Fields ($\mathbb{F}$)

- Infinite: $|\mathbb{F}| = \infty$
- finite: $|\mathbb{F}| < \infty$

Examples:

$\mathbb{F} = \mathbb{Q}$

$\mathbb{R}$

$\mathbb{C} = \{a+ib \mid a,b \in \mathbb{R}\}$

$\mathbb{Q}[i] = \{a+ib \mid a,b \in \mathbb{Q}\}$

$\mathbb{Q}^2 = \mathbb{Q} \times \mathbb{Q}$

$\mathrm{chr}(\mathbb{Q}) = \mathrm{chr}(\mathbb{R}) = \mathrm{chr}(\mathbb{C}) = 0$

Examples:

$\mathbb{F} = \mathbb{F}_q = GF(q)$

$|\mathbb{F}_q| = q$ $\quad q = p^s$

For $s=1$

$GF(q) = GF(p) = \mathbb{Z}_p = \{0,1,2,\dots,p-1\}$ $+_p \cdot_p$

$\mathrm{Char}(GF(q)) = p$

To construct a field with p^m elements you need a root of an equation of degree m which has no solution on $\mathbb{Z}_p = GF(p)$

Tower of finite fields

$p=2$
$GF(2^3)$
⋮
$GF(2^4)$
|
$GF(2^3)$
|
$GF(2^2)$
|
$GF(2) = \mathbb{Z}_2$

$GF(p^3)$ ⋮ $GF(p^4)$ \| $GF(p^3)$ \| $GF(p^2)$ \| $GF(p) \overset{*}{=} \mathbb{Z}_p$

$\{a+\omega b \mid a,b \in \mathbb{Z}_p\} =$ $GF(p^2)$

s.t. $f(\omega) = 0$, $\deg f = 2$, and f has no root in $\mathbb{Z}_p$

— A field with q number of elements exist iff $q = p^s$ (some prime power)

Rings (R)

Infinite $|R| = \infty$ | finite $|R| < \infty$

Examples:

$R = \mathbb{Z}$

$2, 3, 5, 7, 11, \ldots$ primes in $\mathbb{Z}$

$R = \mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$

What are the primes in $\mathbb{Z}[i]$?

Gaussian primes

↓

Ring of Gaussian integers

Note 2 is not a prime in $\mathbb{Z}[i]$

$\because \quad 2 = (1+i)(1-i) = 2+0i \in \mathbb{Z}[i]$

$\mathbb{Z}[\sqrt{n}] = \{a + \sqrt{n}\, b \mid a, b \in \mathbb{Z}\}$

$\mathbb{Z}[i\sqrt{n}] = \{a + i\sqrt{n}\, b \mid a, b \in \mathbb{Z}\}$

$\mathbb{Z}[\sqrt{3}] = \{a + \sqrt{3}\, b \mid a, b \in \mathbb{Z}\}$

Units of $\mathbb{Z}$ are $\{1, -1\}$

Examples:

$R =$

$\mathbb{Z}_4$ ✓

$\mathbb{Z}_6$

$\mathbb{Z}_8$

⋮

$\mathbb{Z}_{2^3}$

⋮

$\mathbb{Z}_m$ s.t. $m \neq$ prime

$\mathbb{Z}_{p^s}$

p – prime

$s > 0$ integer

$\mathbb{Z}_{p^s} = \{0, 1, 2, 3, \ldots, p^s - 1\}$

For any prime p and s a +ve integer

Set of all zero divisors of $\mathbb{Z}_{p^s}$

$Z(\mathbb{Z}_{p^s}) = \{ap \mid 0 \leq a \leq p^{s-1} - 1\}$

$= \{0, p, 2p, 3p, 4p, \ldots, (p^{s-1}-2)p, (p^{s-1}-1)p\}$

$\Rightarrow |Z(\mathbb{Z}_{p^s})| = p^{s-1}$

Set of all units of $\mathbb{Z}_{p^s}$

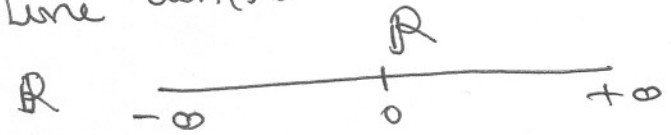
$U(\mathbb{Z}_{p^s}) = \{ap + b \mid 0 \leq a \leq p^{s-1} - 1,\ 1 \leq b \leq p-1\}$

