<u>Problem 2</u>): Let $\mathcal{G}$ be a finite group and $g \in \mathcal{G}$. Now define $\langle g \rangle \equiv g^0, g^1, g^2, \ldots, g^k, \ldots$, where $k \in \mathbb{N}$.

Beginning with the multiplicative case, let $m, n \in \mathbb{N}$ so that we have

$$g^m \, g^n = g^{m+n}$$

Since $m, n \in \mathbb{N}$ and $\mathbb{N}$ is closed under addition, $(m + n) \in \mathbb{N}$, it is clear that $g^{m+n} \in \langle g \rangle$. Therefore, $\langle g \rangle$ is closed under its operation. From our definition of $\langle g \rangle$, we know that $g^0 \in \langle g \rangle$. Additionally, $g^0 \equiv e = 1$; therefore $\langle g \rangle$ contains the identity element. Now, let $m \in \mathbb{Z}^+$ and write $g^{-m} \, g^m$. Using $g^{-m} \equiv \left(g^{-1}\right)^m$, this yields

$$g^{-m} \, g^m = \left(g^{-1}\right)^m \, g^m = \left(g^{-1} \, g\right)^m = (e)^m = e = 1$$

which implies the existence of an inverse for each element in $\langle g \rangle$. Finally, let $m, n, k \in \mathbb{N}$, then we have

$$g^m \left(g^n \, g^k\right) = g^m \left(g^{n+k}\right) = g^{m+(n+k)} \tag{2.1}$$

Since $\mathbb{N}$ is associative under addition, the expression in 2.1 may be rewritten as

$$g^{m+(n+k)} = g^{(m+n)+k} = \left(g^{m+n}\right) g^k = \left(g^m \, g^n\right) g^k$$

thereby demonstrating the associativity of operations in $\langle g \rangle$. Since $\mathcal{G}$ is finite, it has order $m = |\mathcal{G}|$. Therefore, the elements of $\langle g \rangle$ will be repeats of elements in $\mathcal{G}$ starting with g^{m+1}. Moreover, this means that $\langle g \rangle \subseteq \mathcal{G}$, thus satisfying the last condition for $\langle g \rangle$ to be a sub-group of $\mathcal{G}$.

Continuing with the additive case, let $m, n \in \mathbb{N}$ so that we have

$$m \times g \, n \times g = (m + n) \times g$$

Since $m, n \in \mathbb{N}$ and $\mathbb{N}$ is closed under addition, $(m + n) \in \mathbb{N}$, it is clear that $(m + n) \times g \in \langle g \rangle$. Therefore, $\langle g \rangle$ is closed under its operation. From our definition of $\langle g \rangle$, we know that $0 \times g \in \langle g \rangle$. Additionally, $0 \times g \equiv e = 0$; therefore $\langle g \rangle$ contains the identity element. Now, let $m \in \mathbb{Z}^+$ and write $(-m) \times g\, m \times g$. Using $(-m) \times g \equiv m \times (-g)^m$, this yields

$$(-m) \times g\, m \times g = m \times (-g)\, m \times g = m \times (-g\, g) = m \times (e) = e = 0$$

which implies the existence of an inverse for each element in $\langle g \rangle$. Finally, let $m, n, k \in \mathbb{N}$, then we have

$$m \times g\, (n \times g\, k \times g) = m \times g\, ((n + k) \times g) = (m + (n + k)) \times g \tag{2.2}$$

Since $\mathbb{N}$ is associative under addition, the expression in 2.2 may be rewritten as

$$(m + (n + k)) \times g = ((m + n) + k) \times g = (m + n) \times g\, k \times g = (m \times g\, n \times g)\, k \times g$$

thereby demonstrating the associativity of operations in $\langle g \rangle$. Since $\mathcal{G}$ is finite, it has order $m = |\mathcal{G}|$. Therefore, the elements of $\langle g \rangle$ will be repeats of elements in $\mathcal{G}$ starting with $(m + 1) \times g$. Moreover, this means that $\langle g \rangle \subseteq \mathcal{G}$, thus satisfying the last condition for $\langle g \rangle$ to be a sub-group of $\mathcal{G}$.