Abstract algebra

Lecture note 1. Binary operations and groups

Lecturer : O-joung Kwon
Spring, 2019

We consider addition and multiplication to be *binary operations*. We abstract this notion and examine sets where we have one or more binary operations. We think of a binary operation on a set as giving an agebra on the set, and interested in the structural properties of that algebra.

Definition 1. *A* binary operation $*$ *on a set* S *is a function mapping* $S \times S$ *into* S*. For each* $(a, b) \in S \times S$*, we denote* $*((a, b))$ *of* S *by* $a * b$*.*

Example 1. Our usual addition $+$ is a binary operation on the real numbers $\mathbb{R}$.

Example 2. Let $M(\mathbb{R})$ be the set of all matrices with real entries. The usual matrix addition $+$ is not a binary operation on $M(\mathbb{R})$, because sometimes we cannot apply the matrix addition when two matrices have different sizes.

Definition 2. *Let* $*$ *be a binary operation on* S *and let* H *be a subset of* S*. The subset* H *is* closed under $*$ *if for all* $a, b \in H$*, we also have* $a * b \in H$*.*

Three basic properties on a binary operation.

Definition 3. *A binary operation $*$ on a set S is* commutative *if $a * b = b * a$ for all $a, b \in S$.*

Definition 4. *A binary operation $*$ on a set S is* associative *if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.*

Table
For a finite set, a binary operation on the set can be defined by means of a table.
Example of table :

Isomorphic binary structures

We are interested in studying the different types of structures that binary operations can provide on sets having the same number of elements. We consider $< S, * >$ as a binary algebraic structure. We define isomorphism as binary algebraic structures, where the binary operations result in the corresponding elements.

Definition 5. *Let $< S, * >$ and $< S', *' >$ be binary algebraic structures. An* isomorphism *of S with S' is one-to-one function ϕ mapping S onto S' such that*

- *$\phi(x * y) = \phi(x) * \phi(y)$ for all $x, y \in S$. (we call it* homomorphism property*)*

If such a map ϕ exists, then S and S' are isomorphic *binary structures, which we denote by $S \simeq S'$.*

How to show that two binary structures are isomorphic?

(1) Define a function ϕ.
(2) Show it one-to-one (injective).
(3) Show it onto (surjective).
(4) Show that $\phi(x * y) = \phi(x) * \phi(y)$ for all $x, y \in S$ (homomorphism).

Let $\mathbb{Z}$ be the set of all integers. and $2\mathbb{Z} := \{2n : n \in \mathbb{Z}\}$.

Lemma 1. $< \mathbb{Z}, + >$ *and* $< 2\mathbb{Z}, + >$ *are isomorphic.*

Sometimes, we want to solve an equation like $a+x=b$. What is necessary?

$5+x=2$ has a solution.

$$\begin{aligned}
5+x &= 2 && \text{given} \\
-5+(5+x) &= -5+2 && \text{adding } -5 \\
(-5+5)+x &= -5+2 && \text{associative law} \\
0+x &= -5+2 && \text{computing } -5+5 \\
x &= -5+2 && \text{property of 0} \\
x &= -3 && \text{computing } -5+2
\end{aligned}$$

Definition 6. *A group $< G, * >$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied.*

- *For all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$. (associativity)*
- *There is an element e in G such that for all $x \in G$, $e * x = x * e = x$ (identity element e)*
- *For each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = e$ (inverse a' of a)*

Definition 7. *A group G is* abelian *if its binary operation is commutative.*

Example 1. The set $\mathbb{Z}^+ = \{1, 2, \ldots\}$ under addition is not a group. There is no identity.

Example 2. The set of all non-negative integers is still not a group. There is no inverse of 2.

Example 3. $< \mathbb{Z}, + >$ is an abelian group.

Example 4. The set $M_n(\mathbb{R})$ of all $n \times n$ matrices under matrix multiplication is not a group. All-0 matrix has no inverse.

Exercise 1. *The set of all invertible $n \times n$ matrices under matrix multiplication is a group.*

Elementary properties of groups

Theorem 1. *If G is a group with binary operation $*$, then the left and right cancellation laws hold in G. That is, $a*b = a*c$ implies that $b = c$, and similarly, $b * a = c * a$ implies $b = c$ for all $a, b, c \in G$.*

Theorem 2. *If G is a group with binary operation $*$, and $a, b \in G$, then the linear equations $a * x = b$ and $y * a = b$ have unique solutions x, y in G.*

Theorem 3. *In a group G with binary operation $*$, there is only one element e in G such that $e * x = x * e = x$ for all $x \in G$. Also, for each $a \in G$, there is only one element a' in G such that $a' * a = a * a' = e$.*

Theorem 4. *Let G be a group. For all $a, b \in G$, we have $(a * b)' = b' * a'$. (a' denotes the inverse of a)*

Examples of groups.