Vector Spaces and Their Subspaces

A Powerful Abstraction

A. Havens

Department of Mathematics
University of Massachusetts, Amherst

March 19, 2018

Outline

1. Definition of a Vector Space
   - Fields
   - Defining Vector Spaces Axiomatically
   - Examples
2. Subspaces
   - Definition of a Vector Subspace
   - The Subspace Test
   - Examples
3. Linear Maps and Associated Subspaces
   - Linear Transformations of Vector spaces
   - Images and Kernels
   - Column and Null Spaces

Introduction

Thus far, we have studied linear maps between real vector spaces $\mathbb{R}^n$ and $\mathbb{R}^m$ using matrices and phrasing results both in the language of linear functions and in the language of solutions to linear systems.

We now undertake to uncover a generalization of the language of vectors, linear maps, and spaces which proves useful throughout mathematics and physics, and has applications in areas such as information theory, computer science and engineering.

That is, we wish to define a general notion of *vector space*, which will give us the freedom to study a richer set of objects with the same language.

Introduction

For example, one can study spaces of

- polynomials,
- binary codes,
- infinite sequences,
- continuous, analytic, and differentiable functions,
- differential equations,
- tangent data to geometric objects, such as tangent spaces to surfaces and manifolds,
- "infinitesimal symmetries" of dynamical systems. . .

all endowed with a "vector arithmetic" and a "scalar action" appropriate to the collection of objects, and all capable of supporting a theory of linear maps and linear equations.

An Initial Abstraction: Fields

Before we fully abstract the notion of vectors, let's look at a simpler example of abstraction which will appear in our definition of vector spaces: that of an *algebraic field*. This will generalize the idea of a number system with two compatible operations called addition and multiplication.

Consider the arithmetic of the following sets: the integers $\mathbb{Z}$, the rationals $\mathbb{Q} := \{p/q \,|\, p, q \in \mathbb{Z},\ \gcd(p, q) = 1\}$, and the real numbers $\mathbb{R}$. Note that $\mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$.

Each of these sets has an addition and a multiplication. We will examine the common algebraic features of these before abstracting.

Properties of Arithmetic on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$

The addition for all three sets is *commutative* and *associative*. Moreover, the element 0 is in each set, and acts as an *identity element for addition*. Finally, addition is invertible for each of these sets.

The multiplication in each set is also *commutative* and *associative*. The element 1 is in each of these sets, and acts as an *identity element for multiplication*. The multiplication is invertible for the reals and the rationals (except 0), but not for the integers! E.g. there is no 2^{-1} in $\mathbb{Z}$.

Finally, observe that in all cases multiplication *distributes over addition*.

How to Abstract: Definition by Axioms

We can define a notion of a *binary operation* to capture the notion of having an addition or a multiplication, and from there we can define a generalization by asking that a set have one or more binary operations, and we can list the features we expect our operations to satisfy.

Such a definition is one made *axiomatically*.

What do we do with the information we have about arithmetic in $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$? First, we decide which properties are important enough to include, then we make our axioms.

How to Abstract: Definition by Axioms

If we include only one operation and forget about commutativity, but keep associativity, identity, and inverse, we end up with the mathematical notion of a *group*. The integers with addition are a simple example.

Groups are interesting to study as they are the natural setting for studying symmetries of objects. We want a more specific (less abstract?) notion to correspond to a field. We'll say a tiny bit more about groups later.

The mathematical notion of a field will generalize the reals and the rationals, in that we want an abstraction with an *invertible multiplication*, and we want both addition and multiplication to be *commutative*. Finally, we want a distributive property for multiplication over sums.

Binary Operations

First, we formally define *binary operations*, which will be an important notion when we define vector spaces.

Definition

Given a set S, a *binary operation on S* is a function $\mu : S \times S \to S$. Thus, μ is an S-valued map on ordered pairs $(s, t) \in S \times S$.

A binary operation μ on S is said to be *commutative* if for any elements $s, t \in S$, $\mu(s, t) = \mu(t, s)$. A commutative binary operation is said to be *invertible* if there is a function $\nu : S \times S \to S$ such that for any $s, t \in S$, $\nu(s, \mu(s, t)) = t$ and $\mu(\nu(s, t), s) = t$.

