Math 350: Linear Algebra

Wolmer V. Vasconcelos

Set 1

Spring 2010

Outline

- Pre-requisites: Calc 4, Math 300,
  needs basic linear algebra
- webpage:www.math.rutgers.edu/(tilde)vasconce
- email : vasconce AT math.rutgers.edu
- General Information: Look up in Info page webpage
- Syllabus: See Info page

Outline

What is Linear Algebra?

It is the integrated study of several mathematical structures: fields, abelian groups, vector spaces, linear transformations.

- What is the general nature of a field?
- An abelian group?
- A vector space?
- A linear transformation?
- Part of Linear Algebra is called Multilinear Algebra: determinants, tensors, etc.
- Why should we care about Linear Algebra? Because...

What are we going to learn?

Two examples:

Understand Spectral Theorems:

These are assertions about when an $n \times n$ matrix (set $n = 3$)

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \longrightarrow \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}$$

When this can't be done, what?

Complex Matrices are put together from Jordan blocks

Let **A** be a 8-by-8 matrix with 3 eigenvalues $\lambda_1, \lambda_2, \lambda_3$ of multiplicities $3, 2, 3$ resp. Underneath it looks like:

$$\mathbf{A} = \begin{bmatrix} \mathbf{J}_1 & O & O \\ O & \mathbf{J}_2 & O \\ O & O & \mathbf{J}_3 \end{bmatrix} = \begin{bmatrix} \lambda_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_3 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 \end{bmatrix}$$

The color coded blocks are called **Jordan Blocks**

$$\mathbf{J} = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}$$

Part of the usefulness of these blocks is that we can define and calculate functions such as $\exp \mathbf{J}$, $\sin \mathbf{J}$, etc and have an analysis based on them.

Abelian Group $\longrightarrow$ Vector Space

For the next definition, it is helpful to have in mind several sets:

- Integers: $\mathbb{Z}$
- Continuous functions on some interval
- Matrices of a fixed size
- Polynomials in one or several variables

These sets share a common structure which we want to highlight.

Structure: Means What?

A composition on a set $\mathbb{X}$ is a function assigning to pairs of elements of $\mathbb{X}$ an element of $\mathbb{X}$,

$$(a, b) \mapsto \mathbf{f}(a, b).$$

That is a function of two variables on $\mathbb{X}$ with values in $\mathbb{X}$. It is nicely represented in a composition table

$\mathbf{f}$	$*$	b	$*$
$*$	$*$	$*$	$*$
a	$*$	$\mathbf{f}(a, b)$	$*$
$*$	$*$	$*$	$*$

We represent it also as

$$\mathbb{X} \times \mathbb{X} \xrightarrow{\mathbf{f}} \mathbb{X}$$

An abelian group is a set $\mathbf{G}$ with a composition law denoted '$+$'

$$\mathbf{G} \times \mathbf{G} \to \mathbf{G},$$

$$a, b \in \mathbf{G}, \quad a + b \in \mathbf{G}$$

satisfying the axioms

- associative $\forall a, b, c \in \mathbf{G}, \quad (a+b)+c = a+(b+c)$
- commutative $\forall a, b \in \mathbf{G}, \quad a+b = b+a$
- existence of O

$$\exists O \in \mathbf{G} \quad \text{such that } \forall a \quad a + O = a$$

- existence of inverses

$$\forall a \in \mathbf{G} \quad \exists b \in \mathbf{G} \quad \text{such that } a + b = O$$

This element is unique and denoted $-a$.

For example, if $\mathbb{X}$ is the set of real continuous functions on the interval $(-1, 1)$, the fact that the sum of two continuous functions is continuous says that addition

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

is a composition law that makes $\mathbb{X}$ into an abelian group.

It is not a good idea to confuse the scalar 0 with the zero function O: $O(x) = 0 \quad \forall x$.

Let us get confused a bit!