$= \{1, p+1, 2p+1, \ldots, (p^{s-1}-1)p+1;\ ?, p+2, \ldots, (p^{s-1}-1)p+2, \ldots, (p^{s-1}-1)p + (p-1)\ ?\}$

$|U(\mathbb{Z}_{p^s})| = (p-1)p^{s-1}$

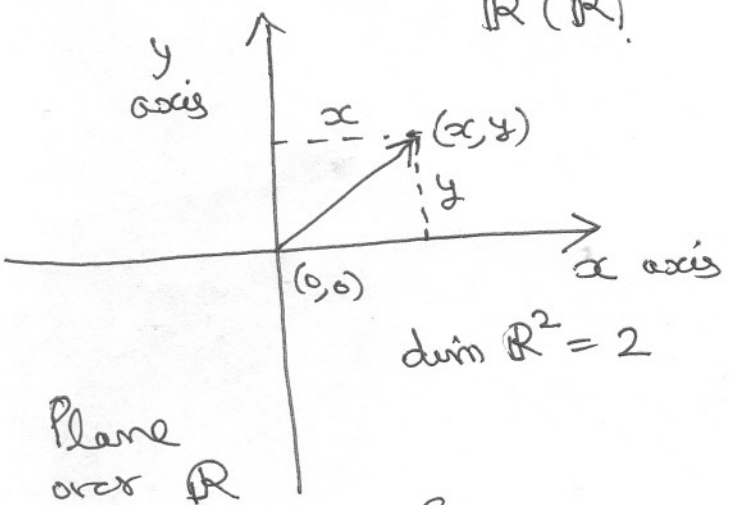
$\mathbb{R}(\mathbb{R})$ Vector space over a field

