Objectives

1. Define a field
2. Give examples of vector spaces over fields.

<u>Previously</u>:

$\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^n$, $\{$polynomials over $\mathbb{R}\}$, $+$, $\cdot$

operations '+' and '·' looked pretty similar.

<u>ex</u>. $(f+g)(x) = f(x) \underbrace{+}_{\text{addition in } \mathbb{R}} g(x)$

<u>Today</u> Vector spaces with more general operations.

Q Is $\mathbb{R}_+ \underbrace{:=}_{\text{defined to be}} \underbrace{\{}_{\text{the set of}}\, x \overset{\text{in}}{\in} \mathbb{R} \underbrace{\,|\,}_{\text{such that}} x \geq 0 \}$ a vector space?

No.

ex. $-x \underbrace{\notin}_{\text{not in}} \mathbb{R}_+ \rightsquigarrow$ no additive inverse.

Check "well-definedness" first (my personal rule of thumb)

Is $c \cdot x \in \mathbb{R}_+ \ \forall\, c \in \mathbb{R}$ and $x \in \mathbb{R}_+$?

no if $c < 0$ then $c \cdot x < 0$.

$\boxed{Q}$ Are there different definitions of '+' and '·' that could make $\mathbb{R}_+$ into a vector space?

$$\mathbb{R}_+ \xrightarrow{\log} \mathbb{R}$$

So define: $x + y$ by

$$\log^{-1}\left[\log(x) + \log(y)\right]$$

Define

$$x + y = x \cdot y$$

$$c \cdot x = x^c$$

Let's check some vector space properties:

1. $x + y := xy = yx =: y + x$ ✓

2. Additive identity? $1 + x := 1x = x$ ✓

3. Additive inverse? $\frac{1}{x} + x := \frac{1}{x}x = 1$ ✓

4. $1 \cdot x = x$? $1 \cdot x := x^1 = x$.

Q/ Why does 'c' have to be in $\mathbb{R}$?

A/ No reason. We can replace $\mathbb{R}$ by any <u>field</u>.

<u>Defn</u>. A field $\mathcal{F}$ is a set with operations $+, \cdot$ satisfying

$\forall x, y \in \mathcal{F}$, $x + y \in \mathcal{F}$ and $x \cdot y \in \mathcal{F}$

① $\forall a, b, c \in \mathcal{F}$, $\left.\begin{aligned} a + (b + c) &= (a + b) + c \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \end{aligned}\right\}$ associativity

② $\forall a, b \in \mathcal{F}$, $a + b = b + a$ and $a \cdot b = b \cdot a$ } commutativity

③ $\exists\ 0, 1 \in \mathcal{F}$ $\underbrace{\text{s.t.}}_{\text{such that}}$ $\forall a \in \mathcal{F}$, $0 + a = a$ and $1 \cdot a = a$

④ $\forall a \in \mathcal{F}$ $\exists -a \in \mathcal{F}$ s.t. $a + (-a) = 0$

⑤ $\forall a \in \mathcal{F} \wedge a \neq 0$ $\exists\ a^{-1} \in \mathcal{F}$ s.t. $a \cdot a^{-1} = 1$

6) $\forall\, a,b,c \in \mathbb{F}$ $\quad a\cdot(b+c) \underbrace{=}_{\text{distributivity}} a\cdot b + a\cdot c$

Examples of fields

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$

for some people, this is always assumed. Let me know if you want me to make slides.

Examples of non-fields

$\mathbb{Z}$, $\mathbb{N}$

no additive inverses

no multiplicative inverses.

② Adjoining elements

ex. $\mathbb{Q}(\sqrt{2}) := \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$

w/ addition and multiplication inherited

from $\mathbb{R}$.

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) =$$

$$a \cdot c + a \cdot d\sqrt{2} + c \cdot b\sqrt{2} + d \cdot b \cdot 2.$$

the multiplicative inverse of $\sqrt{2}$ is

$\frac{1}{2} \cdot \sqrt{2}$.

ex. $\mathbb{R}(i) = \mathbb{C}$.

③ Finite fields

i) $\mathbb{Z}_2 := \{0, 1\}$

$$0 + 0 = 0 \qquad 0 \cdot 0 = 0$$

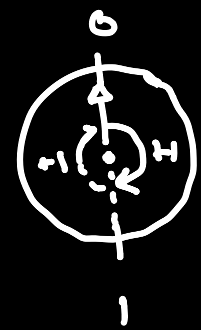
additive identity

$$0 + 1 = 1 \qquad 0 \cdot 1 = 0$$

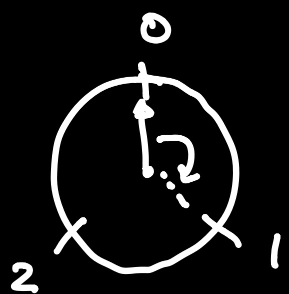
$$1 + 1 = 0 \qquad 1 \cdot 1 = 1$$

mult. identity

"modular arithmetic"



