Group isomorphism

Tuesday, June 29, 2021 3:29 PM

Let's write the addition table of $\mathbb{Z}_3$.

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

, now let's use Roman numbers

$+$	O	I	II
O	O	I	II
I	I	II	O
II	II	O	I

or we can persian numbers.

+	٠	١	٢
٠	٠	١	٢
١	١	٢	٠
٢	٢	٠	١

Clearly all of these are the same groups only written in different symbols. We only need a translator to tell us which one is which. What is a translator (at least in the context of groups)? It should be a bijection which preserves the operation table. Notice that preserving the operation table simply means that it should be a group homomorphism. This brings us to the definition of group isomorphism.

<u>Def.</u> Suppose $(G, \cdot)$ and $(H, *)$ are two groups. We say $f: G \to H$ is an isomorphism if it is a bijective group homomorphism. If there is an isomorphism $f: G \to H$,

Group isomorphism and cyclic groups

Tuesday, June 29, 2021 3:29 PM

we say G is isomorphic to H and write $G \simeq H$.

Ex. Suppose C_n is a cyclic group of order n. Then

$\mathbb{Z}_n \simeq C_n$.

Pf. Since C_n is a cyclic group of order n, $C_n = \langle g \rangle$ for some g and $o(g) = n$. Saying that $o(g) = n$ means that $g^k = e_G \iff n \mid k$. (I)

Let $f : \mathbb{Z}_n \to C_n$, $f([k]_n) := g^k$.

Well-defined. Definition of f is given in terms of a representative k of the residue class $[k]_n$. Hence we need to make sure that it is independent of the choice of this representative.

$$[k_1]_n = [k_2]_n \Rightarrow k_1 \overset{n}{\equiv} k_2 \Rightarrow k_1 = k_2 + nq \text{ for some } q \in \mathbb{Z}$$

$$\Rightarrow g^{k_1} = g^{k_2} \cdot g^{nq}$$

$$\Rightarrow g^{k_1} = g^{k_2}. \qquad \text{(by (I))}$$

Homomorphism. $f([k]_n + [l]_n) = f([k+l]_n) = g^{k+l}$

$$= g^k \cdot g^l = f([k]_n) \cdot f([l]_n).$$

Group isomorphism and cyclic groups

Tuesday, June 29, 2021 3:29 PM

Injective. $f([k]_n) = f([l]_n) \Rightarrow g^k = g^l$

$$\Rightarrow g^{k-l} = e_G$$

$$\Rightarrow n \mid k-l \quad (\text{by } o(g)=n)$$

$$\Rightarrow k \overset{n}{\equiv} l$$

$$\Rightarrow [k]_n = [l]_n .$$

Surjective. Every element of $\langle g \rangle$ is of the form g^k for some integer k. Because $g^k = f([k]_n)$, every element of C_n is in the image of f. Therefore f is surjective

(Alternatively $f: \mathbb{Z}_n \to C_n$ is an injective function and $|\mathbb{Z}_n| = |C_n| = n$, and so f is surjective. We usually use this type of argument as often it is not easy to show a function is surjective!)

Altogether f is a bijective group homomorphism, and so it is an isomorphism. Therefore $\mathbb{Z}_n \simeq C_n$. ∎

Ex. $(\mathbb{R}^{>0}, \cdot) \simeq (\mathbb{R}, +)$.

Pf. $\ln : \mathbb{R}^{>0} \to \mathbb{R}$ is a group homomorphism as

Examples of isomorphisms

Tuesday, June 29, 2021 3:29 PM

$\ln(x \cdot y) = \ln(x) + \ln(y)$. The natural logarithm is a bijection as $\exp: \mathbb{R} \to \mathbb{R}^{>0}$, $\exp(x) := e^x$ is its inverse. Hence $\ln: \mathbb{R}^{>0} \to \mathbb{R}$ is an isomorphism. ∎

Ex. $\mathbb{Q} \not\simeq \mathbb{Z}$.

