Cayley's Theorem

How can we understand all finite groups? One way, which we return to later, is to try and classify, i.e. list, all groups up to isomorphism. Here is another way to "understand all finite groups": show that all such groups are isomorphic to subgroups of groups we understand. This can be done using the following theorem.

▸ **Cayley's Theorem**: **Let G be a finite group, and $|G| = n$. Then there is a 1-1 homomorphism $\phi : G \to S_n$. In particular, G is isomorphic to a subgroup of S_n.**

Before proving this theorem, let's see why it does what we want. Given any homomorphism $\phi : G \to G'$ we can define a new homomorphism $\psi : G \to \mathrm{im}(\phi)$ by setting $\psi(a) = \phi(a)$ for all $a \in G$; we have only changed the definition of the target group. The homomorphism $\psi : G \to \mathrm{im}(\phi)$ has the advantage that it is *onto*. The 1st Isomorphism Theorem for ψ yields

$$G/\ker(\phi) \cong \mathrm{im}(\phi)$$

In particular, when ϕ is 1-1, we have $G \cong \mathrm{im}(\phi)$. Now return to the statement of Cayley's Theorem, which gives a 1-1 homomorphism $\phi : G \to S_n$. Then $G \cong \mathrm{im}(\phi)$, and $\mathrm{im}(\phi) \subset S_n$ is a subgroup of S_n. Thus G is isomorphic to a subgroup of S_n.

Proof. Label elements of G as $a_1, a_2, \ldots, a_n$. Let $a \in G$. (This a is among the a_i, but we will just write a for it.) Define a function $\sigma_a : \{1, \ldots, n\} \to \{1, \ldots, n\}$ as follows:

$$aa_i = a_{\sigma_a(i)}$$

In other words, given $i \in \{1, \ldots, n\}$, we take the product $aa_i \in G$, and it is equal to some a_k where $k \in \{1, \ldots, n\}$; we let $\sigma_a(i) = k$. The map σ_a is 1-1: suppose $\sigma_a(i) = \sigma_a(j)$. Then

$$aa_i = aa_j \quad \Longrightarrow \quad a_i = a_j \quad \Longrightarrow \quad i = j$$

The map σ_a is onto: suppose $k \in \{1, \ldots, n\}$. Let a_i be such that $a = a_k a_i^{-1}$. Then

$$aa_i = a_k a_i^{-1} a_i = a_k \quad \Longrightarrow \quad \sigma_a(i) = k$$

Thus σ_a is 1-1 and onto, and therefore a permutation, i.e. $\sigma_a \in S_n$.

Now we are in a position to define the sought after homomorphism:

$$\phi : G \longrightarrow S_n$$

For $a \in G$ we declare $\phi(a) = \sigma_a$. We check this is a homomorphism. Let $a, b \in G$. We must compare $\phi(a)\phi(b) = \sigma_a \circ \sigma_b$ with $\phi(ab) = \sigma_{ab}$. We compute

$$a_{\sigma_{ab}(i)} = (ab)a_i = a(ba_i) = aa_{\sigma_b(i)} = a_{\sigma_a(\sigma_b(i))}$$

for any $i \in \{1, \ldots, n\}$, which shows that $\sigma_{ab} = \sigma_a \circ \sigma_b$. To show ϕ is 1-1, we compute its kernel. Suppose $\phi(a) = e$, i.e. $\sigma_a(i) = i$ for all $i \in \{1, \ldots, n\}$. This means

$$aa_i = a_{\sigma_a(i)} = a_i$$

which implies $a = e$. Thus $\ker(\phi) = \{e\}$ and therefore ϕ is 1-1. □

Let us see Cayley's Theorem in action. To clarify the main point, take G to be an interesting group which is not defined using permutations. Let us introduce the *quaternion group*

$$Q_8 = \{ 1, -1, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$$

of order 8, with the relations that -1 commutes with everything, $(-1)^2 = 1$, and also $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, and $\mathbf{ij} = \mathbf{k}$. These relations generate the Cayley table of Q_8 as follows:

	1	-1	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
1	1	-1	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
-1	-1	1	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{i}$	-1	1	$\mathbf{k}$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$
$-\mathbf{i}$	$-\mathbf{i}$	$\mathbf{i}$	1	-1	$-\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$	-1	1	$\mathbf{i}$	$-\mathbf{i}$
$-\mathbf{j}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$	1	-1	$-\mathbf{i}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{i}$	$\mathbf{i}$	1	-1
$-\mathbf{k}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{i}$	$-\mathbf{i}$	-1	1

