Isomorphisms continued

Recall: Groups G, G'. A map $\varphi: G \to G'$ is called an isomorphism if:

- it is a bijection (one-to-one + onto)
- $\forall\, x, y \in G$ we have

$$\boxed{\varphi(xy) = \varphi(x)\varphi(y).} \quad (*)$$

If there is an isomorphism $\varphi: G \to G'$ we say G and G' are isomorphic and write $G \cong G'$.

Let's prove some properties of isomorphisms.

Proposition: If $\varphi: G \to G'$ is an isomorphism then:

i) $\varphi(e) = e'$ (e' = identity of G')

ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$

and more generally $\varphi(x^k) = \varphi(x)^k \ \forall\, k \in \mathbb{Z}$

$$\mathrm{ord}(\varphi(x)) = \mathrm{ord}(x)$$

iii) $\varphi^{-1}: G' \to G$ is also an isomorphism.

<u>Proof</u>: i) Let $\varphi(e) = g \in G'$.

Then since $e = e \cdot e$ we have

$$g = \varphi(e) = \varphi(e \cdot e) \overset{(*)}{=} \varphi(e)\varphi(e) = g^2$$

Multiply both sides by g^{-1}: get

$$g^{-1}g = g^{-1}g^2$$, which is the same as

$$e' = g^{-1}(g \cdot g) \underset{\text{associativity}}{=} (g^{-1}g)g = e'g = g$$

So $g = e'$ as required.

ii) Let's show $\varphi(x)\varphi(x^{-1}) = e'$: this proves

that $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Now $\varphi(x)\varphi(x^{-1}) \underset{(*)}{=} \varphi(xx^{-1}) = \varphi(e) = e'$

(Similarly $\varphi(x^{-1})\varphi(x) = e'$).

So $\varphi(x^{-1}) = \varphi(x)^{-1}$ as claimed.

Also $\varphi(x^2) = \varphi(x \cdot x) \overset{(*)}{=} \varphi(x)\varphi(x) = \varphi(x)^2$

By induction can prove the general case

$$\varphi(x^n) = \varphi(x)^n \qquad (n \in \mathbb{Z}).$$

Orders: recall $\text{ord}(x) = n$ means that

$x^n = e$ and n is the smallest such number.

Let $\varphi(x) = y$. Then

$$y^n = \varphi(x)^n \underset{(ii)}{=} \varphi(x^n) = \varphi(e) = e'.$$

Suppose $y^m = e'$ for some $m < n$.

Then $\varphi(x^m) = \varphi(x)^m = y^m = e'$.

Since φ is a bijection and $\varphi(e) = e'$,

this means $x^m = e$. Contradicts the

assumption that $\text{ord}(x) = n$.

So $\text{ord}(y) = n$, as required.

iii) φ is a bijection $\Rightarrow$ φ^{-1} is a bijection.

To prove it satisfies (*): Let $a, b \in G'$.

Want to show: $\boxed{\varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b)}$

Now $a = \varphi(x)$ and $b = \varphi(y)$

forsome $x, y \in G$ (since φ is onto.)

So $\varphi^{-1}(ab) = \varphi^{-1}(\varphi(x)\varphi(y))$

$\overset{(*)}{=} \varphi^{-1}(\varphi(xy))$

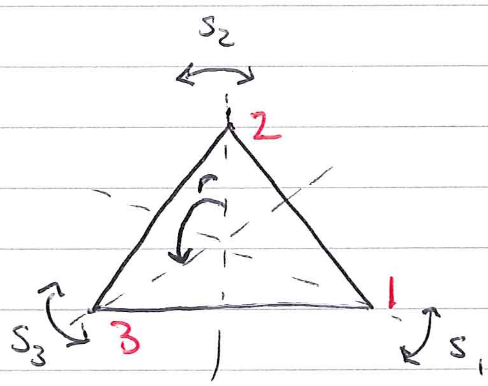
$= xy = \varphi^{-1}(a)\,\varphi^{-1}(b).$ ∎

Examples of Isomorphisms

i) Any cyclic group of order n is isomorphic to $\mathbb{Z}_n$ – proved in Lecture 16

ii) Dihedral group D_3
$\cong$ } proved ~~last time~~ in Lecture 16
Symmetric group S_3

Recall the isomorphism:



$\varphi: D_3 \longrightarrow S_3$

$e \longmapsto id$

$r \longmapsto (1\,2\,3)$

$r^2 \longmapsto (1\,3\,2)$

$s_1 \longmapsto (2\,3)$

$s_2 \longmapsto (1\,3)$

$s_3 \longmapsto (1\,2).$

iii) $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \times)$ multiplication

$\varphi : \quad x \longmapsto e^{x}$ is an isomorphism

- it is a bijection, with inverse

$\varphi^{-1} = \ln \; : \; y \mapsto \ln y$

natural logarithm

> 0

- $\varphi(x+y) = e^{x+y} = e^{x}e^{y} = \varphi(x)\varphi(y)$

$\Rightarrow$ (*) is satisfied.

How to prove two given groups are <u>not</u> isomorphic? This is the case if, for example, any of the following is true:

i) $|G| \neq |G'|$ (since an isomorphism is a bijection $\Rightarrow$ sets must have same cardinality)

ii) $\exists\, x \in G$ with $\mathrm{ord}(x) = n$ (some n) but there is no $y \in G'$ with $\mathrm{ord}(y) = n$ (since we proved $\mathrm{ord}(\varphi(x)) = \mathrm{ord}(x)$).

[More generally, if for some n,

$\#$(elements of order n in G) $\neq$

$\#$(elements of order n in G')

then G and G' are not isomorphic.]

iii) G is commutative ($xy = yx \ \forall x, y \in G$)

but G' is not $\Longrightarrow$ $G \not\cong G'$.

Examples.

i) $\mathbb{Z}_n \not\cong \mathbb{Z}_m$ for $n \neq m$

because $|\mathbb{Z}_n| = n \neq m = |\mathbb{Z}_m|$.

ii) $\mathbb{Z}_6 \not\cong D_3$ even though $|\mathbb{Z}_6| = |D_3| = 6$.

Why not? $\mathbb{Z}_6$ is commutative but D_3 isn't:

for example $rs \neq sr$ in D_3.

iii) $(\mathbb{Q}, +) \not\cong (\mathbb{Q}_{>0}, \times)$ (trickier)

Why not? Assume $\varphi : (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}_{>0}, \times)$

is an isomorphism. Consider $x \in \mathbb{Q}$

such that $\varphi(x) = 2$.

Then

$$2 = \varphi(x) = \varphi(\underset{\in \mathbb{Q}}{\frac{x}{2}} + \underset{\in \mathbb{Q}}{\frac{x}{2}})$$

$$= \varphi(\tfrac{x}{2})\,\varphi(\tfrac{x}{2})$$

So if $y = \varphi(\frac{x}{2})$, then y satisfies

$$y^2 = 2.$$

But this is impossible: by definition $y \in \mathbb{Q}_{>0}$ but there is no rational number whose square equals 2. ∎