CH 15. Quotient groups

Thm 1: $H \triangleleft G \Leftrightarrow aH = Ha$ for every $a \in G$

Pf: Assume $H \triangleleft G$. then $\forall a \in G, h \in H$, $aha^{-1} \in H \Rightarrow aHa^{-1} \subset H$

$$\Downarrow$$

$$\left.\begin{array}{r} aH \subset Ha \\ a^{-1}ha \in H \Rightarrow aH \supset Ha \end{array}\right\} \Rightarrow Ha = aH$$

Assume $aH = Ha$. then $\forall a \in G, h \in H$. $ah = h'a$ for $h' \in H \Rightarrow aha^{-1} \in H$ $\Rightarrow H \triangleleft G$

Thm Coset multiplication: $Ha \cdot Hb = H(ab)$. This is well defined if and only if $H \triangleleft G$.

Pf: Assume $H \triangleleft G$. $h_1 a \cdot h_2 b = h_1(ah_2a^{-1}) a \cdot b$ with $h_1(ah_2a^{-1}) \in H$.

So $H \cdot (h_1 a)(h_2 b) = H(ab) \Rightarrow (Ha) \cdot (Hb) = H(ab)$ is well defined:

In other words, $Ha = Hc$ and $Hb = Hd$ imply $H(ab) = H(cd)$.

Conversely, if coset multiplication is well defined, then $Ha \cdot H = Ha$ $\forall a \in G, h \in H$, $Ha \cdot Hh = Hah$

So $a = h'ah$ for $h' \in H \Rightarrow aha^{-1} = h'^{-1} \in H \Rightarrow H \triangleleft G$.

Coset multiplication well defined means: If $Ha = Hc$ and $Hb = Hd$, then $Hab = Hcd$.

Thm: If $H \triangleleft G$, then G/H with coset multiplication is a group.

Pf:
- associativity: $(Ha \cdot Hb) \cdot Hc = Habc = Ha \cdot (Hb \cdot Hc)$
- identity element: $Ha \cdot H = Ha = H \cdot Ha$
- inverse: $Ha \cdot Ha^{-1} = He = H = Ha^{-1} \cdot Ha \Rightarrow (Ha)^{-1} = Ha^{-1}$

Def: If $H \triangleleft G$, then the group G/H is called the quotient group of G by H, or the factor group of G by H.

Thm: G/H is a homomorphic image of G.

Pf: $f: G \to G/H$

$g \mapsto Hg (= gH)$

$$f(g_1 g_2) = Hg_1g_2 = Hg_1 \cdot Hg_2 = f(g_1)f(g_2)$$

Ex: $\mathbb{Z}/\langle n\rangle = \mathbb{Z}_n$. $S_n/A_n = \mathbb{Z}_2$

In practical instances, we can often choose H so as to factor out unwanted properties of G and preserve in G/H only desirable traits.

Ex: Let G be an abelian group and let H consist of all the elements of G which have finite order. $H = \{g \in G;\ \exists k \in \mathbb{Z}\ s.t.\ g^k = e\}$.

Because G is abelian, it's easy to see that H is a normal sbgp.

Prop: In the above situation, for the quotient group G/H, no element except the neutral element has finite order.

Pf: $(Ha)^k = Ha^k = H \Rightarrow a^k \in H \Rightarrow \underset{a^{kn}}{(a^k)^n} = e$ for some $n \in \mathbb{Z}$

$\Rightarrow a \in H \Rightarrow Ha = H$ is the identity element in G/H.

Ex: G is any group. a commutator of G is any element of the form $aba^{-1}b^{-1}$, $a,b \in G$

$aba^{-1}b^{-1} = e \Leftrightarrow ab = ba$

Prop: If $H \lhd G$ and $H \ni aba^{-1}b^{-1}\ \forall a,b \in G$, then G/H is abelian

Pf: $Ha \cdot Hb \cdot (Ha)^{-1}(Hb)^{-1} = Ha \cdot Hb \cdot Ha^{-1}Hb^{-1} = H(aba^{-1}b^{-1}) = H$

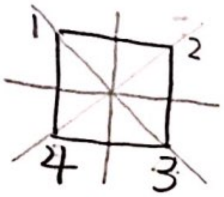
$\Rightarrow Ha \cdot Hb = Hb \cdot Ha\ \forall a,b \in G$ i.e. G/H is abelian.