A point worthy of discussion: Is it possible for the same set, say $\mathbb{R}$, to be an abelian group in more than one way? To show this, let us define a new addition of real numbers. We are going to call it 'O plus' $\oplus$:

$$a \oplus b := a + b - 1$$

Call this set $\mathbb{R}_{\oplus}$. It is easy to see that it is an abelian group [e.g. $(a \oplus b) \oplus c = a = b + c - 2$ so composition is associative] in which 0 is 1: $a \oplus 1 = a$!

Group of Rotations

Let C be the set of all complex numbers $a + bi$, with $a^2 + b^2 = 1$. Graphically this is just the unit circle centered ao the origin of a plane. Ths set has the following properties:

- $a + bi \in C$, then $(a + bi)^{-1} \in C$. This because

$$(a + bi)^{-1} = (a - bi) \in C$$

- If $a + bi, c + di \in C$ then $(a + bi)(c + di) \in C$. This follows from $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ and

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) = 1.$$

Each element of C can also be written

$$a + bi = e^{i\theta}$$

Field

A field **F** is a set with two composition laws, called ‘addition’ and ‘multiplication’, say $+$ and $\times$: $\forall a, b \in \mathbf{F}$ have compositions $a + b$ and $a \times b$. (The second composition is also written $a \cdot b$, or simply ab.)

- $(\mathbf{F}, +)$ is an abelian group
- $(\mathbf{F}, \times)$: multiplication is associative, commutative and distributive over $+$, that is $\forall a, b, c \in \mathbf{F}$,

$$(ab)c = a(bc), \quad ab = ba, \quad a(b + c) = ab + ac$$

- existence of identity $\exists e \in \mathbf{F}$ such that

$$\forall a \in \mathbf{F} \quad a \times e = a$$

- existence of inverses For every $a \neq 0$, there is $b \in \mathbf{F}$

$$a \times b = e.$$

There is a unique element e, usually we denote it by 1. For $a \neq 0$, the element b such that $ab = 1$ is unique; it is often denoted by $1/a$ or a^{-1}.

We can now define scalars: the elements of a field.

Fields are ubiquotous:

- $\mathbb{R}$: real numbers
- The integers $\mathbb{Z}$ is not a field (not all integers have inverses), but $\mathbb{Q}$, the rational numbers is a field.
- $\mathbb{C}$: complex numbers, $z = a + bi$, $i = \sqrt{-1}$, with compositions

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

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

The arithmetic here requires a bit more care:

If $a + bi \neq 0$,

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

Exercise: Number fields

Let **F** be the set of all real numbers of the form

$$z = a + b\sqrt{2}, \quad a, b \in \mathbb{Q}$$

prove that **F** is a field.

- Check that **F** is closed for addition and multiplication
- If $a + b\sqrt{2} \neq 0 \Rightarrow (a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in \mathbf{F}$
- Axioms of a field.

$\mathbb{Z}_2$

A noteworthy example is $\mathbb{F}_2$, the set made up by two elements $\{0, 1\}$ (or (even, odd))with addition defined by the table

$+$	0	1
0	0	1
1	1	0

$1 + 1 = 0!$

and multiplication by

$\times$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$

$\mathbb{F}_3 = \{0, 1, 2\}$ with addition defined by the table

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$1 + 2 = 0$!

and multiplication by

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$2 \times 2 = 1$!

Exercise 1: Prove that in any field **F** the rule minus times minus is plus holds, that is for any $a, b \in \mathbf{F}$,

$$-(-a) = a, \quad (-a)(-b) = ab.$$

Solution: The first assertion folllows from

$a + (-a) = (-a) + a = O$: a is the negative of $-a$.

