Section 3: Isomorphic binary structures and Section 4: Groups

Last time, we defined:

Definition 0.1. 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.**

We did some examples showing things were isomorphic. What about showing two things are not isomorphic?

Example 0.2. Are the binary structures $(\mathbb{Z}_3, +_3)$ and $(\mathbb{Z}_4, +_4)$ isomorphic?

No, because $\mathbb{Z}_3$ has three elements and $\mathbb{Z}_4$ has four elements, so there is no bijective function mapping on to the other.

Example 0.3. Are the binary structures $(\mathbb{Z}, \cdot)$ and $(\mathbb{Z}^+, \cdot)$ isomorphic?

No, because there are two elements x such that $x \cdot x = x$ in $(\mathbb{Z}, \cdot)$: 0 and 1, but there is only one such element in $(\mathbb{Z}^+, \cdot)$: 1.

Definition 0.4. An identity element for a binary operation $\star$ on a set S is an element $e \in S$ such that $e \star a = a \star e = a$ for every $a \in S$.

Example 0.5. The identity element of $(\mathbb{Z}, +)$ is 0 and the identity element of $(\mathbb{Z}, \cdot)$ is 1.

Theorem 0.6. *If $(S, \star)$ has identity element e, it is unique.*

Proof. If there is another element e' that is also an identity element, then we must have $e \star e' = e$ and $e \star e' = e'$, hence $e = e'$. □

Definition 0.7. A **group** $(G, \star)$ is a set G with binary operation $\star$ such that

($\mathcal{G}_1$) $\star$ is associative: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$

($\mathcal{G}_2$) There exists an identity element $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$.

($\mathcal{G}_3$) There exist inverse elements: for all $a \in G$, there exists $a' \in G$ such that $a \star a' = a' \star a = e$.

Example 0.8. $(\mathbb{Z}, +)$ is a group with identity 0 and the inverse of n is $-n$. $(\mathbb{Z}, \cdot)$ is not a group: the identity is 1 but most elements do not have inverses (i.e. there is not an integer such that $2 \cdot n = 1$).

Definition 0.9. A group G is **abelian** if its binary operation is commutative.

Example 0.10. The set $M_n(\mathbb{Z})$ is the set of $n \times n$ matrices with entries in $\mathbb{Z}$ (could replace $\mathbb{Z}$ with $\mathbb{Q}, \mathbb{R}$, etc. For example, $M_2(\mathbb{R})$ is the set of 2×2 matrices with entries in $\mathbb{R}$.

$(M_n(\mathbb{Z}), \cdot)$ is not a group because most matrices do not have inverses.

Some group properties!

Theorem 0.11 (Cancellation)**.** *If $(G, \star)$ is a group, then $a \star b = a \star c$ implies that $b = c$. Similarly, $b \star a = c \star a$ implies that $b = c$.*

Proof. Assume $a \star b = a \star c$. By $\mathcal{G}_3$, there exists an element a' that is the inverse of a, and

$$a' \star (a \star b) = a' \star (a \star c).$$

By associativity, we have

$$(a' \star a) \star b = (a' \star a) \star c$$

and by the definition of a', we have

$$e \star b = e \star c$$

and finally, by the definition of e, we must have

$$b = c.$$

The proof for the second case is similar. □

Theorem 0.12. *If $(G, \star)$ is a group and $a, b \in G$, then there is a unique solution to the equations $a \star x = b$ and $x \star a = b$.*

Proof. By $\mathcal{G}_3$, there is an inverse element a', and hence

$$a' \star (a \star x) = a' \star b.$$

Similarly to above, we get that

$$x = a' \star b.$$

□

Theorem 0.13. *If $(G, \star)$ is a group, the identity element e is unique, and given an element a, the inverse a' is unique.*

Proof. We already proved (Theorem 0.6) that the identity element is unique. Assume there are two inverses a' and a''. Then, $a \star a' = a \star a'' = e$, and by Theorem 0.13, $a' = a''$. □

Theorem 0.14. *Let $(G, \star)$ be a group. For all $a, b \in G$, we have $(a \star b)' = b' \star a'$.*

Proof. Because inverses are unique, we just have to check that $(a \star b) \star (b' \star a') = e$ and $(b' \star a') \star (a \star b) = e$. We check this using the associative law and properties of e. □