Groups, rings & fields, lecture 1

Abstract algebra: Study of „sets with operations"

Group: • Set with „multiplication & division"
• Often the set of symmetries of some structure

Examples • $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, with operation $+$
• $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ with operation $\cdot$
• The set of all rotations of a triangle/square/circle.
• All ways to shuffle a deck of cards

Ring: Set with addition, subtraction, multiplication

Examples: • $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
• $M_n(\mathbb{R}) = \{(n \times n)$ real matrices$\}$
• $\mathbb{R}[x] = \{$real polynomials in variable $x\}$.

Field: Ring with division

Examples: • $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
• Lots of examples E with
$$\mathbb{Q} \subset E \subset \mathbb{R}.$$

Thm (Abel 1826): Let $f(x) = ax^5 + bx^4 + \cdots + e$. There is no formula for the solutions of

$$f(x) = 0$$

using only the operations $+ \; - \; \cdot \; \div$ & $\sqrt[n]{\;}$ & a, b, c, d, e.

Let $f(x) = ax^2 + bx + c$.

$$f(x) = 0 \iff x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Proof uses groups to understand fields to understand solutions of equations (Galois theory).

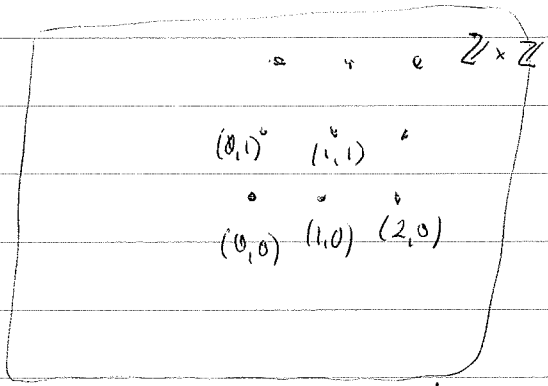
BINARY OPERATIONS

Def Let S be a set. Then

$$S \times S = \{ (a, b) \mid a, b \in S \}.$$

Def A binary operation $*$ on a set S is a function

$$* : S \times S \longrightarrow S$$



Write $a * b$ for $*(a, b)$. The pair $(S, *)$ is called "binary algebraic structure".

→

Examples:
- $S = \mathbb{Z}$ with $*(a, b) = a + b$,
- $S = \mathbb{Z}^+$ with $*(a, b) = ab$
- $S = \mathbb{Q}$ with $*(a, b) = a$
- Non-example: $S = \mathbb{Z}$ with $*(a, b) = \frac{a}{b}$, $\frac{a}{b} \notin \mathbb{Z}$ in general
- Non-example: $S = \mathbb{R}^3$ with $*(\vec{v}, \vec{w}) = \vec{v} \cdot \vec{w}$.

$\vec{v} \cdot \vec{w} \in \mathbb{R} \neq \mathbb{R}^3$.

- $S = \mathbb{R}^3$, $*(\vec{v}, \vec{w}) = \vec{v} \times \vec{w}$.

Next: Visualising $*$

- Possible good properties of $(S, *)$
- When is $(S, *)$ equivalent to $(S', *')$?

TABLES

Let S be finite, $*$ bin. op. on S. Visualise by table, e.g.

$S = \{a, b, c\}$

$*$	a	b	c
a	c	a	b
b	b	a	b
c	b	c	b

$*(a, b) = a$

$*(c, c) = b$.

GOOD PROPERTIES A binary operation $*$ on S is commutative if for all $a, b \in S$, have

$$a * b = b * a.$$

$(a+b = b+a)$ $(ab = ba)$

Examples: $S = \mathbb{Z}$, $* = +$ or $* = \cdot$

Non-example: $S = \mathbb{Z}$, $*(a, b) = a - b$. $(a - b \neq b - a)$.

S finite: $*$ commutative $\iff$ table is symmetric

$*$	a	b
a	a	b
b	b	b

comm.

$*$	a	b
a	a	a
b	b	a

non-comm.

Def A binary op $*$ is associative if for all $a, b, c \in S$, we have

$$(a*b)*c = a*(b*c).$$

Example: $S = \mathbb{Z}$, $* = +$, $* = \cdot$

Non-example: $S = \mathbb{Z}$, $* = -$, since

$$(a-b)-c = a-b-c$$
$$a-(b-c) = a-b+c,$$ these differ in general.

Def An identity element for $*$ is an $e \in S$ such that, for all $a \in S$, we have

$$e*a = a, \quad a*e = a.$$

Example: • $S = \mathbb{Z}$, $* = +$, $\Rightarrow$ 0 is identity elt,

$$0+a = a+0 = a$$

• $S = \mathbb{Z}$, $* = \cdot$ $\Rightarrow$ 1 is identity elt.

Thm: Let $e, e' \in S$ be identity elts for $*$. Then $e = e'$.

Pf: Since e is id. elt, have $e*e' = e'$.

– " – e' — " — $e*e' = e$

So $e' = e*e' = e$. □

Def SUBSETS Let $(S, *)$ be a bin. alg. str. A set $H \subseteq S$ is closed under $*$ if for all $a, b \in H$,

$$a*b \in H.$$

$2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\} = \{\text{even nos}\}$.

Example • $S = \mathbb{Z}$, $* = +$. $H = \{a \in \mathbb{Z} \mid a \text{ is even}\}$ is closed under $+$, since if $a, b \in H$ ($\Leftrightarrow a, b$ even)

$a + b \in H$ ($\Leftrightarrow a+b$ even)

• $H = \{a \in \mathbb{Z} \mid a \text{ is odd}\}$ is not closed under $+$;
Take $a = b = 1 \in H$. Then

$a + b = 2 \notin H$.

ISOMORPHISMS

Example: Let $S = \{1, 2, 3\}$, $S' = \{a, b, c\}$. Define $*$ on S, $*'$ on S' by

$*$	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

$*'$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

Then $(S, *)$ & $(S', *')$ are "equivalent" under dictionary $1 \leftrightarrow a$, $2 \leftrightarrow b$, $3 \leftrightarrow c$.

Def Let $(S, *)$ & $(S', *')$ be binary algebraic structures
An isomorphism of S with S' is a map $\phi: S \to S'$ which is

(1) one-to-one
(2) onto
(3) $\forall x, y \in S$, $\phi(x *' y) = \phi(x) * \phi(y)$.

Say $(S, *)$ & $(S', *')$ are isomorphic, write $S \simeq S'$, if there exists an isomorphism.

Example Let $S = \mathbb{R}$, $* = +$, $S' = \mathbb{R}^+$, $* = \cdot$.
Then $\phi : \mathbb{R} \longrightarrow \mathbb{R}^+$ ~~is an isomorphism~~ this is an isomorphism when

$$\phi(x) = e^x.$$

It is

(1) One-to-one: $e^x = e^y \iff x = y$
(2) Onto: $x \in \mathbb{R}^+$, $x = e^{\log x} = \phi(\log x)$
(3) For all $x, y \in \mathbb{R}$, $\phi(x+y) = \phi(x)\phi(y)$, since

---

~~Pf.~~

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y).$$