Math 52 0 - Linear algebra, Spring Semester 2012-2013
Dan Abramovich

Fields.

We learned to work with fields of numbers in school:

$\mathbb{Q}$ = fractions of integers

←hardest in school

$\mathbb{R}$ = all real numbers, represented by infinite decimal expansions.

$\mathbb{C}$ = complex numbers, written as $\{a + b\sqrt{-1},$ where $a, b \in \mathbb{R}\}$.

These satisfy the usual commutativity and associativity of addition and multiplication, they have 0 and 1, oppostites $-x$ and inverses of nonzero elements $1/x$, and satisfy distributivity.

why→ Note: $\mathbb{Z}$ = all integers is **not** a field
$\mathbb{N}$ = positive integers even more so

math 153 0→

Also note that $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are **subfields**, since they are closed under all operations, including negatives and inverses.

You can't be a **computer scientist** without working also with the field

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

with usual multiplication and **boolean** addition defined by $1 + 1 = 0$.
Is $\mathbb{F}_2$ a subfield of $\mathbb{Q}$?

a bit of a→ YOU MUST NOW BECOME

A MATHEMATICIAN ←preach

Fix a field $\mathbb{F}$- almost always we'll work with $\mathbb{F} = \mathbb{R}$. Elements of the field will be called **scalars**.

Definition. A **vector space** is a set V with two operations: **addition**

$$V \times V \longrightarrow V$$

$$(v, w) \longmapsto v + w$$

and **multiplication by scalars**

$$\mathbb{F} \times V \longrightarrow V$$

$$(c, v) \longmapsto cv$$

satisfying axioms: ←big breath

satisfying axioms: for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, $c, d \in \mathbb{F}$

(1) $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$;

(2) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$;

(3) there is $\mathbf{0} \in V$ such that
$\mathbf{0} + \mathbf{v} = \mathbf{v}$;

(4) there is $-\mathbf{v} \in V$ such that
$-\mathbf{v} + \mathbf{v} = \mathbf{0}$;

(5) $c(\mathbf{u} + \mathbf{v}) = c\mathbf{u} + c\mathbf{v}$;

(6) $(c + d)(\mathbf{v}) = c\mathbf{v} + d\mathbf{v}$;

(7) $(cd)(\mathbf{v}) = c(d\mathbf{v})$; and

(8) $1\mathbf{v} = \mathbf{v}$.

examples

$\mathbb{R}^n$ is an $\mathbb{R}$-vector space. ←of dimension n

examples

of dimension $n \rightarrow$ $\mathbb{R}^n$ is an $\mathbb{R}$-vector space.

of dimension $n \rightarrow$ $\mathbb{Q}^n$ is a $\mathbb{Q}$-vector space.

of dimension $n \rightarrow$ $\mathbb{C}^n$ is a $\mathbb{C}$-vector space.

of dimension $n \rightarrow$ $\mathbb{F}_2^n$ is a $\mathbb{F}_2$-vector space.

examples

$\mathbb{R}^n$ is an $\mathbb{R}$-vector space. ←of dimension n

$\mathbb{Q}^n$ is a $\mathbb{Q}$-vector space. ←of dimension n

$\mathbb{C}^n$ is a $\mathbb{C}$-vector space. ←of dimension n

$\mathbb{F}_2^n$ is a $\mathbb{F}_2$-vector space. ←of dimension n

$\mathbb{C}$ is an $\mathbb{R}$-vector space ←what?

$\mathbb{R}$ is a $\mathbb{Q}$-vector space ←huh?

The collection of all real valued functions on a set S, say $S = [0, 1]$, is a real vector space.
Notation: $\mathbb{R}^S$**.**

The collection of all **continuous** real valued functions on, say $S = \mathbb{R}$, is a real vector space.
Notation: $C(\mathbb{R})$**.**

The collection of all **differentiable** real valued functions on, say $S = \mathbb{R}$, is a real vector space.
Notation: $C^1(\mathbb{R})$**.**

The collection of all **polynomials** in variable $t \in \mathbb{R}$, is a real vector space.
Notation: $\mathbb{R}[t]$**.**
Book's notation: $\mathbb{P}$**.** ←yuck

The collection of all **polynomials** in variable $t \in \mathbb{R}$ of degree at most n, is a real vector space.
Book's notation: $\mathbb{P}_n$**.** ←ouch

Definition. A subset $W \subset V$ is **a subspace** of V if it is closed under addition and multiplication by scalars.

examples: $W = V$ is a subspace; $W = \{\mathbf{0}\}$ is a subspace.

