Quiz on Thursday will cover material up to Homework 6

Theorem Let $H \leq G$. Then the operation on cosets of H defined by

$$(aH)(bH) = (ab)H \quad \text{is well-defined}$$

if and only if H is a normal subgroup of G.

Corollary: Let H be a normal subgroup of G, denoted by $H \triangleleft G$. Then $G/H = \{aH : a \in G\}$ is a group under the operation

$$(aH)(bH) = (ab)H.$$

Remark G/H is called the quotient group or factor group of G with respect to H.

Proof: Assume H is normal in G, i.e., $aH = Ha$ $\forall a \in G$, i.e., $aHa^{-1} \subseteq H$ $\forall a \in G$

Assume $aH = \hat{a}H$, $bH = \hat{b}H$, i.e., $a^{-1}\hat{a} = h_1 \in H$, $b^{-1}\hat{b} \in H = h_2 \in H$

$\because \hat{b}H = H\hat{b}$ so that $h_1\hat{b} = \hat{b}h_3$ with $h_3 \in H$

$(ab)^{-1}(\hat{a}\hat{b}) = b^{-1}a^{-1}\hat{a}\hat{b}$ ~~$(ab)^{-1}(\hat{a}\hat{b}) \in H$~~ $= b^{-1}(h_1\hat{b}) = \cancel{b^{-1}\hat{b}h_1h_3}\ b^{-1}\hat{b}h_3 = h_2h_3 \in H$

$\therefore$, $(aH)(bH) = (ab)H = (\hat{a}\hat{b})H = (\hat{a}H)(\hat{b}H)$

Conversely. Suppose $H \leq G$, & $(aH)(bH) = (ab)H$ is well-defined.

We will prove that $aHa^{-1} \subseteq H$ for all $a \in G$.

i.e., to show $aha^{-1} \in H$ $\forall h \in H$

Note that $eH = H = hH$ for any $h \in H$.

Then $aH = a(hH) = aH(hH) = (aH)(eH) = (eH)(aH) = (hH)(aH) = (ha)H$

$eH = a^{-1}aH = (a^{-1}ha)H \quad \therefore \quad (e^{-1})(a^{-1}ha) \in H$

$$(e^{-1})(a^{-1}ha) = a^{-1}ha$$

Corollary: **Proof:** (G0) $aH, bH \in G/H$, $(aH)(bH) = (ab)H \in G/H$.

(G1) $((aH)(bH))(cH) = (abc)H = (aH)((bH)(cH))$ $\forall aH, bH, cH \in G/H$.

$G/Z(G) = \{aZ : a \in G\}$

$\text{Inn}(G) = \{g_a : g_a(x) = axa^{-1}\}$.

~~Every aZ~~ define g_a by $\Phi(g_a) = aZ$.

$g_a = g_b \iff axa^{-1} = bxb^{-1}$

$\iff a^{-1}bx = \cancel{ba^{-1}x}\; x a^{-1}b$

$\iff a^{-1}b \in Z$

$\iff aZ = bZ$

1-1 ✓ onto ✓

$\Phi(g_a g_b) = abxb^{-1}a^{-1} = abZ$

$\Phi(g_a)\Phi(g_b)$.

If G is finite $p \mid G$ then G has an element of order p.

Induction on $|G|$. If $|G| = p$ ✓

~~$H \leq G$~~.

~~If~~ H Let $a \in G$, $a \neq e$, $H = \langle a \rangle = G$

② G/H If $p \mid |H|$ ✓

If G/H has $(a^{p}H)^{p} = H$.

$y^{p} \in H = \langle x \rangle$ $\exists$

y^{p} has order q in H

$(y^{q})^{p} = e$ $H = \langle a \rangle$

Onto. Let $aZ \in G/Z$.

Then $\Phi(\phi_a) = aZ$.

Operation preserving:

Note that $\phi_a\phi_b(x) = a(b\,x\,b^{-1})a^{-1} = \cancel{(ba)^{-1}\,x\,ba}$ $\phi_{ab}(x)\ \forall x \in G$

$\Phi(\phi_a\phi_b) = \Phi(\phi_{ab})$ ~~because~~ $= (ab)Z$

$= aZ\,bZ = \Phi(\phi_a)\,\Phi(\phi_b)\ \ \forall \phi_a, \phi_b \in Inn(G)$

$\therefore\ G/Z(G) \cong Inn(G)$.

Correction:

$\phi_a(x) = axa^{-1}$

Change previous part of the proof by this definition of ϕ_a.

$\therefore$ In $Inn(G)$, $\phi_a\phi_b = \phi_{ab}$.

Theorem 9.4. If $G/Z(G)$ is cyclic then G is Abelian.

Proof: Assume G/Z is cyclic $Z = Z(G)$

i.e. $G/Z = \cancel{\{aZ : a \in G\}} = \langle bZ \rangle$

$= \{b^n Z : n \in \mathbb{Z}\}$

$G = \{b^n z : n \in \mathbb{Z},\ z \in Z\}$

So if $x, y \in G$, $x = b^{n_1}z_1$, $y = b^{n_2}z_2$.