Because of the above, we must show that $(-a)(-b)$ is the negative of $-(ab)$. We first claim $(-a)b = -(ab)$. Note

$$(-a)b + ab = ((-a) + a)b = Ob = O.$$

$$(-a)(-b)-(ab) = (-a)(-b)+(-a)b = (-a)((-b)+b) = (-a)O = O.$$

A field is the mathematical structure of choice to do arithmetic. Given a field **F**, fractions can defined as follows: If $a, b \in \mathbf{F}, \quad b \neq 0,$

$$\frac{a}{b} := ab^{-1}.$$

The usual calculus of fractions then follows, for instance

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Outline

A vector space is a structured set put together from an abelian group **V** and a field **F**. It is helpful to keep in mind the following examples.

Let n be a non-negative integer. $\mathbb{R}^n$: the set of all n-tuples of real numbers, with 2 compositions

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} + \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} v_1 + u_1 \\ v_2 + u_2 \\ \vdots \\ v_n + u_n \end{bmatrix}$$

For $c \in \mathbb{R}$,

$$c \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} cv_1 \\ cv_2 \\ \vdots \\ cv_n \end{bmatrix}$$

Another example is the set of polynomials in one indeterminate over the field **F**: **F**[x] is the set of polynomials

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbf{F}$$

Addition is given by

$$(a_n x^n + \cdots + a_1 x + a_0) + (b_m x^m + \cdots + b_1 x + b_0) = \sum_i (a_i + b_i) x^i$$

and scalar multiplication

$$cf(x) = ca_n x^n + ca_{n-1} x^{n-1} + \cdots + ca_1 x + ca_0$$

Related examples are the subsets $\mathbb{P}_n(x)$ of polynomials of degree at most n.

The set of solutions of the differential equation

$$y^{(3)} - 7y'' + 14y' - 8y = 0$$

is also a vector space over $\mathbb{R}$. It is a consequence of the fact [principle of superposition] that if $y_1(x)$ and $y_2(x)$ are solutions then for $a, b \in \mathbb{R}$

$$ay_1(x) + by_2(x)$$

is also a solution. From Calc 252, it will follow that any solution is a combination

$$ae^x + be^{2x} + ce^{4x}$$

Formally, a vector space over a field **F** is an abelian group **V** admitting a (scalar) multiplication

$$\mathbf{F} \times \mathbf{V} \to \mathbf{V}, \quad c \times u \mapsto cu \in \mathbf{V}$$

with the following properties:

- For $c, d \in \mathbf{F}$, $u \in \mathbf{V}$, $(cd)u = c(du)$
- For $u \in \mathbf{V}$, $1u = u$
- For $c, d \in \mathbf{F}$, $u \in \mathbf{V}$, $(c + d)u = cu + du$
- For $c \in \mathbf{F}$, $u, v \in \mathbf{V}$, $c(u + v) = cu + cv$

We can now define vectors: the elements of a vector space.

Theorem (First Theorem)

For $u, O \in \mathbf{V}$, $0, c \in \mathbf{F}$

$$0u = O, \quad cO = O, \quad (-c)u = -(cu)$$

Proof. For the first claim, observe

$$0u = (0+0)u = 0u + 0u,$$

so

$$0u = O$$

Similarly for the other claims. □

There are many vector spaces derived from those mentioned already. We give a very general method to form new vector spaces. Let **V** and **W** be vector spaces over the field **F** and let $\mathbf{V} \times \mathbf{W}$ be the set of all ordered pairs (v, w), $v \in \mathbf{V}$, $w \in \mathbf{W}$. If we define an addition and a scalar multiplication by

$$\begin{aligned} (v_1, w_1) + (v_2, w_2) &:= (v_1 + v_2, w_1 + w_2) \\ c(v, w) &:= (cv, cw), \end{aligned}$$

we make $\mathbf{V} \times \mathbf{W}$ into a vector space. It is easy to verify all the requirements. This is the method used to obtain the vector spaces of tuples $\mathbf{F}^2 = \mathbf{F} \times \mathbf{F}$, $\mathbf{F}^3 = \mathbf{F}^2 \times \mathbf{F}$, and so on.

