Math 412. Cayley's Theorem
Professors Jack Jeffries and Karen E. Smith

CAYLEY'S THEOREM: Every finite group G is isomorphic to a subgroup of the symmetric group $\mathcal{S}_n$ for some n.

TERMINOLOGY: If a group G is isomorphic to a subgroup of a group H, we say G **embeds in** H. In this case there is an embedding (another word for injective homomorphism) $G \hookrightarrow H$ which identifies G with its image in H. So Cayley's theorem says that every finite group embeds in a symmetric group.

A. WARM UP.

(1) Explain how to see $\mathbb{Z}_n$ as a subgroup of $\mathcal{S}_n$.
(2) Explain how $\mathbb{Z}_d \times \mathbb{Z}_e$ embeds in $\mathcal{S}_n$, where $n = d + e$.
(3) I claim that $\mathcal{S}_n$ has many subgroups but few quotient groups. What do I mean?

(1) The group $\langle (123\cdots n)\rangle$ is cyclic of order n, and hence isomorphic to $\mathbb{Z}_n$.
(2) The subgroup G of $\mathcal{S}_{d+e}$ generated by $\langle (123\cdots d), (d+1\ \ldots e)\rangle$ is isomorphic to $\mathbb{Z}_d \times \mathbb{Z}_e$. To see this, we map $\mathbb{Z}_d \times \mathbb{Z}_e \to G$ by sending $(a, b) \mapsto (123\cdots d)^a \circ (d+1\ \ldots e)^e$ and observe that this is a well-defined surjective homomorphism with trivial kernel. [Check it!]
(3) Every finite group embeds in $\mathcal{S}_n$ for appropriate n, but the only quotients of $\mathcal{S}_n$ are $\mathcal{S}_n$ (which is the quotient by the trivial group), $\{e\}$, which is the quotient by the whole group, and $\mathcal{S}_n/A_n \cong \{\pm 1\}$, which is the quotient by the alternating group (plus one more quotient $\mathcal{S}_4/K$ of order 6 which is isomorphic to S_3.) This is a far cry from "all groups."

B. Fix a group G.

(1) Show that G acts on itself by left multiplication.
(2) If G has order n, explain how (1) gives rise to a mapping
$$G \to \mathcal{S}_n.$$
[Hint: What is another name for $Bij(X)$ when X has n elements?]
(3) What did you prove on Problem Set 9 about this mapping between two groups G and S_n?

(1) We verify that $g \cdot x = gx$ is an action of G on itself. This is easy: $e \cdot x = x$ and $g \cdot (h \cdot x) = g(hx) = (gh)x$ by the associative axiom of a group.
(2) We take each $g \in G$ to the map $G \xrightarrow{g} G$ sending $x \mapsto gx$, which is a bijection of the n-element set G. This defines a map $G \to S_n$.
(3) We proved this map $G \to S_n$ is a group homomorphism! More generally, for any group action on a set X, there is a group homomorphism $G \to Bij(X)$.

C. THE PROOF OF CAYLEY'S THEOREM Prove Cayley's theorem by considering the action of G on itself by left multiplication.

Your proof actually proves a stronger statement than the above, in which the size of the needed symmetric group is predicted. State this stronger theorem.

When G acts on itself by left multiplication we get a group homomorphism $G \to S_n$, where $n = |G|$. We only need to show that this map is injective, then the first isomorphism theorem will imply that G is isomorphic to its image in S_n. To prove the map is injective, say that $g \in G$ is in the kernel. This means that multiplication by g gives the identity map in $\mathcal{S}_n$. But then $g = e$. QED.

Note that we have actually proved that G embeds in $\mathcal{S}_n$ where $n = |G|$. So not just that there exists some n that works, but for this specific $n = |G|$, we know G is isomorphic to a subgroup of S_n.

D. The proof of Cayley's Theorem shows that if G has n elements, then G is isomorphic to a subgroup of $\mathcal{S}_n$.

(1) Explain why G can be viewed as a subgroup of $\mathcal{S}_m$ for all $m \geq |G|$.
(2) Show that the group $\mathbb{Z}_p$ embeds in $\mathcal{S}_n$ if and only if $n \geq p$, so that this result is sharp in general.
(3) For the group $G = D_4$, however, show that G embeds in a much smaller symmetric group (namely S_4).
(4) Show that if G acts faithfully on a set of d elements, then G embeds in $\mathcal{S}_d$. [Recall that a **faithful** action is one satisfying the following: for each $g \in G$, there is an $x \in X$ such that $g \cdot x \neq x$.]
(5) What is the smallest symmetric group in which the dihedral group D_n embeds?

(1) We can embed G in $S_{|G|}$ and for any n and $m \geq n$, we can embed $\mathcal{S}_n \hookrightarrow \mathcal{S}_m$ just by extending any permutation of $\{1, 2, \ldots, n\}$ to the "same" permutation on $\{1, 2, \ldots, n, n+1, \ldots, m\}$ which fixes the elements $n+1, \ldots, m$. So the composition of embeddings $\mathcal{G} \hookrightarrow S_{|G|} \hookrightarrow S_m$ is an embedding.
(2) If we could embed $\mathbb{Z}_p$ in $\mathcal{S}_n$, then $\mathcal{S}_n$ would have to have an order p element. As a product of disjoint cycles, then, it could only be a p-cycle. But there are no p-cycles is $p > n$.
(3) The action of D_4 on the vertices of the square induces a group homomorphism $D_4 \to \mathcal{S}_4$. It is injective, because if a symmetry fixes all four vertices, it must fix the whole square.
(4) In general, if G acts faithfully on X (cardinality n), then the map $G \to S_n$ is injective (you proved this on problem set 9).
(5) D_n embeds in $\mathcal{S}_n$ because it acts faithfully on the vertices of the regular n-gon. In general, this is the best we can do. For example, if p is prime, then D_p contains a p-cycle, so if we could embed D_p in $\mathcal{S}_n$, then we could embed a cyclic group of order p as well (generated by the p-cycle). We already saw in (2) that this is impossible if $n < p$. So in general, we can embed D_n in S_n for all n, but we can not embed all D_n in smaller S_m.
(6)