Student: Yu Cheng (Jade)

Math 412

Worksheet #3

August 04, 2010

Worksheet #3

Question 1: Let G be a group and fix an element $a \in G$. Show that the map $\gamma : G \to G$ by $\gamma(x) = a^{-1}xa$ is an automorphism. (This map is called *conjugation* by a.)

Answer: We need to prove two conditions, γ is a one-to-one map and γ is a homomorphism. Then, we can conclude that γ is an isomorphism over itself, and thus γ is an automorphism.

We will first show γ is a *one-to-one* map. Let $x_1, x_2 \in G$, and $a^{-1}x_1a = a^{-1}x_2a$.

$$a^{-1}x_1a = a^{-1}x_2a$$

$$\Rightarrow aa^{-1}x_1aa^{-1} = aa^{-1}x_2aa^{-1}$$

$$\Rightarrow x_1 = x_2 .$$

Now we will show that γ is a *homomorphism* from G to itself. Let $x_1, x_2 \in G$

$$\gamma(x_1x_2) = a^{-1}x_1x_2a$$

$$= a^{-1}x_1 \cdot (aa^{-1}) \cdot x_2a$$

$$= (a^{-1}x_1a) \cdot (a^{-1}x_2a)$$

$$= \gamma(x_1) \cdot \gamma(x_2) .$$

At this point, we've shown that $\gamma : G \to G$ is an isomorphism from G to itself, γ is therefore an automorphism.

Question 2: Let $N \leq G$. Prove that if $x^{-1}Nx \subseteq N$ for every $x \in G$, then in fact $x^{-1}Nx = N$ for every $x \in G$.

Answer: We need to show for any $n_1 \in N$, we also have $n_1 \in x^{-1}Nx$. In other words, $n_1 = x^{-1}n_2x$, for all $x \in G$ and for some $n_2 \in N$.

$$x^{-1}Nx \subseteq N$$

$$\Rightarrow x^{-1}n_1x = n_2 \text{ for all } x \in G \text{ and some } n_2 \in N$$

$$\Rightarrow xx^{-1}n_1xx^{-1} = xn_2x^{-1}$$

$$\Rightarrow n_1 = xn_2x^{-1} \text{ for all } x \in G$$

$$\Rightarrow n_1 \in x^{-1}Nx\,.$$

So, we've shown that for any $n_1 \in N$, it follows that $n_1 \in x^{-1}Nx$. Therefore, $N \subseteq x^{-1}Nx$, and since $x^{-1}Nx \subseteq N$. $N = x^{-1}Nx$ holds for all $x \in G$.

Question 3: Let $H \leq G$ and $N \lhd G$.

a. Show that $NH = HN$.

Answer: We need to show for any $x_1 \in NH$, it follows $x_1 \in HN$, and for any $x_2 \in HN$, it follows $x_2 \in NH$. Let's have $x_1 = n_1h_1 \in NH$, where $n_1 \in N$ and $h_1 \in H$.

$$n_1h_1 = h_1h_1^{-1}n_1h_1 = h_1n_2 \text{ for some } n_2 \in N$$

$$\Rightarrow n_1h_1 \in HN$$

$$\Rightarrow x \in HN \text{ for any } x \in NH$$

$$\Rightarrow NH \subseteq HN\,.$$

Similarly, we can prove for any $x_2 \in HN$, $x_2 \in NH$ also holds, $HN \subseteq NH$. Therefore, $NH = HN$.

b. Prove that HN is a subgroup of G, indeed, the smallest subgroup containing both H and N.

Answer: We will first show that HN is a <u>*subgroup*</u> of G. HN is closed under the group operation, $\cdot$. Let's have $x_1 = h_1n_1 \in HN$ and $x_2 = h_2n_2 \in HN$, where $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Since $NH = HN$,

$$n_1h_2 = h_2'n_1' \text{ for some } n_1' \in N \text{ and } h_2' \in H$$

$$\Rightarrow x_1x_2 = h_1n_1h_2n_2 = h_1h_2'n_1'n_2$$

$$\Rightarrow x_1x_2 \in HN\,.$$

The group operation is associative, since $NH = HN$ is a sub set of G. The identity, $e \in HN$.

$$N \lhd G \Rightarrow e \in N$$

$$H \leq G \Rightarrow e \in H$$

$$\Rightarrow ee = e \in HN\,.$$

The inverse of $x = hn \in HN$, where $h \in H$ and $n \in N$, is $x^{-1} = n^{-1}h^{-1}$.

$$NH = HN$$

$$\Rightarrow x^{-1} = (hn)^{-1} = n^{-1}h^{-1} \in HN\,.$$

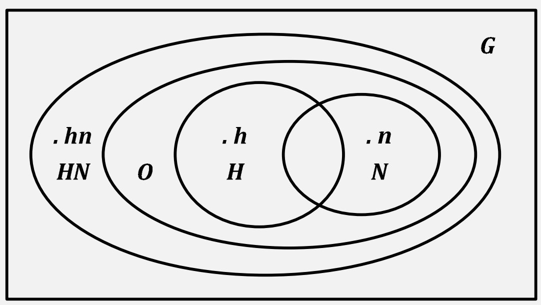
At this point, we've shown that HN satisfies the conditions for a group, and HN is a subset of G. HN is, therefore, a subgroup of G.

