YXD34

9/24

Examples / Non-examples of Isomorphisms

1) Any infinite cyclic group $\cong \mathbb{Z}$

There is a generator for G, call it a

so... $\langle a \rangle = G$

$\phi : a^k \to k \in \mathbb{Z}$

onto
1:1

G $\qquad$ $\mathbb{Z}$

$\phi(a^{k_1} \cdot a^{k_2}) \overset{?}{\to} \phi(a^{k_1}) + \phi(a^{k_2})$

$\phi(a^{k_1+k_2}) \qquad k_1 + k_2$

$k_1 + k_2$ $\longleftrightarrow$ same

so O.P. exists

$\phi : \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$

$\phi : \mathbb{R} \to \mathbb{R} \qquad \phi(x) = x^3$

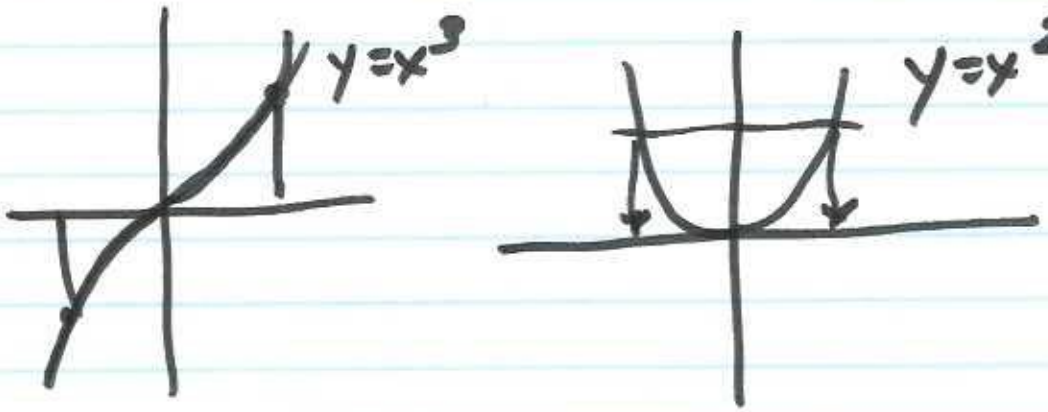
1:1 ✓

onto ✓

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$$

$(r_1 + r_2)^3 = r_1^3 + r_2^3$ not true

so ϕ does not preserve operation (+)



$y = \sinh x = \dfrac{e^x - e^{-x}}{2}$ quadratic in e^x

$2y = e^x - e^{-x}$

$2ye^x = e^{2x} - 1 \Rightarrow e^{2x} - 2ye^x - 1 = 0$

(3)

$(e^x)^2 - 2y(e^x) - 1 = 0$

$e^x = \dfrac{2y \pm \sqrt{4y^2+4}}{2}$

$e^x = y \pm \sqrt{y^2+1}$ so eliminate (−)

$\ln(e^x) = x = \ln(y + \sqrt{y^2+1})$ ✓

$U(10) \cong \mathbb{Z}_4$ and $U(5) \cong \mathbb{Z}_4$

3
$3^2 = 9$
$3^3 = 7$
$3^4 = 1$

3
$3^2 = 4$
$3^3 = 2$
$3^4 = 1$

$a^k \to k \bmod n$ so

cyclic group of order $n \cong \mathbb{Z}_n$

Is $\langle \mathbb{Q}, + \rangle \cong \langle \mathbb{Q}^*, \cdot \rangle$

Suppose $\phi : \langle \mathbb{Q}, + \rangle \to \langle \mathbb{Q}^*, \cdot \rangle$ is iso^{m}

$\phi(a) = -1$ pick -1

$r^2 = -1$

$$-1 = \phi(a) = \phi\left(\tfrac{a}{2} + \tfrac{a}{2}\right) = \phi\left(\tfrac{a}{2}\right) \cdot \phi\left(\tfrac{a}{2}\right)$$

OP condition

$G = SL(2, \mathbb{R})$

Define mapping $\phi_M = MAM^{-1}$ for all $A \in G$

conjugation by M

Want to show conjugation (of matrices) is always an iso^{m}

1) Show $\phi : G \to G$ is well-defined

This means we need to show

$\det(NAN^{-1}) = 1$

↳ $\det(N) \cdot \det(A) \cdot \det(N^{-1}) = 1 \cdot 1 \cdot 1 = 1$ ✓

2) Show ϕ_M is injective

Assume $\phi_M(A) = \phi_M(B)$ want to show $A = B$

$$MAM^{-1} = MBM^{-1}$$

$$M^{-1}MAM^{-1}M = M^{-1}MBM^{-1}M$$

$$\Rightarrow A = B$$

3) Show ϕ_N is surjective (onto)

Take B in range of ϕ_M

Want to find $A \cdot 3 \cdot MAM^{-1} = B$

$$M^{-1}MAM^{-1}M = M^{-1}BM$$

$$A = M^{-1}BM$$

4) $\phi_M(AB) \stackrel{?}{=} \phi_M(A)\phi_M(B)$

$$MABM^{-1} \stackrel{?}{=} (MAM^{-1})(MBM^{-1})$$

$$MAM^{-1}MBM^{-1}$$

$$I$$

$$= MABM^{-1}$$

Z_{12}, D_{12}, A_4 ← common order is 12

max order	12	6	3

from scratch series.....

