SOLUTIONS FOR THE FIRST PROBLEM SET

Page 2, problem 1: We are given that

(1) If $a, b \in S$, then $a \ast b = a$.

(2) If $a, b \in S$, then $a \ast b = b \ast a$.

We are asked to prove that $S$ has at most one element. If $S$ is empty, then it has 0 elements and we are done. Assume that $S$ is not empty. Let $s$ be one element of $S$. If $a \in S$, then (1) implies that $a \ast s = a$ and that $s \ast a = s$. On the other hand, (2) implies that $a \ast s = s \ast a$. Hence

$$a = a \ast s = s \ast a = s$$

Hence $s$ is the only element of $S$. Therefore, if $S$ is not empty, then $S$ has only one element. So, as stated, $S$ has at most one element.

Page 3, problem 3: (a) It is clear that $a \ast b \in S$ by the definition of $\ast$. (b) If $a = \square$, then both sides are $b \ast c$. If $b = \square$, then both sides are $a \ast b$. If $c = \square$, then both sides are $a \ast b$. Hence the equality (i.e., the associative law) holds if $a, b$ or $c$ is $\square$. The one remaining case is $a = b = c = \triangle$. In that case, we have

$$(\triangle \ast \triangle) \ast \triangle = \square \ast \triangle = \triangle, \quad \triangle \ast (\triangle \ast \triangle) = \triangle \ast \square = \triangle$$

and the stated equality again holds.

Page 13, problem 6: We must prove that $g(t) = h(t)$ for all $t \in T$. Suppose $t \in T$. Since $f$ is onto, there exists an element $s \in S$ such that $f(s) = t$. Since $g \circ f = h \circ f$, we have

$$g(f(s)) = h(f(s)).$$

Since $t = f(s)$, it follows that $g(t) = h(t)$. Since this is true for any $t \in T$, we have proved that $g = h$.

Page 13, problem 8: (a) Yes, $f$ is a function from $S$ to $T$. Every integer is odd or even. No integer is both odd and even. (b) The function $f$ can be described by

$$f(s) = (-1)^s.$$
using the law of exponents for powers of -1. The fact that $f$ has this property is equivalent to the facts that (i) $s_1 + s_2$ is even if $s_1$ and $s_2$ are both even or both odd, (ii) $s_1 + s_2$ is odd if $s_1$ is even and $s_2$ is odd or $s_1$ is odd and $s_2$ is even. In case (i), one uses the fact that $1 \cdot 1 = (-1) \cdot (-1) = 1$. In case (ii), one uses the fact that $1 \cdot (-1) = (-1) \cdot 1 = -1$.

As for (c), this is clearly false. For $f(1 \cdot 1) = f(1) = -1$, but $f(1)f(1) = 1$.

Page 14, problem 9: (a) $(f \circ g)(s) = (s + 1)^2$. (b) $(g \circ f)(s) = s^2 + 1$. (c) The two functions $f \circ g$ and $g \circ f$ are obviously different. For $(f \circ g)(1) = 4$, but $(g \circ f)(1) = 2$.

Page 14, problem 12: (a) The function $f$ is not well-defined. For example, note that $1/2 = 2/4$, but $2^12^2 \neq 2^23^1$. (b) If $s \in S$, then we can write $s = u/v$ where $v$ is a positive integer and $u$ is an integer (which is necessarily nonnegative). There are many ways to do this. For a fixed $s$, consider the set
\[ \{v \mid vs \in \mathbb{Z}\}. \]
This is a nonempty subset of the natural numbers $\mathbb{N}$. It has a uniquely determined smallest element which we will call $n$. Thus, $s = m/n$. Clearly, $m$ is also uniquely determined. We refer to the representation $s = m/n$ as the “reduced form” for $s$. We can then make the following definition. For $s \in S$, write $s = m/n$ in the uniquely determined reduced form described above. Then define $f(s) = 2^m3^n$. This defines a function $f : S \to T$.

Page 15, problem 25: The function $f : S \to T$ defined by $f(s) = e^s$ has all the required properties. It is a strictly increasing function on $S = \mathbb{R}$ because its derivative is positive for all $s \in \mathbb{R}$. Therefore, $f$ is injective. As $s \to -\infty$, $f(s) \to 0$. As $s \to +\infty$, $f(s) \to +\infty$. Since $f(s)$ is continuous, the intermediate value theorem implies that $f$ is onto. (Note that $T$ is the set of positive reals.) Hence $f$ is $1 - 1$ and onto. Also, we have
\[ f(s_1 + s_2) = e^{s_1+s_2} = e^{s_1}e^{s_2} = f(s_1)f(s_2) \]
as required.

