MATH 415

Modern Algebra I

Lecture 3: Isomorphism of binary structures. Groups.

Binary operations

Definition. A **binary operation** $*$ on a nonempty set S is simply a function $* : S \times S \to S$.

The usual notation for the element $*(x, y)$ is $x * y$.

The pair $(S, *)$ is called a **binary algebraic structure**.

"Structures are the weapons of the mathematician."

Nicholas Bourbaki

Isomorphism of binary structures

Definition. A function $f : S_1 \to S_2$ is called an **isomorphism** of binary structures $(S_1, *)$ and $(S_2, \bullet)$ if it is bijective and $f(x * y) = f(x) \bullet f(y)$ for all $x, y \in S_1$.

Two binary structures $(S_1, *)$ and $(S_2, \bullet)$ are called **isomorphic** if there is an isomorphism $f : S_1 \to S_2$.

The word "isomorphism" applies when two complex structures can be mapped onto each other, in such a way that to each part of one structure there is a corresponding part in the other structure, where "corresponding" means that the two parts play similar roles in their respective structures.

Douglas Hofstadter

Alternative terminology

General maps

one-to-one	injective
onto	surjective
one-to-one and onto	bijective

Maps preserving a structure

any map	homomorphism
one-to-one	monomorphism
onto	epimorphism
one-to-one and onto	isomorphism

Self-maps preserving a structure

any map	endomorphism
one-to-one and onto	automorphism

Isomorphism of binary structures

Theorem Isomorphy is an equivalence relation on binary structures.

Proof. We need to check three conditions.

Reflexivity:
For any binary operation $*$ on a set S, the identity map $\mathrm{id}_S : S \to S$ is an automorphism of the binary structure $(S, *)$.

Symmetry:
Suppose $(S_1, *)$ and $(S_2, \bullet)$ are binary structures and $f : S_1 \to S_2$ is an isomorphism. Then the inverse map $f^{-1} : S_2 \to S_1$ is also an isomorphism.

Transitivity:
Suppose $(S_1, *)$, $(S_2, \bullet)$ and $(S_3, \star)$ are binary structures. If $f : S_1 \to S_2$ and $h : S_2 \to S_3$ are isomorphisms then the composition $h \circ f : S_1 \to S_3$ is also an isomorphism.

Examples of isomorphic binary structures

- $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$.

An isomorphism $\phi : \mathbb{Z} \to 2\mathbb{Z}$ is given by $\phi(x) = 2x$.

- $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$.

An isomorphism $\phi : \mathbb{R} \to \mathbb{R}^+$ is given by $\phi(x) = e^x$. Indeed, $e^{x+y} = e^x \cdot e^y$ for all $x, y \in \mathbb{R}$.

- Union and intersection of sets.

$\mathcal{P}(X)$ is a set of all subsets of some set X. An isomorphism between binary structures $(\mathcal{P}, \cup)$ and $(\mathcal{P}, \cap)$ is given by $\phi(A) = X \setminus A$. Indeed, $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ for all $A, B \subseteq X$.

Non-isomorphic binary structures

A property of a binary operation is called **structural** if it is preserved under isomorphisms. A usual way to prove that two binary structures are not isomorphic is to identify a structural property that is featured by one of them but not by the other.

Structural properties are to be worded properly. For example, the following property of $(\mathbb{R}, \cdot)$ is not structural:

$$x \cdot 0 = 0 \text{ for all } x \in \mathbb{R}.$$

However it can be reformulated as a structural property:

$$\text{there exists } z \in \mathbb{R} \text{ such that } x \cdot z = z \text{ for all } x \in \mathbb{R}.$$

This structural property shows, for example, that the binary structure $(\mathbb{R}, \cdot)$ is not isomorphic to $(\mathbb{R}^+, \cdot)$ or to $(\mathbb{R}, +)$.

The simplest structural characteristic of a binary structure is the cardinality of the underlying set.

Useful (structural) properties of binary operations

Suppose $(S, *)$ is a binary structure.

- Commutativity:

$g * h = h * g$ for all $g, h \in S$.

- Associativity:

$(g * h) * k = g * (h * k)$ for all $g, h, k \in S$.

- Existence of the identity element:

there exists an element $e \in S$ such that $e * g = g * e = g$ for all $g \in S$.

- Existence of the inverse element:

for any $g \in S$ there exists an element $h \in S$ such that $g * h = h * g = e$ (where e is the identity element).

- Cancellation:

$g * h_1 = g * h_2$ implies $h_1 = h_2$ and $h_1 * g = h_2 * g$ implies $h_1 = h_2$ for all $g, h_1, h_2 \in S$.

Groups

Definition. A **group** is a binary structure $(G, *)$ that satisfies the following axioms:

(G0: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G1: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G2: existence of identity)
there exists an element $e \in G$, called the **identity** (or **unit**) of G, such that $e * g = g * e = g$ for all $g \in G$;

(G3: existence of inverse)
for every $g \in G$ there exists an element $h \in G$, called the **inverse** of g, such that $g * h = h * g = e$.

The group $(G, *)$ is said to be **commutative** (or **abelian**) if it satisfies an additional axiom:

(G4: commutativity) $g * h = h * g$ for all $g, h \in G$.

Basic examples. • Real numbers $\mathbb{R}$ with addition.

