Math 113, Fall 2019
Lecture 3, Thursday, 9/5/2019

Topics Today:

- Isomorphisms
- Binary (Algebraic) Structures
- Structural Properties

Reading for Tuesday: up to (and including) §5
Homework due Sept 12 : §2 : 3, 6, 10, 22, 33, 36 and §3 : 2, 10, 16a, 27, 31, 33

1 Clicker Questions:

The binary operation $*$ on $\mathbb{Z}$ given by $n * m = 2n + 2m$ is:
(a) commutative but not associative
(b) associative but not commutative
(c) both
(d) neither
(e) the dog ate my clicker

The following is (are) NOT a structural property of a binary structure $\langle S, * \rangle$.
(a) $\{x * x \mid x \in S\}$ has 3 elements
(b) The function $x \mapsto 2 * x$ is injective
(c) The set $\{x * x * x \mid x \in S\}$ is all of S.
(d) All of the above
(e) Two or more of the above are NOT structural properties
The answer here is (b) because 2 would have to be an element of S for this property to be valid. As proof of (a) (and c similarly), consider:
If $f : S \to S'$ is an isomorphism, then

$$\begin{aligned} f[\{x * x \mid x \in S\}] &= \{f(x * x) \mid x \in S\} \\ &= \{f(x) *' f(x) \mid x \in S\} \quad \text{(homomorphism property)} \\ &= \{x' *' x' \mid x' \in S'\}, \end{aligned}$$

and now since f is injective,

$$\{x * x \mid x \in S\} \text{ and } \{x' *' x' = x' \in S'\}$$

have the same cardinality.

2 Binary Structures

Definition: Binary Algebraic Structure -

A **binary algebraic structure** $\langle S, * \rangle$ is a set S, equipped with a binary operation $*$ on S. We also call it a **binary structure** (for short).
Examples include:

$$\langle \mathbb{R}, + \rangle, \langle \mathbb{R}, - \rangle, \langle \mathbb{R}, \times \rangle, \langle U, \times \rangle, \langle U, / \rangle, \langle \mathbb{R}_2, +_2 \rangle, \langle \mathbb{Z}_{23}, +_{23} \rangle.$$

Definition: Isomorphism -

An **isomorphism** from a binary algebraic structure $\langle S, * \rangle$ to a binary algebraic structure $\langle S', *' \rangle$ is a bijection $\varphi : S \to S'$ such that:

$$\varphi(x * y) = \varphi(x) *' \varphi(y), \quad \forall_{x,y \in S},$$

which we call the 'homomorphism property', and $*'$ is a binary operation in S'.

If such an isomorphism exists, then we say that $\langle S, * \rangle$ and $\langle S', *' \rangle$ are **isomorphic**, and we write:

$$\langle S, * \rangle \simeq \langle S', *' \rangle,$$

(or equivalently $\langle S, * \rangle \cong \langle S', *' \rangle$).
Also, $\varphi : \langle S, * \rangle \xrightarrow{\sim} \langle S', *' \rangle$ says that φ is an isomorphism as above. Then it will be clear what $*$ and $*'$ are, so we omit them from the notation and simply say:

$$S \simeq S' (\text{ or } S \cong S'),$$

and S and S' are isomorphic, with $\varphi : S \xrightarrow{\sim} S'$.
We claim:
As with cardinalities, if Σ is a collection of binary algebraic structures, then isomorphism defines an **equivalence relation** on Σ.

Proof. The proof here is essentially the same as with cardinalities. The identity map $S \to S$ is an isomorphism $S \xrightarrow{\sim} S$. If $\varphi : S \to S'$ is an isomorphism, then so is $\varphi^{-1} : S' \to S$. If $\varphi : S \to S'$ and $\psi : S' \to S''$ are isomorphisms, then so is $\psi \circ \varphi : S \to S''$. □

As we recall, we had binary algebraic structures $\langle U, \times \rangle$ where $U := \{z \in \mathbb{C} : |Z| = 1\}$ (on the unit circle). Taking $\langle \mathbb{R}_{2\pi}, +_{2\pi} \rangle$, we have:

$$\mathbb{R}_{2\pi} = [0, 2\pi)$$
$$\theta +_{2\pi} \varphi = \begin{cases} \theta + \varphi, & \theta + \varphi < 2\pi \\ \theta + \varphi - 2\pi, & \theta + \varphi \geq 2\pi \end{cases}$$