Outline

Last Class...and...Today

We introduced and gave the first examples of the following basic algebraic structures:

- Abelian group: $\mathbb{Z}$, complex numbers of magnitude 1, polynomials in x with coefficients in $\mathbb{C}$
- Field: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_2$
- Vector space: Ingredients are an abelian group **V**, a field **F** and a multiplication $(r, v) \rightarrow r \cdot v$, for $r \in \mathbf{F}$ and $v \in \mathbf{V}$ with some properties
- Subspace: nonempty subset $\mathbf{W} \subset \mathbf{V}$ of a vector space that is a vector space for same operations
- Quick subspace test
- Lots more examples plus ...

Outline

We are now in a position to introduce a basic concept, that of a subspace of a vector space. [It is a subset but with special properties, like a child of a vector space, carrying part of its DNA.]

Definition

A non-empty subset **S** is a subspace of a vector space **V** if **S** is a vector space for the same operations of **V**.

Example

Let **V** be the set of all real polynomials, $\mathbf{f} = a_0 + a_1 x + a_2 x^2 + \cdots$. **V** is a vector space over $\mathbb{R}$. Let **S** be the subset of all polyomials where the coefficients of all odd powers are zero: $a_1 = a_3 = \cdots = 0$. Clearly **S** is also a vector space over $\mathbb{R}$ for the same operations: So **S** is a subspace of **V**.

There is a very simple test to check whether a subset **S** of a vector space **V** over a field **F** is a subspace:

Proposition (Subspace Test)

S *is a subspace iff the following hold: (i)* $O \in \mathbf{S}$*; (ii) if* $u, v \in \mathbf{S}$*, then* $u + v \in \mathbf{S}$*; (iii) if* $c \in \mathbf{F}$ *and* $u \in \mathbf{S}$*, then* $cu \in \mathbf{S}$*.*

Note that (i) says that **S** is non-empty, and (ii) and (iii) say that we are using the operations of **V**. The beauty of this criterion is that it does not asks us to check the axioms of vector spaces: It was done already in **V**. We can paraphrase by saying: A subspace of a vector space is a non-empty subset closed under addition and scalar multiplication.

Examples

$\{O\}$ is always a subspace.

Consider the following subsets of $\mathbb{R}^2$:

$$\begin{aligned} \mathbf{S}_1 &:= \{(a,b) \mid a-b=0\} \\ \mathbf{S}_2 &:= \{(a,b) \mid a,b \geq 0\} \\ \mathbf{S}_3 &:= \{(a,b) \mid a=0\} \end{aligned}$$

$\mathbf{S}_1$ and $\mathbf{S}_3$ pass the test but $\mathbf{S}_2$ is closed under addition but not scalar multiplication:

$$(-1)(2,3) = (-2,-3) \notin \mathbf{S}_2$$

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 2 & 3 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

- row space: subspace of $\mathbf{F}^5$
- column space: subspace of $\mathbf{F}^3$
- nullspace: all vectors v of $\mathbf{F}^5$ such that

$$Av = O$$

Let us talk about this last set.

Nullspace

- The nullspace **S** of this matrix consists of the vectors $v \in \mathbf{F}^5$ such that

$$\mathbf{A}v = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 2 & 3 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = O$$

- If $v, u \in \mathbf{S}$, $\mathbf{A}(v+u) = \mathbf{A}v + \mathbf{A}u = O + O = O$, so $v + u \in \mathbf{S}$
- If $v \in \mathbf{S}$ and $c \in \mathbf{F}$, $\mathbf{A}(cv) = c\mathbf{A}(v) = cO = O$, so $cv \in \mathbf{S}$
- Conclusion: **S** passes the subspace test.

Example

Let V be the vector space $\mathbb{Z}_2^n$: This is the set of all n-tuples

$$(x_1, x_2, \ldots, x_n),$$

with $x_i = 0, 1$. This space has many interesting subspaces.