(G0) $x, y \in \mathbb{R} \implies x + y \in \mathbb{R}$

(G1) $(x + y) + z = x + (y + z)$

(G2) the identity element is 0 as $x + 0 = 0 + x = x$

(G3) the inverse of x is $-x$ as $x + (-x) = (-x) + x = 0$

(G4) $x + y = y + x$

• Nonzero real numbers $\mathbb{R} \setminus \{0\}$ with multiplication.

(G0) $x \neq 0$ and $y \neq 0 \implies xy \neq 0$

(G1) $(xy)z = x(yz)$

(G2) the identity element is 1 as $x1 = 1x = x$

(G3) the inverse of x is x^{-1} as $xx^{-1} = x^{-1}x = 1$

(G4) $xy = yx$

The two basic examples give rise to two kinds of notation for a general group $(G, *)$.

Multiplicative notation: We think of the group operation $*$ as some kind of multiplication, namely,

- $a * b$ is denoted ab,
- the identity element is denoted 1,
- the inverse of g is denoted g^{-1}.

Additive notation: We think of the group operation $*$ as some kind of addition, namely,

- $a * b$ is denoted $a + b$,
- the identity element is denoted 0,
- the inverse of g is denoted $-g$.

Remarks. Default notation is multiplicative (but the identity element may be denoted e or id or 1_G). The additive notation may be used only for commutative groups.

Example: addition modulo n

Given a natural number n, let
$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$.
A binary operation $+_n$ (**addition modulo** n) on $\mathbb{Z}_n$ is defined for any $x, y \in \mathbb{Z}_n$ by

$$x +_n y = \begin{cases} x + y & \text{if } x + y < n, \\ x + y - n & \text{if } x + y \geq n. \end{cases}$$

Now let n be a positive real number and $\mathbb{R}_n = [0, n)$. The binary operation $+_n$ on $\mathbb{R}_n$ is defined by the same formula as above.

Theorem Each $(\mathbb{Z}_n, +_n)$ and each $(\mathbb{R}_n, +_n)$ is a group. All groups $(\mathbb{R}_n, +_n)$ are isomorphic.

Example: invertible functions

- Symmetric group $S(X)$: all bijective functions $\pi : X \to X$ with composition ($=$ multiplication).

(G0) π and σ are bijective functions from the set X to itself $\implies$ so is $\pi\sigma$

(G1) $(\pi\sigma)\tau$ and $\pi(\sigma\tau)$ applied to $x \in X$ both yield $\pi(\sigma(\tau(x)))$

(G2) the identity element is the identity function id_X as $\pi \, \mathrm{id}_X = \mathrm{id}_X \, \pi = \pi$

(G3) the inverse function π^{-1} satisfies $\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}_X$ (conversely, if $\pi\sigma = \sigma\pi = \mathrm{id}_X$, then $\sigma = \pi^{-1}$)

(G4) fails if the set has more than 2 elements

Example: set theory

• All subsets of a set X with the operation of symmetric difference: $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

(G0) $A, B \subseteq X \implies A \triangle B \subseteq X$.

(G1) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ consists of those elements of X that belong to an odd number of sets A, B, C (either to just one of them or to all three)

(G2) the identity element is the empty set $\emptyset$ since $A \triangle \emptyset = \emptyset \triangle A = A$ for any set A

(G3) the inverse of a set $A \subseteq X$ is A itself: $A \triangle A = \emptyset$

(G4) $A \triangle B = B \triangle A = (A \cup B) \setminus (A \cap B)$

Example: logic

- Binary logic $\mathcal{L} = \{\text{“true”}, \text{“false”}\}$ with the operation XOR (eXclusive OR): “x XOR y” means “either x or y (but not both)”.

(G0) $\text{“true XOR false”} = \text{“false XOR true”} = \text{“true”}$, $\text{“true XOR true”} = \text{“false XOR false”} = \text{“false”}$

(G1) “$(x \;\mathrm{XOR}\; y) \;\mathrm{XOR}\; z$”$=$“$x \;\mathrm{XOR}\; (y \;\mathrm{XOR}\; z)$”

(G2) the identity element is “false”

(G3) the inverse of $x \in \mathcal{L}$ is x itself

(G4) “$x \;\mathrm{XOR}\; y$”$=$“$y \;\mathrm{XOR}\; x$”

More examples

- Any vector space V with addition.

Those axioms of the vector space that involve only addition are exactly axioms of the commutative group.

- Trivial group $(G, *)$, where $G = \{e\}$ and $e * e = e$.

Verification of all axioms is straightforward.

- Positive real numbers with the operation $x * y = 2xy$.

(G0) $x, y > 0 \implies 2xy > 0$
(G1) $(x * y) * z = x * (y * z) = 4xyz$
(G2) the identity element is $\frac{1}{2}$ as $x * e = x$ means $2ex = x$
(G3) the inverse of x is $\frac{1}{4x}$ as $x * y = \frac{1}{2}$ means $4xy = 1$
(G4) $x * y = y * x = 2xy$

Counterexamples

- Real numbers $\mathbb{R}$ with multiplication.

0 has no inverse.

- Positive integers with addition.

No identity element.

- Nonnegative integers with addition.

No inverse element for positive numbers.

- Irrational numbers with addition.

The set is not closed under the operation.

- Integers with subtraction.

The operation is not associative: $(a - b) - c = a - (b - c)$ only if $c = 0$.

- All subsets of a set X with the operation $A * B = A \cup B$.

The operation is associative and commutative, the empty set is the identity element. However there is no inverse for a nonempty set.