CHAPTER 3 HW

Sam Chyau
Math 540A

Sec 3.1 # 1, 3, 4, 5, 20, 22a, 36, + A, B, C

1.) Let $\phi: G \to H$ be a Homomorphism. Let $E \leq H$.

a.) Prove: $\phi^{-1}(E) \leq G$

Pf: i.) $\phi(1_G) = 1_H \in E$, so $1_G \in \phi^{-1}(E)$

ii.) Let $x, y \in \phi^{-1}(E)$

$\Rightarrow \phi(x), \phi(y) \in E$

$\Rightarrow \phi(y)^{-1} \in E$

$\Rightarrow \phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} \in E$

$\Rightarrow xy^{-1} \in \phi^{-1}(E)$

$\therefore \phi^{-1}(E) \leq G$ ▨

b.) Prove: If $E \trianglelefteq H$, then $\phi^{-1}(E) \trianglelefteq G$

Pf: Suppose $E \trianglelefteq H$. Let $a \in G$ & $k \in \phi^{-1}(E)$

$\Rightarrow \phi(k) \in E$

$\Rightarrow \phi(aka^{-1}) = \phi(a)\phi(k)\phi(a^{-1}) = \phi(a)\phi(k)\phi(a)^{-1} \in E$, since $E \trianglelefteq H$

$\Rightarrow aka^{-1} \in \phi^{-1}(E)$

$\Rightarrow a\phi^{-1}(E)a^{-1} \subseteq \phi^{-1}(E)$

$\Rightarrow \phi^{-1}(E) \trianglelefteq G$ ▨

c.) Prove: $Ker(\phi) \trianglelefteq G$

Pf: Let $a \in H$

$\Rightarrow a\{1_H\}a^{-1} = \{a1_Ha^{-1}\} = \{aa^{-1}\} = \{1_H\}$

$\Rightarrow \{1_H\} \trianglelefteq H$

$\Rightarrow Ker(\phi) = \phi^{-1}(\{1_H\}) \trianglelefteq G$ ▨

3.) a.) Let A be Abelian & let $B \trianglelefteq A$. Prove A/B is Abelian.

Pf: Let $xB, yB \in A/B$

$\Rightarrow (xB)(yB) = (xy)B = (yx)B = (yB)(xB)$

$\therefore A/B$ is Abelian. ▨

b.) Give an example of a Non-Abelian group G containing a proper normal subgroup N s.t. G/N is Abelian.

Ex.) $G = D_6$, $N = \langle r \rangle = \{1, r, r^2\}$

Since $|G/N| = 6/3 = 2$, we know $N \trianglelefteq D_6$ (so D_6/N is a Group). Also, $D_6/N \cong \mathbb{Z}_2$, since the only group of size 2 (up to isomorphism) is $\mathbb{Z}_2$. $\therefore D_6/N$ is Abelian.

4.) Prove: $(gN)^\alpha = g^\alpha N$ in G/N $\forall\, \alpha \in \mathbb{Z}$

Pf: Let $g \in G$. Let $\alpha \in \mathbb{Z}$

CASE 1: $\alpha \geq 0$. Induct on α

BASIC: $\alpha = 0$

$\Rightarrow (gN)^\alpha = (gN)^0 = N = 1N = g^0 N = g^\alpha N$

INDUCTIVE: Assume $(gN)^\alpha = g^\alpha N$ f.s. $\alpha \geq 0$

$\Rightarrow (gN)^{\alpha+1} = (gN)^\alpha (gN) = (g^\alpha N)(gN) = (g^\alpha g)N = g^{\alpha+1}N$

CASE 2: $\alpha = -1$

$N = 1N = (gg^{-1})N = (gN)(g^{-1}N)$

$\Rightarrow (gN)^\alpha = (gN)^{-1} = g^{-1}N = g^\alpha N$

CASE 3: $\alpha \leq -2$. Let $\beta = -\alpha$ (so $\beta > 0$)

$\Rightarrow (gN)^\alpha = (gN)^{-\beta} = [(gN)^{-1}]^\beta = (g^{-1}N)^\beta = g^{-\beta}N = g^\alpha N$

$\therefore$ $(gN)^\alpha = g^\alpha N$ in G/N $\forall\, \alpha \in \mathbb{Z}$ ▨

5.) Prove: The order of $gN \in G/N$ is n, where n is the least positive integer s.t. $g^n \in N$.

