Lecture 10

TUESDAY,
27th SEPTEMBER, 2022

RECALL:
1) Algebra-like object → FIELD
2) Module-like object → VECTOR SPACE

* $\mathbb{Z}$ is NOT a field as it doesn't have a multiplicative inverse ∈ $\mathbb{Z}$

Field → a set K with add", multiplication, 0, 1, i s.t. (0 → additive identity; 1 → multiplicative identity)
- $(K, +, 0)$ every element in K has an additive inverse
  $\forall x, \exists x' \in K$ s.t $x + x' = 0$
- commutative, associative, follows distributive law
- $(K^* = K \setminus \{0\}, \cdot, 1)$ " " a multiplicative identity (inverse)
  $K - \{0\} = \in$
  $\forall y \in K^*, \exists y' \in K^*$ s.t $y \cdot y' = 1$

e.g: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_p$

$\mathbb{F}_p = \mathbb{Z}/p.\mathbb{Z} = \{0, 1, \cdots, p-1\}$ → Field of integers modulo a given p where p = prime number

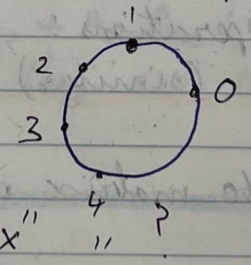
e.g: $F_5 = \{0, 1, 2, 3, 4\}$
$5 \equiv 0$, $6 \equiv 1$, $7 \equiv 2$, $8 \equiv 3$, $9 \equiv 4$

↳ Does every element in $\mathbb{F}_5$ have an "+" inverse?

$2 + 3 = 5 \Leftrightarrow 0$

$1 + 4 = 5 \Leftrightarrow 0$

YES!



↳ " "

1. $\frac{1}{1} = 1$
2. $\frac{3}{3} = 1$
3. $\frac{2}{2} = 1$
4. $\frac{4}{4} = 1$

Q) Does $\mathbb{Z}/6.\mathbb{Z}$ form a field under the natural $(+, \cdot)$?
NO! As $6 = 2.3$ ⇒ not a prime number

If p = prime number, $n \geq 1$ integer, $\exists!$ $\mathbb{F}_{p^n}$ finite field w/ p^n many elements.

quotient ⇓

remove ⇓

x^2+1 → irreducible in $\mathbb{R}$ but reducible in $\mathbb{C}$

Let $f(x) \in \mathbb{F}_p[x]$ w/ variable π w/ coefficient π_p; f is of degree n

[e.g. $p=5 \Rightarrow 3x^3+4x-2 \in \mathbb{F}_5[x]$]

Assume $f(x)$ is irreducible in $\mathbb{F}_p[x]$; i.e $f(x) \neq g(x)\,h(x)$ w/ g, h of smaller degree

$\Rightarrow$ $\mathbb{F}_p[x] / (f(x).\mathbb{F}_p[x])$ is a field of size p^n

Eg: $p=5$; $f(x) = x^2+1 = (x-2)(x-3) = x^2-5x+6$

$(=)\ x^2 - 0 + 1 = x^2+1$ ✗ (doesn't work)

$0^2 = 0$
$1^2 = 1$
$2^2 = 4$
$3^2 = 4$ (9-5)
$4^2 = 1$ (16-15)

$\boxed{f(x) = x^2+2}$ ✓

$\Rightarrow$ $\mathbb{F}_{5^2} = \mathbb{F}_5[x]/(x^2+2)$ → declaring that $x^2+2=0$ & $5=0$

size is 5^2 ← $\mathbb{F}_{5^2}$

e.g. $4 \mid x = 4$

TYPICAL ELEMENT: x, 3, x^5+1

(e.g. $\to x^2+3 = (x^2+2)+1 (=) 1$
$x^2 = -2$
$x^3 = x^2 \cdot x = -2x$)

$\mathbb{K} = \mathbb{F}_5[x]/(x^2+2) = \{ax+b \mid a, b \in \mathbb{F}_5\} \cong (\mathbb{F}_5)^2$ as a vector space

Does every non-zero element in $\mathbb{K}$ has inverse under "."?

$x \cdot 2x = 1$ $\quad x \cdot x = -2$ $\quad -2 \cdot 2 = -4 = 1$ $\quad \} = x \cdot 2x = 1$

YES!

represents field of rational no.

$\mathbb{Q}[\sqrt{-1}] \cong \mathbb{Q}[x]/(x^2+1) \simeq \mathbb{Q}^2$ → 2-D linear space

$= \{ax+b \mid a, b \in \mathbb{Q}\}$

short-hand notation of

$(ax+b).(cx+d)$

$= acx^2 + bd + adx + bcx$

$= (-ac+bd) + (bc+ad)x$

[Size of the field is infinity → irrelevant in this example]

VECTOR SPACE

Let $\mathbb{K}$ be a field. A vector space V over $\mathbb{K}$ is a set s.t

1) $(V, +, 0)$ is an abelian group
2) $K \curvearrowright V$ ⇒ scalar product
   ↳ take an element in K that transforms an element in V back to itself