Exer: 1. $G=\mathbb{Z}_8$, $H=\{\bar{0},\bar{4}\}$.

$G/H=\{H, H+\bar{1}, H+\bar{2}, H+\bar{3}\}$

$+$	H	$H+\bar{1}$	$H+\bar{2}$	$H+\bar{3}$
H	H	$H+\bar{1}$	$H+\bar{2}$	$H+\bar{3}$
$H+\bar{1}$	$H+\bar{1}$	$H+\bar{2}$	$H+\bar{3}$	H
$H+\bar{2}$	$H+\bar{2}$	$H+\bar{3}$	H	$H+\bar{1}$
$H+\bar{3}$	$H+\bar{3}$	H	$H+\bar{1}$	$H+\bar{2}$

A.4 $G=D_4=\langle a,b;\ a^2=b^4=e,\ ba=ab^3\rangle$



$$=\left\{ \underset{e}{\underset{\parallel}{R_0=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}}},\ \underset{b}{\underset{\parallel}{R_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}}},\ \underset{b^2}{\underset{\parallel}{R_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}}},\ \underset{b^3}{\underset{\parallel}{R_3=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}}},\right.$$

$$\left.\underset{a}{\underset{\parallel}{R_4=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}}},\ \underset{ab^2}{\underset{\parallel}{R_5=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}}},\ \underset{ab^3}{\underset{\parallel}{R_6=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}}},\ \underset{ab}{\underset{\parallel}{R_7=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}}}\right\}$$

$H=\{R_0,R_2,R_4,R_5\}=\{e,b^2,a,ab^2\}\triangleleft G$.

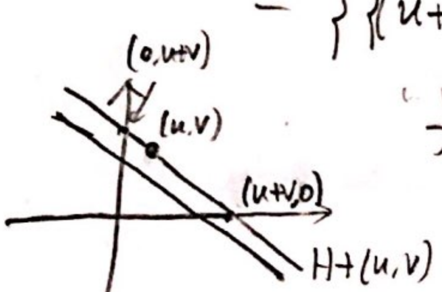
↑ tranformations that presere the diagonal lines

$G/H\cong S_2$ $\quad H\mapsto e$

$\{H, Hb\}$ $\quad Hb\mapsto(12)$ switches horizontal and vertical axis

B. 2. $G=\mathbb{R}\times\mathbb{R}$, $H=\{(x,y): y=-x\}$. G abelian, $H<G$ $\Rightarrow H\triangleleft G$.

$$G/H=\{H+(u,v);\ (u,v)\in\mathbb{R}\times\mathbb{R}\}$$
$$=\{\{(u+x, v-x);\ x\in\mathbb{R}\},\ (u,v)\in\mathbb{R}\times\mathbb{R}\}$$



$f: G/H \overset{\cong}{\to} \mathbb{R}$

$H+(u,v)\longmapsto u+v$

· f is a homomorphism:

$$f((H+(u_1,v_1))+(H+(u_2,v_2))) = f(H+(u_1+u_2, v_1+v_2)) = u_1+u_2+v_1+v_2 = f(H+(u_1,v_1))+f(H+(u_2,v_2))$$

· f is injective: $u+v=0$

$\Rightarrow H+(u,v)=H+(v,-v)+(u,v)$

$=H+(u+v,0)=H+(0,0)=H$.

· f is surjective: $\forall\ u\in\mathbb{R}$, $f(H+(u,0))=u$.

C. 2. $\overset{x^m\in H}{\Rightarrow} (Hx)^m = Hx^m = H \Rightarrow \operatorname{ord}(Hx) \mid m$

Conversely, $\operatorname{ord}(Hx) \mid m \Rightarrow \underset{H}{\underset{\parallel}{(Hx)^m}} = Hx^m \Rightarrow x^m \in H \ \forall x \in G$.

C.4 $\forall\, Hx \in G/H$. $\exists\, Hy$ s.t. $(Hy)^2 = Hy^2 = Hx \Rightarrow$ $\forall x \in G, \exists y \in G$ s.t. $y^2x^{-1} \in G$

$\Downarrow$

$\forall x \in G, \exists y \in G$ s.t. $y^2 x \in G$

Conversely. $\forall\, Hx \in G/H$, $\exists\, y \in G$, s.t. $x^{-1}y^2 \in H$

$\Rightarrow Hx = (Hy)^2$.

