MAT1100

ALGEBRA I

Assignment 1

CONTENTS

Tyler Holden - Fall 2011

999163934

1. Problem 1

If g is an element of a group G, the order $|g|$ of g is the least positive number n such that $g^n = 1$. If $x, y \in G$ show that $|xy| = |yx|$.

Lemma 1. *The following are some important and easily verifiable facts that we will use in our proof.*

1. *If $g \in G$ not identity and $g^n = e$ then $|g| \Big| n$.*
2. *For every $g, h \in G$ we have that $(h^{-1}gh)^n = h^{-1}g^n h$.*
3. *For every $g, h \in G$ we have that $|g| = |h^{-1}gh|$. That is, conjugation preserves order.*

Proof. (1) Assume that $g \in G$ and that $g^n = e$. Since g is not identity, we know that $n > 1$. Since n is an integer, we know $\exists q, r \in \mathbb{Z}$ such that $n = q|g| + r$ where $0 \leq r < |g|$. But then

$$g^n = g^{|g|q+r} = (g^{|g|})^q g^r = g^r = e.$$

This implies that $g^r = e$. However, since $|g|$ is the minimal such integer and $r < |g|$ we conclude that $r = 0$. Thus $n = |g|q$, so $|g| \Big| n$ as required.

(2) Let $g, h \in G$. We will proceed by induction. Clearly $(h^{-1}gh)^1 = h^{-1}g^1 h$ so the base case is satisfies. Assume then that $(h^{-1}gh)^k = h^{-1}g^k h$. Now

$$\begin{aligned}
(h^{-1}gh)^{k+1} &= (h^{-1}gh)^k (h^{-1}gh) \\
&= (h^{-1}g^k h)(h^{-1}gh) && \text{by induction hypothesis} \\
&= h^{-1}g^k gh = h^{-1}g^{k+1}h
\end{aligned}$$

and so $(h^{-1}gh)^{k+1} = h^{-1}g^{k+1}h$ as we required and the result follows.

(3) To show that $|g| = |h^{-1}gh|$ we will show that the numbers divide one another. Indeed, note that

$$(h^{-1}gh)^{|g|} = h^{-1}g^{|g|}h = h^{-1}h = e$$

and so by Property 1 we know that $|h^{-1}gh| \Big| |g|$. Conversely, we know that $(h^{-1}gh)^{|h^{-1}gh|} = e$ so

$$\begin{aligned}
(h^{-1}gh)^{|h^{-1}gh|} &= e \\
h^{-1}g^{|h^{-1}gh|}h &= e && \text{by Property 2} \\
g^{|h^{-1}gh|} &= hh^{-1} && \text{by multiplying by } h \text{ and } h^{-1} \\
g^{|h^{-1}gh|} &= e
\end{aligned}$$

and so we conclude that $|g| \Big| |h^{-1}gh|$. Both divisibility criteria imply that $|g| = |h^{-1}gh|$ as required.

$\square$

Now fix $g, h \in G$, and notice that we can write $gh = ghgg^{-1} = g(hg)g^{-1}$. By Property 3 above, we know that conjugation does not affect the order of an element, hence

$$|gh| = |g(hg)g^{-1}| = |hg|$$

which is precisely what we wanted to show.

2. Question 2

Let G be a group. Show that the function $\phi : G \to G, g \mapsto g^2$ is a group homomorphism if and only if G is abelian.

($\Rightarrow$) Assume that $\phi : G \to G$ is group homomorphism and let $g, h \in G$. By definition of the mapping, we know that $\phi(gh) = (gh)^2 = ghgh$. By assumption, ϕ is a homomorphism and so $\phi(gh) = \phi(g)\phi(h) = g^2h^2 = gghh$. Hence we have that $ghgh = gghh$. Multiplying by g^{-1} on the left and h^{-1} on the right, we get $gh = hg$. Since g, h were chosen arbitrarily, this holds for all elements of the group, hence the group is Abelian.

($\Leftarrow$) Assume that G is an abelian group. Then

$$\begin{aligned}\phi(gh) &= (gh)^2 \\ &= ghgh == gghh && \text{since } G \text{ is abelian} \\ &= g^2h^2 = \phi(g)\phi(h)\end{aligned}$$

hence ϕ is a homomorphism of groups as required.

3. Question 3

Let G be a group. For $a, b \in G$, the commutator $[a, b]$ of a and b is $[a, b] = aba^{-1}b^{-1}$. Let G' be the subgroup of G generated by all commutators of elements of G. Show that G' is normal in G, that G/G' is Abelian, and that any morphism from G into an Abelian group factors through G/G'.