Cayley's Representation Theorem
Every group is isomorphic to a subgroup of some permutation group.

BACKGROUND:

Groups can be pretty abstract objects. When they get big, we lose the ability to visualize how they work even if we are staring at their Cayley tables. Groups that have a foundation in a geometric object, like the dihedral groups, are easier to grasp than those that are the consequence of a clump of seemingly arbitrary rules. Arthur Cayley discovered about 1854 that every group, no matter how abstract, can be given a concrete (relatively speaking) representation in terms of permutations. Recall that group theory until roughly 1870 was preoccupied with permutations...the whole subject grew out of clever attempts to gain insight regarding the solvability of polynomial equations by studying permutations of the roots of those equations. So it is not surprising that a general representation theorem would be developed in this context. Cayley's theorem is self-contained in the sense that the representation of a group is bootstrapped from nothing more than the group itself...no embedding in a more complicated object or other fancy notion is required.

KEY DEFINITIONS:

1) A *permutation* is a bijective mapping from a set S to itself.

2) A *group homomorphism* is an operation preserving mapping between two groups, specifically if G and H are groups and $\phi : G \to H$, then ϕ is a homomorphism iff for all $x, y \in G$ it is true that $\phi(xy) = \phi(x)\phi(y)$. Another way to state the operation preserving property is to say that the group operations and the mapping commute.

3) A group *isomorphism* is a bijective group homomorphism. Group isomorphisms give all of the algebraic properties of the group on one side of the mapping to the group on the other side. Be careful to realize that properties like order and boundedness are not algebraic and do not need to be preserved by isomorphisms.

KEY FACTS:

1) The cancellation law for groups.

PROOF STRATEGY:

We observe that left multiplication of every element in the group by a fixed element in the group constitutes a permutation of those elements. As the fixed elements used as multipliers range over all elements in the group, we get a family of permutations, one for each multiplier. The idea is to show that this family forms a group with the same fundamental structure as the original group.

PROOF:

Given the group G and an element $a \in G$, consider the mapping $\pi_a : G \to G$ where $\pi_a(g) = ag$, that is to say, the mapping indexed by a left multiplies every element in the group by a. This mapping is injective, for if $\pi_a(g) = \pi_a(h)$, then $ag = ah$ yields $g = h$ by left cancellation. Moreover it is surjective, since given any $g \in G$, the pre-image of g is the element $a^{-1}g$, or symbolically, $\pi_a(a^{-1}g) = g$. Thus we have the family of permutations $\mathfrak{F} = \{\pi_a : a \in G\}$. I claim that $\mathfrak{F}$ is a group

under composition ($\circ$). Certainly the composition of any two bijections is bijective, composition of functions is always associative, the identity permutation π_{e_G} is present, and finally, the inverse of any π_a is obviously $\pi_{a^{-1}}$, which is present. This establishes that $\langle \mathfrak{F}, \circ \rangle$ is a group.

Now, not only is $\langle \mathfrak{F}, \circ \rangle$ a group, but it is essentially the same as G. Define $\phi(a) = \pi_a$. I claim that $\phi : G \to \mathfrak{F}$ is an isomorphism. We must establish that ϕ is bijective and operation-preserving. For bijectivity, note first that if $\pi_a = \pi_b$, then $ag = bg$ for some $g \in G$, and by cancellation, $a = b$, hence ϕ is injective. Moreover, given any $\pi_a \in \mathfrak{F}$, it's pre-image under ϕ is obviously $a \in G$, hence ϕ is surjective as well, and therefore bijective. Finally, we ask if $\phi(ab) = \phi(a) \circ \phi(b)$? Well, $\phi(ab) = \pi_{ab}$ and $\phi(a) \circ \phi(b) = \pi_a \circ \pi_b$. But these two mappings are easily seen to be the same, since for any $g \in G$, we have $\pi_{ab}(g) = abg = a(bg) = a\pi_b(g) = \pi_a \circ \pi_b(g)$. This establishes that ϕ is operation-preserving, or respects $\circ$, and hence is an isomorphism. We write $G \cong \mathfrak{F} \leq perm(G)$, where $perm(G)$ is the group of *all* permutations of the elements of G.

(TINY) EXAMPLE:

Consider the cyclic group $Z_3 = \langle \{0,1,2\}, (+)_3 \rangle$. The π's in the proof above add (since this is an abelian group we are using the additive notation) respectively 0, 1, and 2 modulo 3 to the elements of Z_3. So $\pi_0 = (1)$, the identity permutation, $\pi_1 = (1 \quad 2 \quad 0)$, and $\pi_2 = (2 \quad 0 \quad 1)$. The group $\mathfrak{F} = \{\pi_0, \pi_1, \pi_2\}$ with the operation of composition. The group $perm(Z_3)$ consists of the six permutations possible for the three elements of Z_3, which is S_3. So $Z_3 \cong \mathfrak{F} < S_3$. You can see that $\mathfrak{F}$ consists of just the *even* permutations of the elements of Z_3, and you may recall that this would be the alternating group A_3.