Exercise: Prove that the subset S of V consisting of all such tuples where an **even** number of x_i are 1 is a subspace.

Solution

1. $u = (x_1, \ldots, x_n)$ has an even number of entries x_i equal to 1 if and only if
$$x_1 + x_2 + \cdots + x_n = 0$$
2. If another tuple $v = (y_1, y_2, \ldots, y_n)$ has the same property, it is clear that $u + v = (x_1 + y_1, \ldots, x_n + y_n) \in S$. Thus S is closed under addition.
3. It is clear that S is closed under multiplication, since if $u \in S$, $1 \cdot u = u$ and $0 \cdot u = (0, \ldots, 0) \in S$.
4. Thus S passes the subspace test.

Properties

Proposition

If $\mathbf{S}_1$ *and* $\mathbf{S}_2$ *are subspaces of the vector space* $\mathbf{V}$*, then the following subsets of* $\mathbf{V}$ *are subspaces:*

1. $\mathbf{S}_1 \cap \mathbf{S}_2$.
2. $\mathbf{S}_1 + \mathbf{S}_2 = \{a + b : a \in \mathbf{S}_1, \quad b \in \mathbf{S}_2\}$.

Class Proof Check that the subsets are closed under addition and scalar multiplication.

Question

Example

Can we make a vector space out of the people in this room?

Vector Spaces of Matrices

Let **F** be a field. For a fixed pair (m, n) of natural numbers, the set **M** of all $m \times n$ matrices with entries/coefficients in **F**

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

with the usual addition and multiplication by elements of **F** is a vector space. Note that we might as well say that such objects are ordinary $m \cdot n$-tuples organized in a particular way. It is a fact that opens opportunities.

Subspaces of Matrices

Let $\mathbf{M}_3(\mathbf{F})$ be the space of all 3×3 matrices over the field $\mathbf{F}$.

Consider the sets of matrices of the form [schematically]

$$\mathbf{D}_3 : \begin{bmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{bmatrix}$$

$\mathbf{D}_3$ are diagonal matrices

$$\mathbf{U}_3 : \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{bmatrix}$$

$\mathbf{U}_3$ are upper triangular matrices

$$\mathbf{L}_3 : \begin{bmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$\mathbf{L}_3$ are lower triangular matrices

$$\mathbf{S}_3 : \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{bmatrix}$$

$\mathbf{S}_3$ are symmetric matrices

$$\mathbf{K}_3 : \begin{bmatrix} 0 & a_{12} & a_{13} \\ -a_{12} & 0 & a_{23} \\ -a_{13} & -a_{23} & 0 \end{bmatrix}$$

$\mathbf{K}_3$ are skew-symmetric matrices

Sequences

Let **V** be the set of all sequences of real numbers

$$s = (a_1, a_2, \ldots, a_n, \ldots).$$

If we define

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

and scalar multiplication by

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

V becomes a vector space.

Exercise 2: Let **S** be the set of all sequences

$$s = (a_1, a_2, \ldots), \quad \sum_{i \geq 1} a_i^2 < \infty.$$

show that **S** is a subspace.

Solution: We must show that the subset **S** is closed under addition and scalar multiplication.

Suppose that $\sum_{i\geq 1} a_i^2 < \infty$ and $\sum_{i\geq 1} b_i^2 < \infty$. Then

$$\begin{aligned}\sum_{i\geq 1}(a_i+b_i)^2 &= \sum_{i\geq 1} a_i^2 + 2\sum_{i\geq 1} a_i b_i + \sum_{i\geq 1} b_i^2 \\ &\leq 2\sum_{i\geq 1} a_i^2 + 2\sum_{i\geq 1} b_i^2,\end{aligned}$$

since $2a_ib_i \leq a_i^2 + b_i^2$.

The scalar condition is immediate.

