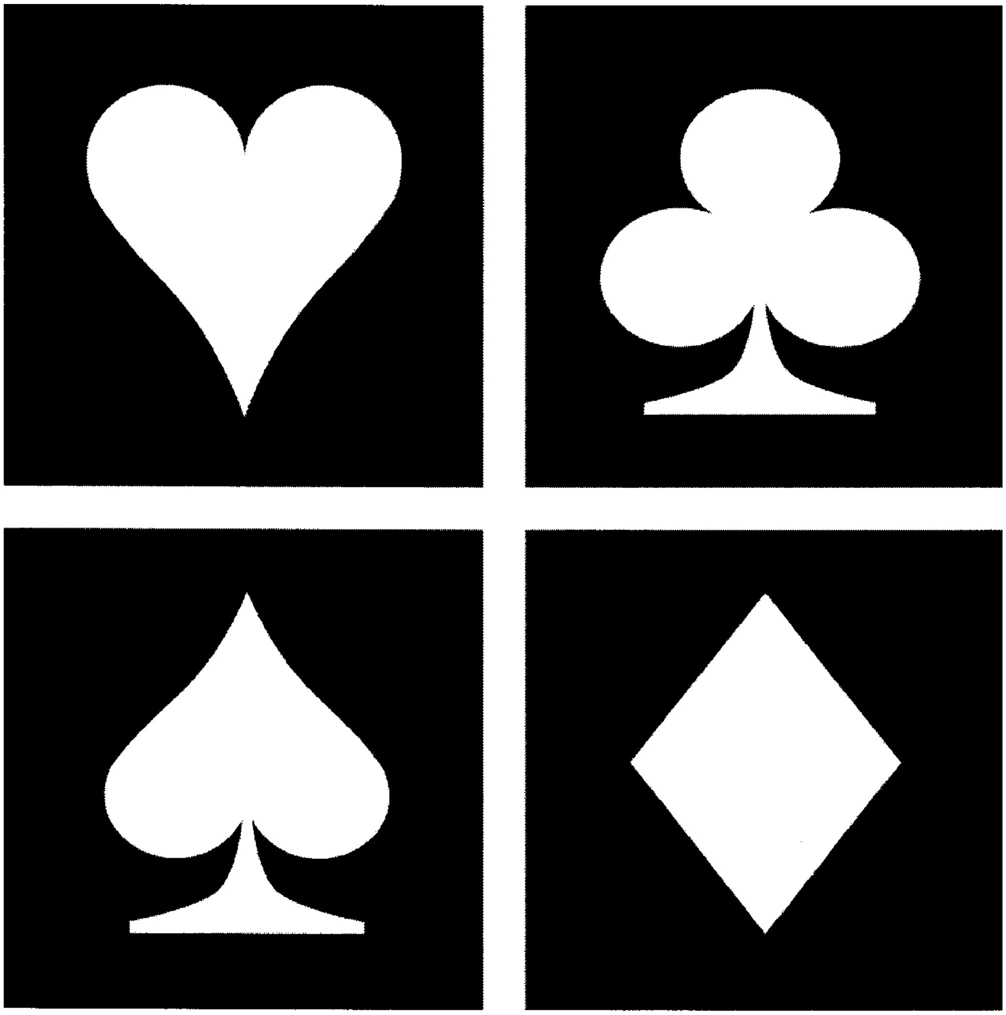
Cayley's Theorem

Amittai Siavava and John Voight

3 november 2022



Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***Abstract Algebra*** by **David S. Dummit & Richard M. Foote**.

(b) ***Algebra*** by **Jacob K. Goldhaber & Gertrude Ehrlich**

Cayley's Theorem

Amittai Siavava and John Voight

3 november 2022

[This is an example of a FLEX paper for Math 71, Fall 2022. It is meant as a sample so you can see how you might approach the paper, a LaTeX template to help you to get started (if you want to), and to provide some general indications of what this might look like. Your paper might have a different structure, length, approach, voice, and composition.]

1. Introduction

When groups are first introduced, they are described as sets equipped with a binary operation satisfying certain axioms (associativity, identity, inverses). As examples, we considered the symmetric groups S_n, the group of permutations of the set $\{1, \dots, n\}$. However, these are not so far apart. Even for Galois (see Dummit–Foote [**DummitFoote**]), groups were made of "substitutions"—i.e., Galois was working with permutation groups!