Pf. Suppose to the contrary that there is an isomorphism $f: \mathbb{Q} \to \mathbb{Z}$. Since f is bijective, there is $\frac{m}{n} \in \mathbb{Q}$ such that $f(\frac{m}{n}) = 1$. Then

$$1 = f\left(\frac{m}{n}\right) = f\left(\frac{m}{2n} + \frac{m}{2n}\right) = \underbrace{f\left(\frac{m}{2n}\right)}_{\text{in } \mathbb{Z}} + f\left(\frac{m}{2n}\right)$$

$\Rightarrow 1 = 2 f(\frac{m}{2n})$ which is a contradiction as the right hand side is even and 1 is not. ∎

It is a good idea to think about equations to show two groups are not isomorphic.

Ex. $(\mathbb{C} \setminus \{0\}, \cdot) \not\simeq (\mathbb{R} \setminus \{0\}, \cdot)$

Pf. Suppose to the contrary that there is an isomorphism $f: \mathbb{C} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$. Then $f(1) = 1$, and so

Examples of isomorphisms

Tuesday, June 29, 2021 3:29 PM

$f(-1)^2 = f((-1)^2) = f(1) = 1$. Hence $f(-1)$ is either 1 or -1. Since f is bijective and $f(1)=1$, $f(-1)\neq 1$. Therefore $f(-1)=-1$. Thus

$$f(i)^2 = f(i^2) = f(-1) = -1.$$

But this is a contradiction as $f(i)\in \mathbb{R}\setminus\{0\}$ and square of a real number is always non-negative and cannot be -1. ∎

Caley proved that every finite group is isomorphic to a subgp of a symmetric group. A subgroup of a symmetric group is called a permutation group. So by Cayley's theorem every group is a permutation group up to an isomorphism.

Theorem. Suppose $(G,\cdot)$ is a group. Then G is isomorphic to a subgroup of S_G.

Pf. For $g\in G$, let $l_g : G\to G$, $l_g(x) := g\cdot x$.

Step 1. l_g is a bijection (and so $l_g \in S_G$).

Pf of Step 1. $l_g \circ l_{g^{-1}}(x) = l_g(g^{-1}\cdot x) = g\cdot(g^{-1}\cdot x) = x$

and $l_{g^{-1}}\circ l_g(x) = l_{g^{-1}}(g\cdot x) = g^{-1}\cdot(g\cdot x) = x$. Hence

Cayley's theorem

Tuesday, June 29, 2021 3:29 PM

$\ell_g \circ \ell_{g^{-1}} = \ell_{g^{-1}} \circ \ell_g = id_G$. Hence ℓ_g is invertible, and so $\ell_g \in S_G$.

Step 2. $\ell : G \to S_G$, $\ell(g) := \ell_g$ is a group homomorphism.

Pf of Step 2. We have to show that $\ell(g_1 \cdot g_2) = \ell(g_1) \circ \ell(g_2)$.

This means we have to prove that, for every $x \in G$,

$$\ell(g_1 \cdot g_2)(x) = (\ell(g_1) \circ \ell(g_2))(x). \qquad (\mathrm{I})$$

The left hand side of (I) is $(g_1 \cdot g_2) \cdot x$, and the right hand side of (I) is

$$\ell(g_1)(\ell(g_2)(x)) = \ell(g_1)(g_2 \cdot x) = g_1 \cdot (g_2 \cdot x).$$

By associativity, we have $(g_1 \cdot g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for every x. Hence (I) holds for every $x \in G$. Therefore $\ell(g_1 \cdot g_2) = \ell(g_1) \circ \ell(g_2)$, which means ℓ is a group hom.

Step 3. ℓ is injective.

Pf of Step 3. Suppose $\ell(g_1) = \ell(g_2)$. Then $\ell_{g_1} = \ell_{g_2}$, and so $\ell_{g_1}(e_G) = \ell_{g_2}(e_G)$ which implies $g_1 = g_2$.

. Therefore $G \simeq \mathrm{Im}\, \ell$ and $\mathrm{Im}\, \ell \leq S_G$. ■

Cayley's theorem

Tuesday, June 29, 2021 3:29 PM

Motivated by Cayley's theorem, we study symmetric groups in more details.