Linear combinations

Let **A** be a set of vectors in a vector space **V**,

$$\mathbf{A} = \{v_1, \ldots, v_m\}.$$

Definition

A linear combination of the v_i is a vector

$$v = c_1 v_1 + \cdots + c_m v_m, \quad c_i \in \mathbf{F}.$$

The set **S** of all these vectors is the span of $\{v_1, \ldots, v_m\}$.

Note the following observation:

Proposition

S *is a subspace of* **V**. **S** *is the smallest subspace that contains all the vectors* v_i.

Proof. If $v = c_1 v_1 + \cdots + c_m v_m$ and $u = d_1 v_1 + \cdots + d_m v_m$ are two linear combinations,

$$v + u = (c_1 + d_1)v_1 + \cdots + (c_m + d_m)v_m$$

is also a linear combination. For any scalar c, cv is a linear combination. Thus the span of a set of vectors passes the subspace test.

The span of the zero vector is just $\{O\}$.

If v is a nonzero vector, its span is the set

$$\mathbf{L} = \{cv \mid c \in \mathbf{F}\}$$

L is said to be the line determined by v.

If u, v are vectors such that neither is a multiple of the other, they span a plane.

Recall that the classical vectors, i, j and k span $\mathbb{R}^3$.

The vector space $\mathbf{M}_2(\mathbf{F})$ is spanned by the 4 matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = a\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + b\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + c\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + d\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

but also by the matrices

$$(a-b)\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + (b-c)\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} + (c-d)\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} + d\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

We can generalize these notions as follows: Let $\mathbf{W}_i$ be a family (finite or infinite) of subspaces of $\mathbf{V}$. The sum of the $\mathbf{W}_i$ is the set of all finite sums

$$w_1 + w_2 + \cdots + w_n, \quad w_i \in \mathbf{W}_i.$$

It is denoted

$$\sum \mathbf{W}_i.$$

Let us look at some interesting examples.

Let **V** be the set of all real functions $f(t)$ of the real variable t. **V** is a vector space over $\mathbb{R}$. A function $f(t)$ is even if $f(-t) = f(t)$. Call **E** the set of all even functions. By the subspace test, **E** is a subspace. We define similarly odd functions, $f(-t) = -f(t)$, and again check that the set **O** they define is a subspace.

Exercise 3: Prove that $\mathbf{V} = \mathbf{E} + \mathbf{O}$.

Solution: For any $F(t)$, we write

$$F(t) = \frac{F(t) + F(-t)}{2} + \frac{F(t) - F(-t)}{2}$$

Observe that the first summand is even, the second odd.

Related exercises are the following. Let $M_n(\mathbb{R})$ be the set of $n \times n$ real matrices. Denote by $\mathbf{S}_n$ the set of symmetric matrices and by $\mathbf{K}_n$ the set of skew-symmetric real matrices [i.e. $a_{ij} = -a_{ji}$; in particular $a_{ii} = 0$].

Exercise 4: Prove that $\mathbf{M}_n(\mathbb{R}) = \mathbf{S}_n + \mathbf{K}_n$.

A matrix is strictly upper triangular if $a_{ij} = 0$ if $i \leq j$. Denote by $\mathbf{U}_n$ the set [subspace] of all such matrices. $\mathbf{L}_n$ is similarly defined: strictly lower triangular

Exercise 5: Prove that $\mathbf{M}_n(\mathbb{R}) = \mathbf{S}_n + \mathbf{U}_n$
You might want to examine the case $n = 2$ first:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{21} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} 0 & a_{12} - a_{21} \\ 0 & 0 \end{bmatrix}$$

Outline

Homework #1

1. 1.1: 1 (This will be a general rule: always scan the first problem of a new section as it reviews the topics discussed.)
2. 1.2: 3(a), 12, 18, 21
3. 1.3: 5, 8(d), 9, 31 (optional)
4. 1.4: 2(a), 3(a), 4(a), 14
5. 1.5: 2(d), 6, 10, 16
6. 1.6: 1, 5, 7, 9, 15, 30

