11-1-1993

# Cayley's theorem.

Cayley's theorem *represents* a group as a subgroup of a permutation group. This is often advantageous, because permutation groups are fairly concrete objects. For example, it's straightforward to write programs to do arithmetic in finite permutation groups.

You can also think of Cayley's theorem as saying that *all groups arise as groups which act on sets.*

**Theorem.** (Cayley) Every group is isomorphic to a subgroup of a permutation group $S_A$ on a set $A$.

**Remark.** The set $A$ is not unique.

The theorem will construct an injective group homomorphism $\phi$ from a group $G$ to a symmetric group $S_A$. Then $\phi : G \approx \phi(G) < S_A$. Such a map $\phi$ is called a **permutation representation**.

In general, a **representation** of a group is a "concrete" group which is at least homomorphic to the given group. For example, a **matrix representation** (over the reals) is a homomorphism $\phi : G \to GL(n, \mathbb{R})$. You can use the homomorphism to think of elements of $G$ as matrices, and you can then use matrix operations to do computations.

**Proof of Cayley's theorem:** Let $G$ be a group. I want to construct an injective homomorphism $\phi : G \to S_A$, for some $A$. First, I need to come up with a set $A$. Since the only set around is $G$, I'll use $A = G$.

Now I'm looking for an injective homomorphism $\phi : G \to S_G$. In other words, for each element $g \in G$, I must come up with a permutation $\phi(g) : G \to G$. (Thus, $\phi$ will be a function whose outputs are functions!)

$\phi(g)$ must take each element of $G$ to another element of $G$. Picture:

$$\begin{array}{cccc} a & b & c & \ldots \\ \phi(g)(a) & \phi(g)(b) & \phi(g)(c) & \ldots \end{array}$$

This looks like a row of a multiplication table!

Now of course, $G$ may not even be countable, but maybe I can use the idea anyway. Try

$$\phi(g)(x) = gx.$$

In other words, $\phi(g)$ is the permutation which multiplies everything on the left by $g$.

I have a number of things to check:

1. Check that $\phi(g)$ (multiplication by $g$) is really a permutation.
2. Check that $\phi$ is a homomorphism.
3. Check that $\phi$ is injective.

1\. $\phi(g)$ is a permutation.

I need to show that $\phi(g)$ is a bijection $G \to G$. But this is easy: The inverse of multiplication by $g$ is multiplication by $g^{-1}$), and a map with an inverse is bijective.

2\. $\phi$ is a homomorphism.

Let $g, h \in G$. I need to show that $\phi(gh) = \phi(g)\phi(h)$. Notice that the things on the two sides of this equation are *maps* — permutations, in fact. To show that two maps are the same, I must show that they do the same thing to the same input. I'll feed $x \in G$ into the left and right sides and compare:

$$\phi(gh)(x) = (gh)x \text{ and } \phi(g)\phi(h)(x) = \phi(g)(hx) = g(hx).$$

Thus, $\phi(gh)(x) = \phi(g)\phi(h)(x)$. Since $x$ was arbitrary, $\phi(gh) = \phi(g)\phi(h)$.

3\. $\phi$ is injective.

It suffices to show that $\ker\phi = \{1\}$. Suppose $\phi(g) = 1$. What does this mean? Since $\phi(g)$ is a permutation, the "1" on the right must be the identity permutation. So this is an equation relating two maps, and I apply both sides to an element $x \in G$: $\phi(g)(x) = 1(x)$, so $gx = x$. Cancelling the $x$, I find that $g = 1$. Thus, if $g \in \ker\phi$, then $g = 1$. The converse is always true, so $\ker\phi = \{1\}$. Therefore, $\phi$ is injective. □

**Example.** For finite groups, you can read off the permutation representation given by Cayley's theorem from the multiplication table for the group.

Here is the multiplication table for the Klein 4-group:

| | 1 | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ |
| $a$ | $a$ | 1 | $c$ | $b$ |
| $b$ | $b$ | $c$ | 1 | $a$ |
| $c$ | $c$ | $b$ | $a$ | 1 |

The representation will be $\phi : V \to S_4$ (since $V$ has 4 elements). Read off the permutations corresponding to each element by looking down a row. For example,

$$\phi(a) = \begin{pmatrix} 1 & a & b & c \\ a & 1 & c & b \end{pmatrix}$$

The "$(1abc)$" is just the table heading. The "$(a1cb)$" is the $a$-th row of the table. Using $\{1, 2, 3, 4\}$ in place of $\{1, a, b, c\}$, this says

$$\phi(a) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34).$$

Likewise,

$$\phi(1) = \mathrm{id}, \quad \phi(b) = (13)(24), \quad \phi(c) = (14)(23).$$

In other words, $V$ is isomorphic to the subgroup

$$\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} < S_4. \ \square$$