MATH223 - Linear Algebra (class notes)

Sandrine Monfourny-Daigneault

McGill University

Contents

1 January 7th 2019

Should know how to solve a linear system and calculate a determinant... things like that.

- Written assignments (5) : 10%
- Webwork assignments (5) : 5%
- Midterm : 20%
- Final : 65%

Textbook: **Schaum's Outline - Linear Algebra**.

1.1 Motivation

We have linear systems, with two equations, like such:

$$\begin{aligned} 3x - 2y + z &= 2 \\ x - y + z &= 1 \end{aligned}$$

There is an algebraic way of seeing this, but we can also see this, from the geometric standpoint, as the intersection of the two planes in R^3. Linear algebra has to do with things that are "flat", like a plane. As soon as we add in exponents to these equations, we get some curvature, and the techniques to solve these are different.

- Linear equations are the simplest kind, so you *must* understand them. Also, you *can* understand 'everything' about them.
- Theory used to describe solutions, etc.
- Linear equations are often used to approximate or model more complicated equations/situations.
- In applications, linear systems are often quite big (10000 equations/variables)

1.2 Complex numbers

Def: Let i be a symbol. We declare $i^2 = -1$.
Now, what we'd like to do is take this symbol i and combine it with the usual real numbers that we are familiar with. We set, for example,

$$\begin{aligned} 3i \\ i - 4 \\ 3i - \pi \\ \sqrt{i} + 21 \end{aligned}$$

Def: The field of complex numbers C consists of all expressions of the form $a + bi$, where $a, b \in R$.
Def: Addition (subtraction) and multiplication of complex numbers is defined by the following rules:

(i)

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

(ii)

$$\begin{aligned} (a + bi)(c + di) &= ac + adi + bci + bdi^2 \\ &= ac + adi + bci - bd \\ &= (ac - bd) + (ad + bc)i \end{aligned}$$

Notation:

- $0 + bi = bi$
- $a + 0i = a$ (a *real* number)
- $0 + 0i = 0$

Ex: If $z_1 = 2 - i$, $z_2 = 5i$, then

$$z_1 + z_2 = 2 + 4i$$

and

$$z_1 z_2 = (2 - i)(5i) = 10i - 5i^2 = 5 + 10i$$

Def: Let $z = a + bi \in C$

(i) $\bar{z} = a - bi$, called the *complex conjugate* of z

(ii) $|z| = \sqrt{a^2 + b^2}$, called the *absolute value* or *modulus*

Def: If $z = a + bi \in C$ and $z \neq 0$ (ie $z \neq 0 + 0i$), then the number

$$\begin{aligned} z^{-1} &= \frac{\bar{z}}{|z|^2} \\ &= \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \end{aligned}$$

is called the (multiplicative) inverse of z. It has the property $zz^{-1} = 1 = z^{-1}z$.

Proof. We have

$$\begin{aligned} zz^{-1} &= (a + bi)\left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i\right) \\ &= \frac{a^2 - abi + abi - b^2 i^2}{a^2 + b^2} \\ &= \frac{a^2 + 0 + b^2}{a^2 + b^2} \\ &= 1 \end{aligned}$$

Note: Since $z \neq 0 + 0i$, $a^2 + b^2 \neq 0$ □

Def: If $z, w \in C$ and $z \neq 0$ then

$$\frac{w}{z} = wz^{-1}$$

Ex: If $z = 1 + 2i, w = 3 - i$ then

$$\begin{aligned}\frac{w}{z} &= wz^{-1} \\ &= (3-i)(\frac{1}{5} - \frac{2}{5}i) \\ &= \frac{3}{5} - \frac{6}{5}i - \frac{i}{5} + \frac{2}{5}i^2 \\ &= \frac{3}{5} - \frac{2}{5} - \frac{7}{5}i \\ &= \frac{1}{5} - \frac{7}{5}i\end{aligned}$$

Or,

$$\begin{aligned}\frac{3-i}{1+2i} \cdot \frac{(1-2i)}{(1-2i)} &= \frac{3-6i-i+2i^2}{1-2i+2i-4i^2} \\ &= \frac{1-7i}{5}\end{aligned}$$

2 January 9th 2019

2.1 Complex numbers as points in R^2

You can view $a + bi$ as a point $(a, b) \in R^2$. The usefulness of this is that we can consider, say, $(3 + 2i)$ and $(3 - i)$ as vectors in R^2, and they will conserve the same properties (addition of complex numbers corresponds to vector addition in R^2). For the interpretation of multiplication to make sense, it's necessary to use polar coordinates.

2.2 Equations with complex numbers

Fact: Every real number $a \neq 0$ has two square roots:

- if $a > 0$, roots $\pm\sqrt{a}$
- if $a < 0$, two roots are $\pm i\sqrt{|a|}$, since:

$$\begin{aligned}(\pm i\sqrt{|a|})^2 &= i^2(\sqrt{|a|})^2 \\ &= -1 \cdot |a| \\ &= a && \text{(since } a < 0\text{)}\end{aligned}$$

Fact: Quadratic equation $ax^2 + bx + c = 0$ has solution

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

which may be in C.

Ex: Solve $x^2 - 2x + 3 = 0$, and factor $x^2 - 2x + 3$.
Sol:

$$\begin{aligned} x &= \frac{-2 \pm \sqrt{4 - 4(1)(3)}}{2} \\ &= \frac{2 \pm \sqrt{-8}}{2} \\ &= \frac{2 \pm i\sqrt{8}}{2} \\ &= \frac{2 \pm i2\sqrt{2}}{2} \\ &= 1 \pm i\sqrt{2} \end{aligned}$$

Note: If $ax^2 + bx + c$ has $a, b, c \in R$ has a non-real root, say z, its other root is $\bar{z}$ ($z = a + bi$, $\bar{z} = a - bi$). This is not necessarily true if $a, b, c \in C$.

Back to problem. Factor $x^2 - 2x + 3 = (x - (1 + i\sqrt{2}))(x - (1 - i\sqrt{2}))$.

Caution: -1 has two roots, namely $\pm i$, so you may write $i = \sqrt{-1}$, but be careful:

$$\begin{aligned} -1 &= i^2 \\ &= i \cdot i \\ &= \sqrt{-1} \cdot \sqrt{-1} \\ &= \sqrt{(-1)(-1)} && \text{(this step doesn't quite work)} \\ &= \sqrt{1} \\ &= 1 \end{aligned}$$

Theorem: (Fundamental Theorem of Algebra) If

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 n^0$$

is a polynomial with $a_n \neq 0$, and $a_n, a_{n-1}, \ldots, a_0 \in C$, then $p(x)$ factors into linear factors,

$$p(x) = a_n \cdot (x - r_1) \cdot (x - r_2) \cdot \ldots \cdot (x - r_n)$$

for some complex numbers $r_1, r_2, \ldots, r_n$. Some r_i's may be equal.

Corollary: Every such polynomial has at least one root, and at most n distinct roots.

Note: *Finding* the roots is, in general, quite difficult.

Ex: Factor $2x^3 + 2x$ (over C).
Sol:

$$\begin{aligned} 2(x^3 + x) &= 2(x-0)(x^2+1) \\ &= 2(x-0)(x^2 - i^2) \\ &= 2(x-0)(x-i)(x+i) \end{aligned}$$

Ex: Solve $x^2 - i = 0$
Sol: $x^2 = i$ so $x = \pm\sqrt{i}$. Want $\sqrt{i}$ in format $a + bi$, $a, b \in R$.

$$\begin{aligned} \sqrt{i} &= a + bi \\ i &= (a+bi)^2 \\ &= a^2 + 2abi + b^2 i^2 \\ 0 + i &= (a^2 - b^2) + 2abi \end{aligned}$$

$$\begin{aligned} 0 &= a^2 - b^2 \\ 1 &= 2ab \\ a &= \pm b \\ ab &= \frac{1}{2} && \text{(so a=b both + or both -)} \\ a^2 &= \frac{1}{2} \\ a &= \pm\frac{1}{\sqrt{2}} = b \end{aligned}$$

Two solutions, $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$ and $-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$.

2.3 Vector spaces (Ch 4)

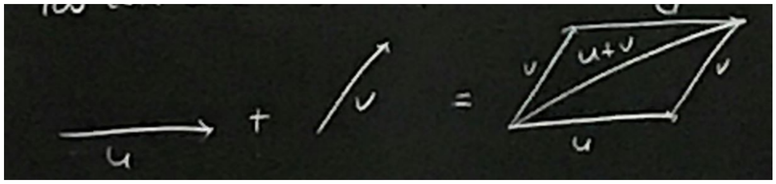
Def. The sets R and C (and also Q, rational numbers, although we won't go into details of this) are called *fields* (or *fields of scalars*). In this class, "a field of K" means that K is either R or C.

3 January 11th 2019

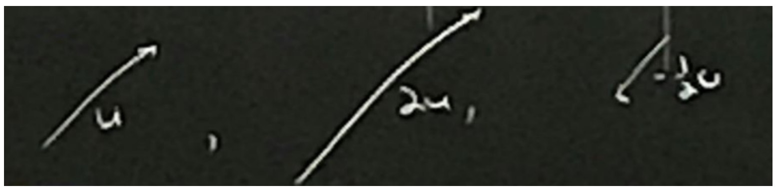
Last time: *Field* K is R or C (for this class).

3.1 Geometric vectors ('arrows')

You can add two vectors (arrows).