Page 19, problem 9: We will represent function in the abbreviated form described in class. Thus
\[ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}. \]
We then find (for (a)):
\[ f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad f^3 = f \circ f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad f^4 = f \circ f^3 = i \]
And for (b), we find: \[ g^2 = i, \quad g^3 = g^2 \circ g = g \]

And for (c) and (d), we find:
\[
fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},
\]
\[
gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}
\]

And for (e), we find
\[
(fg)^3 = i, \quad (gf)^3 = i
\]

And for (f), using parts (a) and (b), we have
\[
f^{-1} = f^3, \quad g^{-1} = g
\]

Page 19, problem 10: In class, we studied \(S_3\) in detail. This is the group \(A(S)\), where \(S = \{s_1, s_2, s_3\}\). We can simply take \(S = \{1, 2, 3\}\). The notation we used in class is as follows:
\[
i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 1 \end{pmatrix}, \quad f' = f^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}
\]
\[
g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad g' = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g'' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}
\]

Obviously, \(i^6 = i\). Also \(f^3 = i\) and hence \(f^6 = f^3f^3 = i^2 = i\). Similarly, \((f')^3 = i\) and so \((f')^6 = (f')^3(f')^3 = i^2 = i\). Now \(g^2 = i\) and therefore \(g^6 = (g^2)^3 = i^3 = i\). Since \((g')^2 = (g'')^2 = i\), the same argument implies that \((g')^6 = (g'')^6 = i\).

Page 46, problem 1:
(a) This isn’t a group. There is no identity element. For if \(e \in \mathbb{Z}\) satisfies \(e \ast a = a = a \ast e\) for all \(a \in \mathbb{Z}\), then \(e - a = a = a - e\) for all \(a \in \mathbb{Z}\). The equation \(a = a - e\) implies \(e = 0\). The equation \(e - a = a\) is then not satisfied for \(a = 1\).

(b) This is not a group. There is an identity, namely \(e = 0\). However, if \(a = 1\), there is no element satisfying \(a \ast b = e\). That equation is equivalent to \(1 + b + b = 0\) which obviously has no solutions where \(b \in \mathbb{Z}\).
(c) This is not a group. There is an identity, namely $e = 0$. But if $a = 1$, there is no element satisfying $a \ast b = e$. namely $e = 0$. However, if $a = 1$, there is no element satisfying $a \ast b = e$. That equation is equivalent to $1 + b = 0$ which obviously has no solutions where $b$ is a nonnegative integer.

(d) This $G$ is a group. Suppose that $a, b \in G$. Thus, $a, b \in \mathbb{Q}$ and $a \neq -1, b \neq -1$. We can view the definition of $\ast$ as follows:

\[(1 + a)(1 + b) = 1 + a + b + ab = 1 + a \ast b\]

It is clear that $a \ast b \in \mathbb{Q}$. Since $1 + a \neq 0$ and $1 + b \neq 0$, it follows that $(1 + a)(1 + b) \neq 0$. Therefore, $a \ast b \neq -1$. Thus, $a \ast b \in G$.

Secondly, the associative law is valid for $\mathbb{Q}$. Hence, if $a, b, c \in G$, we have

\[(1 + a)((1 + b)(1 + c)) = ((1 + a)(1 + b))(1 + c)\]

If we use (1), the left side of (2) is $1 + a \ast (b \ast c)$ and the right side is $1 + (a \ast b) \ast c$ and the fact that they are equal implies that $a \ast (b \ast c) = (a \ast b) \ast c$.

We can take $e = 0$ as the identity element. Then $1 + e = 1$. The fact that $e \ast a = a = a \ast e$ follows from (1) (or could be checked directly).

Finally, suppose $a \in G$. Then $1 + a \in \mathbb{Q}$ and is nonzero. Choose $b$ such that

\[1 + b = \frac{1}{1 + a}\]

Then $b \in \mathbb{Q}$ and $b \neq -1$ and hence $b \in G$. Since

\[(1 + a)(1 + b) = (1 + b)(1 + a) = 1 + 0,\]

it follows from (1) that $a \ast b = b \ast a = 0 = e$ and so inverses exist in $G$.

(e) This is not a group. The set $G$ is not closed under $\ast$. For example,

\[\frac{1}{5} + \frac{4}{5} = 1\]

and $1 \not\in G$ even though $\frac{1}{5}, \frac{4}{5} \in G$.

(f) This is not a group. It is not possible to find an element $e \in G$ satisfying $e \ast a = a$ for all $a \in G$. For if $e$ were such an element, then we would have $a = e \ast a = e$ for all $a \in G$. Thus $G$ would have only one element, contrary to the assumption.