Finite Fields

We seen two finite fields: $\mathbb{Z}_2$, integers mod 2, and $\mathbb{Z}_3$, integers mod 3. The construction does not work with $\mathbb{Z}_4$ as $2 \times 2 = 4 = 0$. Nevertheless there are fields with 4 elements: Let **F** be the set of polynomials $\{0, 1, x, 1 + x\}$, with coefficients in $\mathbb{Z}_2$. So we add $x + (1 + x) = 1 + 2x = 1$. To multiply we use the table

$\times$	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

, $\quad x \cdot (x + 1) = 1!$

Prime field

Suppose **F** is a finite field and let us try to understand pieces of its structure. **F** has at least two elements, 0 and 1. What else? we could try

$$\begin{aligned}&1\\&1+1\\&1+1+1\\&\vdots\\&1+1+\cdots+1, \quad m \text{ 1's}\end{aligned}$$

Because **F** is finite, there must be repeatitions in this listing.

This means that we have two sums in **F**,

$$1 + 1 + \cdots + 1 = 1 + 1 + \cdots + 1,$$

the first with m 1's and the second with n 1's, $m \neq n$. Say $m > n$.

Subtracting, we get a sum $1 + 1 + \cdots + 1 = 0$, with $m - n$ 1's.

Proposition

The smallest nonzero integer p for which there is a sum $1 + 1 + \cdots + 1 = 0$ of p 1's is a prime number.

Proof

1. We prove that p is prime by contradiction. Suppose $p = a \cdot b$, $a, b > 1$.
2. Then

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

   where the first term has a $1's$, the second b 1's.
3. Since **F** is a field, one of these terms must be zero.
4. But this is a contradiction since they have fewer 1's than the choice of p.

This prime number p is called the characteristic of **F**.

Corollary

In a finite field $\mathbf{F}$ *the subset* $\mathbf{F}_0$ *of sums of* 1*'s forms a field with* p *elements,* p *prime.* $\mathbf{F}_0$ *is called the prime field of* $\mathbf{F}$ *and there is a natural identification of* $\mathbf{F}_0$ *to* $\mathbb{Z}_p$*, the integers mod* p*.*

Corollary

$\mathbf{F}$ *is a vector space over* $\mathbb{Z}_p$*.*

It will follow from this corollary that the cardinality of a finite field $\mathbf{F}$ is always a power p^n, where p is its characteristic. It is a theorem of Galois theory that for any prime p and any natural number n there is a finite field of cardinality p^n. (Up to some equivalence, there is just one such field.)

Outline

HomeQuiz #1

1. Let $\mathbf{A} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 2 & 3 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$ Prove that the set of vectors $\mathbf{a} \in \mathbb{R}^3$ such that $\mathbf{A}v = \mathbf{a}$ for some $v \in \mathbb{R}^5$ is a subspace of $\mathbb{R}^3$.
2. Prove that $\mathbf{M}_n(\mathbb{R}) = \mathbf{S}_n + \mathbf{K}_n$.
3. Give 2 examples of a vector space $\mathbf{V}$ that has only 4 vectors.
4. Explain why a vector space cannot have just 6 vectors.

Answers

1: We apply the subspace test to show that the set $\mathbf{S}$ of vectors $\mathbf{a} \in \mathbb{R}^3$ such that $\mathbf{A}v = \mathbf{a}$ for some $v \in \mathbb{R}^5$ is a subspace of $\mathbb{R}^3$.