Observation: $\vec{u} + \vec{v} = \vec{v} + \vec{u}$.
You can rescale a vector:



Observation: $a(b\vec{u}) = (ab)\vec{u}$.
Also: $1\vec{u} = \vec{u}$
Question: What properties are interesting? What other objects obey the same properties?
Abstraction: Focus on properties more than on the objects.

3.2 Definition of a vector space

Let V be a set, called set of "vectors", and let K be a field (R or C) (elements of K called *scalars*). Assume that we have already defined two operations:

(1) One called *addition*, which takes two vectors $\vec{u}, \vec{v} \in V$ and produces another vector denoted $\vec{u} + \vec{v} \in V$.

(2) One called *scalar multiplication* which takes a vector $\vec{u} \in V$ and a scalar $a \in K$ and produces another vector denoted $a\vec{u} \in V$

Then if, for all vectors $\vec{u}, \vec{v}, \vec{w} \in V$ and all scalars $a, b \in K$, the following 8 properties are true, then V is called a *vector space* (over K).

(A1) $u + v = v + u$ (commutative laws)

(A2) There exists a vector in V, named *zero vector* and denoted 0 (or $\vec{0}$) such that for all $u \in V$, $u + 0 = u$

(A3) For each $u \in V$, there is a vector in V, called the (additive) inverse of u and denoted $-u$, having the property $u + (-u) = 0$ (where 0 is the zero vector defined in A2)

(A4) $(u + v) + w = u + (v + w)$

(SM1) $a(u + v) = au + av$ (distributive laws)

(SM2) $(a+b)u = au + bu$

(SM3) $a(bu) = (ab)u$

(SM4) $1u = u$ ($1 \in R$ or C)

These are called the vector space *axioms*.

3.3 Examples of vector spaces

Some examples:

(1) $K^n = \{(a_1, a_2, \ldots, a_n) | a_1, a_2, \ldots, a_n \in K\}$, with addition defined by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

and scalar multiplication by

$$c(a_1, a_2, \ldots, a_n) = (ca_1, ca_2, \ldots, ca_n)$$

where $c \in K$ (and K = set of scalar).

Proof that K^n is a vector space
Need to prove all 8 properties. We will do 2, the rest are exercises.

(A4) To prove for all $u, v \in V$, $u + v = v + u$.
Proof concept: To prove "for all $x \in A$, something", say "let $x \in A$" (means x is an arbitrary element of A, ie you only know $x \in A$). Then, prove something for that x.
Proof: Let $u, v \in K^n$. This means $u = (a_1, a_2, \ldots, a_n)$, $v = (b_1, b_2, \ldots, b_n)$ for some $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in K$. Then

$$\begin{aligned} u + v &= (a_1, \ldots, a_n) + (b_1, \ldots, b_n) \\ &= (a_1 + b_1, \ldots, a_n + b_n) && \text{(definition of addition in } K^n\text{)} \\ &= (b_1 + a_1, \ldots, b_n + a_n) && \text{(since } a + b = b + a \text{ for } R \text{ and } C\text{)} \\ &= (b_1, \ldots, b_n) + (a_1, \ldots, a_n) && \text{(definition of addition in } K^n\text{)} \\ &= v + u \end{aligned}$$

(A2) *Proof concept:* To prove "there exists" something, one method is to describe the thing directly.
Define $0 = (0, 0, \ldots, 0)$ (which *is* in K^n). To prove for all $u \in K^n$, $u + 0 = u$, let $u \in K^n$. This means $u = (a_1, a_2, \ldots, a_n$, so

$$\begin{aligned} u + 0 &= (a_1, a_2, \ldots, a_n + (0, 0, \ldots, 0) \\ &= (a_1 + 0, a_2 + 0, \ldots, a_n + 0) \\ &= (a_1, a_2, \ldots, a_n) \\ &= u \end{aligned}$$

(2) In the vector space C^2, $(2+3i, 5-7i) \in C^2$ is an example of a vector and $2i \in C$ is a scalar, so an example of scalar mult is :

$$\begin{aligned} 2i(u) &= 2i(2+3i, 5-7i) \\ &= (4i+6i^2, 10i-14i^2) \\ &= (-6+4i, 14+10i) \end{aligned}$$

4 January 14th 2019

Problem: Let $J = \{(x,y)|x \in R, y \in R\}$ but define addition by

$$(x_1, y_1) + (x_2, y_2) = (-x_1 - x_2, y_1 + y_2)$$

and scalar multiplication by

$$c(x,y) = (cx, cy)$$

Show that J is not a vector space.
Solution: Show *one* of the 8 vector space axioms is false. Consider (A1):

$$(x_2, y_2) + (x_1, y_1) = (-x_2 - x_1, y_2 + y_1)$$

This is actually ok! Now consider (A4):

$$\begin{aligned} (x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) &= (x_1, y_1) + (-x_2 - x_3, y_2 + y_3) \\ &= (-x_1 - (-x_2 - x_3), y_1 + y_2 + y_3) \\ &= (-x_1 + x_2 + x_3, y_1 + y_2 + y_3) \end{aligned}$$

While

$$\begin{aligned} ((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) &= (-x_1 - x_2, y_1 + y_2) + (x_3, y_3) \\ &= (-(-x_1 - x_2) - x_3, y_1 + y_2 + y_3) \\ &= (x_1 + x_2 - x_3, y_1 + y_2 + y_3) \end{aligned}$$

This does not quite yet prove that the axiom is false. To do so, give *specific* case where the equation is false.
Actual proof: Let $u = (1,1)$, $v = (2,2)$ and $w = (3,3)$. Then,

$$\begin{aligned} u + (v + w) &= (1,1) + ((2,2) + (3,3)) \\ &= (1,1) + (-2-3, 5) \\ &= (1,1) + (-5, 5) \\ &= (-1+5, 6) \\ &= (4, 6) \end{aligned}$$

Whereas,

$$
\begin{aligned}
(u+v)+w &= ((1,1)+(2,2))+(3,3) \\
&= (-1-2,3)+(3,3) \\
&= (-3,3)+(3,3) \\
&= (-(-3)-3,6) \\
&= (0,6)
\end{aligned}
$$

Hence, the axiom does not hold.

4.1 More examples of vector spaces

(1) K^n (ie R^n or C^n). See before

(2) $P(K)$ = polynomials, where coefficients are in K. Addition, scalar multiplication are "as expected", ie for multiplication:

$$
\begin{aligned}
f(x) &= x^2+2ix-4 \quad \in P(C) \\
g(x) &= -x^2+ix \quad \in P(C) \qquad\qquad \text{(and also in } P(R))
\end{aligned}
$$

For addition,

$$f(x)+g(x) = 3ix-4$$

And for scalar multiplication,

$$
\begin{aligned}
2if(x) &= 2ix^2+4i^2x-8i \\
&= 2ix^2-4x-8i
\end{aligned}
$$

(3) $P_n(K)$ = polynomials of degree n or less, coefficient from K. For example,

$$
\begin{aligned}
x^2-2x+2 &\in P_2(R) \\
x^2-2x+2 &\in P_3(R) \\
x^2-2x+2 &\in P_2(C) \\
x^2-2x+2 &\notin P_1(R)
\end{aligned}
$$

Note: In $P(K), P_n(K)$ the "vectors" are polynomials.

(4) $M_{m\times n}(K) = m\times n$ matrices with entries from K. Scalars are K, addition

and scalar multiplication as expected.

$$\begin{aligned}
A &= \begin{pmatrix} 2 & i \\ 0 & \pi \end{pmatrix} \in M_{2\times 2}(C) \\
B &= \begin{pmatrix} -2 & 1 \\ 1+i & -\pi \end{pmatrix} \in M_{2\times 2}(C) \\
A+B &= \begin{pmatrix} 0 & 1+i \\ 1+i & 0 \end{pmatrix} \\
2iA &= \begin{pmatrix} 4i & 2i^2 \\ 0 & 2i\pi \end{pmatrix} \\
&= \begin{pmatrix} 4i & -2 \\ 0 & 2\pi i \end{pmatrix}
\end{aligned}$$

The “zero vector” in $M_{m\times n}(K)$ is the $m \times n$ matrix with all entries 0.

(5) Let X be any set (think $x = R$ or C, but not required). Define $F(X, K) = \{f : X \to K\}$ = all functions from X to K.
Ex: $f(x) = x^2 \in F(R, R)$.
Ex: Let $x = \{1, 2\}$. Then g defined by

$$\begin{aligned}
g(1) &= 3 \\
g(2) &= \sqrt{2}
\end{aligned}$$

Addition in this space is defined by:
If $f, g \in F(X, K)$ then $f + g$ is the function defined by

$$(f + g)(x) = f(x) + g(x)$$

Note that $f(x) \in K$ and $g(x) \in K$, in other words they are *numbers* (scalars). The + in $(f + g)$ is the addition of vectors f and g, while the other + is scalar addition.
Scalar multiplication in this space is defined by: if $f \in F(X, K), c \in K$ then cf is the function defined by

$$(cf)(x) = cf(x)$$

Note that cf is the name of the function, that “multiplication” is scalar multiplication $F(X, \vDash)$ and $cf(x)$ is the multiplication of two scalars (numbers).
The fact that $F(X, K)$ is a vector space and the axioms are followed is not so obvious.
Prove (A2) true for $F(X, K)$**.** Define $z \in F(X, K)$ by

$$z(x) = 0 \qquad \text{(for all } x \in X)$$

Note that 0 here is a scalar. Then if $f \in F(X, K)$ is an arbitrary element, then we need to prove $f + z = f$. This is true since for all $x \in X$,

$$\begin{aligned}(f+z)(x) &= f(x) + z(x) \\ &= f(x) + 0 \\ &= f(x)\end{aligned}$$

Hence, $f+z, f$ have the same output (namely $f(x)$) for every input. Hence, $f + z = f$.
Exercise: Try (A3).

