03.10.2023

Algebra - recap

(al-jabr)

Algebric structure = set + operations

Notations: S set, $*$ operation; $*: S \times S \to S$ operation (internal law)

$(x, y) \longrightarrow x * y$

Properties :- **A**ssociativity: $\forall x, y, z \in S: (x*y)*z = x*(y*z)$

- **i**dentity **E**lement: $\exists e \in S, \forall x \in S: e*x = x*e = e$

- **i**nvertability: $\forall x \in S, \exists x' \in S: x*x' = x'*x = e$

OBS: S set (with internal law)

⊕ A ⇒ semigroup

⊕ i. E. ⇒ monoid semigroup (monoid)

⊕ i ⇒ group

* ⊕ **C**omutativity ⇒ abelian (comutative) group

C: $\forall x, y \in S: x*y = y*x$

Remark: 1) $(G, +)$ group

- $+(x, y) = x + y$

"+ of x and y"

- $+(x, x) = 2x$
- usually $e_G = 0$ and $x' := -x$ (comes from "+")

2) $(G, \cdot)$ group

- $\cdot(x, y) = x \cdot y$
- $\cdot(x, x) = x^2$
- usually $e_G = 1$ and $x' := x^{-1}$ (comes from "$\cdot$")

ex groups $(\mathbb{R}, +)$; $(\mathbb{R}^*, \cdot)$; $(\mathbb{C}^*, \cdot)$; $(GL_n(\mathbb{R}), \cdot)$

monoid that is not a group $(\mathbb{N}, +)$, $(M_n(\mathbb{R}), \cdot)$

(if we include 0)

! $GL_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid \det A \neq 0 \}$

Remember: How to construct the inv. of a matrix?

1) transpose matrix: A^t
2) adjacent matrix: A^* (formed based on A^t)
3) $A^{-1} = \frac{1}{\det A} \cdot A^*$

ex groups: $(\mathbb{Z}_n, +), (S_n, \circ)$ ← comp. functions

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$\forall \bar{a}, \bar{b} \in \mathbb{Z}_n, \ \bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} = a \bmod n$

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

! Permutations $S_n = \{f : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\} \mid f \text{ bij.}\}$

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

! $f : A \to B, \ g : B \to C$

$g \circ f : A \to C, \ x \mapsto g(f(x))$

! A, B sets

$A^B = \{ f : B \to A \}$

$A^A = \{ f : A \to A \} \Rightarrow (A^A, \circ)$ monoid with i.e.

$id_A : A \to A, \quad id_{A(x)} = x, \quad \forall x \in A$

$x \mapsto x$ (maps every elem. to itself)

! $\mathbb{Z}_n \to$ residue classes modulo n

Rings

R set $\quad +, \cdot : R \times R \to R$

$(R, +, \cdot)$ is a **ring** iff:

- $(R, +)$ abelian group
- $(R, \cdot)$ semigroup
- Distributivity: $\forall x, y \in R : x(y+z) = xy + xz$

$(R, +, \cdot)$ is a **unital ring** iff:

- $(R, +, \cdot)$ ring
- $(R, \cdot)$ monoid ($\Leftrightarrow \oplus$ i.e.)

$(R, +, \cdot)$ is a **division ring** iff: → corp

- $(R, +, \cdot)$ ring
- $(R, \cdot)$ group ($\Leftrightarrow \oplus$ invertibility)

! **ring** + "$\cdot$" comutative $\Rightarrow$ **comutative ring**

! **division ring** + "$\cdot$" comutative $\Rightarrow$ **field**

ex - fields: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ only when p is prime

- rings that are not fields: $(\mathbb{Z}, +, \cdot)$, $(M_n(\mathbb{R}), +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ n composite (! prime), $(R[X], +, \cdot)$ where $(R, +, \cdot)$ ring

! **Polinomials**

$(R, +, \cdot)$ ring

A polinomial over R is a formal sum:

$$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

- X = indeterminate, $a_i \in R$, $i = \overline{0,n}$
  ↳ coeficients of "f"
- degree of "f" $= n \xrightarrow{\text{notation}} \boxed{\deg f = n}$

a_n = leading / dominant coef.

a_0 = free term

$R[X] = \{ f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid n \in \mathbb{N}, a_i \in R \}$

- $R_n[X] = \{ f \in R[X] \mid \deg f \leq n \}$
- $f = \sum_{i=0}^{n} a_i \cdot X^i$, $g = \sum_{j=0}^{m} b_j \cdot X^j$

WLOG (without loss of generality):

if $n \geq m \Rightarrow f+g = a_n X^n + \dots + a_{m+1} X^{m+1} + (a_m + b_m) X^m + \dots + (a_0 + b_0)$

$$f \cdot g = \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j X^k$$

ex $(a+bx)(c+dx+ex^2) =$

$= ac + x(ad+bc) + x^2(ae+bd)$

For a set A where "$+$" and "$\cdot$" from $\mathbb{R}$ "make sense", we can define:

$f: A \to A$, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

! An element for which $f(x) = 0$ is called root of the polinomial f

ex $f = ax^2 + bx + c$

The roots are: $x_{1,2} = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$