Revision of Basics

$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ denotes the integers.

$\mathbb{Q} = \{ p/q \mid p, q \in \mathbb{Z},\ q \neq 0 \}$ denotes the rational numbers.

such that

$\mathbb{R}$:= set of real numbers

$\mathbb{C} = \{ a + ib \mid a, b \in \mathbb{R} ;\ i^2 = -1 \}$

denotes the complex numbers.

$\left.\begin{array}{l} \mathbb{Z}^+ = \\ \mathbb{Q}^+ = \\ \mathbb{R}^+ = \end{array}\right\}$ positive (non-zero) elements of $\left\{\begin{array}{l} \mathbb{Z} \\ \mathbb{Q} \\ \mathbb{R} \end{array}\right.$

respectively.

$\left.\begin{array}{l} f : A \longrightarrow B \\ \text{or} \\ A \xrightarrow{f} B \end{array}\right\}$ denote a function f from set A to a set B.

Domain

Co-domain

$a \longmapsto b$

$f(a) = b$

Introduction to Group Theory.

Set having some properties

History.

$ax^2+bx+c=0$; $a,b,c \in \mathbb{R}$

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a} = \frac{-b \pm (b^2-4ac)^{1/2}}{2a}$$

$a_3x^3 + a_2x^2 + a_1x + a_3 = 0$ YES

$\vdots$

$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$; $a_i \in \mathbb{R}$

$n \geq 5$

NO

Group Theory

E. Galois. (17th century)

Basic cryptography

$f(x) = f(y)$

If $x = y$, then ...

$f : \mathbb{Q} \longrightarrow \mathbb{Z}$

$\frac{p}{q} \longmapsto p+q$

$(q \neq 0)$

$x = \frac{1}{2} \longmapsto 3$

$y = \frac{2}{4} \longmapsto 6$

Given a ~~function~~ map $f : A \longrightarrow B$

"Well-defined" (How to check ?)

↪ functions are well-defined (by definition)!!!

→ Now, assume that a map $g : A \to B$ is given (Is this g a function ?)

(– in the sense, well-defined).

Note : It is not clear in general whether a given map (function) is well-defined.

* We need to make sure that what we define, say, $g : A \longrightarrow B$ is indeed "well-defined".

Example. $f : \mathbb{Q} \longrightarrow \mathbb{Z}$

$$\frac{a}{b} \longmapsto a+b \quad ; \quad b \neq 0$$

It is clear that $f(\mathbb{Q}) \subset \mathbb{Z}$

Is this proper ?

Question. Is f well-defined ?

How to check well-defined map :

A function $f: A \longrightarrow B$ is well-defined if $x = y$ implies $f(x) = f(y)$.

$\rightarrow$ $f(A) = \{ b \in B \mid b = f(a) \text{ for some } a \in A \}$

$:=$ range or image of f

(image of A under f)

$f: A \longrightarrow B$

$C \subseteq B$

- For each subset C of B, the set

$$f^{-1}(C) = \{ a \in A \mid f(a) \in C \}$$

(pre-image or inverse image of C)

- Given a function $f: A \longrightarrow B$;

f^{-1} need not be a function (why?).

$f: A \rightarrow B$

$f: \mathbb{Z} \rightarrow \mathbb{Z}$

$x \mapsto x^2$

f is 1-1

not onto

- If $f: A \longrightarrow B$ and $g: B \longrightarrow C$, then $g \circ f: A \longrightarrow C$ is defined by

$$(g \circ f)(a) = g(f(a)).$$

Well-known terminologies:

Let $f : A \longrightarrow B$ is defined.

[Injective or injection]

f is one-one

def^{n} $\Rightarrow$ I $\left\{ \text{If } f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \right.$

Contrapositive.

II whenever $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.

Surjective or surjection: If $\forall$ $b \in B$, there is some $a \in A$

(for all)

s.t. $f(a) = b$.

Bijective or bijection: If f is both injective & surjective.

- f has a <u>left inverse</u> if there is a function

$g : B \longrightarrow A$ such that

$g \circ f : A \longrightarrow A$ is the <u>identity map</u>.

$$(g \circ f)(a) = a \quad \forall a \in A.$$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right] & B \arrow[r, "g"] & A \end{tikzcd}$$

$g \circ f = Id_A$

left

$$\begin{tikzcd} B \arrow[r, "h"] \arrow[rr, bend right] & A \arrow[r, "f"] & B \end{tikzcd}$$

Right inverse of f $\quad f \circ h(b) = b \;\; \forall\, b \in B$

$\quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \; \| $

$\quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \; Id_B$ (right to f)

Question: Given a function $f : A \to B$;

(i) If f has a left inverse, then does it always have a right inverse?

