Generalized Cayley's Theorem

July 2023
Tim Bates

Everyone who has taken an introductory course in algebra has likely seen Cayley's theorem: that every group G of order n can be embedded into S_n. It is one of the first applications that we see of group actions which yields a rather pretty result. It is also likely the first representation theorem that we encounter. We will remind ourselves of the proof:

Proof. Let G act on itself via left translation. Fix $a \in G$, then $g \mapsto ag$ is a bijection on G (since we can compose with the action by a^{-1} and obtain identity). Now let us view the left action by a as a permutation calling it L_a. $L_a \in S_G$ is clearly a symmetry of G by the previous discussion, now we simply need to show that the following map $\varphi : G \to S_G$ defined by $a \mapsto L_a$ is an injective homomorphism. To show it is a homomorphism let $a, b \in G$, then $L_{ab}(x) = (ab)x = a(bx) = L_aL_b(x)$ is a homomorphism by the associativity of group actions. Injectivity follows since if $a, b \in G$ with $a \neq b$ then $L_a(e) = a \neq b = L_b(e)$. □

Notice that this proof does not suppose the order of G to be finite; however, we will be interested in cases where $|G| < \infty$. Another thing to note is that the embedding of G (with $|G| = n$) in S_n is a simply transitive group acting on G (which we identified with $\{1, \dots, n\}$). A simply transitive group action is one where given $a, b \in G$ there is a unique σ such that $\sigma(a) = \sigma(b)$. This follows immediately from the cancellation property of groups ($ax = bx \Rightarrow a = b$). Now we want to show what Rotman [1] calls a generalization of Cayley's theorem.

Theorem 1. *If $H \leq G$ is a subgroup of G with $[G : H] = n$, then there exists a homomorphism $\varphi : G \to S_n$ with $\ker \varphi \leq H$.*

It is a generalization since if G is finite and we take $H = \langle e \rangle$, then we can find a homomorphism $\varphi : G \to S_n$ with $\ker \varphi = \langle e \rangle$, thus forcing φ to be injective. Now we prove this statement.

Proof. Let $\mathscr{H}$ denote the collection of all left cosets of H in G. We will let G act on $\mathscr{H}$ and then find our homomorphism. Let $a \in G$ and define $\varphi_a : \mathscr{H} \to \mathscr{H}$ by $gH \mapsto agH$. This is a well defined function on $\mathscr{H}$ since if gH and $g'H$ represent the same coset then $(ag')^{-1}ag = g'^{-1}a^{-1}ag = g'^{-1}g \in H$. It also again represents a bijection on $\mathscr{H}$ due to the existence of inverses which compose to form the identity permutation for any $a \in G$. Now let $\varphi : G \to S_{\mathscr{H}} \cong S_n$ by $g \mapsto \varphi_a$. This clearly is a homomorphism by the same argument as in the proof of Cayley's theorem. Now let $a \in \ker \varphi$, then it follows that $aH = H$ which in turn implies $a \in H$, thus $\ker \varphi \leq H$ and we are done. □

Now a couple of nice results follow from this.

Corollary 1. *Let G be a simple group with a subgroup H of index n, then G can be embedded in S_n.*

Proof. We know from Theorem 1 that there is a homomorphism $\varphi : G \to S_n$ with $\ker \varphi \leq H$, but since G is normal, it follows that $\ker \varphi = \langle e \rangle$ thus φ is injective and constitutes an embedding. □

This corollary can be quite useful when analyzing the subgroup structure of simple groups.

Corollary 2. *A_6 has no subgroup of prime index.*

Proof. First, $|A_6| = 360 = 2^3 \cdot 3^2 \cdot 5$. By Lagrange's theorem, the index of any subgroup must divide the order of A_6. Thus if A_6 were to have a subgroup of prime index, then the index would need to be either 2, 3, or 5. Since A_6 is simple, it follows from the previous corollary to the generalized Cayley theorem that if there were to be subgroups of index 2, 3, or 5, then A_6 could be embedded into S_2, S_3, or S_5. However, $|S_2| = 2 < |A_6|$, $|S_3| = 6 < |A_6|$, and $|S_5| = 120 < |A_6|$, thus no embedding can exist because not even an injective map could exist from A_6 to $S_{2,3,5}$. We conclude that A_6 admits no prime index subgroups. □

This means for example that A_6 does not admit a subgroup of order 64. We can potentially generalize this to other cases. Recall that A_n is simple for $n > 4$.

