Cayley's Theorem

Cayley's theorem

Let S_n be the symmetric group on n elements.

Any finite group is isomorphic to a subgroup of S_n for some n.

<u>Proof</u>

Let $G = (G, \circ)$ be a group of n elements with binary operation $\circ$

For each g in G define a mapping as follows

Let t_g be the mapping $t_g : x \to g \circ x$ for every $x \in G$.

An equivalent notation for this is $t_g(x) = gx$.

If $x_1, x_2 \in G$ and $t_g(x_1) = t_g(x_2)$ we have $gx_1 = gx_2$ and thus $x_1 = x_2$.

This means that t_g is injective.

For any $y \in G$ we have $t_g(g^{-1}y) = y$ with $g^{-1}y \in G$.

This means that t_g is surjective.

Further, $t_g(G) \subseteq G$.

These altogether mean that t_g is a bijection of G to itself, i.e. t_g is a permutation of the elements of G.

Let $S_n(S_n, \bullet)$ be the set of all permutations of the n elements of G.

(The binary operation of composing permutations is denoted by $\bullet$)

Now

$t_{gh}(x) = g \circ h \circ x = ghx$

But

$t_g \bullet t_h(x) = t_g(hx) = ghx$

$t_{gh}(x) = t_g \bullet t_h(x)$

$t_{gh} = t_g \bullet t_h$

We define a mapping ψ by

$\psi : (G, \circ) \to (S_n, \bullet)$

$\psi : g \to t_g \quad \psi(g) = t_g$

Then since

$\psi(g \circ h) = t_{gh} = t_g \bullet t_h = \psi(g) \bullet \psi(h)$

ψ is a homomorphism.

Now suppose $\psi(g) = e$ where e is the identity permutation in S_n.

But $t_g(x) = g \circ x$

Thus $g = e$ where e is the identity in G

This means that the kernel of the homomorphism is the identity. In symbols: $\ker(\psi) = \{e\}$.

Hence, G is isomorphic to a subset of S_n.

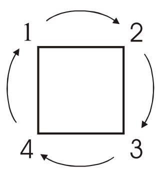
Illustration

To illustrate this proof, consider the group of symmetries of the square. These are

1. <u>Identity</u>

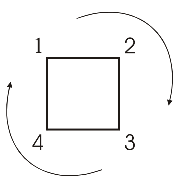
$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

2. <u>Rotation through $\pi/2$</u>



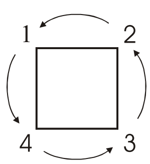
$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

3. <u>Rotation through π</u>



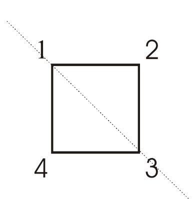
$$r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 2 \end{pmatrix}$$

4. <u>Rotation through $-\pi/2$</u>



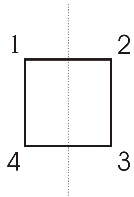
$$r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

5. <u>Reflection through $-\pi/4$</u>



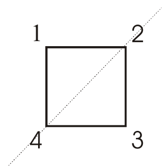
$$q_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

6. Reflection through $\pi/2$



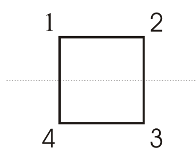
$$q_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

7. Reflection through $+\pi/2$



$$q_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

8. Refleftion through the x-axis



$$q_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

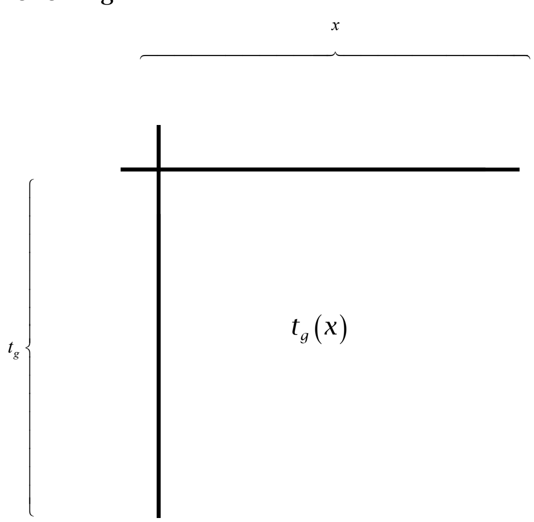
This gives the set $G = \{e, r_1, r_2, r_3, q_1, q_2, q_3, q_4\}$ with group table

	e	r_1	r_2	r_3	q_1	q_2	q_3	q_4
e	e	r_1	r_2	r_3	q_1	q_2	q_3	q_4
r_1	r_1	r_2	r_3	e	q_2	q_3	q_4	q_1
r_2	r_2	r_3	e	r_1	q_3	q_4	q_1	q_2
r_3	r_3	e	r_1	r_2	q_4	q_1	q_2	q_3
q_1	q_1	q_4	q_3	q_2	e	r_3	r_2	r_1
q_2	q_2	q_1	q_4	q_3	r_1	e	r_3	r_2
q_3	q_3	q_2	q_1	q_4	r_2	r_1	e	r_3
q_4	q_4	q_3	q_2	q_1	r_3	r_2	r_1	e

Note, in constructing this table there is no real alternative to just working out most of the entries by hand, the long way. For example, $q_1 r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 4 & 3 & 2 & 1 \end{pmatrix} = q_4$. The mappings, t_g are given by converting the rows of this table into functions

t_g \ x	e	r_1	r_2	r_3	q_1	q_2	q_3	q_4
t_e	e	r_1	r_2	r_3	q_1	q_2	q_3	q_4
t_{r_1}	r_1	r_2	r_3	e	q_2	q_3	q_4	q_1
t_{r_2}	r_2	r_3	e	r_1	q_3	q_4	q_1	q_2
t_{r_3}	r_3	e	r_1	r_2	q_4	q_1	q_2	q_3
t_{q_1}	q_1	q_4	q_3	q_2	e	r_3	r_2	r_1
t_{q_2}	q_2	q_1	q_4	q_3	r_1	e	r_3	r_2
t_{q_3}	q_3	q_2	q_1	q_4	r_2	r_1	e	r_3
t_{q_4}	q_4	q_3	q_2	q_1	r_3	r_x	r_1	e

This exhibits each row as a mapping. The general idea of the mapping can be seen from the following



Each mapping is a permutation of the 8 elements of G, and there are 8 mappings in all. However, in S_8 there are $8! = 40320$ such permutations, and hence 40320 such mappings.

That is rather a lot of mappings, and shows that in some ways Cayley's theorem is interesting only from a theoretical point of view. Since the permutation group in which any other group is embedded is very much larger than that group, this does not tell us much new about its structure. However, it is possible to find a smaller S_n in which to embed a group. In the case of the symmetries of the square, this is S_4, which is the permutation group of four elements, and also the symmetry group of the tetrahedron.

There are 4! = 24 elements in S_4