(ii) Does right inverse of f $\Rightarrow$ left ~~inve~~ inverse of f?

(iii) f is injective if and only if ($\Longleftrightarrow$) f has a left inverse.?

(iv) f is surjective if and only if f has a right inverse.?

(v) $f : A \to B$ is bijective if and only if there exists $g : B \to A$ such that

$$A \xrightarrow{f} B \xrightarrow{g} A \qquad B \xrightarrow{g} A \xrightarrow{f} B$$

$$g \circ f = Id_A \qquad f \circ g = Id_B$$

(vi) Assume that A and B are finite sets, then $f : A \to B$ is bijective $\Longleftrightarrow$ f is injective.

Textbook.

1. Algebra by Michael Artin, Prentice Hall
[Chapter 2, 50-60%.]

2. Contemporary Abstract Algebra by Joseph A. Gallian
8th edition

3. MIT Lecture Notes on "Modern Algebra"
MIT 18.703
Undergraduate course

[Lecture 1 — Lecture 10]

Lecture 7-8

NPTEL courses

We will continue to revise basics, however let us focus now towards "Group Theory".

Binary operation($*$).

$G \neq \phi$

A binary operation $*$ (or f) on a set G is a ~~function~~ map

$$* : G \times G \longrightarrow G.$$

$$(a, b) \longmapsto a * b$$

Examples.

(i) $$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$(a, b) \longmapsto a + b \quad \text{(usual addition)}$$

$\Vert^{ly}$ $$+ : \mathbb{Q} \times \mathbb{Q} \longmapsto \mathbb{Q}$$

$$(r_1, r_2) \longmapsto r_1 + r_2,$$

and $$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

$$(x, y) \longmapsto x + y$$

etc.

More examples:

- $$- : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

$$(a, b) \longmapsto a - b \quad \text{(usual subtraction)}$$

Question: Construct examples of non-binary operation $*$.

[Hint: Modify previous definition in example.]

$A \neq \phi$

$$\varphi : A \times A \longrightarrow B$$
$$(a,b) \longmapsto \varphi(a,b)$$

map

Want : $\varphi(a,b) \in A$ for all $(a,b) \in A \times A$.

$$* : A \times A \longrightarrow A$$
$$(a,b) \longmapsto *(a,b)$$
$$\shortparallel$$
$$a * b$$

Examples.

①
$$\overset{*}{\downarrow}$$
$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(m, n) \longmapsto f(m,n) := m+n$$
$$*(m,n) = m*n \;//$$

Is f a binary operation ? YES

$m+n \in \mathbb{Z}$

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(m,n) \longmapsto +(m,n) := m+n$$

map or $*$

addition in $\mathbb{Z}$

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$(m, n) \longmapsto \begin{cases} \dfrac{m}{n} & ; n \neq 0 \\ m & n = 0 \end{cases}$$

NO

$$\frac{m}{n} \notin \mathbb{Z}$$

$$f(m,n) \notin \mathbb{Z}$$

$M_n(\mathbb{R}) := \{ \text{set of all } n \times n \text{ matrices over } \mathbb{R} \}$

$A + (B + C) = (A + B) + C$

True.

$$f : M_n(\mathbb{R}) \times M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$$

$$(A, B) \longmapsto A + B$$

Is f a binary operation ? YES

" " " abelian " " ?

$A + B = B + A$

Abelian binary operation

[Commutative]

$$\boxed{a * b = b * a}$$

$$f : M_n(\mathbb{R}) \times M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$$

$$(A, B) \longmapsto f(A,B) = AB \in M_n(\mathbb{R})$$

Is f abelian ? $AB = BA$ NO

Non-abelian

Associative : $\boxed{A \cdot (B \cdot C) = (A \cdot B) \cdot C}$ for $A, B, C \in M_n(\mathbb{R})$.

? True/False. True (How to verify ?)

f is a binary operation on a set

— Abelian

— Non-abelian

Associative binary operation ($*$).

