PMTH332 Assignment 1

Jayden Turner (SN 220188234)

21 July 2018

Question 1

Let $\sim$ define an equivalence relation on the set X, and consider the quotient set $X/\sim = \{[x] | x \in X\}$.

For each $[x] \in X/\sim$, the reflexive property of $\sim$ means that $x \in [x]$, so all $[x]$ are nonempty.

Suppose $x, y \in X$ and $y \notin [x]$. That is, $x \sim y$ does not hold. Now suppose that $[x] \cap [y] \neq \varnothing$. Then $\exists t \in [x] \cap [y]$ such that $x \sim t$ and $y \sim t$. By the symmetry of $\sim$, $t \sim y$. Then, by the transitivity of $\sim$, there holds $x \sim y$. However this is a contradiction. Therefore, if $y \notin [x]$, then $[x]$ and $[y]$ are disjoint subsets of X.

As every $x \in X$ has an equivalence class $[x]$, it holds that $\underset{x \in X}{\cup} [x] = X$.

$\implies X/\sim$ defines a partition of X.

Now let $\{X_\lambda | \lambda \in \Lambda\}$ be a partition of X. Define the relation $\sim$ such that $x \sim y$ if and only if $x, y \in X_\lambda$ for some $\lambda \in \Lambda$.

By definition $x \sim x$ holds, as does $y \sim x$ if $x \sim y$ holds. Suppose $x \sim y$ and $y \sim z$ hold. Then $x, y \in X_\lambda$ and $y, z \in X_\mu$ for $\lambda, \mu \in \Lambda$. However, as $\{X_\lambda\}$ is a partition of X, each element of X can belong to only one X_λ. Therefore, $y \in X_\lambda$ and $y \in X_\mu$ implies that $\lambda = \mu$. Further, this implies that $x, z \in X_\lambda = X_\mu$, and so $x \sim z$.

$\implies \sim$ is an equivalence relation on X.

Question 2

Let $\bar{a}$ denote the right inverse of $a \in G$, and e the right neutral element of G. Then

$$\begin{aligned} \text{(G2R)} \implies \bar{a} &= \bar{a} * e \\ &= \bar{a} * (a * \bar{a}) \\ \text{(G1)} \implies &= (\bar{a} * a) * \bar{a} \end{aligned} \tag{1}$$

$$\begin{aligned} \text{(G3R)} \implies e &= \bar{a} * \bar{\bar{a}} \\ (1) \implies &= ((\bar{a} * a) * \bar{a}) * \bar{\bar{a}} \\ \text{(G1)} \implies &= (\bar{a} * a) * (\bar{a} * \bar{\bar{a}}) \\ \text{(G3R)} \implies &= (\bar{a} * a) * e \\ \text{(G1)} \implies &= \bar{a} * a \implies \text{(G3)} \end{aligned}$$

That is, $\forall a \in G, \exists! \bar{a} \in G$ such that $a * \bar{a} = \bar{a} * a = e$. Now,

$$
\begin{aligned}
\text{(G2R)} \implies a &= a * e \\
\text{(G3)} \implies &= a * (\bar{a} * a) \\
\text{(G1)} \implies &= (a * \bar{a}) * a \\
\text{(G3)} \implies &= e * a \implies \text{(G2)}
\end{aligned}
$$

That is, $\exists e \in G$ such that $\forall a \in G, a * e = e * a = a$. Therefore (G1), (G2) and (G3) hold, so (G, $*$) is a group.

Question 3

Firstly, to show that the operation is well defined, let $l, l' \in [l]$ and $k, k' \in [k]$. Consider

$$[l'] + [k'] = [l' + k']$$

Note that $l - l' = cm$ and $k - k' = dm$ for $a, d \in \mathbb{Z}$. Therefore, we have that

$$[l' + k'] = [l - cm + k - dm] = [l + k + em]$$

where $e = -c - d \in \mathbb{Z}$. We also have that $l + k - (l + k + em) = em$, which means that $l + k \cong l + k + em \cong l' + k' \text{mod} m$. That is, $[l + k] = [l' + k']$. Therefore, the binary operation is well defined as it does not depend on the representatives chosen for each equivalence class.

Firstly, we have that for $[a], [b], [c] \in \mathbb{Z}_m$, $[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = ([a + b]) + c = ([a] + [b]) + [c]$, so (G1) holds.

Secondly, note that $[0] \in \mathbb{Z}_m$ and for $[a] \in \mathbb{Z}_m$, $[a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a]$, so (G2) holds.

Finally, for each $[a] \in \mathbb{Z}_m$, there exists $[-a] \in \mathbb{Z}_m$, where $[a] + [-a] = [a - a] = [0] = [-a + a] = [-a] + [a]$, so (G3) holds.

Therefore, $(\mathbb{Z}_m, +)$ is a group.

Question 4

If $(a * b)^2 = a^2 * b$, then it follows that

$$
\begin{aligned}
a * b * a * b &= a * a * b * b \\
\bar{a} * a * b * a * b &= \bar{a} * a * a * b * b \\
e * b * a * b &= e * a * b * b \\
b * a * b * \bar{b} &= a * b * b * \bar{b} \\
b * a * e &= a * b * e \\
\implies b * a &= a * b
\end{aligned}
$$

Therefore, $(G, *)$ is abelian.