Line $\dim(\mathbb{R})=1$



$\mathbb{R}^2 = \mathbb{R}\times\mathbb{R} = \{(x,y) \mid x,y \in \mathbb{R}\}$

$\mathbb{R}^2(\mathbb{R})$

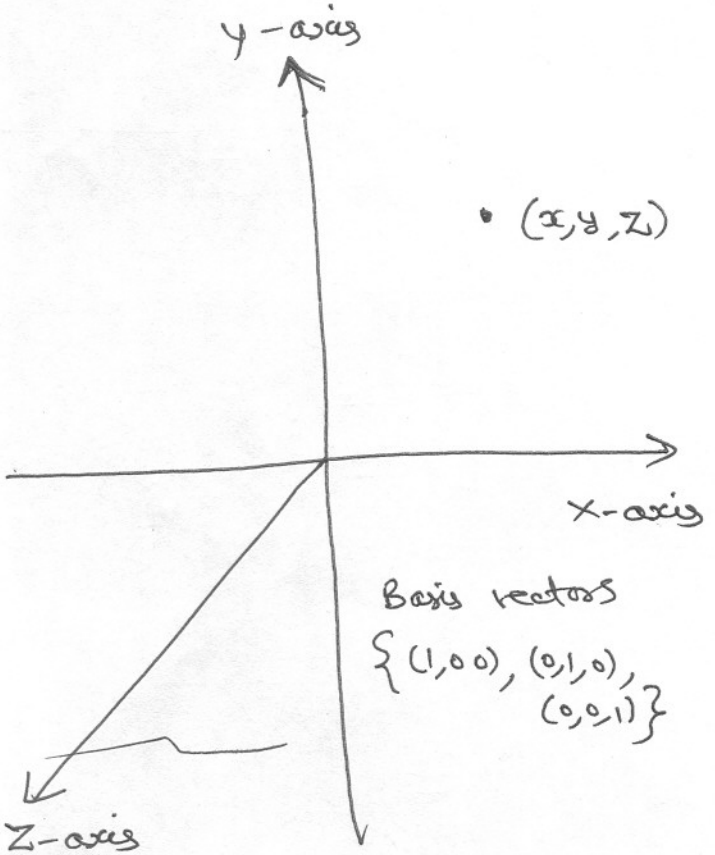


$\dim \mathbb{R}^2 = 2$

Plane over $\mathbb{R}$

$\mathbb{R}^3(\mathbb{R})$ $\dim \mathbb{R}^3 = 3$

$\mathbb{R}^3 = \mathbb{R}\times\mathbb{R}\times\mathbb{R} = \{(x,y,z) \mid x,y,z \in \mathbb{R}\}$



