Section 3: Isomorphic binary structures

A note from last time before we begin: I glibly said that division was a valid binary operation, but it is only valid for $\mathbb{Q}^x, \mathbb{R}^x, \mathbb{C}^x$ because we cannot divide by 0.

Let's start by re-visiting the table from last time. Recall:

Definition 0.1. A binary operation $\star$ on a set S is **commutative** if $a \star b = b \star a$ for all $a, b \in S$.

Definition 0.2. A binary operation $\star$ on a set S is **associative** if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$.

Example 0.3. If $S = \{a, b, c\}$, here's one binary operation.

$\star$	a	b	c
a	b	c	b
b	a	c	b
c	c	a	a

Is this associative? Is it commutative?

Answer: it is neither because, looking at the table, $a\star(b\star c) = a\star b = c$, but $(a\star b)\star c = c\star c = a$. Similarly, $a \star b = c$ but $b \star a = a$.

Example 0.4. Here's the table for $(\mathbb{Z}_3, +_3)$ and $(\mathbb{Z}_3, \cdot_3)$.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

One natural question to ask is: when are two binary operations the same? We first need to make sense of whatever 'the same' means, but here is a motivating example.

Example 0.5. If we go back to the triangle we discussed on Monday, we could consider the set of possible rotations of the triangle. This set $Rot = \{E, R, R^2\}$ and we can make a table using the binary operation that is composition:

$\circ$	E	R	R^2
E	E	R	R^2
R	R	R^2	E
R^2	R^2	E	R

If we simply relabel $0 = E$, $1 = R$, $2 = R^2$, we get the same exact table as the one for $(\mathbb{Z}, +_3)$. So, not only are the elements of the set in one-to-one correspondence, but the binary operations on those objects are the same. If we tried to do the same thing with $(\mathbb{Z}, \cdot_3)$, it wouldn't work: the binary operations are not compatible.

Definition 0.6. A set S with binary operation $\star$ is called a **binary algebraic structure**.

Definition 0.7. Let $(S, \star)$ and $(S', \star')$ be two binary algebraic structures. An isomorphism is a one-to-one and onto (or injective and surjective, or bijective) function $\phi : S \to S'$ such that $\phi(x \star y) = \phi(x) \star' \phi(y)$ for all $x, y \in S$. This last condition is called the **homomorphism condition.**

Definition 0.8. A function that satisfies only the last property is called a **homomorphism**.

Example 0.9. $(\mathbb{Z}, +)$ and $(2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}, +)$ are isomorphic binary structures via the isomorphism $\phi(n) = 2n$. To show this, we must check that this is injective, surjective, and satisfies the *homomorphism condition.*

It is injective because, if $\phi(n) = \phi(m)$, then $2n = 2m$, so $n = m$. It is surjective because, given any element $2n \in 2\mathbb{Z}$, the element $n \in \mathbb{Z}$ satisfies $\phi(n) = 2n$.

TO check the homomorphism condition, we check that $\phi(x \star y) = \phi(x) \star' \phi(y)$. We just check: $\phi(x \star y) = \phi(x + y) = 2(x + y)$, and $\phi(x) \star' \phi(y) = 2x + 2y$, and indeed $2(x + y) = 2x + 2y$.

Example 0.10. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}^+ = \{r \in \mathbb{R} | r > 0\}, \cdot)$ via the isomorphism $\phi(x) = e^x$.

We check the same three conditions as above.

In the examples above, and in general, to determine if two structures are isomorphic, you must:

- Come up with a function mapping one set to the next, $\phi : S \to S'$.
- Show the function is injective (one-to-one), i.e. if $\phi(x) = \phi(y)$, then $x = y$.
- Show the function is surjective (onto), i.e. if z is any element of S', there is some element $x \in S$ such that $\phi(x) = z$.
- Show that the last condition, $\phi(x \star y) = \phi(x) \star' \phi(y)$, holds for all $x, y \in S$.