One often omits writing μ, and instead writes a symbol such as $+$, $\cdot$, $\times$ or $*$ between elements, or merely juxtaposes them.

Defining Fields

We are ready to define (algebraic) fields.

Definition

A *field* is a set $\mathbb{F}$ together with two binary operations $+ : \mathbb{F} \to \mathbb{F}$ and $\times : \mathbb{F} \to \mathbb{F}$, called *addition* and *multiplication* respectively, subject to the following axioms:

(i) addition is commutative: for any $a, b \in \mathbb{F}$, $a + b = b + a$,

(ii) addition is associative: for any $a, b, c \in \mathbb{F}$, $a + (b + c) = (a + b) + c$,

(iii) there is an additive identity element: there exists an element $0 \in \mathbb{F}$ called *zero* such that for any $a \in \mathbb{F}$, $0 + a = a$,

(iv) addition is invertible: for any $a \in \mathbb{F}$ there is an element $(-a)$ such that $a + (-a) = 0$,

Defining Fields (continued)

Definition

(*v*) multiplication is commutative: for any $a, b \in \mathbb{F}$, $a \times b = b \times a$,

(*vi*) multiplication is associative: for any $a, b, c \in \mathbb{F}$, $a \times (b \times c) = (a \times b) \times c$,

(*vii*) there is a multiplicative identity element (also called *one* or *unity*): there exists an element $1 \in \mathbb{F}$ such that for any $a \in \mathbb{F}$ $1 \times a = a$,

(*viii*) multiplication by nonzero elements is invertible: for any $a \in \mathbb{F} - \{0\}$ there is an element a^{-1} such that $a \times a^{-1} = 1$, and

(*ix*) Multiplication is distributive over addition: for any elements $a, b, c \in \mathbb{F}$, $a \times (b + c) = (a \times b) + (a \times c)$.

Fields and Groups

We can make this definition easier to remember by recalling the idea of a *group*. Groups can also be defined axiomatically:

Definition

A group is a set G with a binary operation $*: G \times G \to G$ such that

(*I*) $*$ is associative: $g * (h * k) = (g * h) * k$ for any $g, h, k \in G$:

(*II*) there is an identity element $e \in G$ for $*$ such that $e * g = g = g * e$ for any $g \in G$, and

(*III*) every element of G has an inverse g^{-1} such that $g * g^{-1} = e = g^{-1} * g$.

Call a group *Abelian* if the group operation is commutative, i.e., if for any $g, h \in G$, $g * h = h * g$.

Succinct Definition of a Field

Having defined groups, we can rephrase the definition of a field in the language of groups. Most of the axioms are then built into the group definition.

Definition

A *field* is a set $\mathbb{F}$, containing elements 0 and 1 called *zero* and *one* respectively, endowed with two binary operations $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and $\times : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, called *addition* and *multiplication* respectively, such that:

- $\mathbb{F}$ is an Abelian group with respect to addition with additive identity $0 \in \mathbb{F}$,
- $\mathbb{F} - \{0\}$ is an Abelian group with respect to multiplication with multiplicative identity $1 \in \mathbb{F}$, and
- multiplication distributes over addition.

Examples of Fields: Rational, Real, and Complex Numbers

Example

The rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$ are fields with respect to their usual notions of addition and multiplication. Because $\mathbb{Q} \subsetneq \mathbb{R}$ and inherits its operations from $\mathbb{R}$, we can call it a *subfield* of $\mathbb{R}$.

Example

The complex numbers $\mathbb{C} := \{a + bi \,|\, a, b \in \mathbb{R},\ i^2 = -1\}$ form a field with arithmetic defined by the rules

- $(a + bi) + (c + di) = (a + c) + (b + d)i$,
- $(a + bi) \times (c + di) = (ac - bd) + (ad + bc)i$,
- $(a + bi)^{-1} = \dfrac{1}{a^2 + b^2}(a - bi)$.

Complex Numbers as Linear Combinations of 1 and i

Remark

Note that the underlying additive structure of $\mathbb{C}$ coincides with the vector arithmetic of $\mathbb{R}^2$.

