Section I.3. Isomorphic Binary Structures

Note. In mathematics, an "iso-morphism" is, as the name suggests, a mapping which preserves structure. In a graph, the structure is connectedness. In a group (to be introduced in the next section), the structure is given by the binary operation.

Note. Consider the tables:

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

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*'$	x	y	z
x	x	y	z
y	z	y	x
z	y	x	z

Notice that the *structure* of operation $+$ on $\{0, 1, 2\}$ is the same as the *structure* of $*$ on $\{a, b, c\}$. This can be seen by replacing 0, 1, 2 with a, b, c (respectively) and $+$ with $*$. Then any equation involving the first table yields an equation involving the second table (and vice-a-versa). So the only difference in binary operation $+$ and binary operation $*$ is one of notation. So the first and second tables represent <u>isomorphic</u> binary operations (on the appropriate sets). However, the third table is fundamentally different—in it, the binary operation when applied to a pair of the same elements yields that element (it is an <u>idempotent</u> binary operation—see page 28, Exercise 2.37). This is not the case in the first two tables and so $*'$ is not isomorphic to $+$ nor $*$.

Definition. A *binary algebraic structure* is an ordered pair $\langle S, *\rangle$ where S is a set and $*$ is a binary operation on S.

Definition 3.7. Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary algebraic structures. An *isomorphism* of S with S' is a *one-to-one* function φ mapping S *onto* S' such that

$$\varphi(x * y) = \varphi(x) *' \varphi(y) \text{ for all } x, y \in S.$$

We then say S and S' are *isomorphic* binary structures, denoted $S \simeq S'$.

Note. In this setting (as well as others), an isomorphism is a one-to-one and onto mapping which preserves structure. In a binary algebraic structure, the "structure" is the binary operation. In a vector space, the structure is vector addition and scalar multiplication. In a graph, the structure is connectivity.

Example. In the example above, the isomorphism between the first and second binary algebraic structures is explicitly given as $\varphi(0) = a$, $\varphi(1) = b$, and $\varphi(2) = c$. You can then confirm from the tables that $\varphi(x + y) = \varphi(x) * \varphi(y)$ for all $x, y \in \{0, 1, 2\}$. For example, $\varphi(0 + 1) = \varphi(1) = b$ and $\varphi(0) * \varphi(1) = a * b = b$, and hence $\varphi(0 + 1) = \varphi(0) * \varphi(1)$.

Note. How To Show That Binary Structures Are Isomorphic. Suppose $\langle S, * \rangle$ and $\langle S', *' \rangle$ are binary algebraic structures. To show they are isomorphic with isomorphism φ:

1. Define $\varphi : S \to S'$.
2. Show φ is one-to-one.
3. Show that φ is onto.
4. Show $\varphi(x * y) = \varphi(x) *' \varphi(y)$ for all $x, y \in S$ (the text calls this part the *homomorphism property*).

Example 3.8. Consider $\langle \mathbb{R}, + \rangle$ and $\langle \mathbb{R}^+, \cdot \rangle$. Then

1. define $\varphi : \mathbb{R} \to \mathbb{R}^+$ as $\varphi(x) = e^x$,
2. if $\varphi(x) = \varphi(y)$ then $e^x = e^y$ and so $\ln e^x = \ln e^y$ or $x = y$, and so φ is one-to-one,
3. if $r \in \mathbb{R}^+$, then $\varphi(\ln r) = e^{\ln r} = r$ and φ is onto (that is, $r \in \mathbb{R}^+$ is the image of $\ln r$ under φ), and
4. for all $x, y \in \mathbb{R}$, $\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$.

So $\varphi(x) = e^x$ is an isomorphism and $\langle \mathbb{R}, + \rangle = \langle \mathbb{R}^+, \cdot \rangle$.

Notice. We could have defined φ in the previous example as $\varphi(x) = a^x$ for any $a > 0$, $a \neq 1$.

Definition. A *structural property* of a binary structure $\langle S, * \rangle$ is a property shared by any binary structure $\langle S', *' \rangle$ which is isomorphic to $\langle S, * \rangle$.

Example. Some examples of structural properties are

1. the number of elements in S,
2. the commutativity of $*$,
3. the associativity of $*$,
4. $*$ is idempotent (i.e., $x * x = x$ for all $x \in S$), and
5. the equation $a * x = b$ has a solution $x \in S$ for all $a, b \in S$ (this means the rows of the table for $*$ each contain all the elements of S).

Note. One way to show that $\langle S, * \rangle$ and $\langle S', *' \rangle$ are not isomorphic under a one-to-one and onto mapping φ from S to S' is to show that there is some structural property that φ does not preserve.

Exercise 3.4. Let $\langle S, * \rangle = \langle \mathbb{Z}, + \rangle$ and $\langle S', *' \rangle = \langle \mathbb{Z}, + \rangle$ and $\varphi(n) = n + 1$. Is φ an isomorphism?

Definition 3.12. Let $\langle S, * \rangle$ be a binary structure. An element e of S is an *identity element* of $*$ if $e * s = s * e = s$ for all $s \in S$.

Note. Given your experience with addition and subtraction of real numbers, the following is not surprising. However, you should not expect your experience with these particular structures to extend to general binary structures. What we will accomplish in this class is to study very abstract structures, describe their general properties, and use these properties in particular applications.

Theorem 3.13. Uniqueness of Identity Elements.
A binary structure $\langle S, * \rangle$ has at most one identity element. That is, if there is an identity element, it is unique.

Proof. Suppose e and $\overline{e}$ are both identities of S. Then $e * \overline{e} = \overline{e}$ since e is an identity. Also, $e * \overline{e} = e$ since $\overline{e}$ is an identity. Therefore $e = \overline{e}$ and the identity is unique. ∎

Note. The above is a standard proof of uniqueness—to assume the existence of two elements with a certain property and then to show the two elements are the same.

Note. The existence of an identity element is a structural property.

Theorem 3.14. Suppose $\langle S, * \rangle$ has an identity element e. If $\varphi : S \to S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$, then $\varphi(e)$ is an identity element in $\langle S', *' \rangle$.

Exercise 3.4 (again). The identity of $\langle \mathbb{Z}, + \rangle$ is 0, but $\varphi(0) = (0) + 1 = 1 \neq 0$, so φ does not map the identity of $\langle S, * \rangle = \langle \mathbb{Z}, + \rangle$ to the identity of $\langle S', *' \rangle = \langle \mathbb{Z}, + \rangle$.

Exercise 3.16(a) Let $\langle S, * \rangle = \langle \mathbb{Z}, + \rangle$ and $\langle S', *' \rangle = \langle \mathbb{Z}, \circ \rangle$ where $a \circ b = a + b - 1$. Then $\varphi(n) = n + 1$ is an isomorphism from $\langle \mathbb{Z}, + \rangle$ to $\langle \mathbb{Z}, \circ \rangle$.

Exercise 3.26. If $\varphi : S \to S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$, then φ^{-1} is an isomorphism of $\langle S', *' \rangle$ with $\langle S, * \rangle$.

Exercise 3.33b. Let $H = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$ and $\cdot$ be matrix multiplication (H is closed under $\cdot$ by Exercise 2.23). Prove $\langle \mathbb{C}, \cdot \rangle$ is isomorphic to $\langle H, \cdot \rangle$.

Hint: For $z = a + ib \in \mathbb{C}$, define $\varphi(z) = \varphi(a + ib) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

Revised: 7/7/2023