MA2202S Homework 1

Qi Ji

2nd September 2018

Question 1

Closure and associativity follows.

Let $a \in G$, by RG4 there exists $b \in G$ such that $ab = e$, then

$$\begin{aligned} ab &= e \\ bab &= be \\ &= b && \text{by (RG3)} \end{aligned}$$

by RG4 we also have $c \in G$ such that $bc = e$, then

$$\begin{aligned} babc &= bc \\ ba(bc) &= e \\ bae &= e \\ ba &= e && \text{by (RG3)} \end{aligned}$$

we now have $ab = ba = e$ which proves G4.

Now that we have shown that our inverse is double-sided, let $a \in G$, we have

$$\begin{aligned} ea &= aa^{-1}a \\ &= ae \\ &= e && \text{by (RG3)} \end{aligned}$$

this proves G3, so $(G, *)$ is a group. $\square$

Question 2

Part 0, $ab = e$ implies $ba = e$.

Suppose $ab = e$, then

$$\begin{aligned} bab &= b \\ babb^{-1} &= bb^{-1} \\ ba &= e \end{aligned} \qquad \square$$

Part (i), $\left(a^{-1}\right)^{-1} = a$.

By part 0, we can just show that $a^{-1}a = e$, which is clear from definition of a^{-1}.

Part (ii), $(ab)^{-1} = b^{-1}a^{-1}$.

By part 0, we can just show that $(ab)\, b^{-1}a^{-1} = e$, which is true because

$$abb^{-1}a^{-1} = aa^{-1} = e.$$

Part (iii), cancellation law.

Suppose $ac = bc$, then $acc^{-1} = bcc^{-1} \implies a = b$. Similarly suppose $ca = cb$ then $c^{-1}ca = c^{-1}cb \implies a = b$.

Part (iv), $ax = b$ has unique solution x in G.

Suppose $ax = b$, then $x = a^{-1}b$, which could be verified to be a solution. For uniqueness, suppose there exists $x, x' \in G$ such that $ax = ax' = b$, then $x = x'$ by cancellation law.

Part (v),

Let $m, n \in \mathbb{Z}$, $a \in G$. Note that conclusion trivially holds if $m = 0$ or $n = 0$.

Suppose $n < 0, m > 0$, then

$$\begin{aligned}
a^m a^n &= \underbrace{a \cdot a \cdots a}_{m \text{ times}} \cdot \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{-n \text{ times}} \\
&= \begin{cases} \underbrace{a \cdot a \cdots a}_{m+n \text{ times}} & \text{if } |m| \geq |n| \\ \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{-n-m \text{ times}} & \text{if } |m| < |n| \end{cases}
\end{aligned}$$

In both cases, $a^m a^n = a^{m+n}$. An analogous argument works for the case where $n > 0$ and $m < 0$.

Now suppose $n > 0, m > 0$, then

$$\begin{aligned}
a^m a^n &= \underbrace{a \cdot a \cdots a}_{m \text{ times}} \cdot \underbrace{a \cdot a \cdots a}_{n \text{ times}} \\
&= \underbrace{a \cdot a \cdots a}_{m+n \text{ times}} \\
&= a^{m+n}
\end{aligned}$$

and the exact same argument also works the case where $n < 0, m < 0$ (replace a with a^{-1}). $\square$

Question 3

Part (i)

From elementary set theory we get the result that ϕ^{-1} is a bijection too. It remains to show that ϕ^{-1} is also a group homomorphism.

Let $h, h' \in H$.

$$\begin{aligned}
h \star h' &= \phi\left(\phi^{-1}(h)\right) \star \phi\left(\phi^{-1}(h')\right) \\
&= \phi\left(\phi^{-1}(h) * \phi^{-1}(h')\right) \\
\phi^{-1}(h \star h') &= \phi^{-1}\left(\phi\left(\phi^{-1}(h) * \phi^{-1}(h')\right)\right) \\
&= \phi^{-1}(h) * \phi^{-1}(h')
\end{aligned}$$

$\square$

Part (ii)

Again, from elementary set theory, we have the result that $\psi \circ \phi$ – a composition of two bijections, is a bijection. Let $g_1, g_2 \in G$.

$$\begin{aligned}(\psi \circ \phi)\,(g_1 * g_2) &= \psi\,(\phi\,(g_1 * g_2)) \\ &= \psi\,(\phi(g_1) \star \phi(g_2)) \\ &= \psi\,(\phi(g_1)) \bullet \psi\,(\phi(g_2)) \\ &= (\psi \circ \phi)\,(g_1) \bullet (\phi \circ \phi)\,(g_2)\end{aligned}$$

Hence $\psi \circ \phi$ is a group isomorphism. $\square$