G. Suppose $|G| = p^k$. Let C denote the center of G.

1. The conjugacy class of $a = \{a\}$ iff $bab^{-1} = a\ \forall b \in G$ iff $ba = ab\ \forall b \in G$ iff $a \in C$.

2. $|G| = |C| + k_s + k_{s+1} + \cdots + k_t = c + k_s + k_{s+1} + \cdots + k_t$

where $k_s, \cdots, k_t$ are the sizes of all the distinct conjugacy classes of elements $x \notin C$

3. $\forall i \in \{s, s+1, \cdots, t\}$, k_i is equal to a power of p.

Pf: just need to show $k_i \mid |G|$ since $k_i \neq 1$ (not conj. class of any element from the center)

Suppose $k_i = |[x]|$ where $[x] = \{y \in G;\ y = gxg^{-1}$ for some $g \in G\}$

Fact: $[x] \overset{\text{bijective}}{\longleftrightarrow} G/C_xG$ $\quad \underset{C_x}{\underset{\parallel}{C_xG}} = \{g \in G;\ gx = xg\}$.

$gxg^{-1} \longmapsto g.C_xG$

well-defined: $axa^{-1} = bxb^{-1} \Leftrightarrow (b^{-1}a)\cdot x = x(b^{-1}a) \Leftrightarrow b^{-1}a \in C_xG$

and injective $\Updownarrow$

clearly surjective: $axa^{-1} \mapsto aC_x\ \forall a \in G$ $\quad aC_x = bC_x$

$$\Rightarrow |[x]| = |G/C_x| = \frac{|G|}{|C_x|} \Rightarrow |[x]| \,\big|\, |G|$$

$$x \notin C \Rightarrow C_x \neq G \Rightarrow \frac{|G|}{|C_x|} > 1 \overset{|G|=p^k}{\Rightarrow} |[x]| \text{ is a multiple of } p$$

4. $|G| = c + k_s + \cdots + k_t$ $\quad |G| = p^k$, $p \mid k_i$ $i = s, \cdots, t \Rightarrow p \mid c$.

G.5. $|G|=p^2 \overset{G.4}{\Rightarrow} \left.\begin{matrix} p \mid c \\ \text{and } c \mid p^2 \end{matrix}\right\} \Rightarrow c=p$ or $c=p^2$

if $\underset{|C|}{\overset{\shortparallel}{c}}=p^2$ then Center of $G=G \Rightarrow G$ is abelian

if $c=p$, then G/C is a gp. of order $p \Rightarrow G/C$ is cyclic

$\overset{F.4}{\Longrightarrow}$ G is abelian

G.6 $|G|=p^2$. choose $x \neq e \in G$, $|\langle x\rangle| \mid p^2 \Rightarrow |\langle x\rangle|=p$ or $|\langle x\rangle|=p^2$

- $|\langle x\rangle|=p^2 \Rightarrow G=\langle x\rangle$ is cyclic
- $|\langle x\rangle|=p$, G abelian $\Rightarrow \langle x\rangle \triangleleft G \Rightarrow G/\langle x\rangle \cong \mathbb{Z}_p$

Assume G is not cyclic choose $y \notin \underset{H}{\langle x\rangle}$, then $\mathrm{ord}(y)=p$.
$\Downarrow$
$\langle y\rangle \cong \mathbb{Z}_p$

and $yH \neq H \Rightarrow G/H=\langle yH\rangle \cong \mathbb{Z}_p$

Consider the homomorphism $f: \langle x\rangle \times \langle y\rangle \to G$

$(x^i, y^j) \longmapsto x^i y^j$

- f is injective:

$x^{i_1}y^{j_1}=x^{i_2}y^{j_2} \Rightarrow x^{i_1-i_2}=y^{j_2-j_1} \in \langle x\rangle \cap \langle y\rangle$

$(\Rightarrow (yH)^{j_2-j_1}=e \Rightarrow p \mid j_2-j_1 \Rightarrow)\ x^{i_1-i_2}=y^{j_2-j_1}=e$

$\Rightarrow x^{i_1}y^{j_1}=x^{i_2}y^{j_2}$

- f is surjective:

$\forall g \in G$, $gH=(yH)^k=y^kH$

$\Rightarrow g=y^k \cdot x^i=x^iy^k=f(x^i,y^k)$

So f is an isomorphism giving $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$