Recall: $\mathbb{F}$ field, $(\mathbb{F}, +, \cdot)$

V vector space, $(V, +, \cdot)$

Example:

1. $\mathbb{R}^n$ $\quad (r_1, \dots, r_n) \quad r_i \in \mathbb{R}$ for all i.

   $+$ is componentwise : $(r_1, \dots, r_n) + (s_1, \dots, s_n) = (r_1 + s_1, \dots, s_n + s_n)$.

   $\cdot$ is componentwise : $a \cdot (r_1, \dots, r_n) = (a \cdot r_1, \dots, a \cdot r_n)$

$\mathbb{R}$ is the base field.

$\mathbb{Q}$ can also be the base field.

$\mathbb{C}$ cannot be the base field. $\quad \because \mathbb{C} \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$

$\mathbb{Z}_2 = \{[0], [1]\}$ cannot be the base field.

$(a+b) \cdot x = a \cdot x + b \cdot x$

$x = (1, \dots, 1)$, $a = b = 1$ so LHS: $([1]+[1]) \cdot (1, \dots, 1) = [0] \cdot (1, \dots, 1) =$
$= (0, \dots, 0)$

RHS : $[1] \cdot (1, \dots, 1) + [1] \cdot (1, \dots, 1) =$
$= (1, \dots, 1) + (1, \dots, 1) = (2, \dots, 2)$

Base field: $V \quad + : V \times V \longrightarrow V \quad \cdot : \underbrace{\mathbb{F}}_{\text{base field}} \times V \longrightarrow V$

2. Let S be a set, $\mathbb{F}$ field. The set of functions from S to $\mathbb{F}$ is

2. Let S be a set, $\mathbb{F}$ field. The set of functions from S to $\mathbb{F}$ is

a vector space over $\mathbb{F}$.

$$\underbrace{\mathcal{F}(S,\mathbb{F})}_{V} = \{ f : S \to \mathbb{F} \mid f \text{ function} \}.$$

$+ :\quad f, g \qquad (f+g)(x) = f(x) + g(x) \qquad x \in S$

$\cdot :\quad \underset{\mathbb{F}}{\overset{}{a}}\,\rotatebox{90}{$\in$}, \ f \in V \qquad (a\cdot f)(x) = a \cdot f(x) \qquad a \cdot f : S \longrightarrow \mathbb{F}$

$$x \longmapsto a\cdot f(x)$$

2.1. $\mathcal{C}(\mathbb{R})$

2.2. $\mathbb{F}[x]$

2.3. Symmetric polynomials: polynomials in n variables such that exchanging two variables gives the same polynomial.

$\underline{n=3}$:

$p(x_1, x_2, x_3) = x_1 x_2 x_3$ is symmetric

$p(x_2, x_1, x_3) = x_2 x_1 x_3 = x_1 x_2 x_3$

$q(x_1, x_2, x_3) = x_1 + x_2 + x_3$ is symmetric

$q(x_3, x_2, x_1) = x_3 + x_2 + x_1 = x_1 + x_2 + x_3$

$r(x_1, x_2, x_3) = x_1 x_2 + x_3$ is $\underline{\text{not}}$ symmetric.

$r(x_1, x_2, x_3) = x_3 x_2 + x_1$

3. Matrices $M_{m\times n}(\mathbb{F})$

rows columns

$$\begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} + \begin{bmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nm} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & \cdots & a_{1m}+b_{1m} \\ \vdots & & \vdots \\ a_{n1}+b_{n1} & \cdots & a_{nm}+b_{nm} \end{bmatrix}$$

$$c \cdot \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} = \begin{bmatrix} c \cdot a_{11} & \cdots & c \cdot a_{1m} \\ \vdots & & \vdots \\ c \cdot a_{n1} & \cdots & c \cdot a_{nm} \end{bmatrix}$$

Question: Are matrices a field?

A B

$n \times m$ $p \times q$

$\cdot : M_{n\times n}(\mathbb{F}) \times M_{n\times n}(\mathbb{F}) \longrightarrow M_{n\times n}(\mathbb{F})$

$\cdot : \mathrm{Inv}M_{n\times n}(\mathbb{F}) \times \mathrm{Inv}M_{n\times n}(\mathbb{F}) \longrightarrow \mathrm{Inv}M_{n\times n}(\mathbb{F})$

Multiplication does not commute!

4. $\mathbb{F}(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p, q \in \mathbb{F}[x] \right\}.$ rational field

$$+ : \quad \frac{p(x)}{q(x)} + \frac{r(x)}{s(x)} = \frac{p(x)s(x) + q(x)r(x)}{q(x)s(x)}$$

$$\cdot : \quad \frac{p(x)}{q(x)} \cdot \frac{r(x)}{s(x)} = \frac{p(x)\cdot r(x)}{q(x)\cdot s(x)}$$

$\mathbb{F}(x)$ is a field

$\mathbb{F}(x)$ is a vector space over $\mathbb{F}$.

* Proof techniques

1. Induction: useful is something needs to be true for all $\mathbb{N}$.

Prove the statement for $n=0$ or 1.

Suppose the statement is true for $n-1$.

Prove that the statement is true for n.

Example: $\sum_{i=1}^{n} i = \frac{n\cdot(n+1)}{2}$.

$n=1$: $1 = \frac{1\cdot(1+1)}{2}$

Suppose true for $n-1$.

n: $\sum_{i=1}^{n} i = \left(\sum_{i=1}^{n-1} i\right) + n = \frac{(n-1)((n-1)+1)}{2} + n = \dots = \frac{n(n+1)}{2}$

2. By definition.

3. Using big theorems or results.

Example: Prove that every $p(x) \in \mathbb{C}[x]$ factors into linear terms.

4. Follow your nose.

Example: $\sqrt{2} \notin \mathbb{Q}$

Suppose $\sqrt{2} \in \mathbb{Q}$. $\sqrt{2} = \frac{a}{b}$, $a,b \in \mathbb{Z}$.

$2 = \frac{a^2}{b^2}$ $\quad 2b^2 = a^2$ so a^2 is even.

So a is even. So $a = 2k$ for some $k \in \mathbb{Z}$.

$2b^2 = (2k)^2 = 4k^2$ $\quad b^2 = 2k^2$ $\rightsquigarrow$ so b is even.

Let $\sqrt{2} = \frac{p}{q}$ the irreducible expression of $\sqrt{2}$ in $\mathbb{Q}$. So

$\gcd(p,q) = 1$. However, we proved that 2 divides both p and q.

Contradiction. So $\sqrt{2} \notin \mathbb{Q}$.