Many examples above!

When is a line in $\mathbb{R}^3$ a subspace?

We use the word **vector** for an element in a vector space.

Can we talk about a **linear combination** of vectors

$$\mathbf{v}_1, \ldots, \mathbf{v}_n \in V?$$

Can we talk about the **span** of vectors

$$\mathbf{v}_1, \ldots, \mathbf{v}_n \in V?$$

Let's tie these together:

Theorem. The span of a set of vectors in V is always a subspace of V.

Theorem. A subset $W \subset V$ is a subspace if and only if it is closed under taking linear combinations.

The fundamental subspaces.
Say A is $m \times n$ real matrix. So it gives a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Definition. The null space of A, denoted

$$\textbf{Null } A \subset \mathbb{R}^n,$$

is the set of solutions of

$$A\mathbf{x} = \mathbf{0}.$$

Theorem.
Null A is a subspace of $\mathbb{R}^n$.

Proof.

Example: line in $\mathbb{R}^3$ through $\mathbf{0}$: ←stress advantages

$$\begin{aligned} x_1 \qquad - x_3 &= 0 \\ x_2 - x_3 &= 0 \end{aligned}$$

Parametric, or explicit, equation:

$$\mathbf{x} = t \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Example: plane in $\mathbb{R}^3$ through $\mathbf{0}$:

$$x_1 - x_2 - x_3 = 0$$

Parametric, or explicit, equation:

$$\mathbf{x} = s \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}.$$

Definition The column space **Col** $A \subset \mathbb{R}^m$ of

$$A = [\mathbf{a}_1 \ \cdots \ \mathbf{a}_n]$$

is the span of the columns $\mathbf{a}_1, \ldots, \mathbf{a}_n$.

So we do not need a new theorem: **Col** $A \subset \mathbb{R}^m$ is a subspace.

Interpretation: **Col** A is the set of $\mathbf{b} \in \mathbb{R}^m$ for which the equation

$$A\mathbf{x} = \mathbf{b}$$

has a solution.

So: the set of $\mathbf{b} \in \mathbb{R}^m$ for which the equation $A\mathbf{x} = \mathbf{b}$ has a solution is a subspace!

Definition. Suppose V, W are $\mathbb{R}$-vector spaces.

A **linear transformation**

$$T : V \to W$$

is a function such that

- $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$ and
- $T(c\mathbf{u}) = cT(\mathbf{u})$.

Examples:

- matrices
- derivatives
- integrals

The corresponding notions:

Ker $T = \{\mathbf{x} \in V : T(\mathbf{v}) = \mathbf{0}\} \subset V$ corresponds to **Null** A,

Range $T = \{T(\mathbf{v}) : \mathbf{v} \in V\} \subset W$ corresponds to **Col** A

Linear independence

A set of vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ in a vector space V is **linearly dependent** if there are scalars $c_1, \ldots, c_n$, **not all 0,** such that

$$c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = 0.$$

Otherwise it is **linearly independent.**

This means: the only solution of $c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = 0$ is the trivial solution $c_1 = \cdots = c_n = 0$.

Theorem. $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly **dependent** if and only if some $\mathbf{v}_j$ is a linear combination of

$$\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}.$$

two ways→ **Proof**

A **Basis** of a vector space is what gives it coordinates:

Definition $B \subset V$ is a **basis** if B is **linearly independent** and **spans** V.

This is the same as saying: every $\mathbf{u} \in V$ is written in a **unique way** as

$$\mathbf{u} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$$

with $\mathbf{v}_1, \ldots, \mathbf{v}_n \in B$. ←prove

General examples:

$\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is a basis of $\mathbb{R}^n$.
The columns of an invertible matrix form a basis of $\mathbb{R}^n$.

