1

Proposition. Let \((G, *)\) be a group and \(I\) a set. Let \(G^I\) be the set of all functions \(f : I \rightarrow G\). For all \(f, g \in G^I\) define \(f * g \in G^I\) by

\[
(f * g)(i) = f(i) * g(i) \quad \text{for all} \quad i \in I.
\]

Then \((G^I, *)\) is also a group.

Proof. First, let us consider \((f * (g * h))(i)\) for some \(f, g, h \in G^I\). By definition, \((f * (g * h))(i) = f(i) * (g(i) * h(i))\) where \(f(i), g(i)\) and \(h(i)\) are elements of \(G\). Since \((G, *)\) is a group, it follows that \(f(i) * (g(i) * h(i)) = (f(i) * g(i)) * h(i) = ((f * g) * h)(i)\), and we see that the operation \(*\) is associative in \(G^I\).

Second, let us consider the function \(e_I \in G^I\) that maps every \(i \in I\) to the identity element \(e \in G\). For any \(f \in G^I\), \((f * e_I)(i) = f(i)*e = f(i)\) and \((e_I * f)(i) = e_I(i)*f(i) = e*f(i) = f(i)\). Therefore, the function \(e_I\) is the identity element of \((G^I, *)\).

Third, we must show that every \(f \in G^I\) has an inverse \(f^{-1} \in G^I\) such that \((f * f^{-1})(i) = e_I(i)\). Let \(f\) be an arbitrary function from \(G^I\). By definition, \(f\) maps every element \(i \in I\) to some element \(f(i) \in G\). Consider the relation \(H \subset I \times G\) that pairs each \(i \in I\) with the element \((f(i))^{-1} \in G\). Since \((G, *)\) is a group we know that each \((f(i))^{-1}\) exists and is unique; thus, our relation is actually a function, call it \(h\), and is necessarily an element of \(G^I\). Now, \((f * h)(i) = f(i) * h(i) = f(i) * (f(i))^{-1} = e\). But the function that maps everything to \(e\) is the identity \(e_I(i)\). So \((f * h)(i) = e_I(i)\), and it can be similarly shown that \((h * f)(i) = e_I(i)\). Therefore, \(h = f^{-1}\) and each element of \(G^I\) has an inverse. We can now conclude that \((G^I, *)\) is a group. □

2

Let \(G\) be a finite group of even order. We will show that there exists \(g \in G\) with \(g \neq e\) and \(g^2 = e\). Note that each element of a group has an unique inverse element (Proposition 1.2 of Grove).

Suppose \(n\) is an even integer greater than 0 and \(G = \{x_1, x_2, \ldots, x_n\}\). Let the elements of \(G\) be reordered and reindexed so that \(x_1\) is the identity element and inverse elements are paired together. Certainly \(x_1\) is its own inverse. Thereafter, \(x_3 = x_2^{-1}, x_5 = x_4^{-1}, \ldots, x_{n-1} = x_{n-2}^{-1}\). Consider the element \(x_n\). By the definition of a group it must have an inverse, but the inverse cannot be any of the previous elements because that would violate our note above. Therefore, \(x_n\) must be its own inverse, implying \(x_n^2 = e\).

3

Consider the pre-group \((G, *)\) given in the table below. The simple calculations below show that \(*\) is associative, which means \((G, *)\) is a semi-group.

<table>
<thead>
<tr>
<th></th>
<th>(a)</th>
<th>(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>(a)</td>
<td>(b)</td>
</tr>
<tr>
<td>(b)</td>
<td>(a)</td>
<td>(b)</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
a(aa) &= a = (aa)a & a(ab) &= b = (aa)b & a(ba) &= a = (ab)a & b(aa) &= a = (ba)a \\
b(ba) &= a = (bb)a & b(ab) &= b = (ba)b & a(bb) &= b = (ab)b & b(bb) &= b = (bb)b
\end{align*}
\]
(a) Consider the element $a$. It is true that $a * a = a$ and $a * b = b$, thus $a$ is a left-identity.
(b) Observe that $a * a = a$ and $b * a = a$. We see that each element of $G$ has a right-inverse, namely $a$, such that right-multiplication by this element equals the left-inverse from above.
(c) The semi-group $(G, \ast)$ is not a group because it does not have an identity $e$ such that $g \ast e = e \ast g = g$ for all $g \in G$. The element $a$ cannot be the identity since $b \ast a = a \neq b = a \ast b$. The element $b$ cannot be the identity for the same reason.

4

**Proposition.** If $(G, \ast)$ is a group with $(ab)^n = a^n b^n$ for all $a, b \in G$ and three consecutive integers $n, n + 1$ and $n + 2$, then $G$ is abelian.

**Proof.** Let $n \in \mathbb{N}$. By associativity and the definition of exponents, $(ab)^{n+1} = a(ba)^n b$. By our assumption, $a^{n+1} b^{n+1} = a(ba)^n b$. Since $a^{-1}$ and $b^{-1}$ exist in $G$, we can multiply the former on the left and the latter on the right to get $a^n b^n = (ba)^n$, or equivalently $(ab)^n = (ba)^n$. Note that $(ab)^n$ and $(ba)^n$ must have the same inverse, call it $k$.

The preceding argument can be repeated with $n+1$ in place of $n$ and $n+2$ in place of $n+1$. The result is $(ab)^{n+1} = (ba)^{n+1}$. This equation can be rewritten as $(ab)^n(ab) = (ba)^n(ba)$. Next, we multiply $k$ on the left so that $(k(ab)^n)(ab) = (k(ba)^n)(ba)$. But $k(ab)^n = k(ba)^n = e$ where $e$ is the identity element of $G$. Therefore, $ab = ba$ and we conclude that $(G, \ast)$ is abelian. □

5

**Proposition.** Let $(G, \ast)$ be a non-empty finite semi-group. If for all $a, b, c \in G$,

(i) $ab = ac$ implies $b = c$, and
(ii) $ba = ca$ implies $b = c$,

then $(G, \ast)$ is a group.

