Tuesday
9/24

Previously in 5401

If $N \trianglelefteq G$, then G/N is a group using the operation

$$(aN)(bN) = (ab)N$$

Ex: $D_{14} = \{1, r, r^2, r^3, r^4, r^5, r^6, s, sr, sr^2, sr^3, sr^4, sr^5, sr^6\}$

$$H = \langle r \rangle = \{1, r, r^2, r^3, r^4, r^5, r^6\}$$

$$sH = \{s, sr, sr^2, sr^3, sr^4, sr^5, sr^6\}$$

So, $D_{14}/H = \{H, sH\}$

The le
are th
So,

$r^5, sr^6\}$

$, r^6\}$

$r^6\}$

Check that H is normal

left cosets	right cosets
H	H
sH	$Hs = \{s, rs, r^2s, r^3s, r^4s, r^5s, r^6s\}$

$$Hs = \{s, rs, r^2s, r^3s, r^4s, r^5s, r^6s\}$$
$$= \{s, sr^6, sr^5, sr^4, sr^3, sr^2, sr\} = sH$$

The left and right cosets are the same. So, $H \trianglelefteq G$.

So, $D_{14}/H = \{H, sH\}$ is a group.

D_{14}/H	H	sH
H	H	sH
sH	sH	H

$\mathbb{Z}_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

It's the same table!

So, $D_{14}/H \cong \mathbb{Z}_2$.

using $\psi : D_{14}/H \to \mathbb{Z}_2$

$$\psi(H) = \bar{0}$$
$$\psi(sH) = \bar{1}$$

Theorem: Let G be an abelian group and H is a subgroup of G. Then H is normal in G.

proof: Let $g \in G$. Then

$$gH = \{gh \mid h \in H\} \underset{\text{G is abelian}}{=} \{hg \mid h \in H\} = Hg.$$

Ex:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

$$H = \langle 4 \rangle = 4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\} = 0 + 4\mathbb{Z}$$

$$1 + 4\mathbb{Z} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$

$$2 + 4\mathbb{Z} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$

$$3 + 4\mathbb{Z} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

$$\mathbb{Z}/4\mathbb{Z} = \{\underbrace{0 + 4\mathbb{Z}}_{\text{identity}}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$$

$$(2+4\mathbb{Z})+(2+4\mathbb{Z}) = 4+4\mathbb{Z} = 0+4\mathbb{Z}$$

$0+4\mathbb{Z}$

element	order
$0+4\mathbb{Z}$	1
$1+4\mathbb{Z}$	4
$2+4\mathbb{Z}$	2
$3+4\mathbb{Z}$	4

$$1+4\mathbb{Z} \neq 0+4\mathbb{Z}$$
$$(1+4\mathbb{Z})+(1+4\mathbb{Z}) = 2+4\mathbb{Z} \neq 0+4\mathbb{Z}$$
$$(1+4\mathbb{Z})+(1+4\mathbb{Z})+(1+4\mathbb{Z}) = 3+4\mathbb{Z} \neq 0+4\mathbb{Z}$$
$$(1+4\mathbb{Z})+(1+4\mathbb{Z})+(1+4\mathbb{Z})+(1+4\mathbb{Z}) = 4+4\mathbb{Z} = 0+4\mathbb{Z}$$

So,

$\mathbb{Z}/4\mathbb{Z} = \langle 1+4\mathbb{Z} \rangle$ is cyclic.

Thus,

$$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$$

Corollary's to Lagrange's Theorem

Recall: (Lagrange's Thm)
If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Corollary: Let G be a group of size n.
Let $x \in G$.
Then:

1. the order of x divides $|G| = n$
2. $x^{|G|} = 1$

Proof of 1:

Let $H = \langle x \rangle$.

Let $m = |x|$.

Then

$$H = \{1, x, x^2, \ldots, x^{m-1}\}.$$

So, $|H| = m = |x|$.

By Lagrange, $|H|$ divides $|G|$.

So, $|x|$ divides $|G|$.

Proof of 2:

By Part 1, $|G| = |x| \cdot k$ for some k.

So,

$$x^{|G|} = x^{|x| \cdot k} = \left(x^{|x|}\right)^k = 1^k = 1. \quad \blacksquare$$

Corollary: Let G be a group of size p where p is prime. Then $G \cong \mathbb{Z}_p$. So, in particular G is cyclic.

pf: Since p is prime, $p \geq 2$.

So we can pick some $x \in G$ with $x \neq 1$.

By the previous corollary, $|\langle x \rangle|$ divides $|G| = p$.

So either $|\langle x \rangle| = 1$ or $|\langle x \rangle| = p$.

