

Operations

Abstract Algebra

Lecture 3

Algebraic Objects

- Integers: \mathbb{Z}
- Positive integers: \mathbb{P}
- Rationals: \mathbb{Q}
- Reals: \mathbb{R}
- Complexes: \mathbb{C}
- Polynomials in one variable, $\mathbb{R}[x]$, and more variables $\mathbb{R}[x, y, z]$
- Functions from set X to set Y
- Ladder diagrams
- Braid diagrams
- Elliptic curves: the points in \mathbb{R}^2 that satisfy an equation like $y^2 = x^3 + ax^2 + bx + c$

Unary operators

A unary operator on a set S is a function $f : S \rightarrow S$.

Examples:

- Absolute value is an unary operator on \mathbb{R}
- Negation is a unary operator on \mathbb{R} , \mathbb{Q} or \mathbb{Z} .
- Addition is not a unary operator—it takes two inputs
- The square root function is a unary operator on the nonnegative reals
- It is not a unary operator on the nonnegative rationals, because ____
- Your favorite unary operator is ____

Binary Operators

A **binary operator** on a set S is a function $*$ that assigns to each ordered pair (s_1, s_2) of elements of S an element $s_1 * s_2$ of S .

Examples:

- $+$ is a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$
- $-$ is a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$
- Multiplication is a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$
- Division is not a binary operation on \mathbb{Z} because 3 divided by 5 is not an integer
- Division is not a binary operation on \mathbb{R} , because 3 divided by 0 is not defined.
- Division is a binary operation on the nonzero real numbers.

Discussion

- 1 What are other kinds of binary operations on the reals?
- 2 Are there any binary operations on functions?
- 3 Are there any binary operations on the subsets of a given set X ?
- 4 Given two ladder diagrams L_1 and L_2 is there a natural way to make them into one ladder diagram?
- 5 Given two braids B_1 and B_2 , is there a natural way to make them into one braid?

Main points

Scientists, Mathematicians, Engineers and commoners construct **objects** to better understand a given phenomena.

Ways of combining these objects to get another object leads to (binary) **operations** and algebra.

Three binary operations for Elliptic curves

Let's illustrate all of this with one example: $y^2 = x^3 - 2$

We are going to let E be points (x, y) in \mathbb{R}^2 that satisfy $y^2 = x^3 - 2$, along with the “point at infinity”.

Note: reflection about the x -axis is a unary operation on E .

We'll denote by \bar{P} the reflection of P about the x -axis.

Given 2 points P and Q on the curve, we can define $P \triangleright Q$ to be the third point on the line joining P and Q and on E .

Elliptic curves

What if there isn't a third point?

Only ways this can happen are if line segment joining P and Q is vertical, or $P = Q$.

In former, define $P \triangleright Q$ to be ∞

In latter, define $P \triangleright Q$ to be the point of intersection of the line tangent to the curve at P and the curve.

Elliptic curves

What if P or Q is ∞ ?

If $P \neq \infty$, then take $P \flat Q$ to be the point of the intersection of the vertical line through the point P , and the curve.

Similarly, for $Q \neq \infty$.

If both P and Q are ∞ , then $P \flat Q = \infty$.

In this way \flat defines a binary operation on E .

Elliptic curves

It turns out that \flat by itself isn't so nice.

However, the binary operation $P\#Q$ on E defined by

$$P\#Q = \overline{(P\flat Q)}$$

is very useful.

Operation or Cayley Table

Given a binary operation $*$ on a set S it is sometimes useful to write out a table that lists all the operation outcomes.

This is called a **Cayley** table.

$*$	s_1	s_2	\dots	s_j	\dots	\dots
s_1						
\vdots						
s_i				$s_i * s_j$		
\vdots						

Cayley tables

An operation on $\{1, -1\}$

\cdot	1	-1
1	1	-1
-1	-1	1

An operation on $\{0, 1, 2\}$

\oplus	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

A couple for you

Max on $\{e, \pi, \phi = \frac{1+\sqrt{5}}{2}\}$

max	e	π	ϕ
e			
π			
ϕ			

Symmetric difference, Δ on subsets of $\{1, 2\}$

Δ	

Properties of binary operations

Let \diamond be a binary operation on a set S .

Then (S, \diamond) is **commutative** provided:

$$s_1 \diamond s_2 = s_2 \diamond s_1 \text{ for all } s_1, s_2 \in S.$$

Examples:

Properties of binary operations

Let \diamond be a binary operation on a set S .

Then (S, \diamond) is **associative** provided

$$s_1 \diamond (s_2 \diamond s_3) = (s_1 \diamond s_2) \diamond s_3 \text{ for all } s_1, s_2, s_3 \in S.$$

Examples:

Questions for Field Guide

- 1 How do you tell if an operation is commutative from its Cayley table?
- 2 Can you easily tell whether or not an operation is associative from its Cayley table?
- 3 Are there examples of binary operations that are commutative but not associative?

Identities

Let \diamond be a binary operation on a set S .

Then the element e is an identity of (S, \diamond) provided $e \diamond x = x$ and $x \diamond e = x$ for all $x \in S$.

Examples

Uniqueness of identity

Theorem: If \diamond is a binary operation on a set S , then (S, \diamond) has at most one identity.

Proof:

Inverses

Let \diamond be a binary operation on S and assume that the inverse of (S, \diamond) exists and is e .

The element y of S is **inverse** of $x \in S$ provided:

$$x \diamond y = e \text{ and } y \diamond x = e.$$

Examples:

Uniqueness of inverses

Theorem: Let \diamond be a binary operation on S and assume that the inverse of (S, \diamond) exists and is e .

If (S, \diamond) is associative, and $x \in S$, then x has at most one inverse.

Proof:

Question: Do we really need associativity here?

Aren't you curious?

Let \diamond be a binary operation on S and let $a, b \in S$.

There are some very natural, and fundamental questions:

- Is there an $x \in S$ with $a \diamond x = b$?
- If so, could you describe such x 's?

- Can you give an algorithm for answering (a)?

Note could ask similar, but different questions, for $x \diamond a = b$.

The utility of an inverse & associativity

Theorem:

Assume that (S, \diamond) is associative with identity e , $a \in S$ has inverse r , and $b \in S$.

Then $a \diamond x = b$ has exactly one solution, namely, $x = r \diamond b$.

Proof.

What would the analogous theorem be for $x \diamond a = b$?