$*: G \times G \longrightarrow G$ is associative if

f

for all $a, b, c \in G$, we have

$$\boxed{a * (b * c) = (a * b) * c}$$

$$f(a, f(b,c)) = f(f(a,b), c)$$

Commutative binary operation ($*$).

$*: G \times G \longrightarrow G$ is commutative if for all

Abelian

$a, b \in G$, we have $\boxed{a * b = b * a}$

Examples:

$$\left.\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a,b) &\longmapsto a+b \end{aligned}\right\}$$

abelian
Associative
$a + (b+c) = (a+b) + c$

$$+ : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$$
$$(a, b) \longmapsto a+b$$

$$\times : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \quad [\mathbb{Z} \text{ or } \mathbb{Q}]$$
$$(a,b) \longmapsto a \times b$$

usual multiplication

$$\times : \mathbb{Z}^- \times \mathbb{Z}^- \longmapsto \mathbb{Z}^-$$
$$(a, b) \longmapsto a \times b$$

$$- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a, b) \longmapsto a - b$$

$a - b \neq b - a$

Is this an abelian?

associative? NO

~~Assume that a set G~~

$$\times : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

Cross-product $\quad (\vec{v}, \vec{w}) \longmapsto \vec{v} \times \vec{w}$

Abelian ? NO

$$\times : GL_2(\mathbb{R}) \times GL_2(\mathbb{R}) \longrightarrow GL_2(\mathbb{R})$$

Usual Matrix Multiplication $\quad (A, B) \longmapsto A \times B \in GL_2(\mathbb{R})$

$\det(AB) = \det(A) \cdot \det(B)$

$GL_2(\mathbb{R}) :=$ 2 x 2 invertible matrices over the real numbers. ~~with~~

$$\times_\bullet : M_2(\mathbb{R}) \times M_2(\mathbb{R}) \longrightarrow M_2(\mathbb{R})$$

$$(A, B) \longmapsto A \times B$$

$M_2(\mathbb{R}) :=$ 2 x 2 matrices over the real numbers

Is $\times_\bullet$ a binary operation ?

associative " ?

commutative ?

→ Work out more examples.

Group: A group is an ordered pair $(G, *)$, where G is a non-empty set and $*$ is a binary operation on G satisfying the following axioms:

(i) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$

[Associative]

(ii) there exists an element e in G such that for all $a \in G$,

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

[identity element]

(iii) for each $a \in G$, there is an element $a^{-1} \in G$ such that

$$a * a^{-1} = a^{-1} * a = e$$

[inverse of a]

$\neq \phi$ $\quad G \times G \to G$

In short; $(G, *)$ with

(i) $*$ being associative

(ii) existence of identity element

(iii) inverse for every element in G

When $*$ is clear from the context; we shall simply say "Group G"

Question: Can a group $(G, *)$ be empty set (G)?

$m+(n+l) = (m+n)+l$

Examples of Groups:

- $(\mathbb{Z},+)$
- $(\mathbb{R},+)$
- $G = (\mathbb{C},+)$

$e = ?$ $\quad m + e = m$ for every $m \in \mathbb{Z}$

$e = 0$ identity element

$a^{-1} = -a$

$m + (-m) = e = 0$

$e = 0$

$\boxed{z^{-1} = -z}$

$(\mathbb{Q}-\{0\},\times)$

$(\ ) \cdot z = z$

$z \cdot (1) = z$ $\quad (\mathbb{R}-\{0\},\times)$

$e = 1 \rightarrow (\mathbb{C}-\{0\},\times)$

$z^{-1} = \frac{1}{z}$ $\quad (\mathbb{Q}^+,\times)$

$(\mathbb{R}^+,\times)$

$e = 1$

$a^{-1} = q/p$

$\underline{(\mathbb{Q}-\{0\},\times)}$

$p/q \times (1) = p/q$

$p/q \times (q/p) = 1$

$q \neq 0$ $\quad p \neq 0$

$(\mathbb{Z}-\{0\},\times)$

$(G = \{1, i, -1, -i\}, *)$

Suppose V is a finite dimensional vector space say, $V = \mathbb{R}^n$ for some n over $\mathbb{R}$;

$(\mathbb{R}^n,+)$ $\quad e = (0,0,\dots,0)$

$a = (v_1,\dots,v_n)$ $\quad a^{-1} = (-v_1,-v_2,\dots,-v_n)$

$(GL_2(\mathbb{R}),\times)$, $\quad e =$

$a^{-1} =$