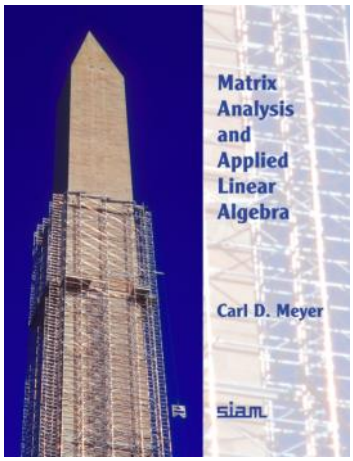
Lecture 5: Vector spaces

Admin: Reading:



VECTOR SPACES

Why? They're everywhere!

$\mathbb{R}^4$ (a,b,c,d)

cubic polynomials ax^3+bx^2+cx+d

2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

multilinear polynomials in x and y $axy+bx+cy+d$

⋮

So it makes sense to abstract their properties and study them together.

And, the best way to understand **matrices** is as linear transformations on vector spaces.

Main properties: "LINEARITY"

Addition: $(a,b,c,d)+(e,f,g,h)$
$=(a+e, b+f, c+g, d+h)$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$(ax^3+bx^2+cx+d)+(ex^3+fx^2+gx+h) = \cdots$$

Scalar multiplication:

$$5(a,b,c,d) = (5a,5b,5c,5d)$$

$$5\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 5a & 5b \\ 5c & 5d \end{pmatrix}$$

$$5(ax^3+bx^2+cx+d) = \cdots$$

These all behave the same way!

Note: Only under scalar multiplication, not arbitrary multiplication.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

$$(ax^3+bx^2+cx+d)(ex^3+fx^2+gx+h)$$
$$aex^6+(af+be)x^5+\cdots$$

$(a,b,c,d)(e,f,g,h)$ is not defined!
(there's just the dot product $ae+bf+cg+dh$)

Definition: A **vector space** consists of

- a set of "vectors" V
- a field $\mathbb{F}$ (often the reals $\mathbb{R}$ or complex #s $\mathbb{C}$)
- operations of
  - vector addition $V \times V \to V$, denoted $\vec{x}+\vec{y}$
  - scalar multiplication $\mathbb{F} \times V \to V$, denoted $\alpha\vec{x}$

that satisfy:

- **closure** under addition & scalar multiplication:
  for all $\alpha \in \mathbb{F}$ $\quad \vec{x}+\vec{y} \in V$

- closure under addition & scalar multiplication:

for all $\alpha \in \mathbb{F}$, $\vec{x}, \vec{y} \in V$

$$\vec{x} + \vec{y} \in V$$
$$\alpha \vec{x} \in V$$

- existence of $\vec{0} \in V$
  $\vec{0} + \vec{x} = \vec{x}$ for all $\vec{x}$
- additive inverses
  for all $\vec{x} \in V$, there exists $\vec{y} \in V$
  s.t. $\vec{x} + \vec{y} = \vec{0}$

for all $\alpha, \beta \in \mathbb{F}$, $\vec{x}, \vec{y}, \vec{z} \in V$:

- commutativity: $\vec{x} + \vec{y} = \vec{y} + \vec{x}$
- associativity: $\vec{x} + (\vec{y} + \vec{z}) = (\vec{x} + \vec{y}) + \vec{z}$, $\alpha(\beta \vec{x}) = (\alpha\beta)\vec{x}$
- distributivity: $(\alpha + \beta)\vec{x} = \alpha\vec{x} + \beta\vec{x}$, $\alpha(\vec{x} + \vec{y}) = \alpha\vec{x} + \alpha\vec{y}$
- $1\vec{x} = \vec{x}$ (identity for multiplication)

Note: The most important properties to check are closure under addition and scalar multiplication. The other properties are usually automatic.

Examples: Vector spaces are everywhere!

1. $\mathbb{R}^n$: real vectors $(x_1, x_2, \ldots, x_n)$
   coordinate-wise addition & multiplication
2. $\mathbb{C}^n$
   matrices $\mathbb{R}^{m \times n}$ or $\mathbb{C}^{m \times n}$
3. the single-point sets $\{0\}$ or $\{(0, 0, \ldots, 0)\}$
   (trivially closed under addition & multiplication)

But these are NOT vector spaces:

$\{1\}$, $\{(1, 0, 0)\}$
$\{(0,0), (1,0)\}$
the interval $[0, 1]$

④ function spaces, eg.,
all functions $\mathbb{R} \to \mathbb{R}$
all functions $[0,1] \to \mathbb{R}$

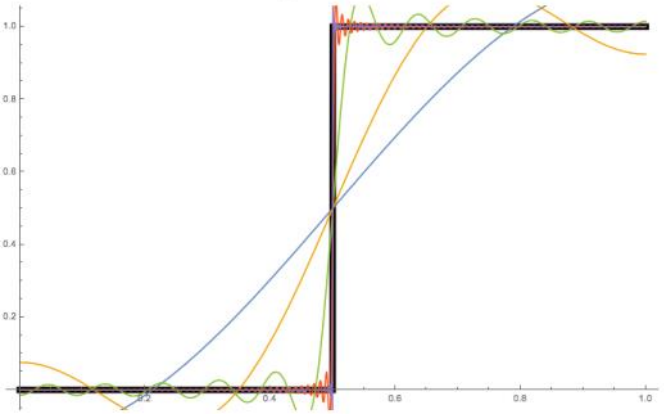
addition $(f+g)(x) = f(x) + g(x)$
multiplication $(cf)(x) = c \cdot f(x)$

Successive Fourier approximations to the step function

```
Table[1/2 - 2/π Sum[(-1)^k/(2 k + 1) Cos[(2 k + 1) π x], {k, 0, kmax}], {kmax, -1, 3}] // Expand // TableForm
```

```
TableForm=
1/2
1/2 - 2 Cos[π x]/π
1/2 - 2 Cos[π x]/π + 2 Cos[3 π x]/(3 π)
1/2 - 2 Cos[π x]/π + 2 Cos[3 π x]/(3 π) - 2 Cos[5 π x]/(5 π)
1/2 - 2 Cos[π x]/π + 2 Cos[3 π x]/(3 π) - 2 Cos[5 π x]/(5 π) + 2 Cos[7 π x]/(7 π)
```

```
step = Plot[If[x < 1/2, 0, 1], {x, 0, 1}, PlotStyle → {Black, Thickness[.01]}];
Show[step, Plot[Evaluate@Table[1/2 - 2/π Sum[(-1)^k/(2 k + 1) Cos[(2 k + 1) π x], {k, 0, kmax}], {kmax, {0, 1, 10, 100, 1000}}], {x, 0, 1}]]
```



Subspaces!

