Last time: $\mathbb{C}$, $e^{i\theta}$ = rotation by θ, $T(z) = \bar{z}$ reflection

Time before last $N < G$ is normal $\Leftrightarrow$ $gN = Ng$ $\forall g \in G$

If $N \trianglelefteq G$ then G/N is naturally a group with the multiplication

$$(aN)\cdot(bN) := (ab)N$$

Today Homomorphism theorem (see 2.7.6 in Goodman)

Suppose $f: G \to H$ is a homomorphism, $N = \ker f$.

Then $\bar{f}: G/N \to H$, $\bar{f}(gN) = f(g)$ is a well-defined injective homomorphism.

Moreover, if f is onto then $\bar{f}: G/N \to H$ is an isomorphism.

(If f is not onto, $\bar{f}: G/N \to f(G)$ is an isomorphism)

Ex $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is a subgroup of $\mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$

$z_1, z_2 \in S^1 \Leftrightarrow |z_1|, |z_2| = 1$.

and $|z_1 z_2^{-1}| = |z_1|\,|z_2|^{-1} = 1/1 = 1$. So S^1 is a subgroup.

(It's also known as $U(1)$)

Consider the homomorphism $f: \mathbb{R} \to S^1$, $f(\theta) = e^{2\pi i\theta}$

$\ker f = \{\theta \in \mathbb{R} \mid 1 = e^{2\pi i\theta} = \cos(2\pi\theta) + i\sin(2\pi\theta)\}$

$= \mathbb{Z}$.

Homomorphism Thm: $\bar{f}: \mathbb{R}/\mathbb{Z} \to S^1$

$\theta + 2\pi\mathbb{Z} \mapsto e^{2\pi i\theta}$

is an isomorphism.

Ex G = any group, $a \in G$, $H = \langle a \rangle$

We have the homomorphism $f: \mathbb{Z} \to H$, $f(k) = a^k$

If $\ker f = \{0\}$, then f is 1-1, all powers a^k of a are distinct and $f: \mathbb{Z} \to \langle a \rangle$ is an isomorphism.

Otherwise $\ker f \neq \{0\}$.

$\Rightarrow$ $\ker f = n\mathbb{Z}$ for some $n > 0$

Homomorphism theorem $\Rightarrow$ $\bar{f}: \mathbb{Z}/n\mathbb{Z} \to \langle a \rangle$

$\bar{f}([k]) = \bar{f}(k+n\mathbb{Z}) = a^k$ is an isomorphism

ie $\langle a \rangle \simeq \mathbb{Z}_n$ and $n = |\langle a \rangle|$.

<u>Ex</u> 3 $\quad 12\mathbb{Z} \le 4\mathbb{Z}$ is a normal subgroup (since $4\mathbb{Z}$ is commutative). $\Rightarrow 4\mathbb{Z}/12\mathbb{Z}$ is a group.

<u>Claim</u> $\quad 4\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}_3$.

<u>Proof</u> Consider $f: 4\mathbb{Z} \to \mathbb{Z}_3$, $f(n) = [n]$

Then $f(0) = [0]$, $\quad f(4) = [4] = [1]$, $\quad f(8) = [8] = [2]$.

$\Rightarrow f: 4\mathbb{Z} \to \mathbb{Z}_3 = \{[0],[1],[2]\}$ is onto.

$\ker f = \{m \in 4\mathbb{Z} \mid 3 \mid m\} = \{4k \mid 3 \mid (4k)\} = \{4k \mid 3 \mid k\}$

since $3 \nmid 4$ and 3 is prime. ($3 \mid (ab) \Rightarrow 3 \mid a$ or $3 \mid b$)

$\Rightarrow \ker f = \{3 \cdot 4\ell \mid \ell \in \mathbb{Z}\} = 12\mathbb{Z}$

$\Rightarrow \bar{f}: 4\mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}_3$, $\quad \bar{f}(4k + 12\mathbb{Z}) = [4k]$

is a well-defined isomorphism.

<u>Proof of homomorphism Theorem</u>

(1) We first check that $\bar{f}$ is well-defined:

suppose $aN = bN$. Do we know that $f(a) = f(b)$?

$aN = bN \Rightarrow a = bn$ for some $n \in N = \ker f$

$\Rightarrow f(a) = f(b)f(n) = f(b) \cdot e = f(b)$.

$\therefore$ $\bar{f}$ is well-defined

(2) $\bar{f}$ is a homomorphism:

$$\bar{f}((aN)\cdot(bN)) \underset{\uparrow \text{ mult. in } G/N}{=} \bar{f}((ab)N) = f(ab) \overset{f \text{ is a homomorph.}}{=} f(a)f(b) = \bar{f}(aN)\,\bar{f}(bN) \checkmark$$

(3) $\bar{f}$ is 1-1.