Cayley's Theorem gives us a way to realize Q_8 as a subgroup of the symmetric group S_8. The construction is as follows. First we label the elements of Q_8 as $a_1, \ldots, a_8$. For example, we may use the following labelling (although any labelling will do):

$$a_1 = 1, \quad a_2 = -1, \quad a_3 = \mathbf{i}, \quad a_4 = -\mathbf{i}, \quad a_5 = \mathbf{j}, \quad a_6 = -\mathbf{j}, \quad a_7 = \mathbf{k}, \quad a_8 = -\mathbf{k}$$

Next, given an element $a \in Q_8$ we define the associated permuation $\sigma_a \in S_8$ by the relation

$$aa_i = a_j \qquad \Longleftrightarrow \qquad \sigma_a(i) = j$$

Let us spell this out for the element $a = \mathbf{i} \in Q_8$. We have

$$\begin{aligned} aa_1 &= (\mathbf{i})(1) = \mathbf{i} = a_3 & aa_2 &= (\mathbf{i})(-1) = -\mathbf{i} = a_4 \\ aa_3 &= (\mathbf{i})(\mathbf{i}) = -1 = a_2 & aa_4 &= (\mathbf{i})(-\mathbf{i}) = 1 = a_1 \\ aa_5 &= (\mathbf{i})(\mathbf{j}) = \mathbf{k} = a_7 & aa_6 &= (\mathbf{i})(-\mathbf{j}) = -\mathbf{k} = a_8 \\ aa_7 &= (\mathbf{i})(\mathbf{k}) = -\mathbf{j} = a_6 & aa_8 &= (\mathbf{i})(-\mathbf{k}) = \mathbf{j} = a_5 \end{aligned}$$

These relations then determine the permutation $\sigma_a = \sigma_{\mathbf{i}}$ as follows:

$$\sigma_a(1) = 3, \quad \sigma_a(2) = 4, \quad \sigma_a(3) = 2, \quad \sigma_a(4) = 1,$$

$$\sigma_a(5) = 7, \quad \sigma_a(6) = 8, \quad \sigma_a(7) = 6, \quad \sigma_a(8) = 5$$

All together we may write our permutation $\sigma_a = \sigma_{\mathbf{i}}$ in cycle notation as

$$\sigma_{\mathbf{i}} = (1324)(5768) \in S_8$$

We may proceed to do this for each element $a \in Q_8$. We get the following subgroup of S_8:

$$\{e,\ (12)(34)(56)(78),\ (1324)(5768),\ (1423)(5867),$$
$$(1526)(3847),\ (1625)(3748),\ (1728)(3546),\ (1827)(3645)\}$$

The elements are listed in the order corresponding to the above ordering of the elements of Q_8. In summary, Q_8 is isomorphic to the subgroup of S_8 displayed above.

Cayley's Theorem is conceptually very important: it says that every finite group, however abstractly defined, is isomorphic to a subgroup of some symmetric group, a very concrete type of group that we understand how to work with. On the other hand, Cayley's Theorem is often not practical: it realizes our group as a subgroup of a generally very large group. For example, in the example above, Q_8 has order 8 and we realized it as a subgroup of S_8 which is of order $8! = 40320$.

The following is a generalization of Cayley's Theorem.

▶ **Let G be a group, $H \subset G$ a subgroup, and suppose $[G : H] = n$ is finite. Then there is a homomorphism $\phi : G \to S_n$. Furthermore, $\ker(\phi)$ is equal to the largest normal subgroup of G which is contained in H.**

To obtain Cayley's Theorem as a special case, let $H = \{e\}$. Then $n = [G : \{e\}] = |G|$. The largest normal subgroup contained in $\{e\}$ is of course $\{e\}$, and so $\ker(\phi) = \{e\}$, i.e. ϕ is 1-1.

The proof of this generalization is similar to that of Cayley's Theorem. We list the distinct cosets in G/H as $a_1H, \ldots, a_nH$. Then define $\phi : G \to S_n$ by $\phi(a) = \sigma_a$ where $\sigma_a \in S_n$ is determined by the relation: $\sigma_a(i) = j$ if and only if $aa_iH = a_jH$, where $i, j \in \{1, \ldots, n\}$. The details for the rest of the proof are left as an exercise.

▶ **Let G be a finite group, $H \subset G$ a proper subgroup, and suppose $|G|$ does not divide $[G : H]!$. Then H contains a non-trivial normal subgroup of G.**

This is a corollary of the above theorem. Suppose H does *not* contain a non-trivial normal subgroup. Then the homomorphism $\phi : G \to S_n$ from the above theorem, where $n = [G : H]$, must have $\ker(\phi) = \{e\}$. Thus $G \cong \mathrm{im}(\phi)$ is isomorphic to a subgroup of S_n. By Lagrange's Theorem, we must have that $|G|$ divides $|S_n| = n! = [G : H]!$.