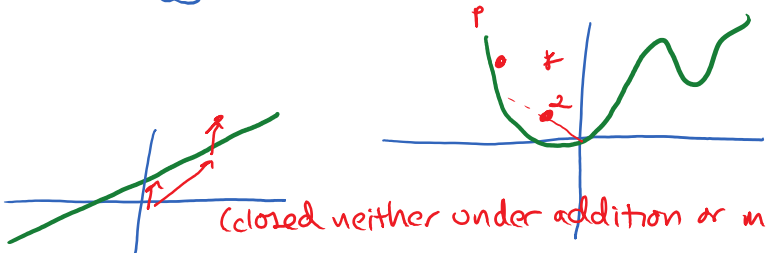
⑤ $\{(x, 2x) : x \in \mathbb{R}\}$
includes $(0,0)$, closed under $+$, $\times$ ✓

ALL subspaces of $\mathbb{R}^2$:

$\{0\}$, lines through 0 $\{(x,y) : ax+by=0\}$, $\mathbb{R}^2$ itself

NOT subspaces:
other lines:

curves:



(closed neither under addition or multiplication!)

Important: Lines/planes/hyperplanes that don't

go through the origin (0) are NOT subspaces!!

③ The SPAN of any (finite or infinite) set of points S

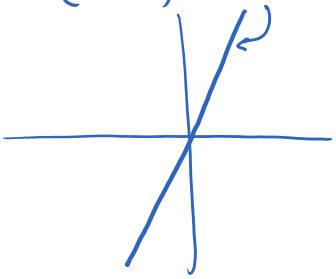
> Span(S) is defined to be the set of all finite linear combinations of elements from S

ie., all sums $\alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2 + \cdots + \alpha_r \vec{v}_r$
for scalars α_j and $\vec{v}_j \in S$

By definition, this is closed under $+, \cdot$, and hence is a vector space.

Examples: What are:

- Span$\{(1,2)\}$ = the line $\{(x,2x) \mid x \in \mathbb{R}\}$



- Span$\{(1,2),(-1,-2)\}$ = the same line

- Span$\{(0,1),(1,0)\}$ = the plane $\mathbb{R}^2$

- Span$\{1, x, x^2, x^3, \ldots\}$ = all polynomials

Note: The infinite sum $\sum_{i=0}^{\infty} x^i$ is not in this span.

- Span$\left\{\begin{matrix}(1,0,0),\\(0,0,1),\\(1,0,1)\end{matrix}\right\}$ = the xz-plane in $\mathbb{R}^3$

(since $\begin{pmatrix}1\\0\\1\end{pmatrix} = \begin{pmatrix}1\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\1\end{pmatrix}$, it doesn't increase the span)

- Span$\left\{\begin{matrix}(1,2,1,1,5),\\(-2,-4,0,4,-2),\\(1,2,2,4,9)\end{matrix}\right\}$

- Span $\left\{ \begin{matrix} (-2,-4,0,4,-2), \\ (1,2,2,4,9) \end{matrix} \right\}$

-this is a subspace of $\mathbb{R}^5$ — it must be either a line, a plane, or a 3D hyperplane

Two approaches to find out:

① Add vectors one at a time

Span$\{(1,2,1,1,5)\}$ is a line.

Does $(-2,-4,0,4,-2)$ give something new, or is it already in that line?

—something new, since it is not a multiple of $(1,2,1,1,5)$

Does $(1,2,2,4,9)$ give something new, or is it already in the plane Span$\left\{ \begin{matrix} (1,2,1,1,5), \\ (-2,-4,0,4,-2) \end{matrix} \right\}$?

It lies in the plane $\iff$ there is a solution to

$$(1,2,2,4,9) = (1,2,1,1,5)x + (-2,-4,0,4,-2)y$$

$$\iff \begin{pmatrix} 1 & -2 \\ 2 & -4 \\ 1 & 0 \\ 1 & 4 \\ 5 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 2 \\ 4 \\ 9 \end{pmatrix} \text{ has a solution}$$

There is a solution: $(x,y) = (2, \frac{1}{2})$

Therefore the span is the 2D plane Span$\left\{ \begin{matrix} (1,2,1,1,5), \\ (-2,-4,0,4,-2) \end{matrix} \right\}$. ✓

② Start with all the vectors, and try to simplify them

This is what Gaussian elimination does:

Let $M = \begin{pmatrix} 1 & 2 & 1 & 1 & 5 \\ -2 & -4 & 0 & 4 & -2 \\ 1 & 2 & 2 & 4 & 9 \end{pmatrix}$ $\begin{matrix} \\ +2 \\ -1 \end{matrix}$

$$M \xrightarrow{GE} \begin{pmatrix} 1 & 2 & 1 & 1 & 5 \\ 0 & 0 & 2 & 6 & 8 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \begin{matrix} \\ \\ -\frac{1}{2} \end{matrix} \xrightarrow{GE} \begin{pmatrix} 1 & 2 & 1 & 1 & 5 \\ 0 & 0 & 1 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} \\ -1 \\ \\ \end{matrix}$$

$$\begin{pmatrix} 0 & 0 & 2 & 6 & 8 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \xrightarrow{\cdot(-1/2)} \begin{pmatrix} 0 & 0 & 1 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\xrightarrow{GE} \begin{pmatrix} 1 & 2 & 0 & -2 & 1 \\ 0 & 0 & 1 & 3 & 4 \\ 0 & 0 & & 0 & 0 \end{pmatrix}$$

Note: Adding a multiple of one row to another does not change the span of the rows.

$$\text{Span}\{\vec{v}_1, \vec{v}_2, \vec{v}_3, \dots\} = \text{Span}\{\vec{v}_1, \underbrace{\vec{v}_2 + \beta\vec{v}_1}_{\vec{v}_2''}, \vec{v}_3, \dots\}$$

since anything you can reach with a linear combination $\alpha_1\vec{v}_1 + \alpha_2\vec{v}_2 + \alpha_3\vec{v}_3 + \cdots$ can also be reached with a linear combination of the new vectors

$$(\alpha_1 - \beta\alpha_2)\vec{v}_1 + \alpha_2(\vec{v}_2 + \beta\vec{v}_1) + \alpha_3\vec{v}_3 + \cdots,$$

and vice versa.

$\Rightarrow$ The nonzero rows left over after Gaussian elimination (are a minimal set of vectors) that span the same set as the original rows.

Claim: Span(S) is the smallest vector space that contains all the points in S.