Pf: Let $g \in G$ & $N \trianglelefteq G$. Let n be the least positive integer s.t. $g^n \in N$.

$\Rightarrow (gN)^n = g^n N = N$, since $g^n \in N$

Now suppose $(gN)^m = N$ f.s. $m \in \mathbb{Z}^+$

$\Rightarrow g^m N = N$

$\Rightarrow g^m \in N$

$\Rightarrow n \leq m$

$\Rightarrow |gN| = n$ in G/N ▨

Give an example to show $|gN|$ in G/N may be strictly less than $|g|$ in G.

Ex.) $G = D_6$, $N = \langle r \rangle = \{1, r, r^2\}$, $D_6/N = \{N, sN\}$

$|rN| = |N| = 1$ in D_6/N

$|r| = 3$ in D_6

$\therefore$ $|rN| < |r|$

20.) Let $G = \mathbb{Z}_{24}$ & $\tilde{G} = G/\langle \overline{12} \rangle$, where we write $\tilde{\bar{a}}$ as $\tilde{a}$.

a.) Show $\tilde{G} = \{\tilde{0}, \tilde{1}, \ldots, \tilde{11}\}$

Pf: $\langle \overline{12} \rangle = \{\bar{0}, \overline{12}\}$

$\tilde{0} = \bar{0} + \langle \overline{12} \rangle = \{\bar{0}, \overline{12}\} = \tilde{12}$

$\tilde{1} = \bar{1} + \langle \overline{12} \rangle = \{\bar{1}, \overline{13}\} = \tilde{13}$

$\tilde{2} = \bar{2} + \langle \overline{12} \rangle = \{\bar{2}, \overline{14}\} = \tilde{14}$

$\tilde{3} = \bar{3} + \langle \overline{12} \rangle = \{\bar{3}, \overline{15}\} = \tilde{15}$

$\tilde{4} = \bar{4} + \langle \overline{12} \rangle = \{\bar{4}, \overline{16}\} = \tilde{16}$

$\tilde{5} = \bar{5} + \langle \overline{12} \rangle = \{\bar{5}, \overline{17}\} = \tilde{17}$

$\tilde{6} = \bar{6} + \langle \overline{12} \rangle = \{\bar{6}, \overline{18}\} = \tilde{18}$

$\tilde{7} = \bar{7} + \langle \overline{12} \rangle = \{\bar{7}, \overline{19}\} = \tilde{19}$

$\tilde{8} = \bar{8} + \langle \overline{12} \rangle = \{\bar{8}, \overline{20}\} = \tilde{20}$

$\tilde{9} = \bar{9} + \langle \overline{12} \rangle = \{\bar{9}, \overline{21}\} = \tilde{21}$

$\tilde{10} = \overline{10} + \langle \overline{12} \rangle = \{\overline{10}, \overline{22}\} = \tilde{22}$

$\tilde{11} = \overline{11} + \langle \overline{12} \rangle = \{\overline{11}, \overline{23}\} = \tilde{23}$

$\therefore \tilde{G} = \{\tilde{0}, \tilde{1}, \tilde{2}, \ldots, \tilde{11}\}$ ▨

b.) Find $|\tilde{a}|$ $\forall \tilde{a} \in \tilde{G}$

By Part (c), $\tilde{G} \cong \mathbb{Z}_{12}$ & $\tilde{G} = \langle \tilde{1} \rangle$. So $|\tilde{a}| = \frac{12}{\gcd(a,12)}$

$|\tilde{0}| = \frac{12}{12} = 1$ $\quad |\tilde{4}| = \frac{12}{4} = 3$ $\quad |\tilde{8}| = \frac{12}{4} = 3$

$|\tilde{1}| = \frac{12}{1} = 12$ $\quad |\tilde{5}| = \frac{12}{1} = 12$ $\quad |\tilde{9}| = \frac{12}{3} = 4$

$|\tilde{2}| = \frac{12}{2} = 6$ $\quad |\tilde{6}| = \frac{12}{6} = 2$ $\quad |\tilde{10}| = \frac{12}{2} = 6$

