Strong Cayley theorem with applications (page 1 of 2)

References: I. N. Herstein, *Topics in Algebra*, 1st (1964) pages 60 – 63.
D. Dummit and R. Foote, *Algebra*, 3rd ed. pages 119 – 121.

Cayley's theorem: Every finite group is isomorphic to a group of permutations.

In other words, for every finite group G there exists an $n \in \mathbf{Z}$ a subgroup $H \leq S_n$ and an isomorphism $\Phi: G \mapsto H$. The proof is almost immediate from the observation that left-multiplication by any group-element is a permutation of the elements of G.

More formally, but not necessarily any clearer, for a given a finite group G with elements g_i, $1 \leq i \leq n$. encode the group operation in a function $\mu: \{1, \ldots n\} \times \{1, \ldots n\} \mapsto \{1, \ldots n\}$ by $g_i \cdot g_j = g_{\mu(i,j)}$. Define a map $\Phi: G \mapsto S_n$ by $\Phi(g_i)(j) = \mu(i,j)$ – i. e., the image of the group-element g_i is the permutation $\Phi(g_i)$ which sends each $j \in \{1, \ldots n\}$ to $\mu(i,j)$. The map Φ is a group homomorphism due to the associativity of the group operation: For $g_i, g_j \in G$ and $k \in \{1, \ldots n\}$, calculate $\Phi(g_i \cdot g_j)(k) = \mu(\mu(i,j),k) = \mu(i, \mu(j,k)) = \Phi(g_i)(\Phi(g_j)(k))$. The map Φ is one-to-one due to the cancellation laws in G: Suppose $g_i, g_j \in G$ and $\Phi(g_1) = \Phi(g_2) \in S_n$. Thus for all $k \in \{1, \ldots n\}$, $\mu(i,k) = \Phi(g_1) = \Phi(g_2) = \mu(j,k)$. But we need only one $g_k \in G$ to conclude from $g_i g_k = g_j g_k$ that $g_i = g_j$. Thus Φ is an isomorphism of G onto some subgroup of S_n.

Theorem: Suppose H is a subgroup of a group G with index $|G: H| = m$. Then there exists a homomorphism from G into the symmetric group S_m whose kernel is the largest normal subgroup of G that is contained in H.

Note that this theorem reduces to the classical Cayley's theorem in the special case of $H = \{e\}$.
It addresses the main drawback of the classical theorem that even for small groups the size of the group $S_{|G|} = |G|!$ is huge. Depending on the special case, one may obtain an isomorphic imbedding of G into some smaller S_n, or one uses the homomorphism to draw conclusions about the structure of G.

After above nitpicking excursion, from now on we again liberally identify (maps into) the set of permutations of a set X with n elements with (maps into) the set of permutations of the set $\{i \in \mathbf{Z}^+ : i \leq n\}$.

Proof. Suppose $H \leq G$ and $|G: H| = m$. Consider the set $\mathcal{L}_H = \{aH : a \in G\}$ of left cosets of H in G. The action of G by left multiplication on $\mathcal{L}_H$ induces a map $\Phi: G \mapsto S_{\mathcal{L}_H} \cong S_m$ via $\Phi(g)(aH) = (ga)H$. It is immediate that Φ is a group homomorphism.
The action is transitive since for any $aH, bH \in \mathcal{L}_H$ there exists $g \in G$, namely $g = ba^{-1}$, such that $\Phi(g)(aH) = bH$. The stabilizer of the action in G at $H = eH \in \mathcal{L}_H$ is $C_G(H) = \{g \in G : \Phi(g)(H) = H\} = H$.
We next identify the kernel of the map Φ:

$$\begin{aligned}
\ker \Phi &= \{g \in G : \forall a \in G,\ \Phi(g)(aH) = aH\ \} \\
&= \{g \in G : \forall a \in G,\ (ga)H = aH\ \} \\
&= \{g \in G : \forall a \in G,\ (a^{-1}ga)H = H\ \} \\
&= \{g \in G : \forall a \in G,\ a^{-1}ga \in H\ \} \\
&= \{g \in G : \forall a \in G,\ g \in aHa^{-1}\ \} \quad = \quad \textstyle\bigcap_{a \in G} aHa^{-1} \quad \leq \quad H.
\end{aligned}$$

As the kernel of a group homomorphism $\ker \Phi$ is automatically a normal subgroup of G.
(It is a nice exercise to verify directly that the set $K = \bigcap_{a \in G} aHa^{-1}$ is normal in G – e.g. for any $x \in K$ and any $g \in G$, verify that $gxg^{-1} \in K$ by manipulating this intersection.)
Now suppose $N \trianglelefteq G$ is any normal subgroup of G contained in H. Using $N \leq H$, it is immediate that for every $a \in G$, $N = aNa^{-1} \subseteq aHa^{-1}$ and hence $N \leq \bigcap_{a \in G} aHa^{-1} = \ker \Phi$.