Proof:

- Let T be a vector space containing all of S.
  Goal: Show $\text{Span}(S) \subseteq T$.
- Let $\vec{v} \in \text{Span}(S)$.
  $\Rightarrow \vec{v} = \alpha_1\vec{v}_1 + \alpha_2\vec{v}_2 + \cdots + \alpha_r\vec{v}_r$, with all $\vec{v}_i \in S$
  $\Rightarrow$ all $\vec{v}_i \in T$
  $\Rightarrow$ all $\alpha_i\vec{v}_i \in T$ (closure under mult.)
  $\Rightarrow \vec{v} = \sum_i \alpha_i\vec{v}_i \in T$ (closure under addition)

$\Rightarrow \text{Span}(S) \subseteq T$. ✓ □

⑦ Polynomials $= \text{Span}\{1, x, x^2, x^3, \ldots\}$

Continuous functions

Differentiable functions

Functions f with $f(1)=0$, $f'(2)=0$

Definition: Affine subspace = translated subspace

i.e., a set $\vec{u}+V$ for a vector $\vec{u}\neq\vec{0}$ and subspace V.

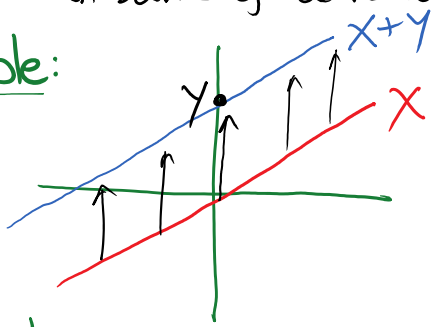
⑧ The Sum of two subspaces is a subspace.

Definition: For subsets X and Y of a vector space,

$$X+Y = \{x+y \mid x\in X, y\in Y\}.$$

(In English: all sums of a vector in X and a vector in Y.)

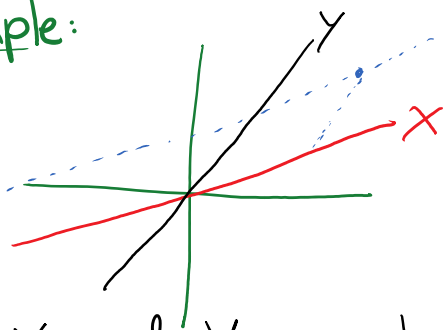
Example:



← not a subspace!

(sometimes called an "affine subspace")

Example:



What is $X+Y$?

Answer: The whole plane!

For any other point, draw this parallelogram ✓

Claim 1: If X and Y are subspaces, then $X+Y$ is a subspace.

Proof: The key properties to check are closure under $+$ and $\times$.

Closure under addition:

Want to show (WTS) if $a, b\in X+Y$, then $a+b\in X+Y$.

$a \in X+Y \Rightarrow a = x+y$ for some $x \in X, y \in Y$

$b \in X+Y \Rightarrow b = x'+y'$ " x' " y' "

$a+b = (x+y)+(x'+y')$

$= (x+x')+(y+y') \in X+Y$ ✓

($x+x' \in X$, $y+y' \in Y$)

Closure under multiplication:

WTS: If $a \in X+Y$, then for all scalars α, $\alpha a \in X+Y$:

$a = x+y$

$\alpha a = \alpha(x+y) = (\alpha x) + (\alpha y)$ ✓

($\alpha x \in X$, $\alpha y \in Y$) □

Claim 2: For subsets S and T of a vector space V,

$\text{Span}(S) + \text{Span}(T) = \text{Span}(S \cup T)$

Proof: $\text{Span}(S) = \{$finite linear combinations of elts of $S\}$

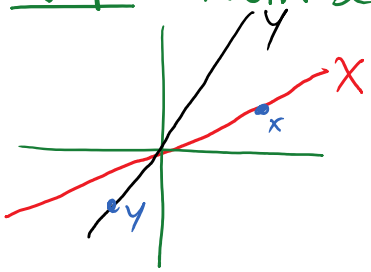
$\text{Span}(T) = \{$ " " " " $T\}$

$\therefore x \in \text{Span}(S) + \text{Span}(T)$

$\Leftrightarrow x = \sum_{j=1}^{k} \alpha_j s_j + \sum_{j=1}^{\ell} \beta_j t_j$ ($s_j \in S$, $t_j \in T$)

$\Leftrightarrow x$ is a finite linear combination of elements of $S \cup T$. ✓ □

Example: From before



$X = \text{Span}(\{x\})$

$Y = \text{Span}(\{y\})$

$\text{Span}(\{x, y\}) = \mathbb{R}^2 = X+Y$

More examples of vector spaces

Space	Closed under addition?	Closed under multiplication?	Vector space?
$V_1 = \{(b_1, b_2, b_3) \in \mathbb{R}^3 \text{ st. } b_1 - 2b_2 + 3b_3 = 0\}$	✓	✓	✓yes
$V_2 = \{(b_1, b_2, b_3) \in \mathbb{R}^3 \text{ st. } b_2 b_3 = 0\}$	✗	✓	✗no

$V_2 = \{(b_1, b_2, b_3) \in \mathbb{R}^3 \text{ s.t. } b_2 b_3 = 0\}$ ✗ ✓ ✗

$\{b \in \mathbb{R}^3 \mid b_1 + b_2 = 1\}$ ✗ ✗ ✗

affine subspace $= \{(1,0)\} + V_1$

$\text{Span}(\{(1,1,0),(2,0,1)\})$ ✓ ✓ ✓

$\{\text{upper-triangular } m \times n \text{ matrices}\}$ ✓ ✓ ✓

$\{\text{Diagonal } n \times n \text{ matrices}\}$ ✓ ✓ ✓

$V_7 = \{10 \times 10 \text{ matrices } A \text{ with } \text{Trace}(A) = \sum_{j=1}^{10} a_{jj} = 0\}$ ✓ ✓ ✓

$\{10 \times 10 \text{ matrices } A \text{ with } \text{Tr}(A) = 1\}$ ✗ ✗ ✗

affine subspace $= V_7 + \left\{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & & \end{pmatrix}\right\}$

$\{3 \times 3 \text{ matrices } A \text{ with } A\begin{pmatrix}1\\1\\1\end{pmatrix} = 0\}$ ✓ ✓ ✓

$\{\text{symmetric } n \times n \text{ matrices (ie. } A = A^T)\}$ ✓ ✓ ✓

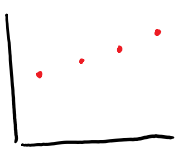
$\{\text{arithmetic progressions, i.e., sequences } (x_1, x_2, x_3, \ldots) \text{ with } x_j - x_{j-1} \text{ constant}$ (e.g., $(0,2,4,6,8,10,\ldots)$) ✓ ✓ ✓

