

Recall

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

- (S, \diamond) is **commutative** provided: $s_1 \diamond s_2 = s_2 \diamond s_1$ for all $s_1, s_2 \in S$.
- (S, \diamond) is **associative** provided $s_1 \diamond (s_2 \diamond s_3) = (s_1 \diamond s_2) \diamond s_3$ for all $s_1, s_2, s_3 \in S$.
- e is an **identity** of (S, \diamond) provided $e \diamond x = x$ and $x \diamond e = x$ for all $x \in S$.
- y of S is **inverse** of $x \in S$ provided: $x \diamond y = e$ and $y \diamond x = e$.

Uniqueness of identity

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

Proof:

Assume that both e and f are identities of S .

Consider $e \diamond f$.

Since e is an identity, $e \diamond f = e$

Since f is an identity, $e \diamond f = f$

So $e = f$. ■

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:

Assume that both y and z are inverses of x .

Consider $y \diamond (x \diamond z)$.

Since z an inverse of x : $y \diamond (x \diamond z) = y \diamond e = y$

Since \diamond is associative and y is an inverse of x :
 $y \diamond (x \diamond z) = (y \diamond x) \diamond z = e \diamond z = z$.

So $x = z$. ■

Example of non-associative

\diamond	a	b	c	d
a	a	b	c	a
b	b	d	d	b
c	c	d	d	c
d	a	b	c	d

Notes:

- Commutativity iff Cayley table is symmetric
- No easy way to check associativity from table
- $\#$ on Elliptic curve is associative—this comes down to a geometric result called Serre's theorem.

Product of invertibles

Let x and y be elements in (S, \diamond) with inverses x' and y' , where \diamond is associative. Then $x \diamond y$ is invertible, and its inverse is $y' \diamond x'$.

(The inverse of a product is the product of the inverses in the reverse order).

Proof:

$$\begin{aligned}(x \diamond y) \diamond (y' \diamond x') &= ((x \diamond y) \diamond y') \diamond x' \\ &= (x \diamond (y \diamond y')) \diamond x' \\ &= (x \diamond e) \diamond x' \\ &= x \diamond x' \\ &= e\end{aligned}$$

Similarly, $(y' \diamond x') \diamond (x \diamond y) = e$.



Notation

When we know that \diamond is commutative, we often use 0 to denote the identity (if it exists); and $-x$ denote the inverse of x if it exists.

Otherwise, we often use 1 to denote the identity and x^{-1} to denote the inverse.

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 all such x 's?
- Can you give an algorithm for answering (a)?

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

Specific examples

- Let $f = x^3 - 5$ and $y = x^2 + 1$.
Is there a real valued function g such that
 $f \circ g = x^2 + 1$?

- For the elliptic curve $y^2 = x^3 + 1$, is there a point Q
such that $(2, -3) \# Q = (1, \sqrt{2})$?

The utility of an inverse & associativity

Theorem

(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. Uniqueness:

Suppose $x = u$ and $x = v$ are both solutions.

then $a \diamond u = a \diamond v$.

Pre-multiplying by r gives:

$$u = r \diamond a \diamond u = r \diamond a \diamond v = v$$

Existence:

Consider $x = r \diamond b$.

Note $a \diamond r \diamond b = e \diamond b = b$.

So $x = r \diamond b$ is a solution to $a \diamond x = b$. ■

- What would the analogous theorem be for $x \diamond a = b$?
- When \diamond is associative and x has an inverse, then each element occurs exactly once in x 's row of the Cayley table, and exactly one in x 's column of the Cayley table.

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	0	3	0
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Can't solve $0x = 3$ in this system; because 2 doesn't have an inverse here.

Can't solve $2x = 3$ in this system; because 2 doesn't have an inverse here.

New topic: Permutations

There are 3 major species of algebraic objects; Groups, Rings and Fields.

The integers with addition and multiplication are a prototype for a ring.

The rationals with addition and multiplication are a prototype for a field.

We'll discuss these more later.

A group has just one operation; and the **permutations of a set** are a prototype for a group.

Functions

Which functions $f : X \rightarrow X$ are invertible (using composition as the operator)?

Note if f has inverse g , then for each $y \in X$ there is at most one solution to $f(x) = y$.

Why? $f(x_1) = y$ and $f(x_2) = y \Rightarrow$
 $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$.

If f has inverse g , then for each $y \in X$ there is at least one solution to $f(x) = y$:

Why? $y = \text{id}(y) = f(g(y))$. So $x = g(y)$ is a solution.

Upshot: If $f : X \rightarrow X$ is invertible, then for each y the equation $f(x) = y$ has exactly one solution.

One-to-one & onto functions

Let X, Y be a sets, and $f : X \rightarrow Y$ be a function.

- 1 f is **one-to-one** provided for each $y \in Y$ there is at most one $x \in X$ with $f(x) = y$
- 2 f is **onto** provided for each $y \in Y$ there is at least one $x \in X$ with $f(x) = y$.
- 3 f is a **one-to-one correspondence** provided for each $y \in Y$ there is exactly one $x \in X$ with $f(x) = y$.

Functions

Examples:

Graphical interpretations:

- f is one-to-one if its graph passes the horizontal line test (i.e. each horizontal line intersects graph in at most one place)

- f is onto if each horizontal line (with y -intercept in Y) intersects the graph in at least one place

Functions

When $X = Y$, composition is a binary operation on the set of all functions $f : X \rightarrow X$.

What's the identity for this operation?

$$e(x) = x$$

Which functions have an inverse?

Precisely, the one-to-one correspondences.

Permutations

A **permutation** of the set X is just a one-to-one correspondence from X to X .

Examples.

$f : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ by $f(1) = 4$, $f(2) = 3$, $f(3) = 2$ and $f(4) = 1$.

In discrete math this permutation would correspond to the permutation 4, 3, 2, 1.

Number of permutations of $1, 2, \dots, n$ is ${}_n P_n = n!$.

Permutations: Two line notation

Given a permutation f of $1, 2, \dots, n$, we can write it as

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

Examples: composition, inverse

Permutations arise in many settings

- Rigid Motions
- Perfect Shuffles
- Ladder diagram
- Pancake Problem

Picture of a Permutation

Given a permutation f on $\{1, 2, \dots, n\}$, we associate with it a diagram with vertices $1, 2, \dots, n$ and arcs from i to $f(i)$.

Example:

Cycles

Shorthand notation

Every permutation is a product of disjoint cycles

Multiplying in cycle notation

Inverses in cycle notation

Powers in cycle notation