5 January 16th 2019

Theorem: ("Cancellation Law") Suppose v is a vector space over K. For all vectors $u, v, w \in V$, if $u + w = v + w$ then $u = v$.
Note: To prove "for all" you say let $u \in V$ (means u is an arbitrary vector).

To prove "if p then q", denoted $p \to q$, assume p is true and use it to prove q.

Proof. Let $u, v, w \in V$. Assume $u + w = v + w$. By vector space axiom A3, there is a vector $(-w) \in V$. Add $(-w)$ to both sides:

$$\begin{aligned}(u+w)+(-w) &= (v+w)+(-w) \\ u+(w+(-w)) &= v+(w+(-w)) && \text{(by A1)} \\ u+\vec{0} &= v+\vec{0} && \text{(by A3)} \\ &= u = v && \text{(by A2)}\end{aligned}$$

□

Theorem:

1. The zero vector is unique
2. For each $u \in V$, $-u$ is unique

Note: To prove something is unique, suppose you have two of them and show they are the same.

Proof. 1) Assume 0 and z both satisfy the property (A2: $\forall u \in V, u + 0 = u$ (*) and $u + z = u$ (**)). Goal is to prove $0 = z$.

$$\begin{aligned}z &= z + 0 && \text{(by *, with } u = z\text{)} \\ &= 0 + z && \text{(by A4)} \\ z &= 0 && \text{(by **, with } u = 0\text{)}\end{aligned}$$

So the zero vector is unique.

2) Exercise.

$\square$

Theorem: $\forall u \in V, c \in K$,

1) $c\vec{0} = \vec{0}$
2) $0u = \vec{0}$
3) $-(cu) = ((-c)u)$

Proof. Of 2). Let $u \in V$. Then,

$$
\begin{aligned}
0u + 0u &= (0+0)u && \text{(By SM2)} \\
0u + 0u &= 0u && \text{(by R addition)} \\
0u + 0u &= 0u + \vec{0} && \text{(by A2)} \\
0u + 0u &= \vec{0} + 0u && \text{(by A4)} \\
0u &= \vec{0} && \text{(by cancellation law)}
\end{aligned}
$$

$\square$

Note: $0 + u = u$ is true for all $u \in V$ (same as $u + 0 = u$ then apply A4)

5.1 Linear combinations and spans

Def: Let $u, v_1, v_2, \ldots, v_n \in V$. If there are scalars $a_1, a_2, \ldots, a_n \in K$ such that $u = a_1v_1, a_2v_2 \ldots a_nv_n$ then u is said to be a linear combination of $v_1, v_2, \ldots, v_n$.
Ex: In $P(R)$, $x^2 + 2x - 4$ is a linear comb of $x^2, x, 1$.

Important problem: Given vectors $u, v_1, v_2, \ldots, v_n$, determine if u is a linear combination of $v_1, v_2, \ldots, v_n$ and if so find $a_1, a_2, \ldots, a_n$.

Ex: Determine if $f(x) = 2x^2 + 6x + 8$ is a linear combination of

$$
\begin{aligned}
g_1(x) &= x^2 + 2x + 1 \\
g_2(x) &= -2x^2 - 4x - 2 \\
g_3(x) &= 2x^2 - 3
\end{aligned}
$$

Sol. Are there a_1, a_2, a_3 s.t.

$$
\begin{aligned}
2x^2 + 6x + 8 &= a_1(x^2 + 2x + 1) + a_2(-2x^2 - 4x - 2) + a_3(2x^2 - 3) \\
&= (a_1 - 2a_2 + 2a_3)x^2 + (2a_1 - 4a_2)x + (a_1 - 2a_2 - 3a_3)
\end{aligned}
$$

Equating coefficients,

$$
\begin{aligned}
a_1 - 2a_2 + 2a_3 &= 2 \\
2a_1 - 4a_2 &= 6 \\
a_1 - 2a_2 - 3a_3 &= 8
\end{aligned}
$$

Solve the linear system:

$$\left[\begin{array}{ccc|c} 1 & -2 & 2 & 2 \\ 2 & -4 & 0 & 6 \\ 1 & -2 & -3 & 8 \end{array}\right]$$
$$\downarrow$$
$$\left[\begin{array}{ccc|c} 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \qquad \text{(row reduce)}$$

$\therefore$ No solution, because of the last row. f is not a linear combination of g_1, g_2, g_3.

Def: Let $S \subseteq V$ (S is a subset fof V) and assume $s \neq 0$. The span of s, denoted $span(s)$ is the set of all linear combinations of vectors from S, ie

$$\begin{aligned} span(s) = \{u \in V |\ &\exists\ v_1, v_2, \ldots, v_n \in S \\ &\text{and scalars } a_1, a_2, \ldots, a_n \text{ s.t.} \\ &u = a_1v_1 + a_2v_2 + \ldots + a_nv_n\} \end{aligned}$$

6 January 18th 2019

6.1 Last class

$$\begin{aligned} S &\subseteq V \\ span(s) = \{u \in V |\ &\exists\ v_1, v_2, \ldots, v_n \in S \\ &\text{and scalars } a_1, a_2, \ldots, a_n \text{ s.t.} \\ &u = a_1v_1 + a_2v_2 + \ldots + a_nv_n\} \end{aligned}$$

Ex: $S = \{\binom{1}{2}, \binom{3}{1}\} \subseteq R^2$. Prove $span(S) = R^2$.
Note: $\binom{a}{b}$ means (a, b).
Proof note: To prove two sets A, B are equal, ie $A = B$, you can prove $A \subseteq B$ and $B \subseteq A$.
Sol:

(1) Prove $span(S) \subseteq R^2$. Trivial, since any linear combination of vectors in R^2 is still in R^2.

(2) Prove $R^2 \subseteq span(S)$. Let $\binom{a}{b} \in R^2$ (arbitrary). To prove that there exists scalars $x_1, x_2 \in K$ so that

$$\begin{pmatrix} a \\ b \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + x_2 \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

In other words,

$$\begin{aligned} a &= x_1 + 3x_2 \\ b &= 2x_1 + x_2 \end{aligned}$$

Want to show this has a solution (for all a, b). System is:

$$\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

But,

$$\begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} = 1 - 2(3) \neq 0$$

hence the system has (exactly one) solution. $\binom{a}{b} \in span(S)$ so $R^2 \subseteq span(S)$. So by (1), (2), $span(S) = R^2$. $\square$

Note: $Ax = b$, $A_{n\times n}$ if A inv, $x = A^{-1}b$.
Theorem: Let $S \subseteq V$, $S \neq \emptyset$ ($\emptyset$ = empty set). Then,

(1) If $u, v \in span(S)$ then $u + v \in span(S)$

(2) If $u \in span(S)$ and $c \in K$, then $cu \in span(S)$

(3) $\vec{0} \in span(S)$

Proof. By direct proof.

(1) (Note, "if $u, v \in span(S)$" means for all $u, v \in span(S)$).
Let $u, v \in span(S)$. Then,

$$u = a_1u_1 + a_2u_2 + \ldots + a_nu_n \text{ where } u_1, \ldots, u_n \in S, a_1, \ldots, a_n \in K$$
$$v = b_1v_1 + b_2v_2 + \ldots + b_mv_m \text{ where } v_1, \ldots, v_m \in S, b_1, \ldots, b_m \in K$$

Then $u + v = a_1u_1 + \ldots + a_nu_n + b_1v_1 + \ldots b_mv_m$ which is in $span(S)$ since $u_1, \ldots, u_n, v_1, \ldots, v_m \in S$.

(2) Let $u \in span(S), c \in K$. Then,

$$u = a_1u_1 + a_2u_2 + \ldots + a_nu_n \text{ where } u_1, \ldots, u_n \in S, a_1, \ldots, a_n \in K$$

So,

$$\begin{aligned} cu &= c(a_1u_1) + c(a_2u_2) + \ldots + c(a_nu_n) \\ &= (ca_1)u_1 + (ca_2)u_2 + \ldots (c_na_n)u_n \end{aligned}$$

Note: If you want to be very formal, you need to write down all of the vector space axioms. Which is in $span(S)$ since it is a linear combination of $a_1, \ldots, a_n$ which are in S.

(3) (Prove $\vec{0} \in span(S)$) Let $u \in S$. **Note**: This is possible only because $S \neq \emptyset$.
Then $u = 1u$, so $u \in span(S)$. Then using $c = 0$ and (2) and fact that $u \in span(S)$,
$$cu = 0u = \vec{0}$$
is also in $span(S)$. **Note:** Since $u = 1u$, $S \subseteq span(S)$.

□

6.2 Subspaces

Def. Let V be a vector space and $W \subseteq V$ (subset). If W, using addition and scalar multiplication as defined in V, satisfies the definition of vector space, then W is called a subspace of V, denoted $W \leq V$ (less than equal sign, read as "subspace").
Note: Main issue is that addition and scalar multiplication with vector from W produce vectors which are still in W.
Theorem: Let $W \subseteq V$. Then, if the following three properties hold, then $W \leq V$ (subspace).