- A function (= map) on a set S, valued in $\mathbb{K}$, is an assignment to each element in S to some element in $\mathbb{K}$
  ⇒ the set of all functions from S to $\mathbb{K}$ is

$$\text{Map}(S, \mathbb{K}) = \mathbb{K}^S$$

e.g → if $S = \{*\}$ (→ 1 point) ; $\mathbb{K}^S = \mathbb{K}$

→ if $S = \{a, b\}$; $\mathbb{K}^S = \mathbb{K}^2$

→ if $S = \emptyset$; $\mathbb{K}^\emptyset = \mathbb{K}^0 = \{pt\}$ → zero-dimensional vector space

If $f, g : \{1, 2\} \to \mathbb{R}$, $f, g \in \text{Map}(\{1, 2\}, \mathbb{K})$

- $(f+g)(x) = f(x) + g(x)$ $\forall$ $x \in \{1, 2\}$ ⇒ map ⇒ $f+g$
- $\forall$ $c \in \mathbb{K}$, $(c.f)(x) = c.f(x)$

★ **Abelian Group** ⇒ a group in which the law of composition is commutative

↳ a set G w/ $m : G \times G \to G$ s.t

$m(m(a,b),c) = m(a, m(b,c))$ & if $\exists$ $e \in G$,

$\{ m(e,a) = a$ & $\forall$ $g \in G$, $\exists g' \in G$ s.t. $m(g,g') = e \}$

identity ; inverse

e.g: $S = \{1, 2, \dots, n\} = [n]$; $\mathbb{K}^S = \mathbb{K}^n$,

$\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \dots$ ⇒ a field

$S = [n] \times [m]$

$= \{(i,j) \mid 1 \le i \le n,\ 1 \le j \le m,\ \text{integers}\}$

$$\mathbb{K}^S = \left\{ \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} \;\middle|\; a_{ij} \in \mathbb{K} \right\}$$

- Let V be a vector space over $\mathbb{K}$. A **subspace** of a vector space satisfies the axioms of a vector space on its own $W \subset V$ is a subset, that is closed under $+$ and $\mathbb{K}$.

e.g: $\mathbb{K} = \mathbb{R}$

⇒ $V = \mathbb{R}^{\mathbb{R}} = \text{Map}(\mathbb{R}, \mathbb{R})$ ⇝ all functions on $\mathbb{R}$

$W = \mathbb{R}[x] = \{a_n x^n + \cdots + a_0 \mid a_i \in \mathbb{R}, n \in \mathbb{Z}_{\ge 0}\}$ polynomials

Upper, lower, block triangular $n \times n$ matrices form subspaces that are closed ⇒ is a vector space

★ every subspace of a $\mathbb{K}$-vector space is an example of a $\mathbb{K}$-vector space ★

CATEGORY THEORY

→ a set of objects

→ morphisms b/w objects

→ composition of morphisms

→ Morphism of a set is a set

→ " " linear space is a lin. spa

MORPHISM

↳ structure-preserving map from 1 mathematical structure to another of the same type

Ex 1: Set : the category of sets

→ objects : any set

→ morphisms : Given S_1, S_2, two sets: $\text{Mor}(S_1, S_2) = \text{Map}(S_1, S_2)$

→ composition : $\text{Mor}(S_1, S_2) \times \text{Mor}(S_2, S_3) \to \text{Mor}(S_1, S_3)$

$f_{12} \cdot f_{23} = f_{23}(f_{12}(\_))$

Ex 2: $\mathrm{Vect}_{\mathbb{K}}$: the category of vector spaces / $\mathbb{K}$

→ object : vector space over $\mathbb{K}$

→ morphism b/w V_1, V_2 is a linear map

$\mathrm{Mor}(V_1, V_2) = \mathrm{LinMap}(V_1, V_2)$

NOTE : the set $\mathrm{LinMap}(V_1, V_2)$ also forms a vector space (Dual Space)

Let $f : V \to W$ be a linear map

(kernal) • $\ker(f) := \{v \in V \mid f(v) = 0\} \subset V$ ⇒ null space of f

(image) • $\mathrm{im}(f) := \{w \in W \mid \exists\, v \in V,\ w = f(v)\} \subset W$ ⇒ range of f

(cokernal) • $\mathrm{coker}(f) = \frac{W}{\mathrm{im}(f)}$

[Linear map conserves linear structure under add" & multi"]

$A(\lambda u + \mu v) = \lambda Au + \mu Av \quad \forall\ \lambda, \mu \in \mathbb{K}$ & $u, v \in V$

→ A linear map is INJECTIVE iff its kernal is trivial ⇒ $\ker(f) = \{0\}$

SURJECTIVE if $\mathrm{range}(f) = W = f(V)$

→ If a linear map is BIJECTIVE, it establishes a 1-1 correspondence b/w V & W in a way that repects vector operation

↳ f establishes an ISOMORPHISM b/w V & W ⇒ $V \cong W$

ISOMORPHISM

↳ structure-preserving mapping b/w 2 structures of the same type that can be reversed by an inverse mapping

↳ missing from 'morphism' definition