MATH 171 LECTURE 2

Def: Cartesian product $A \times B = \{(a,b) \mid a \in A, b \in B\}$

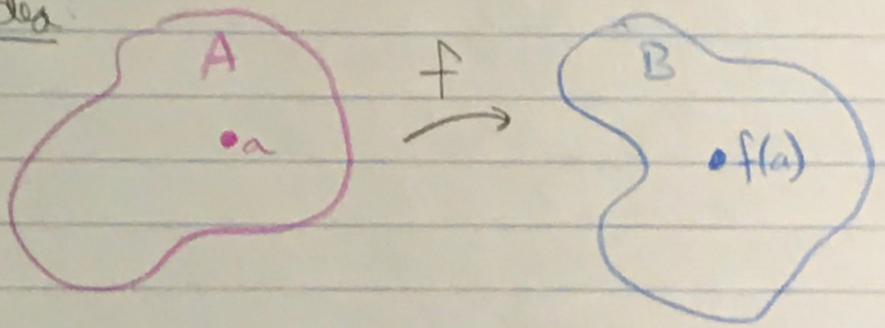
Def: Let A and B be sets. A map of sets from A to B (also called a function from A to B) is a subset $f \subseteq A \times B$ such that for each $a \in A$ there is a unique $b \in B$ with $(a,b) \in f$.

We use functional notation

$$(a,b) \in f \Leftrightarrow f(a) = b.$$

$\left\{ \forall a \in A \ \exists!\, b \in B \text{ s.t. } f(a) = b \right\}$ short hand

Idea:



Def:

A binary operation on a set A is a map

$$* : A \times A \to A.$$

(For each $x, y \in A$, $x * y \in A$)

Def: The binary operation $*$ on A is associative if

$$x * (y * z) = (x * y) * z$$

for all $x, y, z \in A$.

Def: The binary operation $*$ on A has an identity element $e \in A$ if

$$e * x = x * e = x$$

for all $x \in A$.

Def: If $(A, *)$ has an identity, then $a \in A$ has an inverse if there is a $b \in A$ such that

$$a * b = b * a = e$$

We write $b = a^{-1}$.

Def: A group is a pair $(G, *)$ of a set G with binary operation $*$ such that
(1) $*$ is associative
(2) $(G, *)$ has an identity element
(3) $(G, *)$ has inverses

NIELS HENRIK ABEL
NORWAY
1802–1829
26Y.O.
ABEL PRIZE PROPOSED IN 1899

Def: G is Abelian or commutative if $x * y = y * x$ for all $x, y \in G$.
Note: Since $* : G \times G \to G$, this presupposes closure, that $\forall x, y \in G$, $x * y \in G$.

Ex: (1) $(\mathbb{N}, -)$ Not closed, no identity
SAME SET
(2) $(M_2(\mathbb{R}), +)$
(3) $(M_2(\mathbb{R}), \times)$

ARTHUR CAYLEY
1821–1895
BRITISH

Def: The multiplication table is called the Cayley table.

Proposition: In a group $(G, *)$, the identity is unique

Proof. Suppose $e_1, e_2 \in G$ are both identities, ie

(1) $e_1 * x = x * e_1 = x \quad \forall x \in G$

(2) $e_2 * y = y * e_2 = y \quad \forall y \in G$.

QUOD ERAT DEMONSTRATUM

Then

$$e_1 \overset{(2)}{=} e_1 * e_2 \overset{(1)}{=} e_2$$

Thus $e_1 = e_2$. QED

Notation: e ~ 1

Proposition: Inverses are unique. Let $x \in G$. Then $\exists!\, y$ s.t. $x * y = y * x = e$.

Proof: Let y and z be inverses of x, ie

(1) $x * y = y * x = e$

(2) $x * z = z * x = e$

Then

$$\begin{aligned} y \overset{(e)}{=} y * e &\overset{(2)}{=} y * (x * z) \\ &\overset{(A)}{=} (y * x) * z \\ &\overset{(1)}{=} e * z \\ &\overset{(e)}{=} z \end{aligned}$$

Thus $y = z$. QED

Notation: $\boxed{x^{-1}}$.

Solo/group work

Prop: Let $a, b \in (G, *)$. Then

$$(ab)^{-1} = b^{-1} a^{-1}$$

Prop: $(a^{-1})^{-1} = a$

Prop: Let $a, b \in G$. Then

$$ax = b \quad \text{and} \quad ya = b$$

have unique solutions.

Prop: Let $a, b, c \in G$.

$$ab = ac \Rightarrow b = c, \qquad ba = ca \Rightarrow b = c.$$

Thm: For $x, y \in G$, $n, m \in \mathbb{Z}$

(1) $x^{n+m} = x^n \cdot x^m$

(2) $(x^n)^m = x^{nm}$

(3) $(xy)^n = (y^{-1} x^{-1})^{-n}$

(4) If G is abelian $(xy)^n = x^n y^n$