We also need to show that HN is the _smallest_ subgroup containing both H and N. It is clear that $H \subseteq HN$ and $N \subseteq NH$.

$$h \in H \Rightarrow h = he \in HN$$

$$n \in N \Rightarrow n = en \in HN\,.$$

Assume there is another set O, such that $O \leq G$, $H \subseteq O$, $N \subseteq O$, and $O \subseteq HN$. We can pick an element hn from HN, where $h \in H$ and $n \in N$, and $hn \notin O$.



We have a contradictory.

$$h \in H, n \in N$$

$$\Rightarrow h, n \in O$$

$$\Rightarrow hn \in O\,.$$

The assumption, $hn \notin O$, is therefore not true. There is no such element, $x = hn \in HN$ but $x \notin O$. In other words, $HN = NH$ is the smallest subgroup of G that contains both H and N.

c. What is $|HN|$?

Answer: $|HN|$ is the lest common multiple of $|H|$ and $|N|$, and $|HN|$ divides $|G|$.

d. Prove that $N \lhd HN$ and $H \cap N \lhd H$.

Answer: We need to show that N is closed under conjugation over HN. So we want to show $xnx^{-1} \in N$ for any $x \in HN$. Since N is a normal subgroup of G, $xnx^{-1} \in N$ for any $x \in G$.

Now we need to show that $H \cap N$ is closed under conjugation over H. So we want to show $hah^{-1} \in H \cap N$, where $a \in H \cap N$ for all $h \in H$.

$$a \in H \cap N \Rightarrow a \in N, a \in H$$

$$N \lhd G, a \in N \Rightarrow hah^{-1} \in N$$

$$H \leq G, a \in H \Rightarrow hah^{-1} \in H\,.$$

$$\Rightarrow hah^{-1} \in H \cap N \text{ for any } h \in H.$$

In summary, N is a normal subgroup of HN, and $H \cap N$ is a normal subgroup of H.

e. Show that $HN/N \cong H/(H \cap N)$.

Answer: Let's define $\phi : H \to HN/N$ and $\phi(h) = hN$, where $h \in H$. ϕ is clearly a homomorphism. Since $N \lhd G$, we have the following.

$$\begin{aligned}\phi(h_1)\phi(h_2) &= (h_1N)(h_2N) \\ &= h_1h_2N \\ &= \phi(h_1h_2)\,.\end{aligned}$$

ϕ is, in addition, onto. For any coset of N in HN, it can be written as $hN, h \in H$, and $\phi(h) = hN$. HN/N is therefore the image of ϕ, $Image(\phi) = HN/N$. The kernel of ϕ is by definition, $\{x : \phi(x) = N, x \in H\}$.

$$\phi(x) = xN = N \Rightarrow x \in N$$

$$\Rightarrow x \in H, x \in N$$

$$\Rightarrow x \in H \cap N$$

$$\Rightarrow Kernal(\phi) = H \cap N\,.$$

First Isomorphism Theorem states, if $f : G_1 \to G_2$ is a homomorphism with kernel K, then the image of f is isomorphism to G_1/K. We've shown $\phi : H \to NH/N$ is a homomorphism with kernel $H \cap N$ and image HN/N. Therefore, HN/N is isomorphic with $H/(H \cap N)$.

f. If H and K are subgroups of G, is HK a subgroup?

Answer: Let's assume the answer is yes. $HK \leq G$ if $H \leq G$ and $K \leq G$. Let's have $x_1 = h_1k_1 \in HK$, and

$x_2 = h_2 k_2 \in HK$. We can derive the following relationship based on the fact that subgroup HK is closed under the group operation.

$$x_1 x_2 = h_1 k_1 h_2 k_2 \in HK$$

$$\Rightarrow h_1 k_1 h_2 k_2 = h_3 k_3 \text{ for some } h_3 \in H \text{ and } k_3 \in K$$

$$\Rightarrow h_1^{-1} h_1 k_1 h_2 k_2 k_2^{-1} = h_1^{-1} h_3 k_3 k_2^{-1}$$

$$\Rightarrow k_1 h_2 = (h_1^{-1} h_3)(k_3 k_2^{-1})$$

$$\Rightarrow k_1 h_2 \in HK \text{ for any } k_1 \in K \text{ and } h_2 \in H$$

$$\Rightarrow KH \subseteq HK$$

$$\text{The order of } H \text{ and } K \text{ shouldn't matter} \Rightarrow KH = HK\,.$$

This conclusion is clearly not true for general subgroups H and K. The answer should be No.