(SS1) For all $w_1, w_2 \in W$, we have $w_1 + w_2 \in W$ ("closure under addition")

(SS2) For all $w \in W$ and scalars $c \in K$, we have $cw \in W$ ("closure under scalar multiplication")

(SS3) $\vec{0} \in W$.

These are the same properties we just proved for spans; in other words, we proved earlier that $span(S)$ is a subspace.

Proof. For W to have operatios addition, scalar multiplication, just means (SS1) and (SS2) are true. So now, check (A1) - (SM4). Most of them are true because they are true in a larger vector space.

(A1) Let $u, v, w \in W$. Then since $u, v, w \in V$, and (A1) holds in V, $u+(v+w) = (u+v)+w$.

(A2) This is (SS3).

(A3) This is the one we have to do a bit more work for. Let $w \in W$. Want to show $-w \in W$. Then, using (SS2) with $c = -1$ gives
$$-1(w) = -w \qquad \text{(thm from last class)}$$
is in W, as needed.

(A4) Still true because it is true in V.

(SM1-SM4) All hold because they hold in V.

□

7 January 21st 2019

7.1 A note on logic

Let P, Q be statements that are true or false.

(1) "If P then Q", also written symbolically as "$P \Rightarrow Q$" (P *implies* Q) means if P is true, then Q is also true. To *prove* "$P \Rightarrow Q$", assume P and prove Q is true. If you *know* that "$P \Rightarrow Q$" is true, you can *use it*: if you can establish that P is true, you may conclude Q is true.
Ex: Let A be an $n \times n$ matrix:

$$P : dot(A) = 1 \quad Q : \text{"A is invertible"}$$

Thm: $P \Rightarrow Q$

(2) The *converse* of "$P \Rightarrow Q$" is "$Q \Rightarrow P$". This is a (logically) different statement.
Ex: With P and Q as above, "$Q \Rightarrow P$" is not true because $A_{inv} \not\Rightarrow det(A) = 1$.

(3) The *contrapositive* of "$P \Rightarrow Q$" is "$\neg Q \Rightarrow \neg P$" ie "if Q false, then P also false". Logically, this is the same as "$P \Rightarrow Q$".

(4) The *equivalence* "P if and only if Q", written "$P \iff Q$" means "$P \Rightarrow Q$ and also $Q \Rightarrow P$" is true. Also means that either both P and Q are true or both are false.
Ex: $det(A) \neq 0 \iff$ A is invertible.
To prove "$P \iff Q$", need to prove "$P \Rightarrow Q$" and "$Q \Rightarrow P$".
Note: $\neg P \Rightarrow \neg Q$ is the same as $Q \Rightarrow P$.

7.2 Subspaces (cont'd)

Thm (last class): Let $W \subseteq V$ (*subset*). If

1. For all $u, v \in W$, $u + v \in W$
2. For all $u \in W$, $c \in K$, $cu \in W$
3. $\vec{0} \in W$

then $W \leq V$ (*subspace*). (ie: $(1), (2), (3)$ are true $\Rightarrow W \leq V$)
Thm. Let $W \subseteq V$. Then

$$W \leq V \Rightarrow (1), (2), (3) \text{ are true}$$

(ie the converse of last theorem is true).
Proof. Exercise.
Thm. Let $W \subseteq V$. Then

$$W \leq V \iff (1), (2), (3) \text{ are true}$$

7.3 Examples of subspaces and non-subspaces

Is each subset a subspace?

(a) $W = \{\binom{1}{2}, \binom{3}{1}\} \subseteq R^2$. Not a subspace, since the zero vector is not in W. The others are also false, but it's enough to prove that one of the statements does not hold. But $span(W) = R^2$ (so $span(W) \leq R^2$)

(b) $W = \{\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in R^3 | x + y - z = 0\}$. Need to check (1), (2), (3):

(1) Let $\begin{pmatrix} x \\ y \\ z \end{pmatrix}, \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \in W$. Then we know $x+y-z = 0$ and $x'+y'-z' = 0$. Check:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} x + x' \\ y + y' \\ z + z' \end{pmatrix}$$

Verify

$$\begin{aligned} (x + x') + (y + y') - (z + z') &= (x + y - z) + (x' + y' - z') \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

So yes, it is in W.

(2) Let $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in W$ (means $x + y - z = 0$), let $c \in K$. To prove

$$c \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} cx \\ cy \\ cz \end{pmatrix} \in W$$

Here, $cx + cy - cz = c(x + y - z) = c(0) = 0$. So $c \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in W$

(3) $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \in W$, since $0 + 0 - 0 = 0$

Since (1), (2), (3) true, $W \leq R^2$ (subspace)

(c) $W = \{\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in R^3 | x + y - z = 1\}$. This is *not* a subspace. (3) is false.

(d) $W = \{A \in M_{2\times 2} | A_{ij} \geq 0 \forall i,j\}$, where A_{ij} is the entry of A in row i, column j. (1) and (3) are true:

(1) Add two matrices with non-negatives entries, result has non-negative entries.

(2) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in W$

Note, we wrote these out very informally. Now, (2) is false since, for example $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in W$ but

$$(-1)\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} \notin W$$

7.4 Two special subspaces

Let V be a vector space.

(1) $V \leq V$ is true

(2) $\{\vec{0}\} \leq V$ is true ("zero subspace")

7.5 A refinement on the definition of span

Def. If $S = \emptyset$ (emptyset), define $span(S) = \{\vec{0}\}$ (if $S \neq \emptyset$, $span(S)$ defined as before).
Thm. $span(S) \leq V$.
Proof Two cases :

1. If $S = \emptyset$, $span(S) = \{\vec{0}\} \leq V$
2. If $S \neq \emptyset$, you already proved $span(S)$ satisfies (1), (2), (3).
   So $span(S) \leq V$.

Thm. (improved version of subspace conditions) Let $W \subseteq V$. Then

$$\begin{aligned} W \leq V \iff & W \neq \emptyset \text{ and} \\ & \forall w_1, w_2 \in W \text{ and } c \in K \text{ we have } cw_1 + w_2 \in W \end{aligned}$$

Proof We will actually prove $(1),(2),(3) \iff RHS$ (right-hand side). Two parts to proof.

(1) "$(1),(2),(3) \Rightarrow RHS$" or "$\Rightarrow$"

8 January 23rd 2019

Recap:

(1) If $u, v \in W$ then $u + v \in W$

(2) if $u \in W, c \in K$ then $cu \in W$

(3) $\vec{0} \in W$

Theorem: Let $W \subseteq V$. Then

$$W \leq V \iff W \neq \emptyset \text{ and } \forall u, v \in W, c \in K \text{ we have } cu + v \in W$$

Proof: Suffices to prove $(1), (2), (3) \iff RHS$.

1. $\Rightarrow$ Assume $(1), (2), (3)$ (prove right-hand side). Two things to prove:
   (1) Since $\vec{0} \in W$ (by (3)), $W \neq \emptyset$
   (2) Let $u, v \in W$ and $c \in K$. Since (2) holds, $cu \in W$. Since (1) holds, $cu \in W$ and $v \in W$, so $cu + v \in W$.

2. $\Leftarrow$ Assume RHS, prove (1), (2), (3).
   (1) Let $u, v \in W$. Apply RHS with $\Leftarrow$ to get

   $$cu + v = 1u + v = u + v \in W$$

   (2) (Prove $\vec{0} \in W$) Since $W \neq \emptyset$, there is a vector $w \in W$. Apply right-hand side with $u = w$, $v = w$, $c = -1$. So $cu + v = (-1)w + w = -w + w = \vec{0} \in W$.
   (3) Let $u \in W, c \in K$. Apply RHS ($cu + v \in W$) with $u = u$, $c = c$, $v = \vec{0}$ (note: $\vec{0} \in W$ by (3) above). Then $cu + v = cu + \vec{0} = cu \in W$ $\square$

Ex: In $F(R, R) = V$ (functions $f : R \to R$), prove that

$$W = \{f \in V | f(3) = 0\}$$

is a subspace. Eg: $f(x) = (x - 3)e^x \in W$.
Solution: (1), (2) together (by last thm). Let $f, g \in W, c \in R$ (prove $cf + g \in W$). We know $f(3) = 0$ and $g(3) = 0$. Then, check $(cf + g)(3) = cf(3) + g(3) = 0 + 0 = 0$. So $cf + g \in W$.

Also, prove $w \neq \emptyset$. $f(x) = x - 3 \in W$, since $f(3) = 0$ (or, $z(3) = 0$ satisfies $z(3) = 0$ so $z \in W$. Note that z is he zero vector of $F(R, R)$).

Theorem: Let $A \in M_{m \times n}(K), b \in K^m$. Define

$$S = \{x \in K^n | Ax = b\}$$

ie $S =$ solution set to linear system $Ax = b$. Then,

$$S \leq K^n \iff b = \vec{0} \text{ (ie system is homogeneous)}$$

Proof

(i) $\Rightarrow$ Assume $S \leq K^n$. Then $\vec{0}_n \in S$ (by (3)). So $A\vec{0} = b$ but $A\vec{0}_n = \vec{0}_m$ so $\vec{0} - b$.