For now, we restrict attention to *finite* groups (but see section 4 below for infinite groups). So the symmetric groups S_n (for $n \geq 1$) are finite groups. Is every finite a group a permutation group? No: we have $\#S_n = n!$, so a group of order 4 cannot be isomorphic to S_n since $2! < 4 < 3!$. But if we all ourselves *subgroups* of permutation groups, the answer is yes. Our main result is as follows.

Theorem 1.1 (Cayley). Every finite group is isomorphic to a subgroup of S_n for some $n \geq 1$.

Contents. In section 2, we get set up by describing how the group operation naturally describes permutations of the elements of the group. We then prove Cayley's theorem in section 3. We then conclude in section 4 with some applications and next steps.

2. Setup

We start with a motivating example. Recall the Cayley table for D_6, the dihedral group of order 6:

	1	r	r^2	s	sr	sr^2
1	1	r	r^2	s	sr	sr^2
r	r	r^2	1	sr^2	s	sr
r^2	r^2	1	r	sr	sr^2	s
s	s	sr	sr^2	1	r	r^2
sr	sr	sr^2	s	r^2	1	r
sr^2	sr^2	s	sr	r	r^2	1

We observed that Cayley table have the Sudoku property, as in the following lemma.

Lemma 2.1. Each row (and column) of the Cayley table of a finite group G contains all elements of G.

As a reminder, this lemma follows directly from the cancellation law.

Returning to the above example, if we pick off just one row—say the row sr—by this property we get a permutation of the set D_6:

$$\begin{pmatrix} 1 & r & r^2 & s & sr & sr^2 \\ sr & sr^2 & s & r^2 & 1 & r \end{pmatrix} \tag{2.2}$$

We denote this element $\sigma_{sr} \colon D_6 \to D_6$, since it is a symmetry that depends on sr: it is defined by $\sigma_{sr}(sr) = 1, \ldots,$ $\sigma_{sr}(sr^2) = r$, reading the input from the top row of the table and the output from the bottom row. This is visibly a bijection from D_6 to itself: each element of D_6 appears exactly once.

Recall that we write the set of bijections from a set A to itself as

$$\mathrm{Sym}(A) := \{\sigma \colon A \to A \text{ bijection}\}$$

and this forms a group under composition. This works for every set A, even though we mostly worked with $A = \{1, \ldots, n\}$ and then abbreviate $S_n = \mathrm{Sym}(\{1, \ldots, n\})$. There is no loss of generality here.

Lemma 2.3. If A is a finite set with $\#A = n$, then the groups $\mathrm{Sym}(A) \simeq S_n$ are isomorphic.

Bewijs. Since $\#A = n$, there is a bijection from A to $\{1, \ldots, n\}$. Each permutation of the elements of A gives a permutation of the elements $\{1, \ldots, n\}$ by how they are numbered. □

Putting these together, we can define a function

$$\begin{aligned}
\sigma \colon D_6 &\to \mathrm{Sym}(D_6) \simeq S_6 \\
1 \mapsto \sigma_1 &= \begin{pmatrix} 1 & r & r^2 & s & sr & sr^2 \\ 1 & r & r^2 & s & sr & sr^2 \end{pmatrix} \\
&\vdots \\
sr^2 \mapsto \sigma_{sr^2} &= \begin{pmatrix} 1 & r & r^2 & s & sr & sr^2 \\ sr^2 & s & sr & r & r^2 & 1 \end{pmatrix}
\end{aligned} \tag{2.4}$$

Usually we write functions like $f(x)$ with input x from the domain; but here the output is itself a function which wants input, so in order not to get confused, we use a subscript.

That is a start, but of course in group theory we want more than just a map of sets: we want to know it is a homomorphism! One case of the homomorphism property in this example would read

$$\sigma_{sr}\sigma_r \overset{?}{=} \sigma_{sr^2} \tag{2.5}$$

This is an equality we need to check on the right-hand side of (2.4). Composing the permutations, we see it checks out! Once we have a homomorphism, we can also see that the kernel of the map σ consists only of the identity: if an element maps to the identity permutation in $\mathrm{Sym}(D_6)$, it would come from a row of the Cayley table where they elements line up according to the identity, and that happens only for the top row. So we get an injective map $D_6 \hookrightarrow S_6$. By the fundamental homomorphism theorem, we see that D_6 is isomorphic to its image under this map; the following lemma reminds us of how this works in general.