ii) $\mathbb{Z}_3 := \{0, 1, 2\}, +, \cdot$



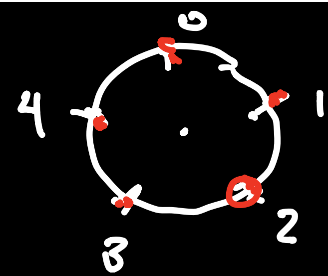
$$1 + 1 = 2 \qquad 0 \cdot 1 = 0$$

$$1 + 2 = 0 \qquad 2 \cdot 1 = 2$$

$$2 + 2 = 1 \qquad 2 \cdot 2 = 1$$

add 2 twice

iii) $\mathbb{Z}/5\mathbb{Z} := \{0, 1, 2, 3, 4\}, +, \cdot$



$$3 \cdot 4 = 3 + 3 + 3 + 3 = 2$$

Alternatively, write $3 \cdot 4 \equiv 12 \bmod 5$

is congruent to

Note $12 = (2 \cdot 5) + 2$

iv) $\mathbb{Z}/p\mathbb{Z}$, for any prime p.

Note. $\mathbb{Z}/4\mathbb{Z}$ is not a field ... '2' has no multiplicative inverse.

$2 \cdot 0 = 0$
$2 \cdot 1 = 2$
$2 \cdot 2 = 0$
$2 \cdot 3 = 2$

A vector space V over F is a set with operations $+$, $\cdot$ so that

$\forall$ $v_1, v_2 \in V$ and $\forall$ $c \in F$

$v_1 + v_2 \in V$ and

$c \cdot v_1 \in V$ and

the 8 properties that we saw for v.s. over $\mathbb{R}$ hold, with c now living in F.

Examples

$\mathbb{Q}^n$, $\mathbb{C}^n$, $\underbrace{\mathbb{Z}_p^n}_{\text{very cool.}}$

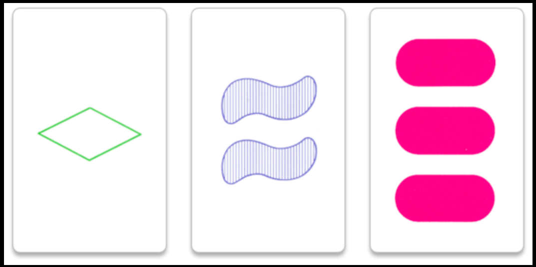
e.g. Binary codes:

$$\left\{\begin{array}{c} \overset{\text{elements}}{001000} \\ 011010 \\ 011100 \\ 100000 \end{array}\right\} \quad \mathbb{Z}_2^6$$

e.g. the game of Set.

A set consists of three cards satisfying all of these conditions:

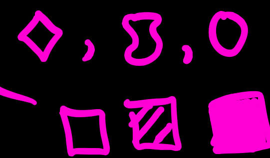
They all have the same number or have three different numbers. 1, 2, 3
They all have the same shape or have three different shapes.
They all have the same shading or have three different shadings.
They all have the same color or have three different colors.

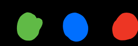


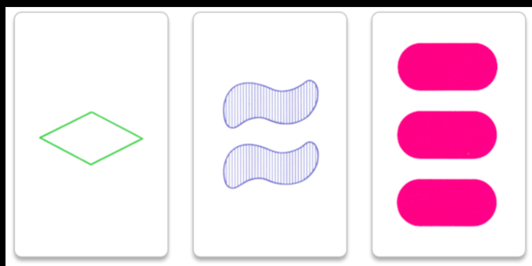
e.g. the game of Set.

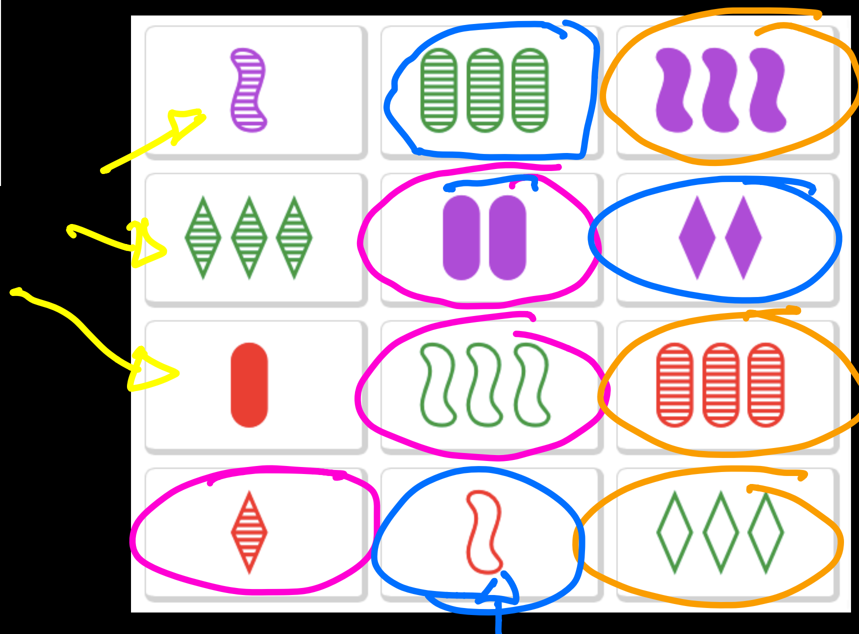
A set consists of three cards satisfying all of these conditions:

They all have the same number or have three different numbers. — 1, 2, 3
They all have the same shape or have three different shapes.
They all have the same shading or have three different shadings.
They all have the same color or have three different colors.









e.g. the game of Set.