(ii) $\Leftarrow$ Assume $b = \vec{0}_m$ (prove $S \leq K^n$). Then $A\vec{0}_n = \vec{0}_m$, so $\vec{0}_n \in S$. Next, let $u, v \in S, c \in K$. So $u, v \in K^n$ and $Au = b, Av = b$. Verify $cu + v$ is a solution.

$$\begin{aligned}
A(cu+v) &= A(cu) + Av && \text{(prop of matrix multiplication)}\\
&= c(Au) + Av && \text{(prop of matrix multiplication)}\\
&= cb + b\\
&= c\vec{0} + \vec{0}\\
&= \vec{0}\\
&= b \quad \square
\end{aligned}$$

Ex: Equation $ax + by + cz = d$ describes a plane in R^3 (eg $x + y + z = 1$) (and also, every plane can be described this way). That is,

$$\{(x, y, z) \in R^3 | ax + by + z = d\}$$

is a plane.

By last thm,

$$\begin{aligned}
P \text{ is a subspace } &\iff ax + by + cz = d \text{ is a homogeneous system}\\
&\iff d = 0\\
&\iff P \text{ passes through origin } (0, 0, 0)
\end{aligned}$$

Theorem: Let $S \subseteq V$. Then,

(1) $span(S) \leq V$ and $S \subseteq span(S)$

(2) If $S \subseteq W$, and $W \leq V$ (subspace) then $span(S) \subseteq W$ (actually, $span(S) \leq W$, subspace by (1))

Proof:

(1) $\leq$ We know already. Let $u \in S$. Then $u = 1u$, so $u \in span(S)$

(2) Assume $S \subseteq W$, and $W \leq V$. Let $v \in span(S)$. Then $v = a_1u_1 + a_2u_2 + \ldots + a_nu_n$ for some scalars and vectors $u_1, u_2, \ldots, u_n \in S$. Since $S \subseteq W$, $u_1, u_2, \ldots, u_n \in W$. But W subspace. So $a_1u_1, a_2u_2, \ldots, a_nu_n \in W$ (by prop (2) subspace) then $a_1u_1 + a_2u_2 \in W$ (by prop (1) of subspaces). So then $(a_1u_1 + a_2u_2) + a_3u_3 \in W$ (etc). So $a_1u_1 + a_2u_2 + \ldots + a_nu_n \in W$. **Note:** "etc" here is actually a proof by mathematical induction. Omit for now.

9 January 25th 2019

9.1 Interlude : Symbolic logic (briefly)

Let P, Q be statements that could be true (T) or false (F). Define:

(1) $\neg P$, "not P", is F when P is T, T when P is F

(2) $P \wedge Q$, "P and Q", is T exactly when P, Q both T

(3) $P \vee Q$, "P or Q" is T when P, Q both F

(4) $P \Rightarrow Q$, "P implies Q", is T *unless* P is T and Q is F. Hence, $P \Rightarrow Q$ is *equivalent to* $\neg P \vee Q$. We will write $P \Rightarrow Q \equiv \neg P \vee Q$.

(5) $P \iff Q$, "P if and only if Q", is T if both T or both F.

9.1.1 De Morgan's Laws

- $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
- $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$

9.1.2 Quantifiers

- $\forall$ means "for all"
- $\exists$ means "there exists"

Ex. (A4) (commutativity) $\forall u, v \in V \quad u + v = v + u$.
Ex. 2 (A2) (zero vector) $\exists z \in V \quad \forall u \in V \quad (u + z = u) \wedge (z + u = u)$ (textbook version)

9.1.3 Negating quantifiers

- $\neg \forall u \in V P(u) \equiv \exists u \in V \neg P(u)$
- $\neg \exists u \in V P(u) \equiv \forall u \in V \neg P(u)$

Ex.

$$\begin{aligned}
\neg(A2) &\equiv \neg \exists z \in V \forall u \in V \quad u + z = u \wedge z + u = u \\
&\equiv \forall z \in V \neg \forall u \in V \quad u + z = u \wedge z + u = u \\
&\equiv \forall z \in V \exists u \in V \quad \neg(u + z = u \wedge z + u = u) \\
&\equiv \forall z \in V \exists u \in V \quad (u + z \neq u \vee z + u \neq u)
\end{aligned}$$

9.1.4 Proof by contradiction

You want to prove some statement P. Proof by contradiction works this way:

(1) Assume $\neg P$

(2) Derive a contradiction (hard part)

(3) Conclude P is true

Ex. Outline of how to prove (A2) *does not hold* in some vector space. You want to prove $\neg(A2)$.

$$\begin{aligned}\neg(A2) &\equiv \neg\exists z \in V\ \forall u \in V \quad u+z=u \wedge z+u=u \\ &\equiv \forall z \in V \neg\forall u \in V \quad u+z=u \wedge z+u=u\end{aligned}$$

Let $z \in V$. Prove the right-hand part ($\neg\forall u \in V \quad u+z=u \wedge z+u=u$) by contradiction. Assume (for contradiction) that

$$\forall u \in V \quad u+z=u \wedge z+u=u \tag{1}$$

Use (1) by substituting $u =$ some specific vector (derive a contradiction). Conclude that ($\neg\forall u \in V \quad u+z=u \wedge z+u=u$) is true.

9.2 Last time

Thm. If $S \subseteq W$, $W \leq V$ then $span(S) \subseteq W$.
Note. This means if you "promote" a subset to a subspace, adding in only what's necessary, what you get is $span(S)$. Or, $span(S)$ is the "smallest" subspace containing S.
Fact. Subspaces are "closed under taking linear combinations". Ie if $W \leq V$, $w_1, \dots, w_n \in W$ and $a_1, \dots, a_n \in K$ then

$$a_1w_1 + a_2w_2 + \ldots + a_nw_n \in W$$

Caution. Linear combinations are *finite* sums by definition. So you can't sum up infinitely many vectors.

9.3 Illustration of this theorem

Let $S = \{\begin{pmatrix}1\\2\\0\end{pmatrix}, \begin{pmatrix}1\\3\\0\end{pmatrix}, \begin{pmatrix}2\\4\\0\end{pmatrix}\} \subseteq W = \{\begin{pmatrix}x\\y\\0\end{pmatrix} |x, y \in R\}$. Then $span(S) \subseteq W$ ie $span(S)$ is in xy plan. In fact, $span(S) = W$.

Def. If $W = span(S)$, we say that S spans W or is a spanning set for W.
Ex. $S = \{\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}\}$, $span(S) =$ xy-plane in R^3. So S spans the xy-plane.
Ex. 2. $S = \begin{pmatrix}1\\1\\0\end{pmatrix}\}$, $span(S) = \{\begin{pmatrix}x\\x\\0\end{pmatrix} |x \in R\} =$ line.

9.4 Intersection of two subspaces

Theorem Let $W_1 \leq V, W_2 \leq V$. Then $W_1 \cap W_2 \leq V$ (ie intersection of two subspaces is a subspace).
Proof. $W_1 \cap W_2 = \{w \in V | w \in W_1 \wedge w \in W_2\}$.

(1) $\vec{0} \in W_1, \vec{0} \in W_2$ (because subspace). So $\vec{0} \in W_1 \cap W_2$.

(2) Let $u, v \in W_1 \cap W_2, c \in K$. So $u, v \in W_1$ and $W_1 \in V$ so $cu + v \in W_1$ and $u, v \in W_2$ and $W_2 \in V$ so $cu + v \in W_2$. Hence $cu + v \in W_1 \cap W_2$. $\square$

10 January 28th 2019

Last time: $W_1 \leq V$ and $W_2 \leq V \Rightarrow W_1 \cap W_2 \leq V$.
Corollary: The intersection of any number of subspaces is a subspace.

Problem. Prove that $W = \{f : \mathbb{R} \to \mathbb{R} | f(1) = 0 \wedge f(2) = 0\}$ is a subspace of $F(\mathbb{R}, \mathbb{R})$.
Sol #1: Directly from subspace properties (omit)
Sol #2: We saw an example proving that $\{f : \mathbb{R} \to \mathbb{R} | f(3) = 0\}$ is a subspace. The "3" is not important, so similarly:

$$W_1 = \{f : \mathbb{R} \to \mathbb{R} | f(1) = 0\}$$
$$W_2 = \{f : \mathbb{R} \to \mathbb{R} | f(2) = 0\}$$

both subspaces of $F(\mathbb{R}, \mathbb{R})$. Then $W_1 \cap W_2 = \{f : \mathbb{R} \to \mathbb{R} | f(1) = 0 \wedge f(2) = 0\}$ is a subspace.

Q: Is union of two subspaces also a subspace?
A: Not in general.
Eg: $W_1 =$ x-axis $= \{\binom{x}{0} | x \in \mathbb{R}\} \leq \mathbb{R}^2$
$W_2 =$ y-axis $= \{\binom{0}{y} | y \in \mathbb{R}\} \leq \mathbb{R}^2$
$W_1 \cup W_2 =$ xy-axis $= \{\binom{x}{y} | x = 0 \vee y = 0\}$, which, importantly, is not $\mathbb{R}^2$. *Not* a subspace, since $\binom{1}{0} \in W_1 \cup W_2$, $\binom{0}{1} \in W_1 \cup W_2$, but $\binom{1}{1} = \binom{1}{0} + \binom{0}{1} \notin W_1 \cup W_2$.
Note: To promote $W_1 \cup W_2$ to a subspace, you form $span(W_1 \cup W_2)$.

