Isomorphisms and Cayley's Theorem

Definition: Let G and H be groups.

A mapping $\varphi : G \to H$ is a **homomorphism**

if $\boxed{\varphi(xy) = \varphi(x)\varphi(y)}$ $(*)$ $\forall x, y \in G$.

If φ satisfies $(*)$ and is also a bijection, it is called an **isomorphism**.

Finally, if $\exists$ an isomorphism $\varphi : G \to H$, we say the groups G and H are **isomorphic**.

(**Idea:** Isomorphic groups are "essentially the same".)

Remarks: If $\varphi : G \to H$ is an isomorphism,

then a) $|G| = |H|$

b) $\operatorname{ord}(x) = \operatorname{ord}(\varphi(x))$ $\forall x$

Proposition: Any two cyclic groups of the same order are isomorphic.

Proof: Let $G = \langle x \rangle = \{e, x, \ldots, x^{n-1}\}$ $(x^n = e)$

and $H = \langle y \rangle = \{e, y, \ldots, y^{n-1}\}$ $(y^n = e)$.

Define $\varphi : G \to H$ by

$$\varphi(x^k) = y^k \qquad (k = 0, 1, \dots, n-1).$$

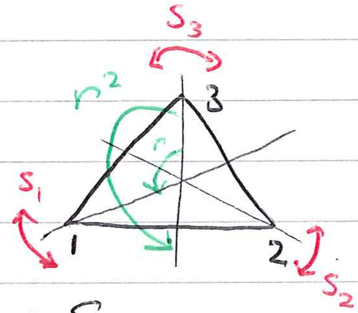
Not hard to check it's an isomorphism. ∎

(In particular, any cyclic group of order n is isomorphic to $\mathbb{Z}_n$.)

<u>Example</u>: Dihedral group D_3 is isomorphic to symmetric group S_3. [$D_3 \cong S_3$].

"isomorphic to"

<u>Proof</u>: Label the vertices of the triangle 1, 2, 3.



For any symmetry $x \in D_3$, define $\varphi(x) \in S_3$ as the corresponding permutation of vertices:

e.g. $$\varphi(s_1) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$$

$$\varphi(r) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

Easy to check this gives a bijection $\varphi : D_3 \to S_3$, and (∗) is satisfied because both groups have operation of composition. ∎

Cayley's Theorem: Let G be a group with n elements, i.e. $|G| = n$. Then G is isomorphic to a subgroup of S_n.

Example: Let $G = \mathbb{Z}_5^\times = \{1, 2, 3, 4\}$

$$(i, j) \longmapsto ij \pmod 5).$$

Why is it "the same as" a subgroup of S_4?

Draw the multiplication table:

	1	2	3	4	
1	1	2	3	4	R_1
2	2	4	1	3	R_2
3	3	1	4	2	R_3
4	4	3	2	1	R_4

Each row gives us a permutation of $\{1,2,3,4\}$, as follows:

$$R_1 \rightsquigarrow \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$$

$$R_2 \rightsquigarrow \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 4\ 3)$$

$$R_3 \rightsquigarrow \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)$$

$$R_4 \rightsquigarrow \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$$

So let $G' = \{e, (1\,2\,4\,3), (1\,3\,4\,2), (14)(23)\} \subset S_4$.

Then $\varphi : \mathbb{Z}_5^\times \longrightarrow G'$ is an isomorphism.

$$i \longmapsto \sigma_i$$

General proof: Exactly the same idea. Suppose G is a group of order n. To keep things clear, write elements of G as $\overset{\text{identity}}{1}, 2, \dots, n$, and write the operation as $(i,j) \mapsto i * j$.

Now look at the multiplication table:

	1	2	$\cdots$	n	
1	1	2	$\cdots$	n	$\rightsquigarrow \sigma_1$
2	2	$2*2$	$\cdots$	$2*n$	$\rightsquigarrow \sigma_2$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
n	n	$n*2$	$\cdots$	$n*n$	$\rightsquigarrow \sigma_n$

Again, each row gives a permutation of $\{1,\dots,n\}$: row R_i gives the permutation σ_i defined by

$$\sigma_i : \{1,\dots,n\} \longrightarrow \{1,\dots,n\}$$
$$k \longmapsto i*k.$$

How do we know σ_i is a permutation, i.e. a bijection?

- If $i*k_1 = i*k_2$ then $i^{-1}*(i*k_1) = i^{-1}*(i*k_2)$

$$\begin{array}{ccc} i^{-1}*(i*k_1) & = & i^{-1}*(i*k_2) \\ \| \text{ assoc.} & & \| \text{ assoc.} \\ (i^{-1}*i)*k_1 & & (i^{-1}*i)*k_2 \\ \| & & \| \\ e*k_1 & & e*k_2 \\ \| & & \| \\ k_1 & & k_2 \end{array}$$

so σ_i is injective.

- For any $l \in \{1, \dots, n\}$ we can find k such that $i * k = l$: Take $k = i^{-1} * l$. So σ_i is surjective.

So σ_i is bijective, i.e. a permutation.

So define $G' = \{\sigma_1, \dots, \sigma_n\} \subset S_n$.

We claim it is a subgroup of S_n, isomorphic to G.

To prove it's a subgroup:

1) $\sigma_i \sigma_j (k) = i * (j * k) = (i * j) * k = \sigma_{i * j}(k)$

So $\sigma_i \circ \sigma_j = \sigma_{i * j} \in G'$.

This shows G' is closed under multiplication.

2) $e = \sigma_1$ so G' contains the identity.

3) Not hard to check that $(\sigma_i)^{-1} = \sigma_{i^{-1}} \in G'$

so G' contains an inverse for each element.

1), 2), 3) together $\Rightarrow$ G' is a subgroup of S_n.

Finally we claim
$$\varphi : G \longrightarrow G'$$
$$i \longmapsto \sigma_i$$

is an isomorphism.

It's clearly a bijection, so we just need to check condition (*) :

checked above

$$\varphi(i * j) = \sigma_{i*j} = \sigma_i \circ \sigma_j = \varphi(i)\varphi(j)$$

as required.

So $\varphi : G \longrightarrow G' \subset S_n$ is indeed an isomorphism. ∎