$\{\text{differentiable functions } f: \mathbb{R} \to \mathbb{R} \text{ with } f'(2) = 3\}$ ✗ ✗ ✗

affine subspace $= 3x + \{f \text{ with } f'(2) = 0\}$

$\{(0,0),(2,1),(4,2),(6,3),\ldots,(94,47),(96,48)\}$ ✗ ✗ ✗

$\subset (\mathbb{Z}/97\mathbb{Z}) \times (\mathbb{Z}/97\mathbb{Z})$ (97 is prime)



{all matrices that commute with a given matrix A} ✓ ✓ ✓

Proof. To prove (4.1.1), demonstrate that the two closure properties **(A1)** and **(M1)** hold for $\mathcal{S} = \mathcal{X}+\mathcal{Y}$. To show **(A1)** is valid, observe that if $\mathbf{u}, \mathbf{v} \in \mathcal{S}$, then $\mathbf{u} = \mathbf{x}_1 + \mathbf{y}_1$ and $\mathbf{v} = \mathbf{x}_2 + \mathbf{y}_2$, where $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{X}$ and $\mathbf{y}_1, \mathbf{y}_2 \in \mathcal{Y}$. Because $\mathcal{X}$ and $\mathcal{Y}$ are closed with respect to addition, it follows that $\mathbf{x}_1 + \mathbf{x}_2 \in \mathcal{X}$ and $\mathbf{y}_1 + \mathbf{y}_2 \in \mathcal{Y}$, and therefore $\mathbf{u} + \mathbf{v} = (\mathbf{x}_1 + \mathbf{x}_2) + (\mathbf{y}_1 + \mathbf{y}_2) \in \mathcal{S}$. To verify **(M1)**, observe that $\mathcal{X}$ and $\mathcal{Y}$ are both closed with respect to scalar multiplication so that $\alpha\mathbf{x}_1 \in \mathcal{X}$ and $\alpha\mathbf{y}_1 \in \mathcal{Y}$ for all α, and consequently $\alpha\mathbf{u} = \alpha\mathbf{x}_1 + \alpha\mathbf{y}_1 \in \mathcal{S}$ for all α. To prove (4.1.2), suppose $\mathcal{S}_X = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_r\}$ and $\mathcal{S}_Y = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_t\}$, and write

$$\mathbf{z} \in span\,(\mathcal{S}_X \cup \mathcal{S}_Y) \Longleftrightarrow \mathbf{z} = \sum_{i=1}^{r} \alpha_i \mathbf{x}_i + \sum_{i=1}^{t} \beta_i \mathbf{y}_i = \mathbf{x} + \mathbf{y} \text{ with } \mathbf{x} \in \mathcal{X},\ \mathbf{y} \in \mathcal{Y}$$
$$\Longleftrightarrow \mathbf{z} \in \mathcal{X} + \mathcal{Y}. \quad \blacksquare$$

Example 4.1.8

If $\mathcal{X} \subseteq \Re^2$ and $\mathcal{Y} \subseteq \Re^2$ are subspaces defined by two different lines through the origin, then $\mathcal{X} + \mathcal{Y} = \Re^2$. This follows from the parallelogram law—sketch a picture for yourself.

Exercises for section 4.1

4.1.1. Determine which of the following subsets of $\Re^n$ are in fact subspaces of $\Re^n$ $(n > 2)$.

(a) $\{\mathbf{x} \mid x_i \geq 0\}$, (b) $\{\mathbf{x} \mid x_1 = 0\}$, (c) $\{\mathbf{x} \mid x_1 x_2 = 0\}$,

(d) $\left\{\mathbf{x} \;\middle|\; \sum_{j=1}^{n} x_j = 0\right\}$, (e) $\left\{\mathbf{x} \;\middle|\; \sum_{j=1}^{n} x_j = 1\right\}$,

(f) $\{\mathbf{x} \mid \mathbf{A}\mathbf{x} = \mathbf{b}$, where $\mathbf{A}_{m\times n} \neq \mathbf{0}$ and $\mathbf{b}_{m\times 1} \neq \mathbf{0}\}$.

4.1.2. Determine which of the following subsets of $\Re^{n\times n}$ are in fact subspaces of $\Re^{n\times n}$.

(a) The symmetric matrices. (b) The diagonal matrices.
(c) The nonsingular matrices. (d) The singular matrices.
(e) The triangular matrices. (f) The upper-triangular matrices.
(g) All matrices that commute with a given matrix $\mathbf{A}$.
(h) All matrices such that $\mathbf{A}^2 = \mathbf{A}$.
(i) All matrices such that $trace\,(\mathbf{A}) = 0$.

4.1.3. If $\mathcal{X}$ is a plane passing through the origin in $\Re^3$ and $\mathcal{Y}$ is the line through the origin that is perpendicular to $\mathcal{X}$, what is $\mathcal{X} + \mathcal{Y}$?

4.1.4. Why must a real or complex nonzero vector space contain an infinite number of vectors?

4.1.5. Sketch a picture in $\Re^3$ of the subspace spanned by each of the following.
(a) $\left\{\begin{pmatrix}1\\3\\2\end{pmatrix}, \begin{pmatrix}2\\6\\4\end{pmatrix}, \begin{pmatrix}-3\\-9\\-6\end{pmatrix}\right\}$, (b) $\left\{\begin{pmatrix}-4\\0\\0\end{pmatrix}, \begin{pmatrix}0\\5\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}\right\}$,
(c) $\left\{\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}\right\}$.

4.1.6. Which of the following are spanning sets for $\Re^3$?
(a) $\{(1\ \ 1\ \ 1)\}$ (b) $\{(1\ \ 0\ \ 0), (0\ \ 0\ \ 1)\}$,
(c) $\{(1\ \ 0\ \ 0), (0\ \ 1\ \ 0), (0\ \ 0\ \ 1), (1\ \ 1\ \ 1)\}$,
(d) $\{(1\ \ 2\ \ 1), (2\ \ 0\ \ -1), (4\ \ 4\ \ 1)\}$,
(e) $\{(1\ \ 2\ \ 1), (2\ \ 0\ \ -1), (4\ \ 4\ \ 0)\}$.

4.1.7. For a vector space $\mathcal{V}$, and for $\mathcal{M}, \mathcal{N} \subseteq \mathcal{V}$, explain why $span\,(\mathcal{M} \cup \mathcal{N}) = span\,(\mathcal{M}) + span\,(\mathcal{N})$.