3-dimal vector space over $\mathbb{R}$

Line

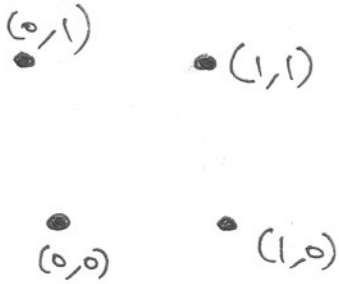
$\mathbb{Z}_2$

$\dim(\mathbb{Z}_2) = 1$

$\mathbb{Z}_2^2(\mathbb{Z}_2)$

$\mathbb{Z}_2^2 = \{(x,y) \mid x,y \in \mathbb{Z}_2\}$

$\dim \mathbb{Z}_2^2 = 2$

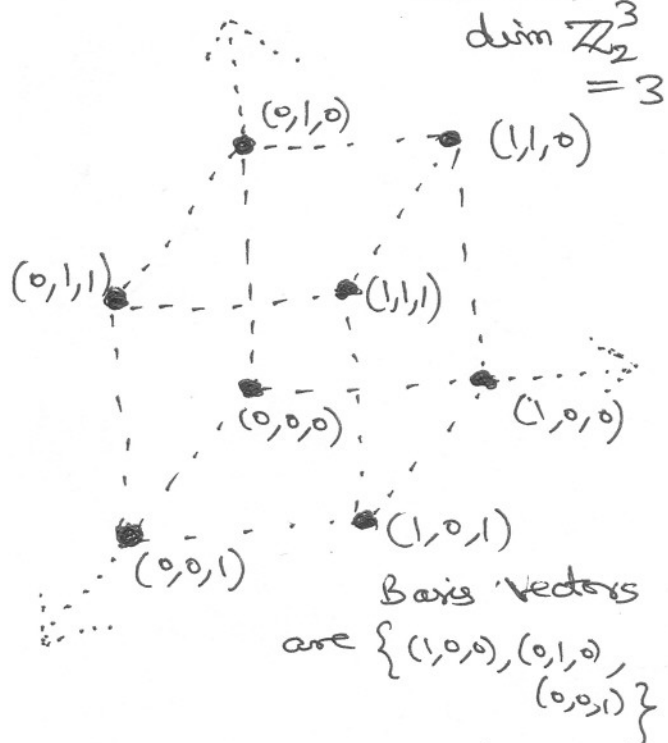


Plane over $\mathbb{Z}_2$

$\mathbb{Z}_2^3 = \{(x,y,z) \mid x,y,z \in \mathbb{Z}_2\}$

$\mathbb{Z}_2^3(\mathbb{Z}_2)$

$\dim \mathbb{Z}_2^3 = 3$



3-dimal vector space over $\mathbb{Z}_2$

Interesting Observations

$\mathbb{R}^2$

$(x,y) = x(1,0) + y(0,1) \in \mathbb{R}^2$

$\forall\ x, y \in \mathbb{R}$

$\mathbb{R}^3$

$(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1) \in \mathbb{R}^3$

$\forall x, y, z \in \mathbb{R}$

$\vdots$

$\mathbb{R}^n$ $\quad \dim \mathbb{R}^n(\mathbb{R}) = n$

$\mathbb{R}^1$

$x \in \mathbb{R}$ ~~$x = x \cdot 1$~~ $\neq 0$

$\mathbb{Z}_2^2$

$(x,y) = x(1,0) + y(0,1) \in \mathbb{Z}_2^2$

$\forall\ x, y \in \mathbb{Z}_2$

$\mathbb{Z}_2^3$

$(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1) \in \mathbb{Z}_2^3$

$\forall\ x, y, z \in \mathbb{Z}_2$

$\vdots$

$\mathbb{Z}_2^n$ $\quad \dim \mathbb{Z}_2^n(\mathbb{Z}_2) = n$

$\mathbb{Z}_2^1 = \langle\ \rangle$

---

① These are l.i. $\forall$ vectors $v \in V$ $v = \sum_{i=1}^{n} \lambda_i v_i$ scalars $\lambda_i \in \mathbb{F}$ are unique

② They are l.i. (Example: $(x,y) = x(1,0) + y(0,1)$

If $\sum_{i=1}^{n} \mu_i v_i = 0 \Rightarrow$ each $\forall\ \mu_i \in \mathbb{F}$ $\mu_i = 0$

then the set of vectors

$B \equiv \{v_1, v_2, \ldots, v_n\}$ are called l.i.

If $\alpha(1,0) + \beta(0,1) = 0$

$\Rightarrow (\alpha, \beta) = 0$

$\Rightarrow \alpha = 0, \beta = 0.$)

We call such a set Basis of a vector space

$V(\mathbb{F})$ B is a basis of $V(\mathbb{F})$

and $|B| = n$ $= \dim V(\mathbb{F})$

$\mathbb{R}^2$: $B = \{(1,0), (0,1)\}$

$\mathbb{R}^3$: $B = \{(1,0,0), (0,1,0), (0,0,1)\}$

$\mathbb{R}$: $B = \{1\}$ Infact $\forall\ \alpha \neq 0$

$\mathbb{Z}_2^2$: $B = \{(1,0), (0,1)\}$

$\mathbb{Z}_2^3$: $B = \{(1,0,0), (0,1,0), (0,0,1)\}$

$\mathbb{Z}_2$: $B = \{1\}$

We also write as

$$\mathbb{R}^2 = \langle (1,0), (0,1) \rangle$$

$$\mathbb{R}^3 = \langle (1,0,0), (0,1,0), (0,0,1) \rangle$$

etc.

$$\mathbb{Z}_2^2 = \langle (1,0), (0,1) \rangle_2$$

2-l.c. means l.c. over $\mathbb{Z}_2$

$$\mathbb{Z}_2 = \langle 1 \rangle_2 = \{0, 1\}$$

Subspaces

$$\mathbb{R}^1 \leq \mathbb{R}^2 \leq \mathbb{R}^3 \leq \mathbb{R}^4 \leq \cdots \leq \mathbb{R}^{n-1} \leq \mathbb{R}^n$$

$$\mathbb{Z}_2^1 \leq \mathbb{Z}_2^2 \leq \mathbb{Z}_2^3 \leq \mathbb{Z}_2^4 \leq \cdots \leq \mathbb{Z}_2^{n-1} \leq \mathbb{Z}_2^n$$

Linear Algebra: Study of linear transformations between vector spaces over some field.

Why Linear Algebra?

- Many Eng. problems give rise to the following sys. of equations:

$$Ax = b$$

Solve for x?

$$\underset{n \times n}{\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}} \underset{n \times 1}{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}} = \underset{n \times 1}{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}}$$