$\ker \bar{f} = \{aN \mid \bar{f}(aN) = e\} = \{aN \mid f(a) = e\}$

$= \{aN \mid a \in N\} = \{N\} = \{e_{G/N}\}$

__Recall__ The __product__ of two groups G and H is $G\times H$ with the multiplication defined "coordinate-wise"

$$(g_1,h_1)\cdot(g_2,h_2)=(g_1g_2,\ h_1h_2)$$

__Lemma__ Suppose $f:K\to G$, $l:K\to H$ are two homomorphisms. Then $f\times l: K\to G\times H$, $(f\times l)(k)=(f(k),l(k))$ is also a homomorphism.

Moreover $\ker(f\times l)=\ker f\cap\ker l$.

__Proof__ $(f\times l)(k_1\cdot k_2)=(f(k_1\cdot k_2),\ l(k_1\cdot k_2))$

for any $k_1,k_2\in K$

$$=(f(k_1)\cdot f(k_2),\ l(k_1)\cdot l(k_2))=(f(k_1),l(k_1))\cdot(f(k_2),l(k_2))$$

$$=((f\times l)(k_1))\cdot((f\times l)(k_2)).$$

$\Rightarrow$ $f\times l$ is a homomorphism.

$$\ker(f\times l)=\{k \mid (f(k),l(k))=(e_G,e_H)\}$$
$$=\{k\mid f(k)=e_G,\ l(k)=e_H\}$$
$$=\ker f\cap\ker l$$

$\square$

__Ex__ $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_3$.

__Reason__ $f:\mathbb{Z}\to\mathbb{Z}_2$ $f(k)=[k]_2$ and $l:\mathbb{Z}\to\mathbb{Z}_3$ $l(k)=[k]_3$ are homomorphisms.

$\Rightarrow$ $h:\mathbb{Z}\to\mathbb{Z}_2\times\mathbb{Z}_3$ $h(k)=([k]_2,[k]_3)$ is a homomorphism.

$\ker h=\ker f\cap\ker l=2\mathbb{Z}\cap3\mathbb{Z}=\{k\mid 2|k \text{ and } 3|k\}$
$=6\mathbb{Z}$

$\Rightarrow$ $\bar{f}:\mathbb{Z}/6\mathbb{Z}\to\mathbb{Z}_2\times\mathbb{Z}_3$

$[k]_6\mapsto([k]_2,[k]_3)$ is a homomorphism,

which is 1-1. $|\mathbb{Z}/6\mathbb{Z}|=6=|\mathbb{Z}_2\times\mathbb{Z}_3|$

$\Rightarrow$ $\bar{f}$ is also onto

$\Rightarrow$ $\bar{f}$ is an isomorphism.

<u>Recall</u> $[k] \in \mathbb{Z}_n$ is a unit $\Leftrightarrow \exists\, [l] \in \mathbb{Z}_n$ s.t. $[k]\cdot[l] = [1]$

$\mathbb{Z}_n^\times = \{ [k] \in \mathbb{Z}_n \mid [k]$ is a unit$\}$.

<u>Lemma</u> $(\mathbb{Z}_n^\times, \cdot, [1])$ is a group.

<u>Proof</u> Clearly any $[l] \in \mathbb{Z}_n^\times$ has an inverse.

Need to check: if $[k], [l] \in \mathbb{Z}_n^\times$ then so is $[k][l]$.

$([k]\cdot[l])\cdot([l]^{-1}\cdot[k]^{-1}) = [k][1][k]^{-1} = [1]$, so yes $\square$

<u>Recall</u> $[k] \in \mathbb{Z}_n$ is a unit $\Leftrightarrow$ $\gcd(k,n) = 1$.

The Euler φ function is defined by

$$\varphi(n) = |\mathbb{Z}_n^\times|.$$

<u>Ex</u> If p is prime, $\mathbb{Z}_n^\times = \{[1], [2], \ldots [p-1]\}$. So $\varphi(p) = p-1$.

<u>Note</u> $\varphi(n) = |\{ k \mid \gcd(k,n) = 1,\ 0 < k < n\}|$

<u>Euler's theorem</u> If $\gcd(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \mod n$.

We first will prove:

<u>Lemma</u> Suppose G is a finite group. Then $g^{|G|} = e$

<u>Proof</u> By Lagrange's theorem $|\langle g\rangle| \mid |G|$. $\Rightarrow |G| = |\langle g \rangle| \cdot k$ for some k.

On the other hand, since $\langle g \rangle \cong \mathbb{Z}_n$ where $n = |\langle g \rangle|$

$e = g^n = g^{|\langle g \rangle|}$.

$\Rightarrow g^{|G|} = g^{|\langle g \rangle| k} = \left(g^{|\langle g \rangle|}\right)^k = e^k = e.$ $\square$