4.1.8. Let $\mathcal{X}$ and $\mathcal{Y}$ be two subspaces of a vector space $\mathcal{V}$.
(a) Prove that the intersection $\mathcal{X} \cap \mathcal{Y}$ is also a subspace of $\mathcal{V}$.
(b) Show that the union $\mathcal{X} \cup \mathcal{Y}$ need not be a subspace of $\mathcal{V}$.

4.1.9. For $\mathbf{A} \in \Re^{m\times n}$ and $\mathcal{S} \subseteq \Re^{n\times 1}$, the set $\mathbf{A}(\mathcal{S}) = \{\mathbf{A}\mathbf{x} \,|\, \mathbf{x} \in \mathcal{S}\}$ contains all possible products of $\mathbf{A}$ with vectors from $\mathcal{S}$. We refer to $\mathbf{A}(\mathcal{S})$ as the set of ***images*** of $\mathcal{S}$ under $\mathbf{A}$.
(a) If $\mathcal{S}$ is a subspace of $\Re^n$, prove $\mathbf{A}(\mathcal{S})$ is a subspace of $\Re^m$.
(b) If $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_k$ spans $\mathcal{S}$, show $\mathbf{A}\mathbf{s}_1, \mathbf{A}\mathbf{s}_2, \ldots, \mathbf{A}\mathbf{s}_k$ spans $\mathbf{A}(\mathcal{S})$.

4.1.10. With the usual addition and multiplication, determine whether or not the following sets are vector spaces over the real numbers.
(a) $\Re$, (b) $\mathcal{C}$, (c) The rational numbers.

4.1.11. Let $\mathcal{M} = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_r\}$ and $\mathcal{N} = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_r, \mathbf{v}\}$ be two sets of vectors from the same vector space. Prove that $span\,(\mathcal{M}) = span\,(\mathcal{N})$ if and only if $\mathbf{v} \in span\,(\mathcal{M})$.

4.1.12. For a set of vectors $\mathcal{S} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$, prove that $span\,(\mathcal{S})$ is the intersection of all subspaces that contain $\mathcal{S}$. **Hint:** For $\mathcal{M} = \bigcap_{\mathcal{S}\subseteq\mathcal{V}} \mathcal{V}$, prove that $span\,(\mathcal{S}) \subseteq \mathcal{M}$ and $\mathcal{M} \subseteq span\,(\mathcal{S})$.

⑥ Examples over other fields

$\mathbb{F}_p$ = field of numbers mod p (for a prime p)

$\mathbb{F}_2 = \{0, 1\}$

Bit strings of length n form a vector space:

n=3:

$(0,0,0), (0,0,1), (0,1,0), (0,1,1)$

$(1,0,0), (1,0,1), (1,1,0), (1,1,1)$

addition is coordinate-wise, mod 2

$(0,0,1) + (0,1,1) = (0,1,0)$

subspace, eg.,

$\text{Span}(\{(0,0,1), (1,0,1)\})$

$= \{(0,0,0), (0,0,1), (1,0,1), (1,0,0)\}$

Problems:

1. How many subspaces are there of $\mathbb{R}^2$?

   Answer: Infinitely many!

   (lines through the origin)

2. How many subspaces are there of $\mathbb{R}$?

   Answer: Two! $\{0\}$ and $\mathbb{R}$ itself.

3. How many subspaces are there of $\{0,1\}^2$?

   $\{(0,0)\}$, everything $\{0,1\}^2$

   $\{(0,0),(0,1)\}$, $\{(0,0),(1,0)\}$

   $\{(0,0),(1,0)\}$, $\{(0,0),(1,1)\}$

   and that's it!

   (if a subspace contains two of the nonzero points, then it also includes their sum, which is the last nonzero point: $(1,0)+(0,1)+(1,1)=(0,0)$ means that any two sum to the third)

   $1 + 4 + 1 = 6$

4. How many subspaces are there of $\{0,1\}^n$?

   We'll answer this later! Definitely $< \infty$ though

vector $(1,1,-1)$ and automatically contains any multiple $(c,c,-c)$:

$$\textbf{Nullspace is a line} \qquad \begin{bmatrix} 1 & 0 & 1 \\ 5 & 4 & 9 \\ 2 & 4 & 6 \end{bmatrix} \begin{bmatrix} c & c & -c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

The nullspace of B is the line of all points $x = c$, $y = c$, $z = -c$. (The line goes through the origin, as any subspace must.) We want to be able, for any system $Ax = b$, to find $\boldsymbol{C}(A)$ and $\boldsymbol{N}(A)$: all attainable right-hand sides b and all solutions to $Ax = 0$.

The vectors b are in the column space and the vectors x are in the nullspace. We shall compute the dimensions of those subspaces and a convenient set of vectors to generate them. We hope to end up by understanding all *four* of the subspaces that are intimately related to each other and to A—the column space of A, the nullspace of A, and their two perpendicular spaces.

Problem Set 2.1

1. Construct a subset of the x-y plane $\mathbf{R}^2$ that is

(a) closed under vector addition and subtraction, but not scalar multiplication.

(b) closed under scalar multiplication but not under vector addition.

Hint: Starting with u and v, add and subtract for (a). Try cu and cv for (b).

2. Which of the following subsets of $\mathbf{R}^3$ are actually subspaces?

(a) The plane of vectors (b_1, b_2, b_3) with first component $b_1 = 0$.

(b) The plane of vectors b with $b_1 = 1$.

(c) The vectors b with $b_2 b_3 = 0$ (this is the union of two subspaces, the plane $b_2 = 0$ and the plane $b_3 = 0$).

(d) All combinations of two given vectors $(1,1,0)$ and $(2,0,1)$.

(e) The plane of vectors (b_1, b_2, b_3) that satisfy $b_3 - b_2 + 3b_1 = 0$.

3. Describe the column space and the nullspace of the matrices

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 0 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

4. What is the smallest subspace of 3 by 3 matrices that contains all symmetric matrices *and* all lower triangular matrices? What is the largest subspace that is contained in both of those subspaces?

5. Addition and scalar multiplication are required to satisfy these eight rules:

1. $x+y=y+x$.
2. $x+(y+z)=(x+y)+z$.
3. There is a unique "zero vector" such that $x+0=x$ for all x.
4. For each x there is a unique vector $-x$ such that $x+(-x)=0$.
5. $1x=x$.
6. $(c_1c_2)x=c_1(c_2x)$.
7. $c(x+y)=cx+cy$.
8. $(c_1+c_2)x=c_1x+c_2x$.