A set consists of three cards satisfying all of these conditions:

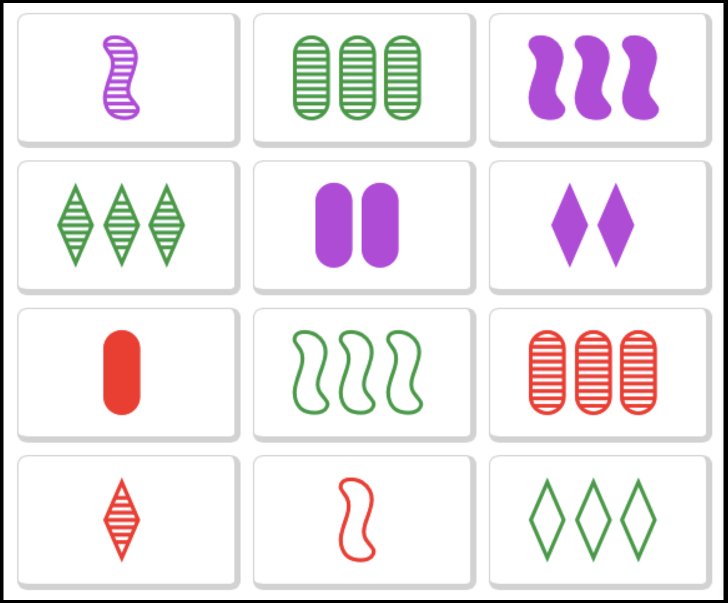
They all have the same number or have three different numbers. — 1, 2, 3
They all have the same shape or have three different shapes.
They all have the same shading or have three different shadings.
They all have the same color or have three different colors.

Described by 4 characteristics.

$\rightsquigarrow$ 4-dim. vector space (?)

Each characteristic can take 3 different values

$\rightsquigarrow$ $(\mathbb{Z}/3\mathbb{Z})^4$



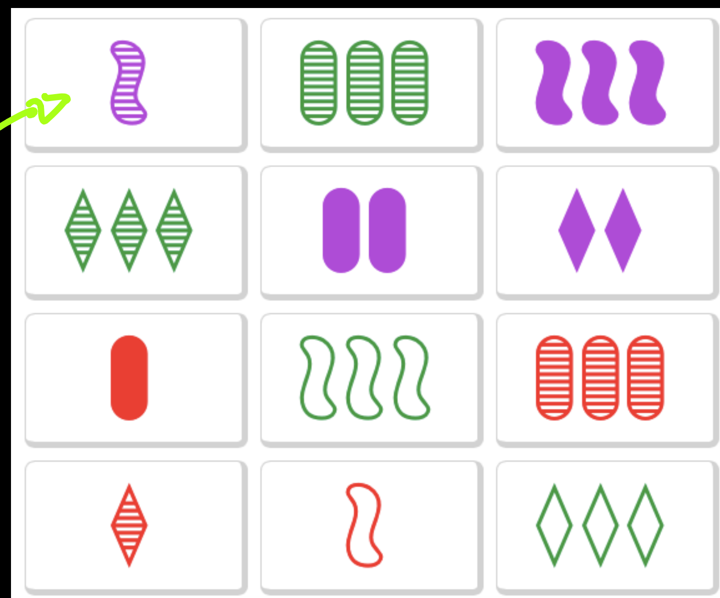
e.g. the game of Set.

A set consists of three cards satisfying all of these conditions:

They all have the same number or have three different numbers.
They all have the same shape or have three different shapes.
They all have the same shading or have three different shadings.
They all have the same color or have three different colors.

0	1	2
one^0	two^1	three^2
^{0}	^{1}	^{2}
^{0}	^{1}	^{2}
^{0}	^{1}	^{2}

What does it mean to get a Set?



If they all have the same number.

$$\begin{bmatrix}0\\2\\1\\1\end{bmatrix}$$

$$\begin{bmatrix}0\\1\end{bmatrix}+\begin{bmatrix}0\\1\end{bmatrix}+\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}$$

$$\begin{bmatrix}1\\1\end{bmatrix}+\begin{bmatrix}1\\1\end{bmatrix}+\begin{bmatrix}1\\1\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}$$

Terry Tao: "Perhaps my favorite open question is the problem on the maximal size of a cap set."

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

a <u>set</u> is 3 cards that sum to $\vec{0}$ when I view them as points in $(\mathbb{Z}_3)^4$.

https://www.wired.com/2016/06/simple-proof-card-game-set-stuns-mathematicians/