**Proof.** First, we consider associativity. This is given by the fact that $(G, \ast)$ is a semi-group, which is associative by definition.

Second, let us consider identity. Since $(G, \ast)$ is non-empty and finite we can consider its multiplication table. Clearly, the product $ab$ appears in row $a$ of the table. Moreover, by (i), the product $ab$ can appear in row $a$ only once. Since $b$ was arbitrary and $G$ is finite, it follows that each element of $G$ appears exactly once in row $a$. This means $a$ appears in row $a$ and there must exist an $a_{e,r} \in G$ such that $a * a_{e,r} = a$.

By (ii), the product $ba$ shows up exactly once in column $a$, and using a similar argument to that above, each element of $G$ appears exactly once in column $a$. Thus, $a$ appears in column $a$ and there exists an $a_{r,l} \in G$ such that $a_{r,l} * a = a$. Next, we will show that this left-identity of $a$ and the right-identity of $a$ are equal.

Consider $aa = (a_{e,r})a = a(e_{r,l}a)$. By (i), we know that $a = a_{e,r}a$ and it becomes clear that $a_{e,r}$ is also the left-identity of $a$; that is, $a_{e,r} = a_{e,l}$. Hereafter we will write simply $a_e$.

Since $a$ was arbitrary, we have shown that each element of $G$ has an identity. In fact, they each have the same identity. Let $a$ and $b$ be any elements of $G$ and let $a_e$ and $b_e$ be their respective identities. Consider $ba_e = (b_{e,r})a_e = b(b_e a_e)$. It follows from (i) that $a_e = b_{e,l}a_e$. Now, consider $b_e a = b_e(a_{e,l}a) = b_(e,l) a_e$ a. It follows from (ii) that $b_e = b_e a_e$. But this means that $a_{e,l} = b_e$, which we may now call $e$, the identity element of $G$ with respect to $\ast$.

Third, we will show that each element has an inverse. Choose $a \in G$. As determined above, $e$ must appear exactly once in row $a$ and exactly once in column $a$. Thus, there exist $a_{e,r}^{-1}, a_{l}^{-1} \in G$ such that $aa_{e,r}^{-1} = e$ and $a_{l}^{-1}a = e$. Let us consider $ae = ea = (aa_{e,r}^{-1})a = a(a_{e,r}^{-1}a)$. But we know from (i) that $ae = a(a_{e,r}^{-1}a)$ implies $e = a_{e,r}^{-1}a$. From this, it is clear to see that $a_{e,r}^{-1}$ is also the left-inverse of $a$; that is, $a_{e,r}^{-1} = a_{l}^{-1} = a^{-1}$. Therefore, every element of $G$ has an inverse.

Having proven associativity, the existence of an identity element, and the existence of inverse elements, we can conclude that $(G, \ast)$ is a group. □
Let $\mathcal{E} = (\mathcal{P}, \mathcal{L}, \mathcal{R})$ be a projective plane of order two. Let $l$ be a line and let

$$H = \{ \phi \in \text{Aut}(\mathcal{E}) \mid \phi(A) = A \text{ for all points incident with } l \}.$$ 

What is the order of $H$? Recall that the mapping of any three noncollinear to any three noncollinear points uniquely determines an automorphism of $\mathcal{E}$ because three noncollinear points uniquely determine the projective plane of order two. Without loss of generality, let $A, B, C \in \mathcal{P}$ be noncollinear and let $l \in \mathcal{L}$ be incident with $A$ and $B$. By definition, $\phi(A) = A$ and $\phi(B) = B$. Let us ponder the image of $C$ under $\phi$.

Since $\mathcal{E}$ has exactly seven points and two of them have already been mapped to, there are five possibilities left for $\phi(C)$. But $C$ cannot be mapped to the remaining point incident with $l$ because that would mean that three noncollinear points $(A, B, C)$ were mapped to three collinear points (those on $l$), which is impossible given the definition of an automorphism. Therefore, only four possibilities exist for $\phi(C)$ that would maintain the noncollinear property of $\phi(A)$, $\phi(B)$, and $\phi(C)$. This means $|H| = 4$.

We know $\text{Sym}(4)$ is a group and $\text{Sym}(3)$ a subgroup under the operation of function composition. The function $\alpha \in \text{Sym}(4)$ is, by definition, a bijection on $\{1, 2, 3, 4\}$. We will write $\alpha$ explicitly as

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) \end{pmatrix}.$$ 

The cosets of $\text{Sym}(3)$ in $\text{Sym}(4)$ are as follows:

$$\begin{array}{c}
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}
\end{array} \text{Sym}(3): 
\begin{array}{c}
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}
\end{array}$$

$$\begin{array}{c}
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}
\end{array} \text{Sym}(3): 
\begin{array}{c}
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}
\end{array}$$

$$\begin{array}{c}
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}
\end{array} \text{Sym}(3): 
\begin{array}{c}
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}
\end{array}$$

Within each of these equivalence classes, any element can be mapped to any other element (or itself) through composition with an element of $\text{Sym}(3)$. Moreover, there does not exist an element of $\text{Sym}(3)$ that will map elements of $\text{Sym}(4)$ between the classes. This is clear because a function $\beta \in \text{Sym}(3)$ can permute only the numbers that are the image of the numbers 1, 2, and 3. It is unable to alter the number that is the image of 4 under the function from $\text{Sym}(4)$ that $\beta$ is composed with.