Further note that $\mathbb{R}$ and $\mathbb{Q}$ are subfields of $\mathbb{C}$. In particular, the elements of $\mathbb{C}$ are real linear combinations of 1 and i.

That is, there is a manner in which 1 and i may be regarded as *vectors*. When we define vector spaces, we will see that fields are vectors spaces.

Field Extensions

Example

Other examples of fields can be built from $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$:

- One can define $\mathbb{Q}(i) := \{a + bi \,|\, a, b \in \mathbb{Q},\ i^2 = -1\}$ with arithmetic analogous to $\mathbb{C}$. This is an example of a *field extension*.
- One can also replace i with something else, such as $\sqrt{5}$, to obtain a field $\mathbb{Q}(\sqrt{5})$ whose elements are rational linear combinations of 1 and $\sqrt{5}$.
- One can adjoin a variable x to $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. The resulting fields are fields of *rational functions*, which are fractions whose numerators and denominators are polynomials. E.g., $\mathbb{R}(x) = \{P(x)/Q(x) \,|\, P, Q \text{ real polynomials in } x,\ Q \neq 0\}$.

Examples of Fields: Finite Fields

Some of the most interesting fields are not built from $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. We look at a particular case of interest: *finite fields with a prime number of elements.*

Fix a prime number p, and let $\mathbb{F}_p$ be the set of *remainder classes modulo* p, which we can identify with the integers $0, 1, \ldots, p-1$. We can define an arithmetic on $\mathbb{F}_p$ by using standard integer addition, and then taking the remainder after dividing by p, and standard multiplication of integers, and then again taking the remainder upon dividing by p.

You should convince yourself that these operations satisfy the conditions necessary of addition and multiplication to make $\mathbb{F}_p$ a field.

The Field with Two Elements

Example

For $p = 2$, we get the *binary field* $\mathbb{F}_2$ whose elements are just 0 and 1, with the arithmetic

$$0+1=1,\ 1+1=0=0+0,\ 1\times 0=0=0\times 0,\ 1\times 1=1\,.$$

Regarding 1 as representing the boolean value *true* and 0 as representing the boolean value *false*, the addition in $\mathbb{F}_2$ corresponds to the boolean operation of *exclusive or*, and the multiplication to the boolean operation of *and*.

Thus, $\mathbb{F}_2$ is the natural field to consider when studying digital logic. We will revisit $\mathbb{F}_2$ in an upcoming example.

The Field with Three Elements

Example

Let $p = 3$. How do we describe $\mathbb{F}_3$?

The remainder classes are 0, 1, and 2, and the arithmetic is encoded in the following table:

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

Abstracting from $\mathbb{R}^n$

As we did when defining fields, we can define a notion of vector space by describing operations on a set, subject to some axioms. We thus must generalize the operations and properties encountered with the real vector space $\mathbb{R}^n$ that we previously defined.

The operations in our generalization will be a notion of vector addition and a notion of multiplication by a scalar. Note that vector addition is a binary operation, while multiplication by a scalar produces a vector from a pairing of a scalar (in the case of $\mathbb{R}^n$, a number from $\mathbb{R}$) with a vector. Our scalars could come from whatever field we would like.

The axioms should mimic the properties we described when we first studied vector arithmetic on $\mathbb{R}^n$.

The Axiomatic Definition of a Vector Space

Definition

Let $\mathbb{F}$ be any field. A *vector space over* $\mathbb{F}$, also called an $\mathbb{F}$-*vector space*, is a set V of objects called vectors, together with a binary operation $+ : V \times V \to V$ called *vector addition*, and a *scalar action* $* : \mathbb{F} \times V \to V$ called *multiplication by a scalar*, subject to the following eight axioms which hold for all vectors $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and scalars $s, t \in \mathbb{F}$:

(*i*) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (vector addition is commutative),

(*ii*) $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ (vector addition is associative),

(*iii*) there is a *zero vector* $\mathbf{0} \in V$ such that $0 + \mathbf{v} = \mathbf{v}$ (additive identity for vector addition),

(*iv*) for each $\mathbf{v}$ there is a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$ (additive inverse for vector addition)

The Axiomatic Definition of a Vector Space (Continued)

Definition

(*v*) $s * (\mathbf{u} + \mathbf{v}) = s * \mathbf{u} + s * \mathbf{v}$ (scalar distributivity over vector sums),

(*vi*) $(s + t) * \mathbf{u} = s * \mathbf{u} + t * \mathbf{u}$ (vector distributivity over scalar sums),

(*vii*) $s * (t * \mathbf{u}) = (st) * \mathbf{u}$ (compatibility with $\mathbb{F}$ product structure),

(*viii*) $1 * \mathbf{u} = \mathbf{u}$ (identity for multiplication by a scalar).