$|\tilde{3}| = \frac{12}{3} = 4$ $\quad |\tilde{7}| = \frac{12}{1} = 12$ $\quad |\tilde{11}| = \frac{12}{1} = 12$

c.) Prove $\tilde{G} \cong \mathbb{Z}_{12}$

Pf: $\langle \tilde{1} \rangle = \langle \bar{1} + \langle \overline{12} \rangle \rangle = \{\langle \overline{12} \rangle, \bar{1} + \langle \overline{12} \rangle, \ldots, \overline{11} + \langle \overline{12} \rangle\}$

$= \{\tilde{0}, \tilde{1}, \ldots, \tilde{11}\}$

$= \tilde{G}$

$\Rightarrow \tilde{G}$ is cyclic of size 12

$\therefore \tilde{G} \cong \mathbb{Z}_{12}$ ▨

22.) Prove if $H \trianglelefteq G$ & $K \trianglelefteq G$, then $H \cap K \trianglelefteq G$

Pf: Assume $H \trianglelefteq G$ & $K \trianglelefteq G$

CLAIM 1: $H \cap K \leq G$

Pf: i.) $1 \in H \wedge 1 \in K$

$\Rightarrow 1 \in H \cap K$

$\Rightarrow H \cap K \neq \emptyset$

ii.) Let $x, y \in H \cap K$

$\Rightarrow x, y \in H \wedge x, y \in K$

$\Rightarrow y^{-1} \in H \wedge y^{-1} \in K$

$\Rightarrow xy^{-1} \in H \wedge xy^{-1} \in K$

$\Rightarrow xy^{-1} \in H \cap K$

$\therefore H \cap K \leq G$

CLAIM 2: $H \cap K \trianglelefteq G$

Pf: Let $g \in G$

$\Rightarrow gHg^{-1} \subseteq H \wedge gKg^{-1} \subseteq K$

$\Rightarrow g(H \cap K)g^{-1} \subseteq H \wedge g(H \cap K)g^{-1} \subseteq K$, since $H \cap K \subseteq H$ and $H \cap K \subseteq K$

$\Rightarrow g(H \cap K)g^{-1} \subseteq H \cap K$

$\therefore H \cap K \trianglelefteq G$ ▨

36.) Prove if $G/Z(G)$ is cyclic, then G is Abelian.

Pf: Assume $G/Z(G)$ is cyclic

$\Rightarrow \exists\, xZ(G) \in G/Z(G)$ s.t. $G/Z(G) = \langle xZ(G) \rangle = \{[xZ(G)]^n : n \in \mathbb{Z}\}$

$= \{\ldots, [xZ(G)]^{-2}, [xZ(G)]^{-1}, Z(G), xZ(G), [xZ(G)]^2, \ldots\}$

$= \{\ldots, x^{-2}Z(G), x^{-1}Z(G), Z(G), xZ(G), x^2Z(G), \ldots\}$

$= \{x^aZ(G) : a \in \mathbb{Z}\}$

$\Rightarrow$ Every element of $G/Z(G)$ is of the form $x^aZ(G)$ f.s. $a \in \mathbb{Z}$

$\Rightarrow$ Every element of G is of the form x^az f.s. $a \in \mathbb{Z}$, $z \in Z(G)$

Now let $g, h \in G$

$\Rightarrow g = x^az_1$ and $h = x^bz_2$ f.s. $a, b \in \mathbb{Z}$ & $z_1, z_2 \in Z(G)$

$\Rightarrow gh = x^az_1x^bz_2 = z_1x^ax^bz_2 = z_1x^{a+b}z_2 = z_1x^{b+a}z_2$

$= z_1x^bx^az_2 = x^bx^az_2z_1 = x^bz_2x^az_1 = hg$

$\therefore G$ is Abelian ▨

A. *Calculate the elements of* $\mathbb{Z}_2 \times \mathbb{Z}_4 / \langle(\bar{0},\bar{1})\rangle$

$$\langle(\bar{0},\bar{1})\rangle = \{(\bar{0},\bar{0}),\ (\bar{0},\bar{1}),\ (\bar{0},\bar{2}),\ (\bar{0},\bar{3})\}$$
$$(\bar{1},\bar{0}) + \langle(\bar{0},\bar{1})\rangle = \{(\bar{1},\bar{0}),\ (\bar{1},\bar{1}),\ (\bar{1},\bar{2}),\ (\bar{1},\bar{3})\}$$

$$\therefore\ \mathbb{Z}_2 \times \mathbb{Z}_4 / \langle(\bar{0},\bar{1})\rangle = \{\langle(\bar{0},\bar{1})\rangle,\ (\bar{1},\bar{0}) + \langle(\bar{0},\bar{1})\rangle\}$$