Special examples:

give some→

Theorem.
Every finite subset $S \subset V$ spanning V contains a basis $B \subset S$ of V.

Lemma. If $\mathbf{v}_k \in S$ is a linear combination of the others, then

$$S \smallsetminus \mathbf{v}_k$$

spans V.

Proof.

Apply this to fundamental spaces:

For **Null** A, row reduction produces an independent set of vectors spanning it. So it is a basis!

For **Col** A we have:

Theorem The pivot columns of A span **Col** A.

Dimension

Theorem. Suppose $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is a basis of V. Then any set $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ of more than m vectors is **linearly dependent**.

Proof. Since $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is a basis, every $\mathbf{w}_j$ is in their span. Write this out this way:

$$\begin{array}{ccccccc} \mathbf{w}_1 & = & a_{11}\mathbf{v}_1 & + & \cdots & + & a_{m1}\mathbf{v}_m \\ \vdots & & \vdots & & & & \vdots \\ \mathbf{w}_n & = & a_{1n}\mathbf{v}_1 & + & \cdots & + & a_{mn}\mathbf{v}_m \end{array}$$

We seek a solution of

$$x_1\mathbf{w}_1 + \cdots x_n\mathbf{w}_n = 0.$$

This means

$$\begin{array}{ccccccc} & (a_{11}x_1 & + & \cdots & + & a_{1n}x_n)\mathbf{v}_1 & + \\ & \vdots & & & & \vdots & \\ + & (a_{m1}x_1 & + & \cdots & + & a_{mn}x_n)\mathbf{v}_m & = 0 \end{array}$$

…This means

$$\begin{array}{l}(a_{11}x_1 + \cdots + a_{1n}x_n)\mathbf{v}_1 + \\ \quad\vdots \qquad\qquad\qquad \vdots \\ + (a_{m1}x_1 + \cdots + a_{mn}x_n)\mathbf{v}_m = 0\end{array}$$

Since $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is independent this must be trivial:

$$\begin{array}{ccccccc}a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & 0 \\ \vdots & & & & \vdots & & \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & 0\end{array}$$

or

$$A\mathbf{x} = \mathbf{0}.$$

Since $n > m$, there are more variables than equations, so there is a non-trivial solution!

Theorem All bases of a vector space have the same size.

Definition. The **dimension** of a vector space V is the size of any of its bases.

←many examples

Proof of theorem.

Theorem. If $\dim V$ is finite, $H \subset V$ a subspace, and $S \subset H$ is linearly independent, then there is a basis B for H containing S.

discussion→

Proof

Theorem. Suppose $\dim V = n$.

(1) suppose $S \subset V$ is linearly independent and of size n. Then S is a basis of V.

(2) suppose $S \subset V$ spans V and of size n. Then S is a basis of V.

Back to fundamental spaces:
dim **Null** A = number of free columns.
dim **Col** A = number of pivot columns.

We give dim **Col** A a name: **Rank** A.

Theorem. for an $m \times n$ matrix A we have

$$\boxed{\textbf{Rank } A + \dim \textbf{Null } A = n}$$

2.3 When is a matrix invertible?

Theorem. T.F.A.E. for $n \times n$ matrix A:

(1) A is invertible
(2) A is row equivalent to I_n
(3) A has n pivot positions
(4) The only solution of $A\mathbf{x} = \mathbf{0}$ is $\mathbf{x} = \mathbf{0}$
(5) $\mathbf{a}_1, \ldots, \mathbf{a}_n$ are linearly independent
(6) The transformation $\mathbf{x} \mapsto A\mathbf{x}$ is 1-to-1.
(7) $A\mathbf{x} = \mathbf{b}$ is consistent for all $\mathbf{b} \in \mathbb{R}^n$.
(8) $Span(\mathbf{a}_1, \ldots, \mathbf{a}_n) = \mathbb{R}^n$
(9) The transformation $\mathbf{x} \mapsto A\mathbf{x}$ is onto.
(10) There is C such that $CA = I_n$
(11) There is D such that $AD = I_n$
(12) A^T is invertible

A basis gives coordinates to the space it spans:

Theorem if $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ is a basis of V, then every $\mathbf{x} \in V$ has a unique expression

$$\mathbf{x} = c_1\mathbf{b}_1 + \cdots + c_n\mathbf{b}_n.$$

Again $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ is a basis of V, and $\mathbf{x} \in V$, so

$$\mathbf{x} = c_1\mathbf{b}_1 + \cdots + c_n\mathbf{b}_n.$$

Then $c_1, \ldots, c_n$ are the **coordinates** of $\mathbf{x}$ in the basis B,

$$[\mathbf{x}]_B = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \in \mathbb{R}^n$$

is the coordinate vector, and $\mathbf{x} \mapsto [\mathbf{x}]_B$ is the coordinate mapping.

←examples

What if $V = \mathbb{R}^n$?

Write $P = P_B = [\mathbf{b}_1 \cdots \mathbf{b}_n]$.

Proposition

(1) $\mathbf{x} = P_B[\mathbf{x}]_B$.

(2) P_B is invertible

(3) $[\mathbf{x}]_B = (P_B)^{-1}\mathbf{x}$.

In general:

Theorem if $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ is a basis of V, then the coordinate mapping

$$\begin{aligned} V &\to \mathbb{R}^n \\ \mathbf{x} &\mapsto [\mathbf{x}]_B \end{aligned}$$

is an invertible linear transformation.

What if I have two bases B and C? In case $V = \mathbb{R}^n$ then we can deduce from above:

- $\mathbf{x} = P_B[\mathbf{x}]_B$,
- $[\mathbf{x}]_C = (P_C)^{-1}\mathbf{x}$

so

$$[\mathbf{x}]_C = (P_C)^{-1} P_B [\mathbf{x}]_B.$$

examples→

We get a hint by understanding what $(P_C)^{-1}P_B$ does to $\mathbf{e}_i$:

$$P_B\mathbf{e}_i = \mathbf{b}_i$$

$$(P_C)^{-1}\mathbf{b}_i = [\mathbf{b}_i]_C$$

so

$$(P_C)^{-1}P_B\mathbf{e}_i = [\mathbf{b}_i]_C$$

Summarizing:

$$\underset{C\leftarrow B}{P} := (P_C)^{-1}P_B = \big[[\mathbf{b}_1]_C \ldots [\mathbf{b}_n]_C\big]$$

Direct calculation:

$$[P_C P_B] \quad \sim \quad [\ I_n \ \ \underset{C\leftarrow B}{P}\ ]$$

Theorem if B and C are two bases for V

define

$$\underset{C\leftarrow B}{P} = \left[[\mathbf{b}_1]_C \ldots [\mathbf{b}_n]_C \right]$$

then for any $\mathbf{x} \in V$

$$[\mathbf{x}]_C \quad = \quad \underset{C\leftarrow B}{P} [\mathbf{x}]_B$$

Row space.

←should have done earlier

the **row space** of a matrix A is the space spanned by the row vectors.

Theorem. if $A \sim B$ then the row spaces are the same.

If B is in echelon form, the nonzero rows form a basis. Its size is the number of pivots.

Theorem.

$$\boxed{\dim \mathbf{Row}(A) = \dim \mathbf{Col}\ (A)}$$

The Fibonacci sequence is defined by a **recursive formula**:

$F_k = F_{k-1} + F_{k-2}$
for all $k \geq 2$, starting from

$F_0 = 0; F_1 = 1.$

It looks like this:
$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$

Of course you can also go backwards, since $F_{k-2} = F_k - F_{k-1}$

so it looks like
$\ldots, -8, 5 - 3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, \ldots$

We want to relate this to linear algebra:

- Think about the space as a vector space
- Think about the recursion as a linear transformation
- Think about the solutions as null space
- Think about the dimension of the solution space
- Find the solution in terms of a basis
- Think about matrices

The space: all sequences, infinite on both sides.

This is just the space of real valued functions on the integers:

$$\mathbb{R}^{\mathbb{Z}}$$

We know it is a vector space. It is infinite dimensional.