Conventionally, the scalar action is written without the '$*$': $s\mathbf{u} := s * \mathbf{u}$.

A note on the definition

Note that we listed eight axioms. Some definitions use 10 axioms, the extras being the assertion that a sum of vectors is also a vector and the assertion that a scalar multiple of a vector is also a vector.

These *closure axioms* are important, but if you re-read our definition carefully, you will see that they are "baked in" when we define vector addition as a *binary operation* $+ : V \times V \to V$ and multiplication by a scalar as an $\mathbb{F}$-action $* : \mathbb{F} \times V \to V$. In each case the codomain is V, so the operations are closed within V by assumption, and including the axioms in the list would be redundant.

As with fields, there is a more concise way to write the definition of a vector space in the language of Abelian groups.

One-Slide Definition of a Vector Space

Definition

Given a field $\mathbb{F}$, an $\mathbb{F}$-vector space is an Abelian Group V with respect to an addition operation $+ : V \times V \to V$ having identity element $\mathbf{0}$, together with a scalar action of $\mathbb{F}$ on V which for any $\mathbf{u}, \mathbf{v} \in V$ and $s, t \in \mathbb{F}$ satisfies

- $s(\mathbf{u} + \mathbf{v}) = s\mathbf{u} + s\mathbf{v}$,
- $(s + t)\mathbf{u} = s\mathbf{u} + t\mathbf{u}$,
- $s(t\mathbf{u}) = (st) * \mathbf{u}$, and
- $1\mathbf{u} = \mathbf{u}$.

The Canonical Example

Example

For any natural number n, $\mathbb{R}^n$ as previously defined is a vector space over $\mathbb{R}$, with vector addition given by the component-wise addition previously defined, and with scalar multiplication $s\mathbf{u}$ given by multiplying each component of $\mathbf{u}$ by s.

More generally, for any field $\mathbb{F}$, one can consider the set $\mathbb{F}^n$ of n-tuples of elements from $\mathbb{F}$, and make it an $\mathbb{F}$-vector space with component-wise addition and scaling.

Spaces of Matrices

Example

The set of all $m \times n$ matrices with real entries, denoted $\mathbb{R}^{m\times n}$, is a vector space with vector addition given by matrix addition, and with matrix scaling as multiplication by a scalar.

Similarly, one can define spaces of matrices $\mathbb{F}^{m\times n}$ for any field $\mathbb{F}$.

The most useful examples are perhaps, for various n, the spaces of $n \times n$ complex matrices $\mathbb{C}^{n\times n}$, which are of great importance in physics, as various operators in quantum theory are expressed via complex matrices.

A Remark on Notation

It is important to note that writing $+$ between two vectors in V by definition denotes a different operation than writing $+$ between two elements of $\mathbb{F}$.

If we were being truly careful, we'd need new symbols for addition in each space; usually we opt to avoid cumbersome notation and use $+$ despite the ambiguity.

The following example illustrates how the operations need not be as simple as component-wise addition of elements of the base field. For this example, to emphasize the difference between vector addition and addition of elements of a field, we denote vector addition with single quotation marks around the $+$.

A Strange Example

Example

The set $\mathbb{R}_+ = \{x \in \mathbb{R} \,|\, x > 0\}$ can be given a vector space structure as follows:

- The vector addition '$+$': $\mathbb{R}_+ \to \mathbb{R}_+$ is defined by $x\,`{+}\textrm{'}\,y := x \cdot y$ where $x \cdot y$ is the usual product of real numbers. The zero vector in $\mathbb{R}_+$ with this operation is $\mathbf{0} := 1$.
- The scalar action of $\mathbb{R}$ is given by exponentiation: for any s in $\mathbb{R}$, define $s * x := x^s$.