- If $\mathbf{a}_1, \mathbf{a}_2 \in \mathbf{S}$, say $\mathbf{A}v_1 = \mathbf{a}_1$, $\mathbf{A}v_2 = \mathbf{a}_2$, then

$$\mathbf{a}_1 + \mathbf{a}_2 = \mathbf{A}v_1 + \mathbf{A}v_2 = \mathbf{A}(v_1 + v_2) \Rightarrow \mathbf{a}_1 + \mathbf{a}_2 \in \mathbf{S}$$

- If $\mathbf{a} = \mathbf{A}v$, then any scalar c, $c\mathbf{a} = \mathbf{A}cv$, hence $c\mathbf{a} \in \mathbf{S}$
- $\mathbf{S}$ passes the test

2: Must show that any square real matrix $\mathbf{A}$ is a sum $\mathbf{A} = \mathbf{B} + \mathbf{C}$, where $\mathbf{B}$ is symmetric and $\mathbf{C}$ is skew-symmetric.
For $n = 3$: Given $\mathbf{A} = [a_{ij}]$ must find $\mathbf{B} = [b_{ij}]$ and $\mathbf{C} = [c_{ij}]$

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{12} & b_{22} & b_{23} \\ b_{13} & b_{23} & b_{33} \end{bmatrix} + \begin{bmatrix} 0 & c_{12} & c_{13} \\ -c_{12} & 0 & c_{23} \\ -c_{13} & -c_{23} & 0 \end{bmatrix}$$

Must solve for all b_{ij} and all c_{ij}.

$$\begin{aligned} b_{ii} &= a_{ii}, \quad \forall i \\ a_{ij} &= b_{ij} + c_{ij}, \\ a_{jj} &= b_{ij} - c_{ij}, \forall i \neq j \end{aligned}$$

Thus $b_{ij} = 1/2(a_{ij} + a_{ji})$ and $c_{ij} = 1/2(a_{ij} - a_{ji})$.

Cool 2: Consider the equality

- $\mathbf{A} = \mathbf{B} + \mathbf{C}$ and take the transposes
- $\mathbf{A}^t = \mathbf{B}^t + \mathbf{C}^t$. But $\mathbf{B}^t = \mathbf{B}$ and $\mathbf{C}^t = -\mathbf{C}$.
- Adding the equalities we get $\mathbf{B} = 1/2(\mathbf{A} + \mathbf{A}^t)$ and $\mathbf{C} = 1/2(\mathbf{A} - \mathbf{A}^t)$

3, 4: If a vector space $\mathbf{V} \neq (O)$ has only finitely many vectors, the field $\mathbf{F}$ must be finite: Otherwise just the multiples cv of a nonzero vector $v \in \mathbf{V}$ would be an infinite set.

$\mathbf{V}$ must have a basis, that is there is a set $v_1, \ldots, v_n$ such that any vector $v \in \mathbf{V}$ is a unique linear combination

$$v = c_1 v_1 + \cdots + c_n v_n$$

Any choice of the n-tuple $(c_1, \ldots, c_n)$ gives rise to a vector. If $\mathbf{F}$ has cardinality q, then there are q^n n-tuples.

We have already seen the number of elements in a field is a power a prime, $q = p^m$. Since 6 is not a power of a prime, there is no field or vectorspace with 6 vectors.

3:

To get two vector spaces with just 4 vectors:

1. Pick $\mathbf{F} = \mathbb{Z}_2$, and $\mathbf{V} = \mathbf{F}^2 = \{(0,0),(0,1),(1,0),(1,1)\}$
2. For **F** pick the field with 4 elements given in class. For $\mathbf{V} = \mathbf{F}$ itself, or another copy of it. [Any field is also a vector space over itself.]

Outline

Sample Quiz

- (4 pts) Prove that a vector space **V** cannot have a basis with 4 elements and another basis with 3 elements.
- (3 pts) Let $f(x)$ be a real polynomial of degree n. Prove that $f(x)$ and its higher derivatives form a basis for the space $\mathbb{R}_n[x]$.
- (3 pts: do one) Give an example of a vector space **V** that has only 4 vectors.

  (b) Explain why a vector space cannot have just 6 vectors.