Exercise: Explicitly write out what Φ is, i.e. make a table of function values for Φ, for examples of small groups, e.g. $G = S_3$ and $H =< (1\ 2) >$ or $G = Z_3$ and $H =< 3 >$.

Strong Cayley theorem with applications (page 2 of 2)

The theorem immediately gives rise to the following useful criterion for simple groups. While a special case of the subsequent proposition, we state and prove it separately as its proof is much more immediate.

Corollary: If G is a finite group, $H \leq G$, $|G\colon H| = m > 1$, and $|G| \nmid m!$ then G is not simple.

Proof: Suppose $H \leq G$ is a subgroup of index $|G\colon H| = m$. Let $\Phi\colon G \mapsto S_m$ be the group homomorphism induced by the action of G on left cosets of H by left multiplication. Then $\Phi(G) \leq S_m$ is a subgroup and $|\Phi(G)| \mid m!$. If $|G| \nmid m!$ then $|\Phi(G)| < |G|$ and Φ is not one-to-one. Hence the kernel $\ker\Phi \trianglelefteq G$ is a nontrivial normal subgroup and G is not simple.

Adding one additional observation, one readily strenthens the preceding result to the following:

Proposition: If G is a finite group, $H \leq G$, $|G\colon H| = m > 1$, and $|G| \nmid \frac{1}{2}m!$ then G is not simple.

Proof: Suppose $H \leq G$ is a subgroup of index $|G\colon H| = m$. Let $\Phi\colon G \mapsto S_m$ be the group homomorphism induced by the action of G on left cosets of H by left multiplication. Then $\Phi(G) \leq S_m$ is a subgroup. If $A_m \cap \Phi(G) \neq \Phi(G)$ then $A_m \cap \Phi(G) \trianglelefteq \Phi(G)$ is a nontrivial normal subgroup of $\Phi(G)$ and hence $\Phi^{-1}(A_m \cap \Phi(G)) \trianglelefteq G$ is nontrivial normal subgroup of G. Thus if G is simple, then $\Phi(G) \leq A_m$ and $\ker\Phi = \{e\}$, i.e. Φ is one-to-one. This requires that $|G| = |\Phi(G)| \mid |A_m| = \frac{1}{2}m!$

Application: There are no simple groups of orders $|G| \in \{12, 36, 80, \ldots\}$: By the first Sylow theorem there exist Sylow-subgroups of small index:
If $|G| = 12$ there exists a Sylow-2-subgroup with index 3, yet $12 \nmid 3! = 6$.
If $|G| = 36$ there exists a Sylow-3-subgroup with index 4, yet $36 \nmid 4! = 24$.
If $|G| = 80$ there exists a Sylow-2-subgroup with index 5, yet $80 \nmid 5! = 120$.

Rather immediate is the consequence:

Corollary: Suppose G is a finite group, and there exists a subgroup $H \leq G$ whose index $|G\colon H| = p$ is the smallest prime dividing the order of G. Then G is not simple.

Remark: Of course, in general there is no reason why there should exist any such subgroup of index p.

Proof: Suppose G is a finite group of order $|G| = mp^s$ with $p < m$ prime, $p \nmid m$, and $H \leq G$ is a subgroup of index $|G\colon H| = p$. Since the only divisors of $p!$ different from p are smaller than p, yet all prime factors of $m > p$ are larger than p it follows that $|G| = mp^s \nmid p!$ and thus G is not simple.

Looking more carefully at the situation, one improves this last statement to the more precise:

Corollary: Suppose G is a finite group, p is the smallest prime dividing the order of G, and $H \leq G$ is a subgroup of index $|G\colon H| = p$. Then $H \trianglelefteq G$ is a normal subgroup of G.

Proof: Suppose G is a finite group of order $|G| = mp^s$ with $p < m$ prime, $p \nmid m$, and $H \leq G$ is a subgroup of index $|G\colon H| = p$. Write $K = \ker\Phi \trianglelefteq G$ for the kernel of the group homomorphism Φ induced by the action of G on left cosets of H, and write $k = |H\colon K|$. By the third isomorphism theorem $|G\colon K| = |G\colon H| \cdot |H\colon K| = pk$. By the first isomorphism theorem, the subgroup $\Phi(G) \leq S_p$ is isomorphic to the quotient group G/K, and hence the index $kp = |G\colon K| = |G/K| = |\Phi(G)| \mid p!$ of K in G divides $p!$. Consequently, k divides $(p-1)!$ and also mp^{s-1}, but mp^{s-1} has no divisors smaller than p. Therefore $k = 1$, and hence $H = K \trianglelefteq G$ is normal in G.

Application: Suppose G is a finite group and $H \leq G$ is a subgroup of index $|G\colon H| = 3$.
Then $H \trianglelefteq G$ is normal, or G contains a subgroup $N \leq G$ of index $|G\colon N| = 2$ (which is normal).