It is left as an exercise to verify that the eight axioms of a vector space are satisfied.

Different Vector Space Structures on One Set

Example

The complex numbers are a vector space over $\mathbb{C}$ in the obvious way (just as $\mathbb{R}$ is a vector space over $\mathbb{R}$ in the obvious way).

But $\mathbb{C}$ also admits a vector space structure over $\mathbb{R}$, when regarded as the set of $\mathbb{R}$-linear combinations of 1 and i.

It is tempting then to say that, as a real vector space, $\mathbb{C}$ is 2 dimensional (since it can be viewed as an $\mathbb{R}$-linear span of two elements).

As a complex vector space, it would then be one dimensional (it's the $\mathbb{C}$-linear span of the single element 1).

We'll generalize this idea and carefully define dimension when we study *bases of vector spaces*.

Spaces of Polynomials

Example

Let $\mathbb{F}$ be an arbitrary field, and denote by $\mathscr{P}_n(\mathbb{F})$ the set of all polynomials of degree $\leq n$ with coefficients in $\mathbb{F}$:

$$\mathscr{P}_n(\mathbb{F}) := \left\{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \,|\, a_0, \ldots, a_n \in \mathbb{F}\right\}.$$

where x is an indeterminate value (so, it is not regarded as an element of $\mathbb{F}$ per se).

Denote by $\mathscr{P}(\mathbb{F})$ the set of *all polynomials over* $\mathbb{F}$, i.e., $\mathscr{P}(\mathbb{F}) = \bigcup_{n\in\mathbb{Z}_{>0}} \mathscr{P}_n(\mathbb{F})$. You can regard $\mathscr{P}(\mathbb{F})$ as the set of all *finite* $\mathbb{F}$-linear combinations of nonnegative powers of an indeterminate x.

How can we regard $\mathscr{P}_n(\mathbb{F})$ and $\mathscr{P}(\mathbb{F})$ as vector spaces?

Spaces of Polynomials

Example

$\mathscr{P}_n(\mathbb{F})$ can be made into a vector space as follows:

- vector addition is given by polynomial addition, which is performed by summing the coefficients of like terms: if $p(x) = \sum_{k=0}^n a_k x^k$ and $q(x) = \sum_{k=0}^n b_k x^k$ then $p(x) + q(x) = \big(p + q\big)(x) = \sum_{k=0}^n (a_k + b_k)x^k$,
- the scalar action is just scaling the whole polynomial: if $s \in \mathbb{F}$ and $p(x) = \sum_{k=0}^n a_k x^k$, then $sp(x) = s\sum_{k=0}^n a_k x^k = \sum_{k=0}^n (sa_k)x^k$.

Often, the notation $\mathscr{P}_n$ or $\mathbb{P}_n$ is used for $\mathscr{P}_n(\mathbb{F})$, when it is understood what field (usually $\mathbb{R}$) is desired. Algebraists often notate $\mathscr{P}(\mathbb{F})$ by $\mathbb{F}[x]$, which is read "$\mathbb{F}$ adjoin x"

A concrete example: Binary Expansions

Example

We will give a concrete interpretation of the spaces $\mathscr{P}_n(\mathbb{F}_2)$ of polynomials with coefficients in the field with two elements.

Let $m \in \mathbb{N}$ be a natural number, and recall that there is some smallest integer n such that there is a unique way to write m as a *binary expansion with n digits*:

$$m = a_0 2^0 + a_1 2^1 + a_2 2^2 + \ldots + a_n 2^n\,, \; a_0, \ldots, a_n \in \{0, 1\} \sim \mathbb{F}_2$$

where we are identifying the integers 0 and 1 with the corresponding elements of $\mathbb{F}_2$.

A concrete example: Binary Expansions

Example

But then observe that such an expansion corresponds to *evaluating a polynomial in* $\mathscr{P}_n(\mathbb{F}_2)$ *by setting* $x = 2$!

Generally, there is a one-to-one correspondence

$$\mathscr{P}_n(\mathbb{F}) = \left\{ \begin{matrix} \mathbb{F}_2 \text{ polynomials} \\ \text{of degree } \leq n \end{matrix} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{matrix} \text{binary expansions of} \\ \text{integers with } \leq n \text{ digits} \end{matrix} \right\}.$$

One can view the space of all binary polynomials $\mathscr{P}(\mathbb{F}_2)$ as the space of all binary expansions of natural numbers.