(a) Suppose addition in $\mathbf{R}^2$ adds an extra 1 to each component, so that $(3,1)+(5,0)$ equals $(9,2)$ instead of $(8,1)$. With scalar multiplication unchanged, which rules are broken?

(b) Show that the set of all positive real numbers, with $x+y$ and cx redefined to equal the usual xy and x^c, is a vector space. What is the "zero vector"?

(c) Suppose $(x_1,x_2)+(y_1,y_2)$ is defined to be (x_1+y_2,x_2+y_1). With the usual $cx=(cx_1,cx_2)$, which of the eight conditions are not satisfied?

6. Let $\mathbf{P}$ be the plane in 3-space with equation $x+2y+z=6$. What is the equation of the plane $\mathbf{P}_0$ through the origin parallel to $\mathbf{P}$? Are $\mathbf{P}$ and $\mathbf{P}_0$ subspaces of $\mathbf{R}^3$?

7. Which of the following are subspaces of $\mathbf{R}^\infty$?

(a) All sequences like $(1,0,1,0,\dots)$ that include infinitely many zeros. NO

(b) All sequences $(x1,x2,\dots)$ with $x_j=0$ from some point onward. YES

(c) All decreasing sequences: $x_{j+1}\le x_j$ for each j.

(d) All convergent sequences: the x_j have a limit as $j\to\infty$.

(e) All arithmetic progressions: $x_{j+1}-x_j$ is the same for all j.

(f) All geometric progressions $(x_1,kx_1,k^2x_1,\dots)$ allowing all k and x_1.

8. Which of the following descriptions are correct? The solutions x of

$$Ax=\begin{bmatrix}1&1&1\\1&0&2\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}=\begin{bmatrix}0\\0\end{bmatrix}$$

form

(a) a plane.

(b) a line.

(c) a point.

(d) a subspace.

(e) the nullspace of A.

(e) the nullspace of A.

(f) the column space of A.

9. Show that the set of nonsingular 2 by 2 matrices is not a vector space. Show also that the set of *singular* 2 by 2 matrices is not a vector space.

10. The matrix $A = \begin{bmatrix} 2 & -2 \\ 2 & -2 \end{bmatrix}$ is a "vector" in the space **M** of all 2 by 2 matrices. Write the zero vector in this space, the vector $\frac{1}{2}A$, and the vector $-A$. What matrices are in the smallest subspace containing A?

11. (a) Describe a subspace of **M** that contains $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ but not $B = \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}$.

(b) If a subspace of **M** contains A and B, must it contain I?

(c) Describe a subspace of **M** that contains no nonzero diagonal matrices.

12. The functions $f(x) = x^2$ and $g(x) = 5x$ are "vectors" in the vector space **F** of all real functions. The combination $3f(x) - 4g(x)$ is the function $h(x) =$ ____. Which rule is broken if multiplying $f(x)$ by c gives the function $f(cx)$?

13. If the sum of the "vectors" $f(x)$ and $g(x)$ in **F** is defined to be $f(g(x))$, then the "zero vector" is $g(x) = x$. Keep the usual scalar multiplication $cf(x)$, and find two rules that are broken.

14. Describe the smallest subspace of the 2 by 2 matrix space **M** that contains

(a) $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

(b) $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

(c) $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$.

(d) $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$.

15. Let **P** be the plane in $\mathbf{R}^3$ with equation $x + y - 2z = 4$. The origin $(0,0,0)$ is not in **P**! Find two vectors in **P** and check that their sum is not in **P**.

16. $\mathbf{P}_0$ is the plane through $(0,0,0)$ parallel to the plane **P** in Problem 15. What is the equation for $\mathbf{P}_0$? Find two vectors in $\mathbf{P}_0$ and check that their sum is in $\mathbf{P}_0$.

17. The four types of subspaces of $\mathbf{R}^3$ are planes, lines, R^3 itself, or **Z** containing only $(0,0,0)$.

(a) Describe the three types of subspaces of $\mathbf{R}^2$.

(b) Describe the five types of subspaces of $\mathbf{R}^4$.

18. (a) The intersection of two planes through $(0,0,0)$ is probably a ____ but it could be a ____. It can't be the zero vector **Z**!

(b) The intersection of a plane through $(0,0,0)$ with a line through $(0,0,0)$ is probably a ____ but it could be a ____.

(c) If **S** and **T** are subspaces of $\mathbf{R}^5$, their intersection $\mathbf{S} \cap \mathbf{T}$ (vectors in both subspaces) is a subspace of $\mathbf{R}^5$. *Check the requirements on $x+y$ and cx.*

19. Suppose **P** is a plane through $(0,0,0)$ and **L** is a line through $(0,0,0)$. The smallest vector space containing both **P** and **L** is either ____ or ____.

20. True or false for $\mathbf{M}$ = all 3 by 3 matrices (check addition using an example)?

(a) The skew-symmetric matrices in $\mathbf{M}$ (with $A^{\mathrm{T}} = -A$) form a subspace.

(b) The unsymmetric matrices in $\mathbf{M}$ (with $A^{\mathrm{T}} \neq A$) form a subspace.

(c) The matrices that have $(1,1,1)$ in their nullspace form a subspace.

Problems 21–30 are about column spaces $C(A)$ and the equation $Ax = b$.

21. Describe the column spaces (lines or planes) of these particular matrices:

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} 1 & 0 \\ 2 & 0 \\ 0 & 0 \end{bmatrix}.$$

22. For which right-hand sides (find a condition on b_1, b_2, b_3) are these systems solvable?

$$\text{(a)} \quad \begin{bmatrix} 1 & 4 & 2 \\ 2 & 8 & 4 \\ -1 & -4 & -2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}. \qquad \text{(b)} \quad \begin{bmatrix} 1 & 4 \\ 2 & 9 \\ -1 & -4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}.$$

23. Adding row 1 of A to row 2 produces B. Adding column 1 to column 2 produces C. A combination of the columns of ____ is also a combination of the columns of A. Which two matrices have the same column ____?

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} 1 & 3 \\ 2 & 6 \end{bmatrix}.$$

24. For which vectors (b_1, b_2, b_3) do these systems have a solution?

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}.$$

25. (Recommended) If we add an extra column b to a matrix A, then the column space gets larger unless ____. Give an example in which the column space gets larger and an example in which it doesn't. Why is $Ax = b$ solvable exactly when the column space *doesn't* get larger by including b?

26. The columns of AB are combinations of the columns of A. This means: *The column space of AB is contained in* (possibly equal to) *the column space of A.* Give an example where the column spaces of A and AB are not equal.