B.) *Calculate the elements of* $D_8 / \langle s \rangle$

$$\langle s \rangle = \{1, s\}$$
$$r\langle s \rangle = \{r, sr^3\}$$
$$r^2\langle s \rangle = \{r^2, sr^2\}$$
$$r^3\langle s \rangle = \{r^3, sr\}$$

<u>NOTE</u>: $D_8 / \langle s \rangle$ *is a set but* <u>NOT</u> *a group because* $\langle s \rangle \ntrianglelefteq D_8$.

$$\therefore\ D_8 / \langle s \rangle = \{\langle s \rangle,\ r\langle s \rangle,\ r^2\langle s \rangle,\ r^3\langle s \rangle\}$$

C. *Give the order of* $(\bar{2},\bar{1}) + \langle(\bar{1},\bar{1})\rangle$ *in* $\mathbb{Z}_3 \times \mathbb{Z}_6 / \langle(\bar{1},\bar{1})\rangle$

$$\langle(\bar{1},\bar{1})\rangle = \{(\bar{0},\bar{0}),\ (\bar{1},\bar{1}),\ (\bar{2},\bar{2}),\ (\bar{0},\bar{3}),\ (\bar{1},\bar{4}),\ (\bar{2},\bar{5})\}$$

$$(\bar{2},\bar{1})^1 = (\bar{2},\bar{1}) \notin \langle(\bar{1},\bar{1})\rangle$$
$$(\bar{2},\bar{1})^2 = (\bar{1},\bar{2}) \notin \langle(\bar{1},\bar{1})\rangle$$
$$(\bar{2},\bar{1})^3 = (\bar{0},\bar{3}) \in \langle(\bar{1},\bar{1})\rangle$$

$$\therefore\ |(\bar{2},\bar{1}) + \langle(\bar{1},\bar{1})\rangle| = 3 \text{ in } \mathbb{Z}_3 \times \mathbb{Z}_6 / \langle(\bar{1},\bar{1})\rangle$$

Sam Chyau
Math 540A

Sec 3.2 # 4, 5, 8, 16, +18 (Class Example)

4.) Prove: If $|G| = pq$ f.s. primes p & q (not necessarily distinct), then either G is Abelian or $Z(G) = \{1_G\}$.

Pf: Assume $|G| = pq$ f.s. primes p & q.
$\Rightarrow |Z(G)| = 1, pq, p,$ or q by Lagrange.
CASE 1: $|Z(G)| = 1$
Since $1_G x = x 1_G \;\forall x \in G$, we know $1_G \in Z(G)$
$\Rightarrow Z(G) = \{1_G\}$, since the center is trivial.
CASE 2: $|Z(G)| = pq$
$\Rightarrow |Z(G)| = |G|$
$\Rightarrow Z(G) = G$, since G is finite.
$\Rightarrow G$ is Abelian.
CASE 3: $|Z(G)| = p$
$\Rightarrow |G/Z(G)| = |G : Z(G)| = \frac{|G|}{|Z(G)|} = \frac{pq}{p} = q$
$\Rightarrow G/Z(G) \cong \mathbb{Z}_q$ by Lagrange
$\Rightarrow \exists\, aZ(G) \in G/Z(G)$ s.t. $G/Z(G) = \langle aZ(G) \rangle$
$= \{[aZ(G)]^k : k \in \mathbb{Z}\} = \{a^k Z(G) : k \in \mathbb{Z}\}$
$\Rightarrow$ Every element of G is of the form $a^k z$ f.s. $k \in \mathbb{Z}$ & $z \in Z(G)$.
Let $x, y \in G$
$\Rightarrow x = a^h z_1 \wedge y = a^k z_2$ f.s. $h, k \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$
$\Rightarrow xy = (a^h z_1)(a^k z_2) = z_2 a^h a^k z_1 = z_2 a^{h+k} z_1 = z_2 a^{k+h} z_1$
$= z_2 a^k a^h z_1 = (a^k z_2)(a^h z_1) = yx$
$\Rightarrow G$ is Abelian
$\Rightarrow G = Z(G)$
$\Rightarrow |G| = p$, which is CONTRADICTORY.
$\therefore |Z(G)| \neq p$
CASE 4: $|Z(G)| = q$
The same argument of Case 3 shows $|Z(G)| \neq q$