Then $xy = b^{n_1}z_1 b^{n_2}z_2 = b^{n_1+n_2}z_2z_1 = b^{n_2}z_2b^{n_1}z_1 = yx$

$\therefore\ xy = yx\ \ \forall x, y \in G$

$\therefore$ G is Abelian.

Remark: We often consider G/Z.

Unfortunately sometimes $Z = \{e\}$ e.g. $G = S_3$

$\mathbb{Z}_2$

$*$	A_n	$S_n - A_n$
A_n	A_n	$S_n - A_n$
$S_n - A_n$	$S_n - A_n$	A_n

$\cong$

$+$	0	1
0	0	1
1	1	0

Example In S_3, the left cosets of $H = \{\varepsilon, (1,2)\}$ $\boxed{\text{do not form}}$ a factor group.

On the other hand, for each $n \geq 2$, S_n/A_n is a group isomorphic to $\mathbf{Z}_2$.

Remarks If G is Abelian (cyclic), then for any $H \leq G$ the factor group G/H is Ablian (cyclic). Factor groups of a cyclic (Abelian) group has the same property.

$(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$

The order of $aH \in G/H$ is the smallest positive integer m such that $a^m \in H$.

Theorems 9.3, 9.4 Let $Z(G)$ be the center of G. $\boxed{\text{Then } G/Z(G) \sim Inn(G).}$

If $G/Z(G)$ is cyclic, then G is Abelian.

Suppose $G = \langle a \rangle$. $H \leq G$ $\quad G/H = \{a^n H : n \in \mathbb{Z}\}$

$= \{(aH)^n : n \in \mathbb{Z}\}$

$= \langle aH \rangle$.

① $\mathbb{Z}_n = \langle 1 \rangle$, $\quad H \leq \mathbb{Z}_n \quad \mathbb{Z}_n/H = \langle 1 + H \rangle$

$\mathbb{Z}_{12} = \langle 1 \rangle \quad H = \langle 3 \rangle = \{3, 6, 9, 0\}$

$\mathbb{Z}_{12}/\langle 3 \rangle = \{1+H, 2+H, \underset{=0+H}{3+H}\} \cong \mathbb{Z}_3$

② $\mathbb{Z} = \langle 1 \rangle$ $\quad H = \langle 3 \rangle = \{3k : k \in \mathbb{Z}\}$

$\mathbb{Z}/H = \mathbb{Z}_3 = \{[0], [1], [2]\}$.

$= \{0+H, 1+H, 2+H\}$

Proof of Theorem 9.3 / 9.4 :

Let $Z(G) = \{x \in G : xa = ax \ \forall a \in G\}$

$Inn(G) = \{\phi_a : \phi_a : G \to G \text{ defined } \phi_a(x) = a^{-1}xa \ \forall x \in G\}$

Note that $Z = Z(G)$ is normal because

$aZ = \{ax : x \in Z\} = \{xa : x \in Z\} = Za \ \forall a \in G$.

To prove $G/Z \cong Inn(G)$

$G/Z = \{aZ : a \in G\}$

$\Phi : Inn(G) \to G/Z$ defined by $\Phi(\phi_a) = aZ$

Well-defined : Every ϕ_a is mapped to $aZ \in G/Z$ $\quad a^{-1}Z = b^{-1}Z$

1-1: If $aZ = \Phi(\phi_a) = \Phi(\phi_b) = bZ$

then $ab^{-1} \in Z$ $\quad \therefore ab^{-1}x = xab^{-1} \ \forall x \in G \quad \therefore a^{-1}xa = b^{-1}xb \quad \forall x \in G$

$\therefore \phi_a = \phi_b$

Theorem 9.5 Let G be a finite Abelian group, and let p be a **prime** factor of $|G|$. Then G has an element of order p.

Proof: ~~Let~~ Let p be a prime. Prove by induction on $|G| = n \geq p$.

Suppose $|G| = p$. ~~a prime~~ Then $G = \langle a \rangle$ & $|a| = p$.

Assume $|G| = mp$ $m > 1$.

Assume the result is true for group of order $< mp$

Consider $e \neq a \in G$ & $H = \langle a \rangle$.

Case 1° If $p \mid |a|$, then we have an element $|a^q| = p$ if $q = \frac{|a|}{p}$

Case 2° If $p \nmid |a|$. then

G/H has order smaller than $|G|$ & is a multiple of p.

By induction assumption, G/H has an element bH of order p. i.e. $(bH)^p = eH$.

$\therefore$ $b^p \in H$.

If $b^p = e$ then b has order p

If not, then $b^p \in H$ has order q for some q

i.e.. ~~b^{pq}~~ $e = (b^p)^q = (b^q)^p$

$\therefore$ b^q has order q .