Def: Let $W_1 \leq V$m $W_2 \leq V$. The *sum* of W_1 and W_2 is

$$W_1 + W_2 = \{v \in V | \exists w_1 \in W_1, w_2 \in W_2, \text{ such that } v = w_1 + w_2\}$$

Ex:

$$W_1 = \{ax^2 | a \in \mathbb{R}\} \leq P(\mathbb{R})$$
$$W_2 = \{ax | a \in \mathbb{R}\} \leq P(\mathbb{R})$$

We have,

$$W_1 + W_2 = \{ax^2 + bx | a, b \in \mathbb{R}\}$$

Theorem: Let $W_1 \leq V$, $W_2 \leq V$. Then

(a) $W_1 + W_2 = span(W_1 \cup W_2)$ (hence $W_1 + W_2$ is a subspace)

(b) $W_1 \leq W_1 + W_2$, $W_2 \leq W_1 + W_2$

Proof:

(a) (1) Prove $W_1 + W_2 \subseteq span(W_1 \cup W_2)$. Let $v \in W_1 + W_2$, so $v = w_1 + w_2$ where $w_1 \in W_1$ and $w_2 \in W_2$. Then $w_1, w_2 \in W_1 \cup W_2$ so $v \in span(W_1 \cup W_2)$

(2) "$\supseteq$". Let $v \in span(W_1 \cup W_2)$. Means $v = a_1u_1 + a_2u_2 + \ldots a_nu_n, u_1, u_2, \ldots, u_n \in W_1 \cup W_2$ and $a_1, a_2, \ldots, a_n \in K$. Each u_i is in $W_1 \cup W_2$. Separate into two groups and relabel, so that:

- Those in W_1, call these

$$u_1, u_2, \ldots u_l$$

So $0 \leq l \leq n$, $l = 0$ means *none* in W_1.

- Those in $W_2 \backslash W_1 = \{w \in W_2 | w \notin W_1\}$ ("set difference"), call these

$$u_{l+1}, \ldots, u_n$$

So $l = 0$ means all in $W_2 \backslash W_1$, $l = n$ means all in W_1.

Then, let $w_1 = a_1u_1 + a_2u_2 + \ldots + a_lu_l$ (or $w_1 = \vec{0}$ if $l = 0$), $w_2 = a_{l+1}u_{l+1} + \ldots + a_nl_n$ (or $w_2 = \vec{0}$ if $l = n$).
Then $w_1 \in W_1$ since W_1 is a subspace, similarly $w_2 \in W_2$. So

$$\begin{aligned} v &= a_1u_1 + \ldots + a_nu_n \\ &= w_1 + w_2 \in W_1 + W_2 \text{ as required} \end{aligned}$$

(b) $W_1 \leq W_1 + W_2$, $W_2 \leq W_1 + W_2$. Follows from (a), since $S \subseteq span(S)$ $\square$.

10.1 Linear independence

Def: Vectors $u_1, u_2, \ldots, u_n \in V$ (all distinct) are said to be *linearly dependent* if $\exists$ scalars $a_1, a_2, \ldots, a_n \in K$ *not all 0* such that

$$a_1u_1 + a_2u_2 + \ldots + a_nu_n = \vec{0}$$

Above equation called a *dependence relation.*
Note: If $a_1u_1 + a_2u_2 + \ldots + a_nu_n = \vec{0}$ and $a_1 \neq 0$, then you can solve for u_1:

$$u_1 = \frac{-a_2}{a_1}u_2 - \frac{a_3}{a_1}u_3 - \ldots - \frac{a_n}{a_1}u_n$$

ie u_1 = linear combination of others, "depends on" others.
Ex: $\{x^2 + x, 2x^2, \frac{x}{10}\}$ is a dependent set of vectors in $P(\mathbb{R})$ since

$$(x^2 + x) - \frac{1}{2}(2x^2) - 10(\frac{x}{10}) = 0$$

Def: A set of vectors $S \subseteq V$ (possibly infinite) is dependent if $\exists$ a finite subset $\{v_1, v_2, \ldots, v_n\} \subseteq S$ of it which is dependent.

Def: Vectors $v_1, v_2, \ldots, v_n$ are linearly independent if they are *not* dependent. That is,

$$\begin{aligned} \neg\exists a_1, \ldots, a_n \in K \quad & (a_1 u_1 + \ldots + a_n u_n = \vec{0} \wedge \neg(a_1 = 0 \wedge a_2 = 0 \wedge \ldots \wedge a_n = 0)) \\ \forall a_1, \ldots, a_n \in K \quad & \neg(a_1 u_1 + \ldots + a_n u_n = \vec{0} \wedge \neg(a_1 = 0 \wedge a_2 = 0 \wedge \ldots \wedge a_n = 0)) \\ \forall a_1, \ldots, a_n \in K \quad & (\neg(a_1 u_1 + \ldots + a_n u_n = \vec{0}) \vee (a_1 = 0 \wedge a_2 = 0 \wedge \ldots \wedge a_n = 0)) \end{aligned}$$

Note that $P \implies Q \equiv \neg P \vee Q$. In other words, $u_1, u_2, \ldots, u_n$ are linearly independent if

$$\forall a_1, \ldots, a_n \in K(a_1 u_1 + \ldots + a_n u_n = \vec{0} \implies a_1 = 0 \wedge \ldots \wedge a_n = 0)$$

Which is to say that the only solution to $a_1 u_1 + \ldots a_n u_n = \vec{0}$ is the trivial solution $a_1 = 0, a_2 = 0, \ldots, a_n = 0$.

11 January 30th 2019

11.1 Last class

$v_1, v_2, \ldots, v_n$ *independent* if $x_1 v_1 + \ldots + x_n v_n = \vec{0}$ has only trivial solution $x_1 = x_2 = \ldots = x_n = 0$.
Ex: Prove that $\{1 + x^2, x + x^2, 1 + x + x^2\}$ is independent.
Solution: Consider equation

$$a(1 + x^2) + b(x + x^2) + c(1 + x + x^2) = 0 = 0(1) + 0x + 0x^2$$

Want to show $a = b = c = 0$ is the only solution.
Equation means for all $x \in K$ ($\mathbb{R}$ or $\mathbb{C}$),

$$a(1 + x^2) + b(x + x^2) + c(1 + x + x^2) = 0$$

So, substitute any scalar for x:

$$\begin{aligned} x = 0 \quad & a + c = 0 \\ x = 1 \quad & 2a + 2b + 2c = 0 \\ x = -1 \quad & 2a + 0b + c = 0 \end{aligned}$$

Can translate into linear system:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & 3 & 0 \\ 2 & 0 & 1 & 0 \end{pmatrix}$$

Row-reduce:

$$\begin{aligned} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & 3 & 0 \\ 2 & 0 & 1 & 0 \end{pmatrix} &\to \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix} \\ &\to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

Only solution is $a = 0$, $b = 0$, $c = 0$ so vectors are independent. If we obtain infinitely many, then you can find dependent set so dependent.

11.2 Some important cases

(i) $S = \emptyset$ is linearly independent since there are no vectors with which to form a dep. relation.

(ii) If $\vec{0} \in S$, then dependent (since $1\vec{0} = \vec{0}$ *is* a dep. relation)

(iii) $\{u\}$ is independent $\iff u \neq \vec{0}$.
Note: $u + (-1)u = \vec{0}$ is *not* a dep. elation, since u is repeated. But, $\{u, -u\}$ is dependent since

$$u + (-u) = \vec{0}$$

is a dep. relation.

Proposition: Let $A, B \subseteq V$ where $A \subseteq B$.

(i) If A is dependent, B is also dependent

(ii) If B is independent, A is also independent (contrapositive)

Proof:

(i) If A dep, we have a dep relation

$$a_1v_1 + a_2v_2 + \ldots + a_nv_n = \vec{0} \qquad \text{(not all scalars 0, } v_1, \ldots, v_n \in A)$$

which is also a dependence relation in B since $v_1, \ldots, v_n \in B$.

(ii) This is the contrapositive of (i). $\square$

Note: Converse is false, B *dep* $\not\to$ A *dep*.

11.3 Extending an independent set

Theorem: Let $S \subseteq V$ be linearly independent and suppose $u \notin S$. Then, $S \cup \{u\}$ independent $\iff u \notin span(S)$.
Proof:

(i) "$\rightarrow$" We will prove this as the contrapositive, ie $u \in span(S) \rightarrow dep$. Assume $u \in span(S)$. So,

$$\begin{aligned} u &= a_1v_1 + \ldots + a_nv_n \quad \text{where } v_1, v_2, \ldots, v_n \in S \\ \vec{0} &= (-1)u + a_1v_1 + \ldots + a_nv_n \end{aligned}$$

Which is a linear combination of vectors from $S \cup \{u\}$, not all coefficients 0 since first is -1. Also, the vectors $u, v_1, v_2, \ldots, v_n$ are all distinct, since $u \notin S$. So this is a dependence relation on $S \cup \{u\}$, so the set is dependent.

(ii) "$\leftarrow$" Also by contrapositive. Assume $S \cup \{u\}$ dep, want to show that $u \in span(S)$. So there is a dependence relation on $S \cup \{u\}$. Two cases:

- **Case 1:** Dependence relation does not involve u (or, involves u but with coefficient 0), ie we have

$$a_1v_1 + \ldots + a_nv_n = \vec{0} \qquad \text{(not all scalars 0, } v_1, \ldots, v_n \in S)$$

  But this contradicts independence of S, so case 1 does not occur.