So $|Z(G)| = 1$ or pq. $\therefore Z(G) = \{1_G\}$ or G is Abelian ▨

5.) Let $H \leq G$ & fix $g \in G$

a.) Prove $gHg^{-1} \leq G$ and $|gHg^{-1}| = |H|$

Pf(1):

i.) $gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq G$, since G is closed under the operation & inversion.

ii.) $1_G = g 1_G g^{-1} \in gHg^{-1}$, since $1_G \in H$

$\Rightarrow gHg^{-1} \neq \emptyset$

iii.) Let $x, y \in gHg^{-1}$

$\Rightarrow x = gh_1g^{-1} \wedge y = gh_2g^{-1}$ f.s. $h_1, h_2 \in H$

$\Rightarrow y^{-1} = (gh_2g^{-1})^{-1} = (g^{-1})^{-1} h_2^{-1} g^{-1} = gh_2^{-1}g^{-1}$

$\Rightarrow xy^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = gh_1h_2^{-1}g^{-1} \in gHg^{-1}$, since $h_1h_2^{-1} \in H$

$\therefore gHg^{-1} \leq G$ ▨

Pf (2): Define $\phi_g : H \to gHg^{-1}$ by $\phi_g(h) = ghg^{-1} \ \forall h \in H$

i.) Assume $\phi_g(h_1) = \phi_g(h_2)$

$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$

$\Rightarrow g^{-1}(gh_1g^{-1})g = g^{-1}(gh_2g^{-1})g$

$\Rightarrow h_1 = h_2$

$\therefore \phi_g$ is 1-1.

ii.) Let $k \in gHg^{-1}$

$\Rightarrow k = ghg^{-1}$ f.s. $h \in H$

$\Rightarrow \phi_g(h) = ghg^{-1} = k \in gHg^{-1}$

$\therefore \phi_g$ is Onto

$\therefore |gHg^{-1}| = |H|$ ▨

b.) Prove if H is the unique subgroup of G of order $n \in \mathbb{Z}^+$, then $H \trianglelefteq G$.

Pf: Suppose H is the unique subgroup of G of order $n \in \mathbb{Z}^+$.

By (a), we know $gHg^{-1} \leq G$ and $|gHg^{-1}| = |H| = n$.

$\Rightarrow gHg^{-1} = H$, since H is the <u>ONLY</u> subgroup of G of order n.

$\therefore H \trianglelefteq G$ ▨

8.) Prove if H & K are finite subgroups of G whose orders are coprime, then $H \cap K = \{1_G\}$.

Pf: Suppose $H \leq G$ & $K \leq G$ w/ finite coprime orders. Let $x \in H \cap K$

$\Rightarrow |H| = n$ & $|K| = m$ where $\gcd(m, n) = 1$

$\Rightarrow |x| \mid n \wedge |x| \mid m$, since $x \in H$ and $x \in K$

$\Rightarrow |x| = 1$, since $\gcd(n, m) = 1$

$\Rightarrow x = 1_G$

$\Rightarrow H \cap K = \{1_G\}$ ▨

16.) Use Lagrange's Thm in $\mathbb{Z}_p^\times$ to prove Fermat's Little Thm: If p is prime, then $a^p \equiv a \pmod p$ $\forall\, a \in \mathbb{Z}$.