Theorem 2.6 (Fundamental homomorphism theorem). Let $\phi\colon G \to H$ be a group homomorphism. Then $G/\ker\phi \simeq \phi(G) \leq H$.

Corollary 2.7. If $\phi\colon G \to H$ is an injective group homomorphism, then $G \simeq \phi(G)$.

Bewijs. If ϕ is injective, then $\ker\phi = \{1\}$, and then $G/\ker\phi \simeq G$ (the cosets of the identity are just the elements of G!). □

We conclude that D_6 is isomorphic to a subgroup of S_6. This is Cayley's theorem!

3. Main result

We are now ready to prove Cayley's theorem, which we will prove in a slightly stronger form.

Theorem 3.1 (Cayley). Let G be a finite group of order $\#G = n$. Then G is isomorphic to a subgroup of S_n.

We follow what we observed in the case $G = D_6$ in the previous section one step at a time.

Throughout, let G be a finite group. First, we define the permutations that come from the rows of the Cayley table. Recall that in the row labelled a (for $a \in G$), with $b \in G$ the column we have entry ab (as usual suppressing $*$ and writing the group multiplicatively).

Lemma 3.2. Let $a \in G$. Define the map

$$\sigma_a \colon G \to G$$

$$x \mapsto ax$$

Then σ_a is a bijection, i.e., $\sigma_a \in \mathrm{Sym}(G)$.

Bewijs. We proved this in class, showing it is both injective and surjective and then that it has inverse $\sigma_{a^{-1}} \colon G \to G$ defined by $b \mapsto a^{-1}b$. □

We then built on this considering all of these bijections at once.

Proposition 3.3. Define the map

$$\sigma \colon G \to \mathrm{Sym}(G)$$

$$a \mapsto \sigma_a$$

Then σ is an injective group homomorphism.

Bewijs. We first show that the map is a homomorphism. Let $a, b \in G$. We want to check

$$\sigma_a \sigma_b \overset{?}{=} \sigma_{ab}.$$

These are two permutations of the set G. To show that two functions are equal, we show that they give the same outputs. So let $x \in G$. Then on the left-hand side, by definition

$$(\sigma_a\sigma_b)(x) = \sigma_a(\sigma_b(x)) = \sigma_a(bx) = a(bx) = abx.$$

This matches the right-hand side:

$$\sigma_{ab}(x) = (ab)x = abx.$$

Thus $(\sigma_a\sigma_b)(x) = \sigma_{ab}(x)$ for all $x \in G$, so then $\sigma_a\sigma_b = \sigma_{ab} \in \mathrm{Sym}(G)$ as functions.

To show that σ is injective, we show that $\ker \sigma \subseteq \{1\}$. Let $a \in G$ be such that a maps to the identity: $\sigma_a = \mathrm{id}_G$. Then for all $x \in G$ we have $\sigma_a(x) = \mathrm{id}_G(x)$, which means $ax = x$ for all $x \in G$. If we plug in $x = 1$ we get $a = 1$, as desired. □

We may now conclude.

Proof of Theorem 3.1. By Proposition 3.3, we have an injective group homomorphism $G \hookrightarrow \mathrm{Sym}(G)$. By Lemma 2.3, we have an isomorphism $\mathrm{Sym}(G) \simeq S_n$, so composing these we get an injective group homomorphism $G \hookrightarrow S_n$. Finally, by the fundamental homomorphism theorem (Corollary 2.7), we conclude that G is isomorphic to its image, a subgroup of S_n. □

4. CONCLUSION

Cayley's theorem shows that we can see every finite group as a subgroup of some permutation group. There can be more than one way to realize a finite group G as a subgroup of permutations: already for D_6 we showed that $D_6 \simeq S_3$ by considering the action of the dihedral group on the vertices of the triangle.

Returning to our proof, we see that the arguments also work when G is an infinite group: we still get an injective group homomorphism $G \hookrightarrow \mathrm{Sym}(G)$; however, now $\mathrm{Sym}(G)$ consists of permutations of an infinite set, so it is not of the form S_n!

The homomorphism constructed in Proposition 3.3 arises naturally in the context of groups acting on themselves (by left multiplication): this is described in detail by Dummit–Foote [**DummitFoote**], with Cayley's theorem as a corollary [**DummitFoote**]. Indeed, *group actions* allow us to see all homomorphisms from a finite group into permutation groups, whether that be on vertices of an n-gon, or on the cosets of a group.

REFERENTIES

[1] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Hoboken, 2003.