Proposition 1. *Let $k > 3$, A_{2k} has no subgroup of prime index.*

Proof. By Lagrange's theorem, the index must divide the order of A_{2k} so the largest potential prime index subgroup has index $[A_{2k} : H] = 2k - 1$. Suppose that such a subgroup exists, then there is by Generalized Cayley's thereom a homomorphism $\varphi : A_{2k} \to S_{2k-1}$, however

$$|S_{2k-1}| = (2k-1)! < \frac{(2k)!}{2}$$

for $k > 3$. Since such a map cannot be injective, we reach a contradiction since A_{2k} is simple. □

This argument also holds for odd composite A_n; however, fails for A_p when p is prime. This also clearly fails for A_4 since there is an index 3 subgroup isomorphic to V (the Klein-4 Group). Let's explore another example.

Example 1. *Let $D_{2n} = \langle a, b | a^n = e, b^2 = e, bab = a^{-1} \rangle$ denote the dihedral groups (which have order $2n$). Note that for n at least 3, $\langle b \rangle$ (a subgroup of index n) is not a normal subgroup since $aba^{-1} = a^2 b \neq e$. By Theorem 1 we see then that there is an embedding of D_{2n} in S_n, which is a significant improvement over Cayley's theorem.*

Let's continue to think about these types of situations. We have a group G with a subgroup H which contains no normal subgroups and is itself not normal. We can potentially utilize such an H to find better embedding results.

Corollary 3. *Let $H < G$ be a proper subgroup containing no nontrivial normal subgroup of G with $[G : H] = n$, then $G \hookrightarrow S_n$.*

Proof. By Theorem 1, there is a homomorphism $\varphi : G \to S_n$ with $\ker \varphi \leq H$ but since H contains no nontrivial normal subgroups of G it follows $\ker \varphi = \langle e \rangle$ and thus φ is an embedding. □

Proposition 2. *Let $n > 4$, then S_n does not have any index k subgroups with $2 < k < n$.*

Proof. The only normal subgroups of S_n (with $n > 4$) are $\langle e \rangle, A_n$ and S_n. This means that any index k subgroup with $k \in \{3, \ldots, n-1\}$ is not normal and does not contain A_n, thus $\ker \varphi = \langle e \rangle$, but this implies that there is an embedding $S_n \to S_k$ with $k < n$, a contradiction. □

Proposition 3. *There is no embedding of $\mathbb{Z}_p$ into S_n with $n < p$.*

Proof. The only subgroups of $\mathbb{Z}_p$ are the whole group and the trivial subgroup, thus any embedding will be into S_p or S_n with $n \geq p$. □

Notice that we did not need the generalization of Cayley's theorem for the previous proposition as it is obvious that there is no element of order p in S_n with $n < p$ and thus no embedding can exist. Nevertheless we bring it up to demonstrate the versatility of Theorem 1. The utility comes mostly in the fact that we now have some bounds on the index of subgroups of G.

Proposition 4. *A group of order $2n$ with n odd has a subgroup of index two.*

Proof. Here we utilize Cayley's theorem. Let G act on itself by left translation, then we have an embedding φ of G into S_{2n} which we call $\mathrm{im}\varphi$. Since there are elements of order 2 in G we know that these elements in $\mathrm{im}\varphi$ will consist of disjoint transpositions. Since this embedding is simply transitive, it follows that there must be n transpositions. Since n is odd, we know that the elements of order two have a negative sign. Thus the map $Sgn : \mathrm{im}(\varphi) \to \{\pm 1\}$ is surjective and $\ker Sgn \cong \mathrm{Im}(\varphi)/\{\pm\}$ is an index two subgroup. □

Now I want to end with a discussion of representation theory.

Definition 1. *Let V be a vector space over a field of characteristic 0. A representation of a group G on V is a map*

$$\rho : G \to GL(V)$$

This definition can be generalized to R-modules rather than vector spaces, but for the moment a vector space over $\mathbb{C}$ will be sufficient.

Theorem 2. *S_n is isomorphic to the group of $n \times n$ nonsingular matrices with only 1's (the permutation matrices).*

We can see this isomorphism by defining the map which takes $S_n \ni \sigma = \begin{pmatrix} 1 & 2 \dots & n & \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ to the matrix which has a 1 in the $(\sigma(i), i)$th entry. Now this collection of permutation matrices is obviously a subgroup of $GL_n(\mathbb{C})$ and thus a group homomorphism $\varphi : G \to S_n \hookrightarrow GL_n(\mathbb{C})$ constitutes a representation of G in $GL_n(\mathbb{C})$. The representation of G obtained via our proof of Cayley's theorem is often called the left regular representation of G. At the very beginning we could have just as well taken the right action of G on itself and obtained the right regular representation of G.

References

[1] Joseph Rotman. *An introduction to the Theory of Groups*. 1995.