Pf: Let p be prime. Let $\bar{a} \in \mathbb{Z}_p^\times$

$\Rightarrow |\mathbb{Z}_p^\times| = |\{\bar{k} \in \mathbb{Z}_p : \gcd(k,p)=1\}| = |\{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}| = p-1$

$\Rightarrow |\bar{a}| \mid p-1$ in $\mathbb{Z}_p^\times$ by Lagrange

$\Rightarrow p-1 = n \cdot |\bar{a}|$ in $\mathbb{Z}_p^\times$ f.s. $n \in \mathbb{Z}^+$

$\Rightarrow \bar{a}^{p-1} = \bar{a}^{n|\bar{a}|} = (\bar{a}^{|\bar{a}|})^n = \bar{1}^n = \bar{1}$

$\Rightarrow \bar{a}^p = \bar{a}^{p-1} \cdot \bar{a} = \bar{1} \cdot \bar{a} = \bar{a}$

$\Rightarrow a^p \equiv a \pmod p$ ▨

NOTE: The case of $\bar{a} = \bar{0}$ is trivial, since $\bar{a}^p = \bar{0}^p = \bar{0} = \bar{a}$, so $a^p \equiv a \pmod p$.

18.) Let G be finite. Let $H \leq G$. Let $N \trianglelefteq G$, where $\gcd(|H|, |G/N|) = 1$. Prove $H \leq N$.

Pf: Let $a \in H$. Let $|a| = n$ in G. Let $|aN| = m$ in G/N.

$\Rightarrow n \mid |H|$

CLAIM: $m \mid n$

Pf: Divide m into n by the Division Algorithm, so $\exists!\, q, r \in \mathbb{Z}$ s.t. $n = mq + r$, where $0 \leq r < m$.

$\Rightarrow N = a^n N = (aN)^n = (aN)^{mq+r} = [(aN)^m]^q (aN)^r = N^q (aN)^r = (aN)^r$

$\Rightarrow (aN)^r = N$, where $0 \leq r < m$

But $|aN| = m$ in G/N, so $r = 0$

$\Rightarrow n = mq$

$\Rightarrow m \mid n$, which proves the Claim.

By the Claim & Transitivity, $m \mid |H|$

But $m \mid |G/N|$, since $|aN| = m$ in G/N.

$\Rightarrow m = 1$, since $\gcd(|H|, |G/N|) = 1$

$\Rightarrow aN = N$

$\Rightarrow a \in N$

$\therefore H \leq N$ ▨

Sam Chyau
Math 540A

Sec 3.3 #A, B, C

For A & B, find groups that the following are isomorphic to and use the First Isomorphism Thm to prove it.

A. $\mathbb{Z}_2 \times \mathbb{Z}_4 / \langle(\bar{0}, \bar{1})\rangle$. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_4$. Let $H = \langle(\bar{0}, \bar{1})\rangle$

CLAIM: $G/H \cong \mathbb{Z}_2$

Pf: Define $\phi: G \to \mathbb{Z}_2$ by $\phi((\bar{a}, \bar{b})) = \bar{a}$ $\forall (\bar{a}, \bar{b}) \in G$

1.) ϕ is a Homomorphism:

a.) Let $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$ in G
$\Rightarrow \bar{a} = \bar{c}$
$\Rightarrow \phi((\bar{a}, \bar{b})) = \phi((\bar{c}, \bar{d}))$
$\therefore \phi$ is Well-Defined

b.) Let $(\bar{a}, \bar{b}), (\bar{c}, \bar{d}) \in G$
$\Rightarrow \phi((\bar{a}, \bar{b}) + (\bar{c}, \bar{d}))$
$= \phi((\bar{a} + \bar{c}, \bar{b} + \bar{d}))$
$= \phi((\overline{a+c}, \overline{b+d}))$
$= \overline{a+c} = \bar{a} + \bar{c}$
$= \phi((\bar{a}, \bar{b})) + \phi((\bar{c}, \bar{d}))$

2.) $Ker(\phi) = H$:
$Ker(\phi) = \{(\bar{a}, \bar{b}) \in G : \phi((\bar{a}, \bar{b})) = \bar{0}\} = \{(\bar{a}, \bar{b}) \in G : \bar{a} = \bar{0}\}$
$= \{(\bar{0}, \bar{b}) \in G : \bar{b} \in \mathbb{Z}_4\} = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{0}, \bar{3})\}$
$= \langle(\bar{0}, \bar{1})\rangle = H$