The book called it **the space of signals.**

The recursion, also known as **difference equation**:

$$F_{k+2} - F_{k+1} - F_k = 0$$

If we write $G_k = F_{k+2} - F_{k+1} - F_k$ we get a mapping

$$T : \mathbb{R}^{\mathbb{Z}} \to \mathbb{R}^{\mathbb{Z}}$$

$$(\dots F_k \dots) \mapsto (\dots G_k \dots)$$

What are the sequences satisfying the recursion?

These are precisely the subspace

$$\mathrm{Ker}\, T \;\subset\; \mathbb{R}^{\mathbb{Z}}$$

Given a linear recursion of **order** (length) $n \geq 1$, write it this way: ←difference equation

(1) $F_{k+n} + a_1 F_{k+(n-1)} + \cdots + a_n F_k$,

with $\boxed{a_n \neq 0}$.

Theorem. For any choice of "free variables"

$$F_0, \ldots, F_{k-1}$$

the recursion (1) has a unique solution. ←intuit

Corollary. The space of solutions Ker T has dimension $n =$ the order of the recursion.

Basis: $F^{(i)}$ starts just like $\mathbf{e}_i$:

$0, 0, \ldots, 0, 1, 0, \ldots, 0, F_n^{(i)}, F_{n+1}^{(i)}, \ldots$

But how about a closed formula?

Examples:

(1) $F_{k+1} - F_k = 0$

(2) $F_{k+1} + F_k = 0$

(3) $F_{k+1} - 2F_k = 0$

(4) $F_{k+2} - 3F_{k+1} + 2F_k = 0$

Theorem. if r is a solution of the polynomial equation
$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0$

Then the sequence

$$F_k = r^k$$

is a solution of the recursion

$$F_{k+n} + a_1 F_{k+(n-1)} + \cdots + a_n F_k,$$

If the polynomial has n distinct roots r_i then the sequences

$$F_k = r_i^k$$

form a basis.

$$F_{k+2} - F_{k+1} - F_k = 0$$

write the associated polynomial equation

$r^2 - r - 1 = 0$

the solutions are $r_{12} = \frac{1 \pm \sqrt{5}}{2}$

So if $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$

then

$$G_k = \alpha^k \qquad \text{and} \qquad H_k = \beta^k$$

are a basis for solutions.

Write $F_k = x_1 G_k + x_2 H_k$.

Since $F_0 = 0, F_1 = 1$ get
$x_1 + x_2 = 0,$
$\alpha x_1 + \beta x_2 = 1$

$$\boxed{F_k = \frac{\alpha^k - \beta^k}{\sqrt{5}}}.$$

We know that

$$B = \{G, H\}$$

is a basis and

$$C = \{F^{(1,0)}, F^{(0,1)}\}$$

is a basis.

$$G_n = F^{(1,0)} + \alpha F^{(0,1)}$$

$$H_n = F^{(1,0)} + \beta F^{(0,1)}$$

So

$$\underset{C \leftarrow B}{P} = \begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix}$$

So

$$\underset{B \leftarrow C}{P} = (\underset{C \leftarrow B}{P})^{-1} = \frac{-1}{\sqrt{5}} \begin{bmatrix} \beta & -1 \\ -\alpha & 1 \end{bmatrix}$$

$$\left[F^{(0,1)}\right]_C = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

so $\left[F^{(0,1)}\right]_C = \underset{B\leftarrow C}{P} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{-1}{\sqrt{5}} \begin{bmatrix} -1 \\ 1 \end{bmatrix}$

So the Fibonacci sequence, which is $F^{(0,1)}$, is just

$$\boxed{F_k = \frac{\alpha^n - \beta^n}{\sqrt{5}}}.$$

More on Fibonacci:

If $\mathbf{x}_k = \begin{bmatrix} F_k \\ F_{k+1} \end{bmatrix}$

Then $\mathbf{x}_{k+1} = \begin{bmatrix} F_{k+1} \\ F_{k+2} \end{bmatrix} = \begin{bmatrix} F_{k+1} \\ F_k + F_{k+1} \end{bmatrix}$

which is $A\mathbf{x}_k$ with $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

So $\mathbf{x}_k = A^k \mathbf{x}_0 = A^k \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

We “just” need a simple formula for $A^k \ldots$