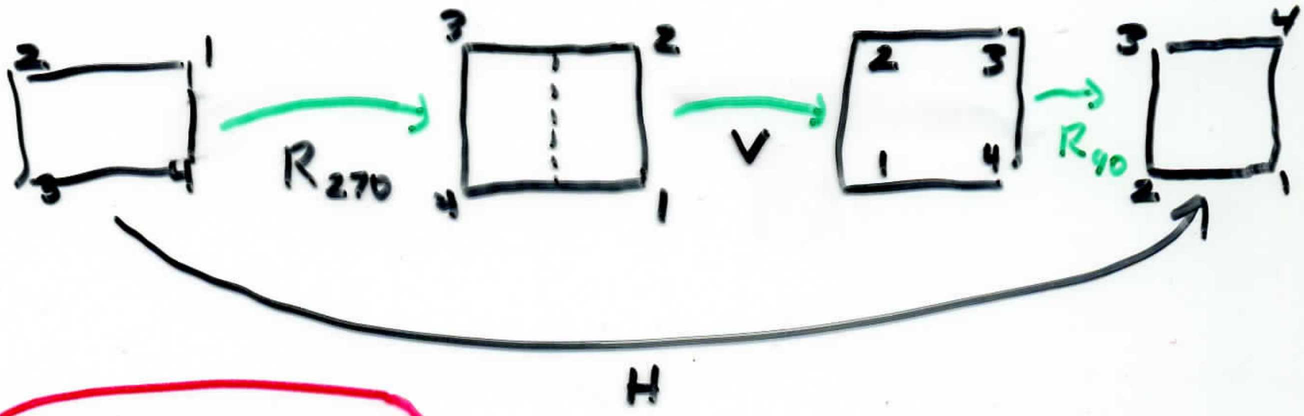
by $a \longmapsto \varphi_a$

Ex. $D_4 / \{R_0, R_{180}\} \approx \mathrm{Inn}(D_4)$.

Inner automorphisms of D_4

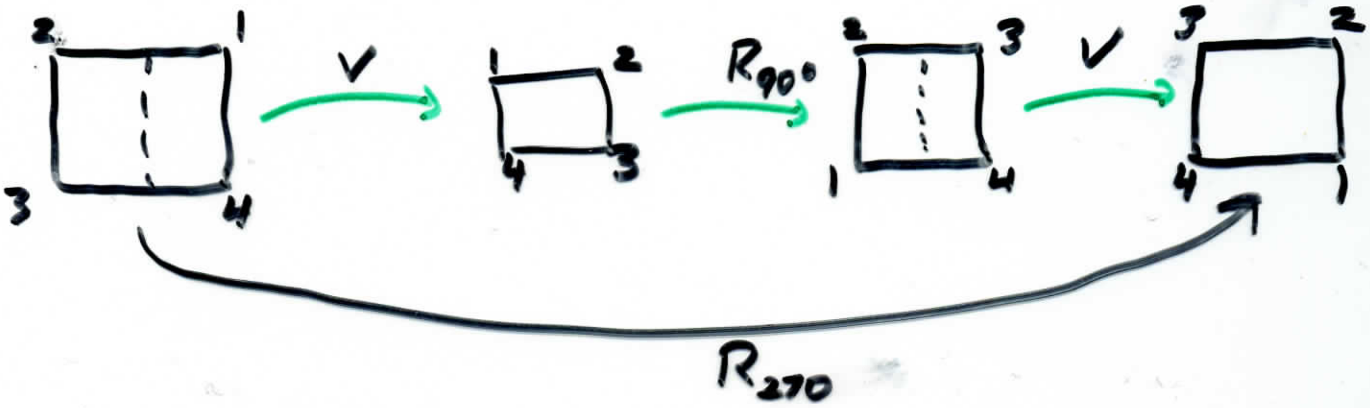
Take $a = R_{90^\circ}$ $a^{-1} = R_{270}$

$a V a^{-1} = ?$



$R_{90} V R_{270} = H$

$V R_{90} V = ?$ (Recall $V = V^{-1}$)



$\therefore\ V R_{90} V = R_{270}$

<u>Note</u>: $\mathrm{Inn}(D_4) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$, so $\varphi_a^2 = id$ $\forall a \in D_4$.

More examples.

Ex 1. If $x \in U(1000)$, then show $x^{100} = 1$

Ans. $U(1000) = U(10^3) \approx U(2^3) \oplus U(5^3)$

$$U(2^3) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$\& \; U(5^3) \approx \mathbb{Z}_{5^3-5^2} = \mathbb{Z}_{100}$$

$y \in U(2^3) \oplus U(5^3)$, then $y = (a,b)$, with

$|a| = 1$ or 2, $|b|$ divides 100

$|(a,b)| = \operatorname{lcm}(|a|,|b|)$, which must divide 100

$$\therefore (a,b)^{100} = 1$$

Since isomorphisms preserve order of elements, $x^{100} = 1 \;\; \forall x \in U(1000)$.

Ex 2 Show that the additive group $\mathbb{R}$ is not isomorphic to the multiplicative group $\mathbb{R}^*$.

Ans Suppose $\varphi: \mathbb{R} \longrightarrow \mathbb{R}^*$ is a homomorphism. Then $\varphi(0) = 1$,

since identity $\longrightarrow$ identity.

If φ is onto, $\exists \; a \in \mathbb{R}$ with $\varphi(a) = -1$. Then $\varphi(2a) = (-1)^2 = 1$

Since $a \neq 0$, then $\varphi(2a) = \varphi(0)$, so φ not 1-1,