3.) ϕ is Onto (i.e. $Im(\phi) = \mathbb{Z}_2$):
$\phi((\bar{0}, \bar{0})) = \bar{0} \wedge \phi((\bar{1}, \bar{0})) = \bar{1}$
$\therefore \phi$ is Onto (so $Im(\phi) = \mathbb{Z}_2$)

$\therefore$ By the F.I.T., $\mathbb{Z}_2 \times \mathbb{Z}_4 / \langle(\bar{0}, \bar{1})\rangle = G/H \cong Im(\phi) = \mathbb{Z}_2$ ▨

B. $\mathbb{Z} \times \mathbb{Z} / \langle(1, 2)\rangle$. Let $G = \mathbb{Z} \times \mathbb{Z}$. Let $H = \langle(1, 2)\rangle$

CLAIM: $G/H \cong \mathbb{Z}$

Pf: Define $\phi: G \to \mathbb{Z}$ by $\phi((a, b)) = b - 2a$ $\forall (a, b) \in G$

1.) ϕ is a Homomorphism: Let $(a, b), (c, d) \in G$
$\Rightarrow \phi((a, b) + (c, d)) = \phi((a+c, b+d)) = (b+d) - 2(a+c)$
$= b + d - 2a - 2c = (b - 2a) + (d - 2c) = \phi((a, b)) + \phi((c, d))$

2.) $Ker(\phi) = H$:
$Ker(\phi) = \{(a, b) \in G : \phi((a, b)) = 0\} = \{(a, b) \in G : b - 2a = 0\}$
$= \{(a, b) \in G : b = 2a\} = \{(a, 2a) : a \in \mathbb{Z}\}$
$= \{\ldots, (-2, -4), (-1, -2), (0, 0), (1, 2), (2, 4), \ldots\} = H$

3.) ϕ is Onto (i.e. $Im(\phi) = \mathbb{Z}$):
For any $b \in \mathbb{Z}$, $\phi((0, b)) = b - 2(0) = b \in \mathbb{Z}$, so ϕ is Onto

$\therefore$ By the F.I.T., $\mathbb{Z} \times \mathbb{Z} / \langle(1, 2)\rangle = G/H \cong Im(\phi) = \mathbb{Z}$ ▨

C. Let $H \trianglelefteq G$ & $H' \trianglelefteq G'$. Let $f: G \to G'$ be a homomorphism. Show f induces a natural homomorphism $g: G/H \to G'/H'$ if $f(H) \subseteq H'$.

Pf: Let $H \trianglelefteq G$ & $H' \trianglelefteq G'$. Let $f: G \to G'$ be a homomorphism. Define $g: G/H \to G'/H'$ by $g(aH) = f(a)H'$, where $f(H) \subseteq H'$

1.) Suppose $aH = bH$

$\Rightarrow \quad a^{-1}b \in H$

$\Rightarrow f(a)^{-1} f(b) = f(a^{-1}) f(b) = f(a^{-1}b) \in f(H) \subseteq H'$

$\Rightarrow f(b)H' = f(a)H'$

$\Rightarrow g(bH) = g(aH)$ $\therefore$ g is Well-Defined.

2.) Let $aH, bH \in G/H$

$\Rightarrow g((aH)(bH)) = g((ab)H) = f(ab)H' = (f(a)f(b))H'$

$= (f(a)H')(f(b)H') = g(aH)\, g(bH)$

$\therefore$ g is a homomorphism.

$\therefore$ f induces a natural homomorphism $g: G/H \to G'/H'$ ▨

Sam Chyau
Math 540A

Sec 3.5 #2

2) Prove: σ^2 is an Even Permutation $\forall\ \sigma \in S_n$

Pf: Let $\sigma \in S_n$ be decomposed into a product of m transpositions, so $\sigma = \underbrace{(x_1, x_2)(x_3, x_4)\cdots(x_{k-1}, x_k)}_{m}$

$\Rightarrow \sigma^2 = \underbrace{(x_1, x_2)(x_3, x_4)\cdots(x_{k-1}, x_k)}_{m}\underbrace{(x_1, x_2)(x_3, x_4)\cdots(x_{k-1}, x_k)}_{m}$

$\Rightarrow \sigma^2$ is the product of 2m transpositions

$\Rightarrow \sigma^2$ is Even $\blacksquare$