27. If A is any 8 by 8 invertible matrix, then its column space is ____. Why?

27. If A is any 8 by 8 invertible matrix, then its column space is ____. Why?

28. True or false (with a counterexample if false)?

(a) The vectors b that are not in the column space $C(A)$ form a subspace.

(b) If $C(A)$ contains only the zero vector, then A is the zero matrix.

(c) The column space of $2A$ equals the column space of A.

(d) The column space of $A - I$ equals the column space of A.

29. Construct a 3 by 3 matrix whose column space contains $(1,1,0)$ and $(1,0,1)$ but not $(1,1,1)$. Construct a 3 by 3 matrix whose column space is only a line.

30. If the 9 by 12 system $Ax = b$ is solvable for every b, then $C(A) =$ ____.

31. Why isn't $\mathbf{R}^2$ a subspace of $\mathbf{R}^3$?

2.2 Solving $Ax = 0$ and $Ax = b$

Chapter 1 concentrated on square invertible matrices. There was one solution to $Ax = b$ and it was $x = -A^{-1}b$. That solution was found by elimination (not by computing A^{-1}). A rectangular matrix brings new possibilities—U may not have a full set of pivots. This section goes onward from U to a reduced form R—**the simplest matrix that elimination can give**. R reveals all solutions immediately.

For an invertible matrix, the nullspace contains only $x = 0$ (multiply $Ax = 0$ by A^{-1}). The column space is the whole space ($Ax = b$ has a solution for every b). The new questions appear when the nullspace contains *more than the zero vector* and/or the column space contains *less than all vectors*:

1. Any vector x_n in the nullspace can be added to a particular solution x_p. The solutions to all linear equations have this form, $x = x_p + x_n$:

   Complete solution $Ax_p = b$ **and** $Ax_n = 0$ **produce** $A(x_p + x_n) = b$.

2. When the column space doesn't contain every b in $\mathbf{R}^m$, we need the conditions on b that make $Ax = b$ solvable.

A 3 by 4 example will be a good size. We will write down all solutions to $Ax = 0$. We will find the conditions for b to lie in the column space (so that $Ax = b$ is solvable). The 1 by 1 system $0x = b$, one equation and one unknown, shows two possibilities:

$0x = b$ has *no solution* unless $b = 0$. The column space of the 1 by 1 zero matrix contains only $b = 0$.

$0x = 0$ has *infinitely many solutions*. The nullspace contains *all* x. A particular solution is $x_p = 0$, and the complete solution is $x = x_p + x_n = 0 + (\text{any } x)$.

More important examples:
SUBSPACES OF A MATRIX

More important examples:

Subspaces of a Matrix

Let $A \in \mathbb{R}^{m \times n}$ be an $m \times n$ real-valued matrix.

- $\text{Range}(A) = \{A\vec{x} \mid \vec{x} \in \mathbb{R}^n\}$

  $= \text{Span}(\text{columns of } A)$

  AKA "column space" of A

  Observe: $\vec{b} \in \text{Range}(A) \iff A\vec{x} = \vec{b}$ has a solution

- $\text{Range}(A^T) = \text{Span}(\text{rows of } A)$

  "row space"

- $\text{Kernel}(A) = \{\vec{x} \in \mathbb{R}^n \mid A\vec{x} = \vec{0}\}$ (solutions to the homogeneous equations)

  AKA "null space" of A

Vector spaces over finite fields

Our examples so far, like $\mathbb{R}^n$, $\mathbb{R}^{m\times n}$ ($m\times n$ matrices), or their subspaces, have been "over $\mathbb{R}$" (real numbers $\mathbb{R}=(-\infty,\infty)$), meaning that the spaces have to be closed under multiplication by arbitrary real numbers $(0, 1, \frac{1}{2}, \sqrt{2}, \pi, \ldots)$.

But linear algebra makes sense over other fields, too, and some are very important!

Example: $\mathbb{C} = \{a+bi \mid a,b\in\mathbb{R}\}$
complex numbers

$i^2 = -1$

$(a+bi)(c+di) = (ac-bd)+(ad+bc)i$

What is a field?

Essentially, a set with
- addition
- subtraction
- multiplication
- division

https://en.wikipedia.org/wiki/Field_(mathematics)#Classic_definition

Formally, a field is a set together with two operations called *addition* and *multiplication*.[1] An operation is a mapping that associates an element of the set to *every* pair of its elements. The result of the addition of a and b is called the *sum* of a and b and denoted $a + b$. Similarly, the result of the multiplication of a and b is called the *product* of a and b, and denoted ab or $a\cdot b$. These operations are required to satisfy the following properties, referred to as *field axioms*. In the sequel, a, b and c are arbitrary elements of F.

- *Associativity* of addition and multiplication: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- *Commutativity* of addition and multiplication: $a + b = b + a$ and $a \cdot b = b \cdot a$.
- *Additive* and *multiplicative identity*: there exist two different elements 0 and 1 in F such that $a + 0 = a$ and $a \cdot 1 = a$.
- *Additive inverses*: for every a in F, there exists an element in F, denoted $-a$, called *additive inverse* of a, such that $a + (-a) = 0$.
- *Multiplicative inverses*: for every $a \neq 0$ in F, there exists an element in F, denoted by a^{-1}, $1/a$, or $\frac{1}{a}$, called the *multiplicative inverse* of a, such that $a \cdot a^{-1} = 1$.
- *Distributivity* of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Example:
$\mathbb{Z}$ = set of integers $\ldots, -2, -1, 0, 1, 2, \ldots$
is not a field
because you can't divide, $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$

Linear algebra over $\mathbb{Z}$ doesn't really work

$\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$ Gaussian elimination ?

We need division!

Example:
$\mathbb{Q} = \{a/b \mid a,b\in\mathbb{Z}, b\neq 0\}$
rational numbers

Example: $\mathbb{F}_2 = \{0, 1\}$ is a finite field

operations defined modulo 2,

so $1 + 1 = 0$

Mathematica

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix};$$

$\xrightarrow{+1} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow{+1}$

```
RowReduce[A, Modulus → 2] // MatrixForm
```

```
MatrixForm=
1 0 1
0 1 1
0 0 0
```

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$\xrightarrow{-1} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow{-1} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 2 \end{pmatrix} \xrightarrow{\times \frac{1}{2}}$

```
RowReduce[A] // MatrixForm
```

```
MatrixForm=
1 0 0
0 1 0
0 0 1
```

Vector spaces over $\mathbb{F}_2$

Bit strings of length n form a vector space over $\mathbb{F}_2$

eg., n=2:

(0,0), (0,1),
(1,0), (1,1)

n=3:

(0,0,0), (0,0,1), (0,1,0), (0,1,1)
(1,0,0), (1,0,1), (1,1,0), (1,1,1)

coordinate-wise addition mod 2,

$(0,1,1) + (1,1,0) = (1,0,1)$.

