Proof Let G be a finite group and H be a subgroup of G of order $o(H)$.

Pick $a \in G$. Let $\{h_1, h_2, \ldots, h_{o(H)}\}$ be the elements of H. It follows that

$$Ha = \{h_1 a, h_2 a, \ldots, h_{o(H)} a\}.$$

Hence Ha contains at most $o(H)$ elements. To show that Ha in fact contains $o(H)$ elements, it is necessary to show that all the elements in the set $\{h_1 a, h_2 a, \ldots, h_{o(H)} a\}$ are distinct.

Indeed, suppose that $h_i a = h_j a$ for some $i, j \in \{1, 2, \ldots, o(H)\}$. By the Cancellation Law 1.9 in G it follows that $h_i = h_j$, i.e. that $i = j$. □

Corollary 3.17. *The right cosets of a subgroup H of order $o(H)$ of a finite group G of order $o(G)$ partition G into $\frac{o(G)}{o(H)}$ subsets, each containing $o(H)$ elements.*

Proof Let G be a finite group of order $o(G)$ and H be a subgroup of G of order $o(H)$.

Suppose that there are k distinct right cosets of H. By Lemma 3.16, each of these right cosets contains $o(H)$ elements. Further, since they are mutually disjoint by Proposition 3.12, the union of these right cosets contains $ko(H)$ elements. Since the right cosets partition G by Proposition 3.12, their union is the set of elements in G. Hence $ko(H) = o(G)$, giving that $k = \frac{o(G)}{o(H)}$. □

Theorem 3.18 (Lagrange's Theorem). *For any subgroup H of a finite group G the order of H, $o(H)$, divides the order of G, $o(G)$.*

Corollary 3.19. *Any group G of prime order $o(G) = p$ has only two subgroups:* **1** *and G itself.*

Example 3.20. Consider the group S_3 of permutations of degree 3. Since $o(S_3) = 3! = 2\times 3$, any subgroup of S_3 must contain 1, 2, 3 or 6 elements. Indeed, the subgroups of S_3 are:

order 1 $\mathbf{1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$;

order 2 $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\},$
$\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\}$;

order 3 $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$;

order 6 $S_3 = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\right.$
$\left.\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\}$.