12. Isomorphisms

Look at the groups D_3 and S_3. They are clearly the same group. Given a symmetry of a triangle, the natural thing to do is to look at the corresponding permutation of its vertices. On the other hand, it is not hard to show that every permutation in S_3 can be realised as a symmetry of the triangle.

It is very useful to have a more formal definition of what it means for two groups to be the same.

Definition 12.1. *Let G and H be two groups. We say that G and H are* ***isomorphic*** *if there is a bijective map $\phi\colon G \longrightarrow H$, which respects the group structure. That is to say, for every g and h in G,*

$$\phi(gh) = \phi(g)\phi(h).$$

The map ϕ is called an ***isomorphism****.*

In words, you can first multiply in G and take the image in H, or you can take the images in H first and multiply there, and you will get the same answer either way.

With this definition of isomorphic, it is straightforward to check that D_3 and S_3 are isomorphic groups.

Lemma 12.2. *Let G and H be two cyclic groups of the same order.*

Then G and H are isomorphic.

Proof. Let a be a generator of G and let b be a generator of H. Define a map

$$\phi\colon G \longrightarrow H$$

as follows. Suppose that $g \in G$. Then $g = a^i$ for some i, and we send g to $g' = b^i$.

We first have to check that this map is well-defined. If G is infinite, then so is H and every element of G may be uniquely represented in the form a^i. Thus the map is automatically well-defined in this case. Now suppose that G has order k, and suppose that $g = a^j$. Then we are trying to send g to both b^i and b^j. We have to check that $b^i = b^j$.

As $a^i = a^j$, $a^{i-j} = e$ and k must divide $i - j$. In this case $b^{i-j} = e$ as the order of H is equal to k. But then $b^i = b^j$. Thus ϕ is well-defined. The map

$$H \longrightarrow G$$

defined by sending b^i to a^i is clearly the inverse of ϕ. Thus ϕ is a bijection.

Now suppose that $g = a^i$ and $h = a^j$. Then $gh = a^{i+j}$ and the image of this element would be b^{i+j}.

On the other hand, the image of a^i is b^i and the image of a^j is b^j and the product of the images is $b^i b^j = b^{i+j}$. □

Here is a far more non-trivial example.

Lemma 12.3. *The group of real numbers under addition and positive real numbers under multiplication are isomorphic.*

Proof. Let G be the group of real numbers under addition and let H be the group of real numbers under multiplication. Define a map

$$\phi \colon G \longrightarrow H$$

by the rule $\phi(x) = e^x$. This map is a bijection, by the well-known results of calculus. We want to check that it is a group isomorphism. Suppose that x and $y \in G$. Then multiplying in G, we get $x + y$. Applying ϕ we get e^{x+y}.

On the other hand, applying ϕ directly we get e^x and e^y. Multiplying together we get $e^x e^y = e^{x+y}$. □

Definition 12.4. *Let G be a group. An isomorphism of G with itself is called an **automorphism**.*

Definition-Lemma 12.5. *Let G be a group and let $a \in G$ be an element of G. Define a map*

$$\phi \colon G \longrightarrow G$$

by the rule

$$\phi(x) = axa^{-1}.$$

Then ϕ is an automorphism of G.

Proof. We first check that ϕ is a bijection.

Define a map

$$\psi \colon G \longrightarrow G$$

by the rule

$$\psi(x) = a^{-1}xa.$$

Then

$$\begin{aligned} \psi(\phi(x)) &= \psi(axa^{-1}) \\ &= a^{-1}(axa^{-1})a \\ &= (a^{-1}a)x(a^{-1}a) \\ &= x. \end{aligned}$$

Thus the composition of ϕ and ψ is the identity. Similarly the composition of ψ and ϕ is the identity. In particular ϕ is a bijection.