Question 4: Let A and B be two finite subgroups of a group G. Show that if $\gcd(|A|, |B|) = 1$, $A \cap B = \{1\}$.

Answer: We will first prove $A \cap B \leq A$ and $A \cap B \leq B$. Let's have $x_1, x_2 \in A \cap B$.

$$A \leq G \Rightarrow x_1 x_2 \in A$$

$$B \leq G \Rightarrow x_1 x_2 \in B$$

$$\Rightarrow x_1 x_2 \in A \cap B\,.$$

The group operation is associative since $A \cap B$ is a subset of G. The identity $e \in A \cap B$

$$A \leq G \Rightarrow e \in A$$

$$B \leq G \Rightarrow e \in B$$

$$\Rightarrow e \in A \cap B\,.$$

The inverse of $x \in A \cap B$ is $x^{-1} \in A \cap B$, since $x, x^{-1} \in A$ and $x, x^{-1} \in B$. We've shown that $A \cap B$ is a subgroup of A and B. *Lagrange's Theorem* states, for any finite group G, the order (number of elements) of every subgroup H of G divides the order of G. So, we should have $|A| = [A : A \cap B] \cdot |A \cap B|$ and $|B| = [B : A \cap B] \cdot |A \cap B|$. $|A \cap B|$ is, therefore, a common divisor of $|A|$ and $|B|$. We also know $\gcd(|A|, |B|) = 1$, the only divisor of $|A|$ and $|B|$ is 1. So $|A \cap B| = 1$, $A \cap B = \{e\}$.

Question 5: Show that if G is a group with $|G| = 2n$, then G has an element of order 2. If n is odd and G is Abelian show that there is only one such element.

Answer: We will first argue that if G is a group with $|G| = 2n$, then G has an element of order 2. Assume we do not have any order 2 element. In other words, $a \in G$ and $a^{-1} \in G$ are always distinctive elements.

$$G = \{e, a_1, {a_1}^{-1}, a_2, {a_2}^{-1}, \cdots\ a_m, {a_m}^{-1}\}$$

Since $a_i \neq {a_i}^{-1}$ for all $a_i \in G$ except for e, we have $|G| = 1 + 2m$. This is a contradictory with $|G| = 2n$. Therefore, at least one element, a', has to pair up with itself. In other words, $a' = a'^{-1}$, $|\langle a' \rangle| = 2$.

Now we will show If n is odd and G is Abelian there is only one such element with order 2. Assume we have more than one element with order 2. Let's select two of such elements, s and t. We can construct the following group.

$$H = \{e, s, t, st\}$$

From the group operation table shown below, we know that H is indeed a group, $H \leq G$.

	e	s	t	st
e	e	s	t	st
s	s	e	st	t
t	t	st	e	s
st	st	t	s	e

According to *Lagrange's Theorem*, $|G| = [G : H] \cdot |H| = [G : H] \cdot 4$. However, $|G| = 2n$, where n is an odd number. 4 does not divide $|G|$. This is a contradiction, We can have only one element with order 2 in the given conditions.

Question 6: Find (up to isomorphism) all groups of orders $1 - 7$ and 10.

Answer: The list of small groups.

Group order	Group	Note
$\|G\| = 1$	$\{e\}$	$e \cdot e = e$
$\|G\| = 2$	$\{e, a\}$	$a \cdot a = e$
$\|G\| = 3$	$\{e, a, a^2\}$	$a \cdot a^2 = e$
$\|G\| = 4$	$\{e, a, a^2, a^3\}$	$a \cdot a^3 = a^2 \cdot a^2 = e$
	$\{e, a, b, c\}$	$a \cdot a = b \cdot b = c \cdot c = e$
$\|G\| = 5$	$\{e, a, a^2, a^3, a^4\}$	$a \cdot a^4 = a^2 \cdot a^3 = e$
$\|G\| = 6$	$\{e, a, a^2, a^3, a^4, a^5\}$	$a \cdot a^5 = a^2 \cdot a^4 = a^3 \cdot a^3 = e$
$\|G\| = 7$	$\{e, a, a^2, a^3, a^4, a^5, a^6\}$	$a \cdot a^6 = a^2 \cdot a^5 = a^3 \cdot a^4 = e$
$\|G\| = 10$	$\{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9\}$	$a \cdot a^9 = \cdots = a^5 \cdot a^5 = e$