Midterm 1

Math 113, Abstract Algebra, Spring 2017

Name:

You may use the backs of the pages if needed. There are ***five*** *pages and* ***four*** *problems, the* ***last page*** *is a* ***blank*** *page for extra space or rough work. You may use any Theorem/Lemma etc. covered in class, in our text, or from homework.*

Problem 1. (15 points.) Let G be a group with $|G| = pq$ where $\gcd(p, q) = 1$. Suppose that there exists elements $a \in G$ and $b \in G$ such that $ab = ba$. Also suppose that $|a| = p$ and $|b| = q$. Show that G is abelian. [*Hint: it may help to consider some, or all, of the subgroups* $\langle a\rangle$, $\langle b\rangle$, $\langle ab\rangle$.]

There are two general approches that could work here, I will decribe both below.

Proof(1): we will first show $G = \langle ab\rangle$.

Note that $(ab)^{pq} = a^{pq} b^{pq}$ since $ab = ba$, so we have that

$$(ab)^{pq} = a^{pq} b^{pq} = (a^p)^q (b^q)^p \underbrace{=}_{\text{since } |a|=p,\ |b|=q} e^q \cdot e^p = e.$$

Suppose that $|\langle ab\rangle| = |ab| = n$, then by Proposition 4.12 $n \mid pq$.

So $(ab)^n = e$, but $(ab)^n = a^n b^n$ (again since $ab = ba$)

$\therefore$ $a^n b^n = e$, now raise both sides to the power p

$\Rightarrow (a^n b^n)^p = e^p = e \Rightarrow a^{np} \cdot b^{np} = e$

but $a^{np} \cdot b^{np} = \underbrace{(a^p)^n}_{= e \text{ (since } |a|=p)} b^{np}$ $\therefore$ $b^{np} = e$. we know $|b| = q$

so then (again by Prop. 4.12, applied to $\langle b\rangle$) we have $q \mid np$, but $\gcd(q, p) = 1 \Rightarrow q \mid n$.

Again consider $a^n b^n = e$, this time raise both sides to the power q

$\Rightarrow (a^n b^n)^q = e^q = e \Rightarrow a^{nq} \cdot b^{nq} = e$

but $a^{nq} \cdot b^{nq} = a^{nq} \underbrace{(b^q)^n}_{= e \text{ (since } |b|=q)}$ $\therefore$ $a^{nq} = e$. we know $|a| = p$

Applying Prop. 4.12 to $\langle a\rangle$ we have that $p \mid nq \Rightarrow p \mid n$ (since $\gcd(q,p) = 1$)

$\therefore$ $p \mid n$ and $q \mid n \Rightarrow pq \mid n$, but since $a \neq e$, $b \neq e$ and since $|ab| = n \leq pq$ (otherwise G would not be closed, and hence not a group) then we have that $|ab| = pq$ $\therefore$ $|\langle ab\rangle| = |G|$

$\therefore$ $G = \langle ab\rangle$, meaning G is a cyclic group and is, hence, abelian by Theorem 4.9.

Proof #2: Let $H_1 = \langle a\rangle$, $H_2 = \langle b\rangle$. Since $ab = ba$ and since H_1, H_2 are cyclic and are generated by a, and b respectivley, we have that $hg = gh$ $\forall h \in H_1, g \in H_2$

On an assignment I would like some more justification of this statement, but didn't reqire it for an exam setting, since it is fairly clear, i.e. since ab=ba, and it is powers of these.

we note that $H_1 \cap H_2 = \{e\}$ since if $h \in H_1$, and $h \in H_2$ then $|h| \mid |a|$, and $|h| \mid |b| \Rightarrow |h| \mid \underbrace{\gcd(|a|, |b|)}_{=1}$ $\therefore$ $|h| = 1$

Hence, $G = H_1 H_2$, that is G is the internal direct product of H_1 and H_2, since this product is defined and $|G| = |H_1 H_2| = pq$. ∎

Problem 2. (15 points.) Let G be a group, N a normal subgroup of G, and H a subgroup of G. Suppose that N is a subgroup of H. Show that H/N is a normal subgroup of G/N if and only if H is a normal subgroup of G using the following steps.

(i) Show that H/N is always a subgroup of G/N whenever H is a subgroup of G.

H/N is a subset of G/N by definition since H is a subset of G

Let $h_1N, h_2N \in H/N$ ($h_1, h_2 \in H$ by definition) we have, $h_1N(h_2N)^{-1} = (h_1h_2^{-1})N$ and H is a group $\therefore h_1h_2^{-1} \in H \therefore (h_1h_2^{-1})N \in H/N$.

So H/N is a subgroup of G/N by Proposition 3.31.

(ii) Suppose H is a normal subgroup of G, show H/N is a normal subgroup of G/N.

Let $gN \in G/N$, $hN \in H/N$ be arbitrary. Then

$$gN(hN)(gN)^{-1} = ghg^{-1}N$$

but H is a normal subgroup, so $ghg^{-1} \in H \Rightarrow ghg^{-1}N \in hN$

$\therefore gN\, H/N\, (gN)^{-1} \subset H/N \therefore H/N$ is a normal subgroup of G/N by Theorem 10.3, part 3.

(iii) Suppose H/N is a normal subgroup of G/N, show H is a normal subgroup of G.

