**Section 4 Solutions**

31. An element $x$ of a group $G$ is called **idempotent** if $x * x = x$. Prove that any group $G$ has exactly one idempotent element.

Proof. Certainly $e$ is idempotent, because $e * e = e$, so $G$ has at least one idempotent element, $e$. Could there be others? Suppose $x \in G$ is idempotent, which means $x * x = x$. Then:

$$\begin{array}{rcll} (x * x) * x' &=& x * x' & \text{(multiply both sides by } x' \text{ on right)} \\ x * (x * x') &=& e & \text{(associative and inverse properties)} \\ x * e &=& e & \text{(inverse property)} \\ x &=& e & \text{(identity property)} \end{array}$$

Thus $x = e$, so $G$ has exactly one idempotent element, and it is $e$.

32. If every element $x$ in a group $G$ satisfies $x * x = e$, then $G$ is abelian.

Proof. Let $a$ and $b$ be arbitrary elements of $G$. We wish to show $a * b = b * a$. Consider the element $a * b \in G$. Since every element $x$ of $G$ satisfies $x * x = e$, we have $(a * b) * (a * b) = e$. Let us work with this equation as follows.

$$\begin{array}{rcll} (a * b) * (a * b) &=& e & \\ a * [(a * b) * (a * b)] &=& a * e & \text{(multiply both sides by } a \text{ on left)} \\ [a * (a * b)] * (a * b) &=& a & \text{(associative and identity properties)} \\ [(a * a) * b)] * (a * b) &=& a & \text{(associative property)} \\ [e * b] * (a * b) &=& a & (a * a = e) \\ b * (a * b) &=& a & \text{(identity property)} \\ [b * (a * b)] * b &=& a * b & \text{(multiply both sides by } b \text{ on right)} \\ b * [(a * b) * b] &=& a * b & \text{(associative property)} \\ b * [a * (b * b)] &=& a * b & \text{(associative property)} \\ b * [a * e] &=& a * b & (b * b = e) \\ b * a &=& a * b & \text{(identity property)} \end{array}$$

This shows $a * b = b * a$, so $G$ is abelian.

34. Let $G$ be a finite group. Show that for any $a \in G$ there is an $n \in \mathbb{Z}^+$ for which $a^n = e$.

Proof. Suppose $G$ is finite, and say it has $m$ elements. Consider the following list of elements of $G$:

$$a^1, a^2, a^3, a^4, \cdots a^{m+1}.$$

Since this list has $m + 1$ items in it, and $G$ contains only $m$ elements, it follows that the list has at least two items that are equal. Thus $a^j = a^k$ for some integers $j$ and $k$ with $1 \leq j < k \leq m + 1$. Then

$$\begin{array}{rcl} a^j &=& a^k \\ a^j (a^{-1})^j &=& a^k (a^{-1})^j \\ a^j a^{-j} &=& a^k a^{-j} \\ a^{j-j} &=& a^{k-j} \\ a^0 &=& a^{k-j} \\ e &=& a^{k-j} \end{array}$$

Setting $n = k - j$, it follows that $a^n = e$.

37. Suppose $a, b, c$ are elements of a group $G$ and $a * b * c = e$. Show $b * c * a = e$.

Proof. The associative property gives us license to omit the parentheses, and since they do not appear in this problem we are invited to not to use them. Starting with $a * b * c = e$ do the following.

$$\begin{array}{rcll} a * b * c &=& e & \\ a' * a * b * c &=& a' * e & \text{(multiply both sides by } a' \text{ on left)} \\ e * b * c &=& a' & \text{(inverse and identity properties)} \\ b * c &=& a' & \text{(identity property)} \\ b * c * a &=& a' * a & \text{(multiply both sides by } a \text{ on right)} \\ b * c * a &=& e & \text{(inverse property)} \end{array}$$

This completes the proof that $b * c * a = e$.