We also had a bijection $\alpha : \mathbb{R}_{2\pi} \to U$ where $\mathbb{R}_{2\pi} \overset{\alpha}{\xrightarrow{\sim}} U$ given by:

$$\alpha(\theta) = e^{i\theta} = \cos\theta + i \sin\theta.$$

We also saw:

$$\alpha\left(\theta +_{2\pi} \varphi\right) = \alpha(\theta) \cdot \alpha(\varphi), \quad \forall_{\theta, \varphi \in \mathbb{R}_{2\pi}}.$$

3 Proving $S \cong S'$:

To prove two binary structures are isomorphic:
(1) We find a candidate isomorphism $\alpha : S \to S'$.
(2) Show that α is injective

Proof. Let $\theta, \varphi \in [0, 2\pi)$. If $e^{i\theta} = e^{i\varphi}$, then we may assume $\theta \leq \varphi$. By properties of the exponential, $e^{i(\theta - \varphi)} = 1$ with $0 \leq \theta - \varphi < 2\pi$.
Then $\cos(\theta - \varphi) = 1$ and $\sin(\theta - \varphi) = 0$, with $0 \leq \theta - \varphi < 2\pi$. Hence we conclude that $\theta - \varphi = 0$, so $\theta = \varphi$. □

(3) Show that α is onto.

Proof. Given $z = x + iy \in U$, let:

$$\theta = \begin{cases} \cos^{-1} x, & y \geq 0 \\ 2\pi - \cos^{-1} x, & y < 0 \end{cases}.$$

□

Then $e^{i\theta} = z$. But z is arbitrary in U, so α is onto.
(4) Check the homomorphism property (which we did already).

Remark: Alternatively, we could have done this using degrees in place of radians.
Let $\mathbb{R}_{360} = [0, 360)$. Then:

$$a +_{360} b = \begin{cases} a + b, & a + b < 360 \\ a + b - 360, & a + b \geq 360 \end{cases}$$

and define $\beta : \mathbb{R}_{360} \to U$ with

$$\beta(a) = \cos(a^o) + i \sin(a^o).$$

We can show this is also an isomorphism.

In general, we can define $\mathbb{R}_c$ and $+_c$ for any $c > 0$ similarly and get

$$\gamma_2 : \mathbb{R}_c \xrightarrow{\sim} U$$

by

$$\gamma_2(a) := \cos\left(\frac{2\pi}{c} a\right) + i \sin\left(\frac{2\pi}{c} a\right).$$

If c is a positive integer n, then something special happens. Let $\mathbb{Z}_n := \mathbb{R}_n \cap \mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. Then $\mathbb{Z}_n \subseteq \mathbb{R}_n$ and $\mathbb{Z}_n$ is closed under $+_n$ with:

$$a +_n b = \begin{cases} a + b, & a + b < n \\ a + b - n, & a + b \geq n \end{cases}$$

So we get a binary structure $\langle \mathbb{Z}_n, +_n \rangle$ (using the induced operation).

Example: $n := 5$. Then

$$\begin{array}{ccc} \gamma_5 : \mathbb{R}_5 & \xrightarrow{\quad bijection \quad} & U \\ \cup\! | & & \cup\! | \\ \gamma_5|_{\mathbb{Z}_5} : \mathbb{Z}_5 & \xrightarrow{\quad bijection \quad} & U_5 \end{array}$$

and notice:

$$\gamma_5(\mathbb{Z}_5) = \{1, e^{\frac{2\pi i}{5}}, e^{\frac{2\pi i}{5} \cdot 2}, e^{\frac{2\pi i}{5} \cdot 3}, e^{\frac{2\pi i}{5} \cdot 4}\} =: U_5$$