We make the following claim:

Lemma 2. *If G is a group and $H \leq G$, then if $\forall \phi_g \in \mathrm{Inn}(G)$ we have that $\phi(H) \subseteq H$ then $H \triangleleft G$.*

Proof. Let G be a group and $H \leq G$ which is preserved under all inner-automorphisms. Let $g \in G, h \in H$ be arbitrary fixed elements. If we denote by $\phi_g \in \mathrm{Inn}(G)$ the inner automorphism $\phi_g(x) = gxg^{-1}$ then $ghg^{-1} = \phi_g(h) \in H$ by hypothesis. Hence $H \triangleleft G$ as required. ☐

Lemma 3. *If $\phi : G \to H$ is an homomorphism of G, then $\phi([g, h]) = [\phi(g), \phi(h)]$ and so $\phi(G') \subseteq H'$.*

Proof. Fix $g, h \in G$. Then

$$\begin{aligned}\phi([g, h]) &= \phi(ghg^{-1}h^{-1}) = \phi(g)\phi(h)\phi(g^{-1})\phi(h^{-1}) \\ &= \phi(g)\phi(h)\phi(g)^{-1}\phi(h)^{-1} \\ &= [\phi(g), \phi(h)]\end{aligned}$$

☐

Lemma 2 and Lemma 3 imply $G' \triangleleft G$. Indeed, we notice by Lemma 3 that $\phi(G') \subseteq G'$ for every automorphism of G, and so in particular this holds for every inner-automorphism. We conclude normality by Lemma 2.

To see that G/G' is abelian, consider the projection homomorphism $\pi : G \to G/G'$. Let $\bar{g}, \bar{h} \in G/G'$ be distinct elements of the quotient group, and let $g, h \in G$ be such that $\pi(g) = \bar{g}, \pi(h) = \bar{h}$.

Now g, h must be distinct elements since otherwise $\bar{g} = \bar{h}$. Now $[g,h] \in G'$ so $\pi([g,h]) = e_{G/G'}$. However, Lemma 3 implies that

$$\phi([g,h]) = [\overline{g}, \overline{h}] = \overline{g}\overline{h}\overline{g}^{-1}\overline{h}^{-1} = e_{G/G'}$$

and so we conclude that $\overline{g}\overline{h} = \overline{h}\overline{g}$. Since $\overline{g}, \overline{h}$ were chosen arbitrarily, we conclude that all elements of G/G' commute and hence the quotient group is abelian.

Finally, we want to show that any homomorphism from G to an abelian group H factors through G/G'. Let $\phi : G \to H$ be such a homomorphism, and notice that $G' \subseteq \ker\phi$. Indeed, let $g \in G'$ and write $g = [g_1, h_1][g_2, h_2] \cdots [g_n, h_n] = \prod_{i=1}^{n} [g_i, h_i]$ for $g_i, h_i \in G$. Now

$$\begin{aligned}
\phi(g) &= \phi\left(\prod_{i=1}^{n}[g_i, h_i]\right) \\
&= \prod_{i=1}^{n} \phi\left([g_i, h_i]\right) && \text{since } \phi \text{ is a homomorphism} \\
&= \prod_{i=1}^{n} [\phi(g_i), \phi(h_i)] && \text{from Lemma 3} \\
&= \prod_{i=1}^{n} e_H = e_H && \text{since } H \text{ is abelian}
\end{aligned}$$

where in the last line, we note that the commutator in an abelian group is always identity. So $G' \subseteq \ker\phi$. By the Lattice Isomorphism theorem, we then know that $G/\ker\alpha \subseteq G/G'$ and so denote the inclusion map $\iota : G/\ker\alpha \hookrightarrow G/G'$ and write

$$G \overset{\pi}{\twoheadrightarrow} G/G' \overset{\iota}{\hookrightarrow} G/\ker\alpha \xrightarrow{\cong} \mathrm{im}(\alpha) \hookrightarrow H$$

where $\pi : G \to G/G'$ is the projection map and $\cong$ denotes the use of the first isomorphism theorem. Hence ϕ factors through G/G' as above.

4. Question 4

Let G be a group. An automorphism of G is an invertible group morphism $G \to G$. An inner automorphism is an automorphism of G given by conjugation by some specific element $gofG$, so $x \mapsto x^g$. Prove that the inner automorphisms of G form a normal subgroup of the group of all automorphisms of G.

Let $\phi \in \mathrm{Aut}(G)$ and $\varphi_g \in \mathrm{Inn}(G)$ given by $\varphi_g : x \to gxg^{-1}$. Now we want to consider the automorphism given by $\phi \circ \varphi_g \circ \phi^{-1}$ and show that this is an element of $\mathrm{Inn}(G)$. Indeed, we claim that $\phi \circ \varphi_g \circ \phi^{-1} = \varphi_{\phi(g)}$ where $\varphi_{\phi(g)}(x) = x^{\phi(g)}$. To see this, we note that an automorphism of G

is determined entirely by its action on elements of G. Let $h \in G$ be arbitrary, and notice that

$$\begin{aligned}
\phi \circ \varphi_g \circ \phi^{-1}(g) &= \phi\left(\varphi_g\left(\phi^{-1}(h)\right)\right) \\
&= \phi\left(g\phi^{-1}(h)g^{-1}\right) && \text{by definition of inner automorphism} \\
&= \phi(g)\phi\left(\phi^{-1}(h)\right)\phi(g^{-1}) && \text{since } \phi \text{ is a homomorphism} \\
&= [\phi(g)]h[\phi(g)]^{-1} \\
&= \varphi_{\phi(g)}(h).
\end{aligned}$$

Hence as claimed, $\phi \circ \varphi_g \circ \phi^{-1} = \varphi_{\phi(g)} \in \mathrm{Inn}(G)$ so $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$ as required.