Algebra – recap

algebraic structure → set + operation(s)

- S set, $*: S \times S \to S$
  $(x,y) \to x*y$ operation (internal law)
- associativity: $\forall x,y,z \in S \quad (x*y)*z = x*(y*z)$

] semi-group

- neutral element: $\exists\, e \in S : \forall x \in S : \quad x*e = x$

] monoid semigroup

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

] group

- commutativity: $\forall x,y \in S : \quad x*y = y*x$

group + commutativity ⇒ abelian (commutative) group

Ex: groups: $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathcal{M}_n(\mathbb{R}),+)$, $(\mathbb{Z}_7,+)$, $(\mathbb{Z}_7^*,\cdot)$, $(\mathbb{Z}_7,\cdot)$

$(S_n,\circ)$, $(\mathbb{Z}^2,+)$

monoids that are not groups: $(\mathcal{M}_n(\mathbb{R}),\cdot)$, $(A^A,\circ)$ with neutral element $id_A : A \to A$, $x \to x$, $(\mathbb{Z}_7,\cdot)$

$GL_n(\mathbb{R}) = \{ A \in \mathcal{M}_n(\mathbb{R}) \mid \det A \neq 0 \}$

How does one invert a matrix?

- A^t
- A^*
- $A^{-1} = \frac{1}{\det A} A^*$

$(\mathbb{Z}_n,+,\cdot)$ field $\Leftrightarrow$ n prime

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

$f: A \to B$ $\quad g: B \to C$ $\quad g \circ f: A \to C$ $\quad x \to g(f(x))$

$S_n = \{ f: \{1, \dots, n\} \to \{1, \dots, n\} \mid f \text{ bijective} \}$ ⟶ injective + surjective (perfect correspondence between the two)

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

R set, $+, \cdot$ operations on R

- $(R, +)$ abelian group
- $(R, \cdot)$ semigroup
- distributivity: $\forall\, x, y, z \in R.\quad x \cdot (y + z) = xy + xz$, $\quad (y + z) \cdot x = yx + zx$

] ring

- "$\cdot$" has a neutral element

] unital ring ("inel")

- $\forall\, x \in R,\ x \neq 0\ \exists\, x' \in R$: $\quad x \cdot x' = x' \cdot x = e$

] division ring = skew field ("corp")

ring + "$\cdot$" commutivience = commutative ring

division ring + "$\cdot$" commutitive = field

Ex: fields: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ (p prime), $R(x) = \{ \frac{f}{g} \mid f, g \in R[x],\ g \neq 0 \}$ ⟶ $\boxed{\int_0^1 \frac{2x^2+1}{(x-2)(x^2+5)}\,dx}$

Ex: rings that are not fields: $(M_n(R), +, \cdot)$ (R-ring), $(\mathbb{Z}, +, \cdot)$ (the ONE ring), $(\mathbb{Z}_6, +, \cdot)$, $R[x]$ (R-ring)

Polynomials

R commutative unital ring (e.g. a field)

A polynomial over R is a formal sum of the form $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 \cdot x + a_0$

don't interpret anything until u have to

x = "indeterminate", $x \cdot x = x^2$, $x \cdot x \cdot \ldots \cdot x = x^n$

$a_i \in R$ the coefficients of x

$n = \deg f$ (degree of f), a_n = leading coefficient

a_0 = free term

Ex: $\deg(x^2 - 5x + 1) = 2$

$\deg(7x - 9) = 1$

$\deg(5) = 0$

$\deg(0) = -\infty$

$\deg(f \cdot g) = \deg f + \deg g$ (if R is field)

Counterexample: $R = \mathbb{Z}_4$

$(\hat{2}x + \hat{3})(\hat{2}x^2 + \hat{1}) = \hat{6}x^2 + \hat{2}x + \hat{3}$

$f \in R[x]$, A - set where the operations from R make sense

we can define $\tilde{f} : A \to A$

$x \to a_n x^n + \dots + a_2 \cdot x^2 + a_1 \cdot x + a_0$

the polynomial function of f on A

Thm] Fundamental theorem of algebra

Any $f \in \mathbb{C}[x]$ has roots in $\mathbb{C}$

Corollary If the roots of f are $x_1, x_2, \dots, x_n \in \mathbb{C}$, then $f = a_n (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n)$

Ex) $f = x^2+1 \in \mathbb{R}[x]$ – irreducible in $\mathbb{R}$
<u>not</u> irreducible in $\mathbb{C}$

$f = (x-i)(x+i)$ reducible in $\mathbb{C}$

Thm) Euclidean division

K - field

$f, g \in K[x]$, $g \neq 0$

$\exists$ $q, r \in K[x]$ with $\deg r < \deg g$ so that $\underbrace{f}_{\text{dividend}} = \underbrace{g}_{\text{division}} \cdot \underbrace{q}_{\text{quotion}} + \underbrace{r}_{\text{remainder}}$

Corr) $\forall f, g \in K[x]$ $\exists$

$d = \gcd(f,g) \in K[x]$

s.t. :
- $d \mid f$ and $d \mid g$
- if $d' \in K[x]$ st. $d' \mid f$ and $d' \mid g$ $\Rightarrow d' \mid d$

d can be found using the Euclidean algorithm (unchanged from $\mathbb{Z}$)

Ex : $f = x^3 - x^2 + 2x + 1 \quad \in \mathbb{Q}[x]$

$g = 2x^2 + 1 \quad \in \mathbb{Q}[x]$

$$
\begin{array}{l|l}
x^3 - x^2 + 2x + 1 & 2x^2 + 1 \\
\hline
-x^3 \qquad - \frac{1}{2}x & \frac{1}{2}x - \frac{1}{2} \\
\quad -x^2 + \frac{3}{2}x + 1 & \\
\quad\ \ x^2 \qquad + \frac{1}{2} & \\
\hline
\qquad \frac{3}{2}x + \frac{3}{2} &
\end{array}
$$

$\Rightarrow q = \frac{1}{2}x - \frac{1}{2}$

$r = \frac{3}{2}x + \frac{3}{2}$

$\mathbb{R}[x] = \{ f = a_n x^n + \dots + a_1 x + a_0 \mid a_i \in \mathbb{R} \}$

$\mathbb{R}_n[x] = \{ f \in \mathbb{R}[x] \mid \deg f \leq n \}$