- **Case 2:** Dependence relation involves u (with coeff *not* 0), so

$$au + a_1v_1 + \ldots + a_nv_n = \vec{0} \quad v_1, \ldots v_n \in S$$

  and $a \neq 0$. Rewrite:

$$u = \frac{-a_1}{a}v_1 - \frac{a_2}{a}v_2 - \ldots - \frac{a_n}{a}v_n \qquad (a \neq 0)$$

  Hence $u \in span(S)$. $\square$

Note: Conclusion can be restated as

$$S \cup \{u\} \textit{ dependent} \iff u \in span(S)$$

11.4 Basis and dimension

Fact: If W is subspace, then $span(W) = W$. (Exercise)
So every subspace *is* a span. But thinking of W as $span(W)$ is excessive. Would like to find the *smallest* S such that

$$span(S) = W$$

Def: Let $W \leq V$. A *basis* of W is a set $B \subseteq V$ such that

(i) $span(B) = W$ ("enough vectors to produce W")

(ii) B is linearly independent ("no extra vectors in B")

Examples:

(i) Let $e_i = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \leftarrow (row\ i)$. Then,

$$\{e_1, e_2, \ldots, e_n\}$$

is a basis for K^n. For example,

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

is a basis for K^3.

More next class.

12 February 1st 2019

Recall: B is a basis of W if $span(B) = W$ and B is linearly independent.
Examples:

(1) $P_n(K)$ has basis $\{1, x, x^2, \ldots, x^n\}$

(2) $P(K)$ has basis $\{1, x, x^2, x^3, \ldots\}$ (infinitely many)

(3) $M_{m\times n}(K)$ has basis $\{E^{ij} | 1 \leq i \leq m, 1 \leq j \leq n\}$ where $E^{ij} = m \times n$ matrix of 0s except 1 in row i, column j. eg: $M_{2\times 2}(\mathbb{R})$ has basis

$$E^{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E^{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E^{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, E^{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

(4) $W = \{\vec{0}\}$ has basis $\emptyset$ since

  (i) span $\emptyset = \{\vec{0}\}$ (by special def)

  (ii) $\emptyset$ is independent

12.1 Two important questions

(1) Does W *always* have basis ? (spoiler: yes)

(2) How to *find* a basis?

Theorem ("bases exist") Let V be vector space and S a *finite* set with $span(S) = V$. Then there is a subset $B \subseteq S$ which is a basis of V.

Proof. Algorithm to produce B.

(1) If $V = \{\vec{0}\}$, use $B = \emptyset$.

(2) Take one vector, $u_1 \in S(u_1 \neq \vec{0})$. Consider $span\{u_1\}$

(3) If $span\{u_1\} = V$, done. $B = \{u_1\}$ is a basis (set of one non-zero vector is independent)

(4) If $span\{u_1\} \neq V$, there must be a vector $u_2 \in S$ where $u_2 \notin span(\{u_1\})$ (Why? If not, $S \subseteq span(\{u_1\}) \leq V$, then $span(S) \subseteq span\{u_1\}$, but $span(S) = V$ contradicts $V \neq span\{u_1\}$). By previous theorem, since $u_2 \notin span\{u_1\}$, $\{u_1, u_2\}$ is linearly independent.

(5) Consider $\{u_1, u_2\}$. If $span\{u_1, u_2\} = V$, done: $B = \{u_1, u_2\}$. Else, continue as before, finding $u_3 \in S$, $u_3 \notin span\{u_1, u_2\}$ (etc)

Since S is *finite*, this must *stop* and at that point you have basis $B \subseteq S$. $\square$

12.2 Illustration of this thm

Find basis of $\mathbb{R}^3$ that is a subset of

$$\left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} \right\}$$

Following this algorithm,

$$u_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad u_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad u_3 = \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}$$

Theorem Let V be a vector space, $L \subseteq V$ a linearly indepedent set, and $S \subseteq V$ a spanning set (ie $V = span(S)$). Then $\exists$ a subset $E \subseteq S$ such that $L \cup E$ is a basis of V (ie you can always *extend* it to a basis)
Proof Omitted.
Theorem Suppose V has a finite spanning set S. Then V has a basis and all bases have the same size, which is at most $|S|$.
Proof Omitted.
Def If V has a finite basis B, then the *dimension* of V is

$$dim\ V = |B|$$

If V does not have a finite basis, it is called *infinite dimensional.*
Ex:

(1) $dim\ K^n = n$.

$$\left(\left\{\begin{pmatrix}1\\0\\\dots\\0\end{pmatrix},\begin{pmatrix}0\\1\\\dots\\0\end{pmatrix},\dots,\begin{pmatrix}0\\0\\\dots\\1\end{pmatrix}\right\}\right)$$

(2) $dim\ P_n(K) = n+1$ (basis $\{1, x, x^2, \dots, x^n\}$)

(3) $P(K)$ is infinite dimensional (A#1, proved a finite set of polynomials cannot span $P(K)$)

(4) $dim\ M_{m\times n}(K) = mn$ (see basis E^{ij}, defined above)

Theorem *Every* vector space (including the infinite dimensional ones) has a basis.
Proof Uses Axiom of Choice. Difficult.
Theorem Suppose $dim\ V = n$. Let $A \subseteq V$. Then,

(1) If $span(A) = V$, then $|A| \geq n$ (or, if $|A| < n$ then A does not span V) and if also $|A| = n$ then A *is* linearly independent, hence basis.

(2) If A is linearly independent, then $|A| \leq n$ (or, if $|A| > n$ then A dep) and if also $|A| = n$ then $span(A) = V$ hence A is a basis.

Proof Omitted.
Note: If you have *correct number* of vectors, you need only check spanning or independent, not both, to check if basis.
Ex: If you have 7 matrices in $M_{3\times 2}(K)$, they *will be* dependent. If you have 5, it's *not* a basis.

13 February 4th 2019

13.1 Last class

Suppose $dim\ V = n$, $S \subseteq V$, $|S| = n$. Then S *span* $V \iff S$ linearly independent (only in case $|S| = dim\ V$).

13.2 Lagrange Interpolation

Problem Given "data points" $(a_1, b_1), (a_2, b_2), \dots, (a_n, b_n)$ where all a_i are different. Find a polynomial $p(x)$ of degree $n-1$, $p(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \dots + c_1x + c_0$ whose graph $y = p(x)$ passes through all the points.
Sol #1 Substitute (a_1, b_1) into $y = p(x)$:

$$b_1 = c_{n-1}a_i^{n-1} + \dots + c_1a_i + c_0 \qquad \text{(for each } i = 1, \dots, n)$$

Which is a system of n linear equations (vars $= c_{n-1}, \dots, c_0$) in n variables. We'll do something different.

Def For scalars $a_1, a_2, \dots, a_n$ (all different), define the *Lagrange polynomials* for each $i = 1, 2, \dots, n$ set

$$\begin{aligned} l_i(x) &= \prod_{k=1, k\neq i}^{n} \frac{(x-a_k)}{(a_i-a_k)} \\ &= \frac{(x-a_1)}{(a_i-a_1)} \cdot \frac{(x-a_2)}{(a_i-a_2)} \cdot \ldots \cdot \frac{(x-a_n)}{a_i-a_n} \qquad \left(\text{omitting } \tfrac{(x-a_i)}{(a_i-a_i)}\right) \end{aligned}$$

Ex For $a_1 = 2, a_2 = 4, a_3 = 6$ we would have

$$\begin{aligned} l_1(x) &= \frac{(x-4)}{2-4} \cdot \frac{(x-6)}{(2-6)} \\ l_2(x) &= \frac{(x-2)}{4-2} \cdot \frac{(x-6)}{(4-6)} \\ l_3(x) &= \frac{(x-2)}{6-2} \cdot \frac{(x-4)}{(6-4)} \end{aligned}$$

Note: All degree 2, $l_1(4) = 0$, $l_1(6) = 0$, $l_1(2) = 1$.
Fact $l_i(a_j) = 0$ if $i \neq j$ and 1 if $i = j$.
Proof If $i \neq j$, there is a factor $\frac{x-a_j}{a_i-a_j}$, so at $x = a_j$, $\frac{a_j-a_j}{a_i-a_j} = 0$. If $i = j$,

$$l_i(a_i) = \prod_{k=1, k\neq i}^{n} \frac{(a_i-a_k)}{(a_i-a_i)} = 1$$

Proposition Lagrange polynomials $l_1(x), \dots, l_n(x)$ form a basis of $P_{n-1}(\mathbb{R})$.
Proof We have n polunomials (they *are* distinct), *dim* $P_{n-1}(\mathbb{R}) = n-1+1 = n$. So correct number. Suffices to prove *span* or lin independence. We'll prove independence. Suppose

$$d_1 l_1(x) + d_2 l_2(x) + \ldots + d_n l_n(x) = 0 \qquad (\text{note: for } \textit{all } x \in \mathbb{R})$$