Then $\gamma_5|_{\mathbb{Z}_5}$ is one-to-one (because γ_5 is one-to-one), and is onto U_5 by definition of U_5. Additionally, $\gamma_5|_{\mathbb{Z}_5}$ satisfies the homomorphism property because γ_5 does.
Also, we can see that $z^5 = 1, \forall_{z \in U_5}$. Since a polynomial $z^5 - 1$ (of degree 5) has at most 5 roots and we've found 5 roots, $z^5 - 1$ has **no other roots**. Therefore,

$$U_5 = \{z \in \mathbb{C} : z^5 = 1\}.$$

If $f : A \to B$ is a function and $A' \subseteq A$, then $f|_{A'}$ is the function $A' \to B$ defined by

$$f|_{A'}(a) = f(a), \quad \forall_{a \in A'}.$$

To prove that $\langle S, * \rangle$ and $\langle S', *' \rangle$ are **not** isomorphic:
Simply find a structural property that one has that the other does not have.

Definition: Structural Property -

A **structural property** of a binary algebraic structure is a property that any two isomorphic binary structures must either both have or neither has. An example of a structural property is: having the same cardinality as some given set.

4 Structural Properties

Let $\langle S, * \rangle$ be a binary structure.

4.1 Commutativity

We say that $*$ is commutative if

$$x * y = y * x, \quad \forall_{x,y \in S}.$$

Then $\langle S, * \rangle$ (or S) is commutative if $*$ is commutative.
For examples, $\langle \mathbb{Z}, + \rangle$ is commutative, whereas $\langle \mathbb{Z}, - \rangle$ is not.

We claim:
If $\langle S, * \rangle$ is commutative, and

$$\langle S, * \rangle \cong \langle S', *' \rangle,$$

with the isomorphism $\varphi : S \to S'$, then $\langle S', *' \rangle$ is commutative.

Proof. Let $a', b' \in S'$. Then $\exists_{a,b \in S}$ such that $\varphi(a) = a'$ and $\varphi(b) = b'$. Then

$$a' *' b' = \varphi(a) *' \varphi(b) = \varphi(a * b) = \varphi(b * a) = \varphi(b) *' \varphi(a) = b' *' a'$$

and hence this proves that commutativity is a structural property.

□

4.2 Associativity

If

$$(x * y) * z = x * (y * z), \quad \forall_{x,y,z \in S}$$

then S is associative. The rest is left as an exercise to show this is a structural property.

4.3 Example

Let A be a set and let S be the set of all functions from A to A, and let $\circ$ be the binary operation on S given by the composition of functions.
If $f, g \in S$, then $f \circ g$ takes $a \in A$ to $f(g(a))$.
This is associative because both $(f \circ g) \circ h$ and $f \circ (g \circ h)$ take

$$a \mapsto f(g(h(a))).$$

However, $\circ$ is **NOT** commutative (unless A has ≤ 2 elements). As an example of where this fails, take

$$A := \mathbb{R}_2, \quad f(x) = 2x, \quad g(x) = e^x.$$

To see this explicitly,

$$f \circ g : x \mapsto 2e^x \implies 0 \mapsto 2$$
$$g \circ f : x \mapsto e^{2x} \implies 0 \mapsto 1$$

From earlier, an example of something that fails to be a structural property is:

$$2 \in S, \text{ or } S \subseteq \mathbb{C}.$$

Notice that $2 \notin U$ but $2 \in \mathbb{R}_{2\pi}$.

5 Clicker Question:

Which of the following following are isomorphic?

$$S_1 : \begin{bmatrix} * & a & b \\ a & a & b \\ b & b & a \end{bmatrix}, \qquad S_2 : \begin{bmatrix} * & a & b \\ a & b & a \\ b & a & b \end{bmatrix}, \qquad S_3 : \begin{bmatrix} * & a & b \\ a & a & b \\ b & a & b \end{bmatrix}$$

The correct answer is: (A) in that

$$S_1 \cong S_2.$$

Our isomorphism simply switches a and b.

Lecture ends here.

Voyta leaves us with a cliff-hanger for next time:
Is $\langle \mathbb{Z}^+, + \rangle$ isomorphic to $\langle \mathbb{N}, + \rangle$? Take $\mathbb{Z}^+ := \{1, 2, 3, \dots\}$ and $\mathbb{N} := \{0, 1, 2, \dots\}$.