Now we check that ϕ is an isomorphism.

$$\begin{aligned}\phi(x)\phi(y) &= (axa^{-1})(aya^{-1}) \\ &= a(xy)a^{-1} \\ &= \phi(xy).\end{aligned}$$

Thus ϕ is an isomorphism. □

There is a particularly simple and easy to understand example of these types of automorphisms. Let us go back to the case of D_3. Choosing a labelling of the vertices is somewhat arbitrary. A different choice of labelling, corresponds to a permutation of the numbers 1, 2 and 3. These will induce an automorphism of S_3, which is given by conjugation by the given permutation.

Theorem 12.6 (Cayley's Theorem)**.** *Let G be a group.*

Then G is isomorphic to a subgroup of a permutation group. If moreover G is finite, then so is the permutation group, so that every finite group is a subgroup of S_n, for some n.

Proof. Let $H = A(G)$, the permutations of the set G. Define a map

$$\phi\colon G \longrightarrow H$$

by the following rule. Given $a \in G$, send it to the permutation $\sigma = \phi(a)$,

$$\sigma\colon G \longrightarrow G,$$

defined as follows

$$\sigma(a) = ag.$$

Note that σ is indeed a permutation, that is, σ is a bijection. In fact the inverse of σ is the map that sends g to $a^{-1}g$.

I claim that ϕ is an isomorphism onto its image. We first check that ϕ is injective. Suppose that a and b are two elements of G. Let σ and τ be the two corresponding elements of $A(G)$. If $\sigma = \tau$, then σ and τ must have the same effect on elements of G. Look at their effect on e, the identity,

$$a = ae = \sigma(e) = \tau(e) = be = b.$$

Thus $\phi(a) = \phi(b)$ implies $a = b$ and ϕ is injective. Thus ϕ is certainly a bijection onto its image. Now we check that $\phi(ab) = \phi(a)\phi(b)$. Suppose that $\sigma = \phi(a)$ and $\tau = \phi(b)$ and $\rho = \phi(ab)$. We want to check that $\rho = \sigma\tau$. This is an equation that involves permutations, so it is enough to check that both sides have the same effect on elements of G. Let $g \in G$. Then

$$\begin{aligned}\sigma(\tau(g)) &= \sigma(bg)\\ &= a(b(g))\\ &= (ab)g\\ &= \rho(g).\end{aligned}$$

Thus ϕ is an isomorphism onto its image. □

In practice Cayley's Theorem is not in itself very useful. For example, if $G = D_3$ then G is isomorphic to S_3. But if we were to apply the machinery behind Cayley's Theorem, we would exhibit G as a subgroup of S_6, a group of order $6! = 720$.

However the idea of trying to put a group inside a permutation group turns out to be extremely powerful. Consider the example of trying to construct a group G of order 4. We have already shown that there are at most two groups of order four, up to isomorphism. One is cyclic of order 4. The multiplication table of the other, if it is indeed a group, is determined as

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

In fact the only thing left to show is that the multiplication is associative.

The idea is to find a subgroup H of S_n, whose multiplication table is precisely the one given. The clue to finding H is given by Cayley's Theorem. For a start Cayley's Theorem shows that we should take $n = 4$.

Now the four permutations of G determined by the multiplication table are

$$\begin{pmatrix} e & a & b & c\\ e & a & b & c\end{pmatrix} \quad \begin{pmatrix} e & a & b & c\\ a & e & c & b\end{pmatrix} \quad \begin{pmatrix} e & a & b & c\\ b & c & e & a\end{pmatrix} \quad \begin{pmatrix} e & a & b & c\\ c & b & a & e\end{pmatrix}.$$

Replacing letters by numbers, in the obvious way, we get

$$\begin{pmatrix} 1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}.$$

This reduces to

$$H = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Now it is easy to see that this subset is in fact a subgroup. In fact the square of any element is the identity and the product of any two elements is the third. Thus H is a subgroup of S_4. Now H is a group of order 4, which is not cyclic.

Thus there are at least two groups of order 4, up to isomorphism.