Substitute $x = a_1$, $x = a_2$, etc into the above. At $x = a_1$, $l_1(a_1) = 1$ but $l_j(a_1) = 0$ for $j \neq 1$ so

$$d_1 1 + d_2 0 + \ldots + d_n 0 = 0$$

so $d_1 = 0$. Similarly, $d_j = 0$ for all j. More formally, for any $j = 1, 2, \dots, n$ we have at $x = a_j$

$$\sum_{i=1}^{n} d_i l_i(a_j) = 0$$

but all terms are 0 *except* when $i = j$. Set

$$d_j = d_j(1) = d_j l_j(a_j) = 0$$

Hence Lagrange polynomials for a basis.
Problem Find poly degree $n-1$ through points $(a_1, b_1), \ldots, (a_n, b_n)$.
Sol: Set $p(x) = b_1 l_1(x) + b_2 l_2(x) + \ldots + b_n l_n(x)$ (it has degree $n-1$). Then

$$\begin{aligned} p(a_1) &= b_1 l_1(a_1) + b_2 l_2(a_1) + \ldots + b_n l_n(a_1) \\ &= b_1(1) + 0 + 0 + \ldots + 0 \\ &= b_1 \end{aligned}$$

For each $i = 1, 2, \ldots, n$,

$$\begin{aligned} p(a_i) &= \sum_{j=1}^{n} b_j l_j(a_i) \\ &= 0 + 0 + \ldots + b_i l_i(a_i) + \ldots + 0 \\ &= b_i \end{aligned}$$

13.3 Dimension of subspaces

Theorem 20: Let $W \leq V$, V finite-dimensional. Then

(i) $\mathit{dim}\ W \leq \mathit{dim}\ V$

(ii) $\mathit{dim}\ W = \mathit{dim}\ V \iff W = V$

Proof

(i) Similar to proof that V has basis. Use W as a spanning set for W. Pick out vectors one at a time (similar to before) to build a basis. You cannot put more than $\mathit{dim}\ V$ vectors into your basis, as this would give an independent set in V of size *more than* $\mathit{dim}\ V$ (impossible). So this process has to stop, and it produces a basis for W.

(ii) "$\rightarrow$" Assume $\mathit{dim}\ W = \mathit{dim}\ V = n$. Take basis B of W. It is a size n linearly independent set inside V, hence B also basis for V, hence,

$$V = \mathit{span}\ B = W$$

"$\leftarrow$" If $W = V$, clearly $\mathit{dim}\ W = \mathit{dim}\ V$. □

Subspaces of $\mathbb{R}^3$ If $W \leq \mathbb{R}^3$, $\mathit{dim}\ W = 0, 1, 2$ or 3.
This allows us to make the following classification:

$\mathit{dim}\ W$	Classification
0	$\{\vec{0}\}$
1	$\mathit{span}\{u\}$ = line through origin
2	$\mathit{span}\{u, v\}$ = plane through origin
3	$\mathbb{R}^3$

Problem Let $W = \{A \in M_{n\times n}(\mathbb{R}) | tr(A) = 0\}$, where $tr(A)$ = trace of A = sum of entries on diagonal $= A_{11} + A_{22} + \ldots + A_{nn}$.
Exercise Prove W is a subspace.
Will do next class: Find $dim\ W$ and find a basis of W.

14 February 6th 2019

14.1 Intuition

Solution set W to a homogeneous system $A\vec{x} = \vec{0}$ is a subspace of K^n(n = # of variables). If no equations, $W = K^n$, $dim\ W = n$. For each equation, *expect* the dimension of W to drop by 1, unless the equation is *redundant*.
Eg: In $\mathbb{R}^3$, one equation

$$\begin{aligned} a_1x + b_1y + c_1z &= 0 && (= \text{plane}) \\ \textbf{add in } a_2x + b_2y + c_2z &= 0 && (\text{intersection of two planes, = line}) \\ \textbf{add in } a_3x + b_3y + c_3z &= 0 && (\text{intersection of three planes, (0,0)}) \end{aligned}$$

Problem: $W = \{A \in M_{n\times n}(\mathbb{R}) | tr\ A = 0\}$. Find $dim\ W$, basis of W.
Solution #1: Clever way: "guess" a basis. Note: $tr\ A = A_{11} + A_{22} + \ldots + A_{nn}$ (*one* linear condition). Expecting

$$dim\ W = n^2 - 1$$

Observe that $dim\ W \neq n^2$. This happens only if $W = M_{n\times n}(\mathbb{R})$, and obviously there are matrices which don't have trace 0. Specifically:

$$tr\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ldots & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}$$

(In proofs, can choose any example, provided property holds).
Know $dim\ W \leq n^2 - 1$. If you can find independent set of size $n^2 - 1$ in W_1, it *will be* a basis. *Try first* $n = 3$. Looking for $3^2 - 1 = 8$ independent 3×3 matrices, all trace 0.
Want trace = 0. Therefore, consider all matrices which have all 0's in the diagonal:

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

These 6 are obviously independent. Now, take two more which are independent:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Now we have 8 independent matrices (check carefully). So for $n = 3$, $dim\ W = 8$, this is a basis.

14.1.1 General case

Two types of basis matrices:

(I) All E^{ij} (1 in (i, j)-pos, 0 elsewhere)) where $i \neq j$. How many are there?

$$\begin{aligned} \#\text{ of non-diagonal entries } &= \text{ entries - entries on diagonal} \\ &= n^2 - n \end{aligned}$$

Or, $\binom{n}{2}$ ways to choose 2 distinct values from $\{1, 2, \ldots, n\}$, 2 ways to order each pair. Total:

$$\begin{aligned} \binom{n}{2} 2 &= \frac{n!}{2!(n-2)!} 2 \\ &= n(n-1) \\ &= n^2 - n \end{aligned}$$

(II) Looking for $n - 1$ more, since $n^2 - n + n - 1 = n^2 - 1$

$$\begin{pmatrix} 1 & & & & \\ & -1 & & & \\ & & \ldots & & \\ & & & 0 & \\ & & & & 0 \end{pmatrix}, \begin{pmatrix} 0 & & & & \\ & 1 & & & \\ & & -1 & & \\ & & & \ldots & \\ & & & & 0 \end{pmatrix}, \begin{pmatrix} 0 & & & & \\ & 0 & & & \\ & & \ldots & & \\ & & & 1 & \\ & & & & -1 \end{pmatrix}, \ldots$$

(n-1 of those)

Formally, let, for $i = 1, 2, \ldots, n-1$, D_i = matrix with 1 in pos (i, i) and -1 in pos $(i+1, i+1)$, 0 elsewhere.
Verifying all matrices E^{ii}, D_i are independent; clear that suffices to check $D_1, D_2, \ldots, D_{n-1}$ independent. Suppose

$$x_1 D_1 + x_2 D_2 + \ldots + x_n D_n = n \times n \text{ zero matrix}$$

The $(1, 1)$-entry on left is x_1, so $x_1 = 0$. The $(2, 2)$-entry on left is $-x_1 + x_2$,

$$x_1 \begin{pmatrix} 1 & & & & \\ & -1 & & & \\ & & \ldots & & \\ & & & 0 & \\ & & & & 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 & & & & \\ & 1 & & & \\ & & -1 & & \\ & & & \ldots & \\ & & & & 0 \end{pmatrix} + \ldots = \begin{pmatrix} 0 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & \ldots & \\ & & & & 0 \end{pmatrix}$$

but $x_1 = 0$ so $x_2 = 0$ also, etc. So similarly for all $x_i = 0$, so independent. Formally you'd do a proof by induction, but this is good enough.
Now have $n^2 - 1$ independent vectors in W_1 so $dim\ W \geq n^2 - 1$. Already, know $dim\ W \leq n^2 - 1$. So $dim\ W = n^2 - 1$, have independent set of correct size, so basis.

Solution #2: Let x_{ij} be the (i,j)-entry of A. So have n^2 variables $(x_{ij}, i, j = 1, 2, \ldots, n)$ one equation,

$$x_{11} + x_{22} + \ldots + x_{nn} = 0 \qquad (tr\ A = 0)$$

Solve system. All $x_{ij}, i \neq j$ free variables, so are $x_{22}, \ldots, x_{nn}$.
Theorem 21: Let U, W be finite dimension subspaces of V. Then,

$$dim(U + W) = dim\ U + dim\ W - dim\ U \cap W$$

It's like sets, $|A \cup B| = |A| + |B| - |A \cap B|$.
Proof Omitted.
Ex: If W is a plane in $\mathbb{R}^3$ (through $(0,0)$) and L is a line in $\mathbb{R}^{\nvDash}$ (through $(0,0)$) and L is not in the plane, prove $W + L = \mathbb{R}^3$.
Sol: L not in plane gives $L \cap W = \{\vec{0}\}$. So

$$\begin{aligned} dim(L + W) &= dim\ L + dim\ W - dim\ L \cap W \\ &= 1 + 2 - 0 \\ &= 3 \end{aligned}$$

Hence $L + W = \mathbb{R}^3$.
Problem: Suppose $dim\ V = n$, and U, W subspaces, each of dimension more than $\frac{n}{2}$. Prove that $U \cap W \neq \{\vec{0}\}$.
Proof By contradiction. Suppose $U \cap W = \{\vec{0}\}$. So $dim\ U \cap W = 0$. Then

$$\begin{aligned} dim(U + W) &= dim\ U + dim\ W - dim\ U \cap W \\ > \frac{n}{2} + \frac{n}{2} - 0 = n \end{aligned}$$

Says $U + W$ is a subspace of V of dim more than $dim\ V$. Impossible, so $U \cap W \neq \{\vec{0}\}$.
END OF MIDTERM MATERIAL