3/24

- Factor Gps
- 1^{st} Isom   and work sheet
- Aut(G)

Daily Plan 3/19 - will put a deadline to submit today. (Extra Credit)

Factor Groups / Quotient Groups

$H \leq G$ $G/H = \{ \text{cosets} \}$ cosets equiv. classes $a \sim b$ iff $b^{-1}a \in H$.

Ex. $|\mathbb{Z}/n\mathbb{Z}| = n$. each $0 + n\mathbb{Z}$, $1 + n\mathbb{Z}$, $\vdots$, $(n-1) + n\mathbb{Z}$. $b - a \in n\mathbb{Z}$.

$a + n\mathbb{Z} = c + n\mathbb{Z}$
$b + n\mathbb{Z} = d + n\mathbb{Z}$
✓ $a + b + n\mathbb{Z} = c + d + n\mathbb{Z}$.

$H \leq G$ and ask when is this a group.

$gH = xH$ and $kH = yH$, then $gkH = xyH$.

when is $gH * kH = gkH$ well-defined

Theorem $(G/H, *, eH)$ is a group iff $*$ is well-def iff $H \trianglelefteq G$.

②

Pf. $\Rightarrow$ $\underline{H \trianglelefteq G}$

$gH = xH$ and $kH = yH$.

$\underline{x^{-1}g \in H}$, $\underline{y^{-1}k} \in H$.

WTS $(gk)H = (xy)H$ i.e. $(xy)^{-1}gk \in H$

$(xy)^{-1}gk = y^{-1}x^{-1}gk$

$= y^{-1}(x^{-1}g)(yy^{-1})k$

$= [y^{-1}(x^{-1}g)y][y^{-1}k] \in H$.

$\phantom{= [y^{-1}(x^{-1}g)y]}\ \in H \quad \in H$

this is a conjugate of H but $H \trianglelefteq G$ means $\forall t \in G$ $tHt^{-1} = H$

$\blacksquare$

$eH * gH = egH = gH$

$gH * eH = = gH$

$(gH)^{-1} = g^{-1}H$.

$a + n\mathbb{Z} = c + n\mathbb{Z}$ $c - a \in n\mathbb{Z}$

$b + n\mathbb{Z} = d + n\mathbb{Z}$ $d - b \in n\mathbb{Z}$

WTS

$a + b + n\mathbb{Z} = c + d + n\mathbb{Z}$

$c + d - (a+b) \in n\mathbb{Z}$.

$\underbrace{(c-a)}_{\in n\mathbb{Z}} + \underbrace{(d-b)}_{\in n\mathbb{Z}} \in n\mathbb{Z}$.

$\Leftarrow$ the operation is well-defined. WTS $H \trianglelefteq G$.

Let $g \in G$ WTS $\underline{gHg^{-1} \subseteq H}$. Let $h \in H$ $\overset{\text{WTS}}{\underline{ghg^{-1} \in H}}$

$u \in H$

$\underline{hH = eH}$

$gHeH = gH$

$eHgH = gH$ $\Rightarrow$ $hg \in gH$. $\Rightarrow \exists\, h_1 \in H$

$hHgH = hgH$.

$\underline{\underline{hg = gh_1}} \Rightarrow g^{-1}hg = h_1 \in H$.

$\blacksquare$

③

$$G = \langle x, y \mid x^m = e = y^n,\ xy = yx^t \rangle$$

$$y^{-1}xy = x^t \qquad \underline{\langle x \rangle \trianglelefteq G}$$

$$\begin{tikzcd}[column sep=small]
& & D_4 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
& \langle s, r^2 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \langle r \rangle \arrow[d, dash] & \langle sr, r^2 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle s \rangle \arrow[drr, dash] & \langle sr^2 \rangle \arrow[dr, dash] & \langle r^2 \rangle \arrow[d, dash] & \langle sr \rangle \arrow[dl, dash] & \langle sr^3 \rangle \arrow[dll, dash] \\
& & \langle e \rangle & &
\end{tikzcd}$$

$Z(G) = \langle r^2 \rangle \trianglelefteq D_4$

$D_4 / \langle r^2 \rangle$ is a group

Lagrange's order.

$$\left| D_4 / \langle r^2 \rangle \right| = 4$$

$$D_4 / \langle r^2 \rangle \cong \mathbb{Z}_4 \text{ or } \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\begin{tikzcd}[column sep=small]
& Q_8 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle i \rangle \arrow[dr, dash] & \langle j \rangle \arrow[d, dash] & \langle k \rangle \arrow[dl, dash] \\
& \langle -1 \rangle \arrow[d, dash] & \\
& \langle 1 \rangle &
\end{tikzcd}$$

$$Q_8 / \langle -1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

4

$(G, *, e_G), (H, \Delta, e_H)\ (K, \square, e_K)$

homomorphisms : $\varphi_1 : G \to H$; $\varphi_2 : H \to K$

φ_1, φ_2 are hom.

$\forall g_1, g_2 \in G \quad \varphi_1(g_1 * g_2) = \varphi_1(g_1) \Delta \varphi_1(g_2)$

$\forall h_1, h_2 \in H \quad \varphi_2(h_1 \Delta h_2) = \varphi_2(h_1) \square \varphi_2(h_2)$

function comp.

$\varphi_2 \circ \varphi_1 : G \to K$. is a gp. hom.

Let $g_1, g_2 \in G$ $\quad (\varphi_2 \circ \varphi_1)(g_1 * g_2) = \varphi_2(\varphi_1(g_1 * g_2))$

$= \varphi_2(\varphi_1(g_1) \Delta \varphi_1(g_2))$

$= \varphi_2(\varphi_1(g_1)) \square \varphi_2(\varphi_1(g_2))$

$= (\varphi_2 \circ \varphi_1)(g_1) \square (\varphi_2 \circ \varphi_1)(g_2)$. ☒

An isom is a gp. hom. that is a bijection.

