• <u>Theorem</u>: (Fundamental Theorem of Homomorphisms).

Let $\varphi: G \to G'$ be an epimorphism. Then the map

$$\psi: G/\ker\varphi \to G'$$
$$a\ker\varphi \mapsto \varphi(a)$$

is an isomorphism.

<u>proof</u>: First need to show well-definedness

Let $g\ker\varphi = h\ker\varphi$. Need to show $\psi(g\ker\varphi) = \psi(h\ker\varphi)$.

Note: $g\ker\varphi = h\ker\varphi$

$\Leftrightarrow h^{-1}g\ker\varphi = \ker\varphi$

$\Leftrightarrow h^{-1}g \in \ker\varphi$.

$\Leftrightarrow g = ha$, $a \in \ker\varphi$ $\Leftrightarrow \varphi(g) = \varphi(h) \Leftrightarrow \varphi(ha) = \varphi(h)$

$\Leftrightarrow \varphi(h) = \varphi(h)$.

$\Rightarrow \psi$ well-defined. ✓

φ homomorphism: $\psi(g\ker\varphi \cdot h\ker\varphi) = \psi((gh)\ker\varphi)$

$= \varphi(gh)$

$= \varphi(g)\cdot\varphi(h)$

$= \psi(g\ker\varphi)\cdot\psi(h\ker\varphi)$. ✓

Injectivity: Need to prove $\ker\psi = \{e\ker\varphi\}$.

Let $g\ker\varphi \in \ker\psi$.

$\psi(g\ker\varphi) = e'$

$\varphi(g) = e'$

$g \in \ker\varphi$

$\Leftrightarrow g\ker\varphi = e\ker\varphi$.

So injective.

Lastly, surjectivity: Let $g' \in G'$. $\underset{\varphi\text{ surj}}{\Rightarrow} \exists\, g$ s.t. $\varphi(g) = g'$. Then $\psi(g\ker\varphi) = \varphi(g) = g'$.

$\Rightarrow g\ker\varphi \mapsto g'$. $\Rightarrow \psi$ surj. $\boxtimes$

ex: $m: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$.

$[x] \longmapsto [2x]$. homomorphism.

$m(\mathbb{Z}_6) = \{[0], [2], [4]\} = G' \cong \mathbb{Z}_3$.

$\varphi: G = \mathbb{Z}_6 \longrightarrow G' = \mathbb{Z}_3$. $\quad \ker\varphi = \{[0], [3]\} \cong \mathbb{Z}_2$

$\psi: \mathbb{Z}_6/\mathbb{Z}_2 \longrightarrow \mathbb{Z}_3 \quad (6 = 2 \cdot 3)$

(by Fundamental Thm of Homomorphisms).

ex: $\varphi: S_n \longrightarrow \mathbb{Z}_2$. epimorphism

even permutation $\longmapsto [0]$

odd permutation $\longmapsto [1]$.

$\ker(\varphi) = \{$even permutations$\} = A_n$ (alternating group).

By Fundamental Thm:

$S_n/A_n \cong \mathbb{Z}_2$

ex: $\mathbb{C} \xrightarrow{\varphi} \mathbb{C}^*$. $\quad e^{2\pi i K} \longmapsto 1$.

$\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^*$

Ker

$$\boxed{\begin{array}{l}\underline{\text{Euler's Formula.}} \\ e^{\theta i} = \cos(\theta) + i\sin(\theta).\end{array}}$$

5.1 Defn of a Ring

• **Defn:** Let R be a set w/ 2 binary operations, denoted by "+" and "·". Then R is a RING if

(1. R is closed under "+") ← redundant b/c "+" is binary.

"+"
2. "+" is associative
3. $\exists$ an additive identity "0" s.t $0+x = x+0 = x, \ \forall x \in R$
4. R has additive inverses: $\exists! -x \in R$ s.t. $x+(-x) = -x+x = 0 \ \forall x \in R$
5. "+" is commutative.

"·"
(6. R is closed under "·")
7. "·" is associative.

"+,·"
8. Two distributive laws hold: $\forall x,y,z \in R$
$$x(y+z) = x\cdot y + xz$$
$$(x+y)z = xz + yz.$$

• **Alternate / condensed Defn of a Ring**
1. R is an abelian group w/ "+"
2. R has associative binary operation "·"
3. Distributive laws hold

ex: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings.

ex: {Even integers} is a ring (w/o multiplicative identity)

ex: Example of a ring w/o mult. identity & w/o "·" commutative.

is $M_{2\times 2}(2\mathbb{Z})$ is a ring!

ex: $\mathbb{Z}_n$ is a ring.

ex: $\{f : [0,1] \to \mathbb{R} \mid f \text{ continuous}\}$

- **Defn:** Let R_2 be a ring. If $R_1 \subset R_2$ is a ring w/ "+" and "·" from R_2, then R_1 is a <u>SUBRING</u>.