Linear operators make sense:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Subspaces make sense:

$\{(0,0), (0,1)\}$ is a subspace of $\{0,1\}^2$

Why?

closure under addition:

+	$\binom{0}{0}$	$\binom{0}{1}$
$\binom{0}{0}$	$\binom{0}{0}$	$\binom{0}{1}$
$\binom{0}{1}$	$\binom{0}{1}$	$\binom{0}{0}$

closure under multiplication by 0 or 1 ($\mathbb{F}_2$): ✓

Exercise: How many subspaces are there of $\{0,1\}^2$ over $\mathbb{F}_2$?

Answer:

$\{(0)\}$, everything $\{0,1\}^2$,

$\{(0),(1)\}$, $\{(0),(0)\}$, $\{(0),(1)\}$

$\Rightarrow \boxed{5}$

$V=\{(0),(1),(1)\}$ is not a subspace

$(1)+(1)=(0)\notin V$

not closed under addition!

Exercise: $\text{Span}\left(\left\{\begin{pmatrix}0\\0\\1\end{pmatrix},\begin{pmatrix}1\\0\\1\end{pmatrix}\right\}\right)=?$ over $\mathbb{F}_2$

$(0,0,0)$, $(0,0,1)$, $(1,0,1)$,

$(1,0,0)=(0)+(1)$

that's it!

How many subspaces are there of $\{0,1\}^3$?

$\{0,1\}^n$?

More finite fields

$\mathbb{F}_3=\{0,1,2\}$ is a field

note $1+2=0$

$2^{-1}=2$ since $2\times 2=1 \bmod 3$

$\{0,1,2,3\}$ is not a field

$1^{-1}=1$, $3^{-1}=3$ $(3\times 3=1 \bmod 4)$

but you can't divide by 2!

2^{-1} does not exist in $\{0,1,2,3\}$

$\{0,1,2,3,4\}$ is a field

$1^{-1}=1$, $2^{-1}=3$, $3^{-1}=2$, $4^{-1}=4$

$\{0,1,2,\ldots,p-1\}$ is a field

if and only if p is prime!

Other important finite fields

Any finite field must have p^k elements for a prime p.

Example: x^2+x+1 is "irreducible" over $\mathbb{F}_2$ (can't be factored)

Consider all polynomials modulo x^2+x+1

$0, 1, x, x+1$

this is a field!

$x^2 = x+1 \pmod{x^2+x+1}$

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

multiplication

	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

inverses: $1^{-1}=1$, $x^{-1}=x+1$

https://en.wikipedia.org/wiki/Finite_field

Applications [edit]

In cryptography, the difficulty of the discrete logarithm problem in finite fields or in elliptic curves is the basis of several widely used protocols, such as the Diffie–Hellman protocol. For example, in 2014 a secure internet connection to Wikipedia involved the elliptic curve Diffie–Hellman protocol (ECDHE) over a large finite field.[5] In coding theory, many codes are constructed as subspaces of vector spaces over finite fields.

⋮

Reed–Solomon codes are a group of error-correcting codes that were introduced by Irving S. Reed and Gustave Solomon in 1960.[1] They have many applications, the most prominent of which include consumer technologies such as CDs, DVDs, Blu-ray Discs, QR Codes, data transmission technologies such as DSL and WiMAX, broadcast systems such as DVB and ATSC, and storage systems such as RAID 6. They are also used in satellite communication.

In coding theory, the Reed–Solomon code belongs to the class of non-binary cyclic error-correcting codes. The Reed–Solomon code is based on univariate polynomials over finite fields.

Data storage [edit]

Reed–Solomon coding is very widely used in mass storage systems to correct the burst errors associated with media defects.

Reed–Solomon coding is a key component of the compact disc. It was the first use of strong error correction coding in a mass-produced consumer product, and DAT and DVD use similar schemes. In the CD, two layers of Reed–Solomon coding separated by a 28-way convolutional interleaver yields a scheme called Cross-Interleaved Reed–Solomon Coding (CIRC). The first element of a CIRC decoder is a relatively weak inner (32,28) Reed–Solomon code, shortened from a (255,251) code with 8-bit symbols. This code can correct up to 2 byte errors per 32-byte block. More importantly, it flags as erasures any uncorrectable blocks, i.e., blocks with more than 2 byte errors. The decoded 28-byte blocks, with erasure indications, are then spread by the deinterleaver to different blocks of the (28,24) outer code. Thanks to the deinterleaving, an erased 28-byte block from the inner code becomes a single erased byte in each of 28 outer code blocks. The outer code easily corrects this, since it can handle up to 4 such erasures per block. $\mathbb{F}_{2^8}$

The result is a CIRC that can completely correct error bursts up to 4000 bits, or about 2.5 mm on the disc surface. This code is so strong that most CD playback errors are almost certainly caused by tracking errors that cause the laser to jump track, not by uncorrectable error bursts.[5]

DVDs use a similar scheme, but with much larger blocks, a (208,192) inner code, and a (182,172) outer code.

Reed–Solomon error correction is also used in parchive files which are commonly posted accompanying multimedia files on USENET. The Distributed online storage service Wuala (discontinued in 2015) also used to make use of Reed–Solomon when breaking up files.

Example: Over $\mathbb{F}_2$,

x^4+1 is reducible

$(x+1)^2 = x^2+2x+1$

$(x^2+1)^2 = x^4+2x^2+1 = x^4+1$

```
FactorList[x^4 + 1, Modulus → 2]
{{1, 1}, {1 + x, 4}}
```

x^4+x+1 is irreducible

```
IrreduciblePolynomialQ[x^4 + x + 1, Modulus → 2]
True
```

$\Rightarrow$ gives a field with 2^4 elements

$0, 1, x, x+1, x^2, \ldots, x^3+x^2+x+1$

Multiplication mod x^4+x+1,

e.g., $x^3 \cdot (x^2+1) = x^5 + x^3$

$= x \cdot x^4 + x^3$

$= x(x+1) + x^3$ [since $x^4 = x+1$]

$= x^3 + x^2 + x$

Represented in binary:

$1000 \times 0101 = 1110$

$x^3\ x^2\ x\ 1 \quad x^3\ x^2\ x\ 1 \quad x^3\ x^2\ x\ 1$