H/N normal in $G/N \Rightarrow \quad gN\, H/N\, (gN)^{-1} \subseteq H/N$

$$= gN\,hN(gN)^{-1} \in H/N \quad \forall h \in H, g \in G$$

Fix an arbitrary $g \in G$, $h \in H$ then, by the above, $\exists\ \tilde{h}N \in H/N$ ($\tilde{h} \in H$) such that

$$gN\,hN(gN)^{-1} = \tilde{h}N$$

$$\therefore (ghg^{-1})N = \tilde{h}N, \text{ so for some } n \in N$$

$ghg^{-1} = \tilde{h}n$, but N is a subgroup of H, so $\tilde{h}n \in H$

$\therefore ghg^{-1} = h' \in H \quad \forall g \in G, h \in H$

$\therefore gHg^{-1} \subseteq H \therefore H$ is a normal subgroup of G.

Problem 3. (15 points)

(i) [7 points.] Let G be a group with $|G| = 25$. Prove that either $G \cong \mathbb{Z}/25\mathbb{Z}$ or all elements $g \in G$ are such that $g^5 = e$ where e is the identity in G.

If $g \in G \Rightarrow |g| \mid 25 \Rightarrow |g| = 1, 5, 25$

If $|g| = 25 \Rightarrow G = \langle g \rangle$, and $\therefore$ $G \cong \mathbb{Z}_{25} \cong \mathbb{Z}/25\mathbb{Z}$.

If no g is such that $|g| = 25$ then G cannot by cyclic

$\therefore$ $g^5 = e$ $\forall g \in G$.

(ii) [8 points.] Describe all possible homomorphisms $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$.

The possible $\ker(\phi)$'s are: $\{0\}$, $\langle 2 \rangle$, $\mathbb{Z}_4$

Possible $\phi(\mathbb{Z}_4)$: $\{(0,0)\}$, $\langle (1,0) \rangle$, $\langle (0,1) \rangle$, $\langle (1,1) \rangle$, $\mathbb{Z}_2 \times \mathbb{Z}_2$

Since $\mathbb{Z}_4$ is <u>not</u> isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ $\phi(\mathbb{Z}_4)$ cannot be $\mathbb{Z}_2 \times \mathbb{Z}_2$

All others work.

$\therefore$ possible hom. are:

$\phi_1 : n \mapsto (0,0)$ $\quad$ $Im(\phi_1) = \{(0,0)\}$, $\ker \phi_1 = \mathbb{Z}_4$

$\phi_2 : n \mapsto (n,0)$ $\quad$ $Im(\phi_2) = \langle (n,0) \rangle$, $\ker \phi_2 = \langle 2 \rangle \leq \mathbb{Z}_4$

$\phi_3 : n \mapsto (0,n)$ $\quad$ $Im(\phi_3) = \langle (0,n) \rangle$, $\ker \phi_3 = \langle 2 \rangle \leq \mathbb{Z}_4$

$\phi_2 : n \mapsto (n,n)$ $\quad$ $Im(\phi_2) = \langle (n,n) \rangle$, $\ker \phi_4 = \langle 2 \rangle \leq \mathbb{Z}_4$

Problem 4. (15 points.)

(i) [7 points.] Consider the subgroup $H = \{5^m 7^n \mid m, n \in \mathbb{Z}\}$ of $\mathbb{Q}^*$. Show that $H \cong \mathbb{Z} \times \mathbb{Z}$.

Define $\phi : H \to \mathbb{Z} \times \mathbb{Z}$
$: 5^m 7^n \mapsto (m, n)$

Let $g = 5^m 7^n$, $h = 5^l 7^k$ be arbitrary elements of H.

1-1: If $\phi(g) = \phi(h) \Rightarrow (m,n) = (l,k)$
$\Rightarrow m = l,\ n = k$
$\Rightarrow 5^m 7^n = 5^l 7^k$
$\Rightarrow g = h \quad \therefore$ 1-1.

Onto: If $(n,m) \in \mathbb{Z} \times \mathbb{Z} \Rightarrow (n,m) = \phi(5^n 7^m)$

homomorphism: $\phi(gh) = \phi(5^m 7^n 5^l 7^k) = \phi(5^{m+l} 7^{n+k})$
$= (m+l, n+k)$
$= (m,n) + (l,k) = \phi(g) + \phi(h)$

(i) [8 points.] Let G be a finite group, N a normal subgroup of G and let $w \in G$. If $\gcd(|w|, |G/N|) = 1$ show that $wN = N$.

Proof: Consider the element $wN \in G/N$, first show that $|wN| \mid |w|$, that is the order of $wN \in G/N$ divides the order of $w \in G$. Let $r = |w|$, working in $\langle wN \rangle$ (or in G/N) we have $(wN)^r = w^r N = eN = N$, so we have $|\langle wN \rangle| \mid r$ by Proposition 4.12, since $(wN)^r = N$ ← identity. Hence $|wN|$ divides $|w|$.

Therefore $\gcd(|w|, |G/N|) = 1$ implies $\gcd(|wN|, |G/N|) = 1$ but $wN \in G/N$, so by Lagrange's Theorem $|wN| \mid |G/N|$.
If $l = |wN|$ is s.t. $\gcd(l, |G/N|) = 1$ and $l \mid |G/N|$
$\Rightarrow l = 1 \quad \therefore \langle wN \rangle = 1$, hence $w \in N$ and $wN = N$ since N is normal.