Def. An isom from G onto itself. is called an automorphism

$\varphi : G \to G$ isom.

$\S$ $\varphi : G \to G$ an automorphism. $\varphi^{-1} : G \to G$ is also a bij.

also a hom. so φ^{-1} is an automorphism.

$i_G : G \to G \quad i_G(g) = g$ is a hom., bij. so it's an automorphism

identity function

⑤ $\varphi_1 : G \to G$ automorphis

$\varphi_2 : G \to G$

$\varphi_2 \circ \varphi_1 : G \to G$ bijection ✓

automorphism.

Thm The set of automorphisms of a group forms a group under composition.

$$(Aut(G), \circ, \iota_G)$$

Questions?

① is $Aut(G) \cong S_G$

φ hom $\varphi(e_G) = e_H$ | aut $\varphi(e_G) = e_G$

only if $G = \{e_G\}$

② $G \cong Aut(G)$?

$G = \langle g \rangle$. ~~φ~~ $\varphi \in Aut(G)$

$\mathbb{Z}_n$ gcd $(x,n)=1$ gen. $U(n)$

Claim $\langle \varphi(g) \rangle = G$

$\langle \varphi(g) \rangle \leq G$ ✓

$x \in G$. ~~$x \in \langle g \rangle$ $\exists n \in \mathbb{Z}$ $x = g^n$~~

~~$\varphi(g)$~~ φ is surjective $\exists\, y \in G$ s.t. $\varphi(y) = x$

$y \in \langle g \rangle$ $y = g^m$ some $m \in \mathbb{Z}$. $x = \varphi(y) = \varphi(g^m) = \varphi(g)^m$.

⑥ $\underline{Aut(\mathbb{Z})} \cong \underline{\mathbb{Z}_2}$

~~B~~ ~~if~~ $\underline{G = \langle g \rangle}$ if y is a gen. for G.

then $\underline{\exists!}$ ~~hom~~ automorphism $\varphi(g) = y$.

take two gen. g, y.

Define $\varphi : G \to G$ by

$\underline{\varphi(g^n) = y^n}$. ... $\underline{\text{show}}$ φ is 1-1 $\underline{\text{onto}}$

$\varphi(g^n \cdot g^m) = \varphi(g^{n+m}) = y^{n+m} = y^n y^m$ hom

$\underline{= \varphi(g^n) \cdot \varphi(g^m)}$

well-defined
1-1
onto

uniqueness

$|Aut(\mathbb{Z}_n)| = \cancel{\phi}(n)$ $\underline{\text{Euler phi-function}}$

(7)

$\underline{Aut(\mathbb{Q})}$?

$1 \to 5$

$n \to 5n.$

$\psi\ \cancel{\phi}\left(\frac{1}{2}+\frac{1}{2}\right) = \cancel{\psi}(1) = 5$

$\cancel{\psi}\left(\frac{1}{2}\right) + \cancel{\psi}\left(\frac{1}{2}\right)$

$2\cancel{\psi}\left(\frac{1}{2}\right) = 5$

$\cancel{\psi}\left(\frac{1}{2}\right) = \frac{5}{2}$

$\psi\left(\frac{1}{n}\right) = \frac{5}{n}$

$\frac{m}{n} = \frac{5m}{5n}.$

$\cancel{\phi(\quad) = \frac{5m}{5n}}$

$\psi\left(\frac{m}{5}\frac{1}{n}\right) = \frac{m}{n} = \frac{5m}{5n}$

$\psi\left(\frac{m}{5n}\right) = \underline{\frac{m}{n}}$

$$\boxed{\underline{Aut(\mathbb{Q})} \cong \mathbb{Q}}$$

$\cancel{Aut(\mathbb{Z}_n) \cong \mathbb{Z}_n}$

MAS 4301 – $G/Z(G)$

$G/Z(G) = \{$cosets of $Z(G)$

Proposition 0.1. *If $G/Z(G)$ is cyclic, then G is abelian.*

Proof. We suppose that $G/Z(G)$ is cyclic. We want to show that G is abelian, which means

for all $x, y \in G$ $xy = yx$

The hypothesis tells us that For all $a \in G/Z(G)$ / There exists $a \in G/Z(G)$ such that

$< a >= G/Z(G)$. Now, a has the form $gZ(G)$ for some $g \in G$.

Next, let $x, y \in G$. Then $xZ(G) = (gZ(G))^n = g^n Z(G)$ since $< gZ(G) >= G/Z(G)$. Similarly,

$yZ(G) = (gZ(G))^m = g^m Z(G)$ for some $n, m \in \mathbb{Z}$.

It follows that $x = g^{n} z_1$ and $y = g^{m} z_2$ for some $z_1, z_2 \in Z(G)$ and some ~~j, k~~ $n, m \in \mathbb{Z}$.

Then

$$\begin{aligned}
xy &= (g^n z_1)(g^m z_2) && \text{By Substitution} \\
&= g^n (z_1 g^m) z_2 && \text{Since} \\
&= g^n (g^m z_1) z_2 = g^{n+m} z_2 z_1 = g^m g^n z_2 z_1 \\
&= \quad = (g^m z_2)(g^n z_1) \\
&= yx
\end{aligned}$$

□

$H \trianglelefteq G$ G/H group.

$g_1 H * g_2 H = g_1 g_2 H$

$gH * gH = g^2 H$

$(gH)^3 = g^3 H$.

$m(a + n\mathbb{Z})$

$= (ma) + n\mathbb{Z}$

$a + n\mathbb{Z} \oplus a + n\mathbb{Z}$

$= a + a + n\mathbb{Z}$

$2a + n\mathbb{Z}$