But $|\langle x \rangle| \neq 1$ since $1 \in \langle x \rangle$ and $x \in \langle x \rangle$ and $1 \neq x$.

So, $|\langle x \rangle| = p$. Thus, $G = \langle x \rangle$. So, G is cyclic and $G \cong \mathbb{Z}_p$. $\blacksquare$

Note: Any $x \neq 1$ generates G when G has prime size.

Theorem: Let G be a group and $H \leq G$. Then H is normal in G iff H is the kernel of some homomorphism $\varphi : G \to G'$ where G' is a group.

proof:

($\Longleftarrow$) Let $H = \ker(\varphi)$ where $\varphi : G \to G'$ is a homomorphism. Let's show $H \trianglelefteq G$ by proving $gHg^{-1} \subseteq H$ for all $g \in G$.

Let $y \in gHg^{-1}$.

So, $y = gkg^{-1}$ where $k \in H = \ker(\varphi)$.

Well, we see that

$$
\begin{aligned}
\varphi(y) &= \varphi(gkg^{-1}) \\
&= \varphi(g)\varphi(k)\varphi(g^{-1}) \\
&= \varphi(g)\varphi(k)[\varphi(g)]^{-1} \\
&\underset{\text{Since } k \in \ker(\varphi)}{=} \varphi(g) \cdot \mathcal{1}_{G'} \cdot [\varphi(g)]^{-1} \\
&= \varphi(g)\varphi(g)^{-1} \\
&= \mathcal{1}_{G'}
\end{aligned}
$$

So, $y \in H = \ker(\varphi)$.

Thus, $gHg^{-1} \subseteq H$.

($\Longrightarrow$) Let $H \trianglelefteq G$.

Then G/H is a group.

Define $\varphi : G \to G/H$ by $\varphi(g) = gH$.

This is called the natural or canonical homomorphism.

Let's verify that φ is a homomorphism.

Pick $x, y \in G$.

Then

$$\varphi(xy) = (xy)H \overset{\text{def of operation in } G/H}{=} (xH)(yH) = \varphi(x)\varphi(y).$$

So, φ is a homomorphism.

Furthermore,

$$\ker(\varphi) = \{ g \in G \mid \varphi(g) = H \}$$

H is identity element of G/H

$$= \{ g \in G \mid gH = H \}$$

$$= \{ g \in G \mid g \in H \}$$

$$= H. \quad \blacksquare$$

$aH = bH$ iff $\boxed{a \in bH}$ iff $b^{-1}a \in H$

Ex: $G = \mathbb{Z} \times \mathbb{Z}_2$

Note: $H = \langle (2,\bar{0}) \rangle$

$H = 2\mathbb{Z} \times \{\bar{0}\} = \{\ldots, (-4,\bar{0}), (-2,\bar{0}), (0,\bar{0}), (2,\bar{0}), (4,\bar{0}), \ldots\}$

$(1,\bar{0}) + H = \{\ldots, (-3,\bar{0}), (-1,\bar{0}), (1,\bar{0}), (3,\bar{0}), (5,\bar{0}), \ldots\}$

$(0,\bar{1}) + H = \{\ldots, (-4,\bar{1}), (-2,\bar{1}), (0,\bar{1}), (2,\bar{1}), (4,\bar{1}), \ldots\}$

$(1,\bar{1}) + H = \{\ldots, (-3,\bar{1}), (-1,\bar{1}), (1,\bar{1}), (3,\bar{1}), (5,\bar{1}), \ldots\}$

Fact: If G_1 and G_2 are both abelian then $G_1 \times G_2$ is abelian

So, $\mathbb{Z} \times \mathbb{Z}_2$ is abelian.

Thus, $H \trianglelefteq \mathbb{Z} \times \mathbb{Z}_2$.

$\mathbb{Z}\times\mathbb{Z}_2/H = \{(0,\bar{0})+H,\ (1,\bar{0})+H,\ (0,\bar{1})+H,\ (1,\bar{1})+H\}$ is a group.

element	order
$(0,\bar{0})+H$	1
$(1,\bar{0})+H$	2
$(0,\bar{1})+H$	2
$(1,\bar{1})+H$	2

You can check (by comparing group tables) that $\mathbb{Z}\times\mathbb{Z}_2/H \cong \mathbb{Z}_2\times\mathbb{Z}_2$

$\mathbb{Z}\times\mathbb{Z}_2/H$ is not cyclic since no element of order 4

$(2,\bar{0}) \in (0,\bar{0})+H$

$(1,\bar{1})+H \neq (0,\bar{0})+H$

$[(1,\bar{1})+H]+[(1,\bar{1})+H] = (2,\bar{2})+H = (2,\bar{0})+H = (0,\bar{0})+H$