However, the vector addition of the space is not the same as integer addition! Instead it performs the *bitwise exclusive or* operation. This is still useful in computing, and plays a role in algorithms for addition using binary circuits and boolean logic.

Binary Expansions and Exclusive Or

Example

Find polynomials representing 46 and 37 in binary, and compute 46 xor 37.

$46 = 32 + 8 + 4 + 2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$, whence the corresponding polynomial in $\mathscr{P}_5(\mathbb{F}_2)$ is $p_{46}(x) = 0x^0 + 1x^1 + 1x^2 + 1x^3 + 0x^4 + 1x^5$. The corresponding binary expansion of 46 is thus the list of coefficients, from highest to lowest degree:

$$46_{10} = 101110_2 \,.$$

Binary Expansions and Exclusive Or

Example

Similarly, 37 corresponds to the polynomial $p_{37}(x) = 1x^0 + 0x^1 + 1x^2 + 0x^3 + 0x^4 + 1x^5 \in \mathscr{P}_5(\mathbb{F}_2)$, so $37_{10} = 100101_2$.

The vector sum is $p_{46}(x) + p_{37}(x) = 1x^0 + 1x^1 + 0x^2 + 1x^3 + 0x^4 + 0x^5$, which corresponds to the binary expansion $001011_2 = 11_{10}$. Thus $46 \operatorname{xor} 37 = 11$. Note that this is quite different from the integer sum $46 + 37$. To compute $46 + 37$ using binary arithmetic, one also needs to use the boolean operation of *and* to account for the "carry" terms.

The xor operation also sees application in pseudo-random number generation.

Example: Spaces of Functions

Example

Let $I \subset \mathbb{R}$ be an interval, and let $\mathscr{C}^0(I, \mathbb{R})$ be the set of continuous real valued functions $f : I \to \mathbb{R}$. This can be made an $\mathbb{R}$-vector space with function addition as vector addition and scaling by constants as the scalar action: for any $f, g \in \mathscr{C}^0(I, \mathbb{R})$ and any constant $c \in \mathbb{R}$

- $(f + g)(x) = f(x) + g(x)$ for all $x \in \mathbb{R}$,
- $(c \cdot f)(x) = cf(x)$.

One has to check that the above defined vector addition and scaling are closed for $\mathscr{C}^0(I, \mathbb{R})$ and satisfy the eight axioms. This is a simple exercise once one recalls the definition of continuity via limits, and the linearity properties of limits.

Example: Spaces of Functions

Example

One can similarly study the space of all *continuously differentiable functions* from I with values in $\mathbb{R}$. Denote this by $\mathscr{C}^1(I, \mathbb{R})$.

It is a good exercise to convince yourself via the vector space axioms and your knowledge of differential calculus that this too is a vector space over $\mathbb{R}$.

Moreover, you should notice that the derivative operator furnishes a map from $\mathscr{C}^1(I, \mathbb{R})$ to $\mathscr{C}^0(I, \mathbb{R})$ which sends any finite linear combination of functions to the corresponding linear combination of their derivatives with the same constant weights.

Example: Spaces of Functions

Example

More generally, if V is any $\mathbb{F}$-vector space, and X is any set, then the set X^V of all V-valued functions on X forms a vector space with addition defined by using the addition of images in V pointwise, and with the natural $\mathbb{F}$-scaling action that acts by scaling the values of functions: for any $f, g \in V^X$ and $c \in \mathbb{F}$

- $(f + g)(x) = f(x) + g(x)$ for all $x \in X$,
- $(c \cdot f)(x) = cf(x)$.

Example: Spaces of Functions

Example

The above cases of $\mathscr{C}^0(I,\mathbb{R})$ and $\mathscr{C}^1(I,\mathbb{R})$ arise as subsets of the space $\mathbb{R}^I$ of *all* real valued functions from the interval I, but additional structures (continuity, respectively differentiability) are assumed. $\mathscr{C}^0(I,\mathbb{R})$ and $\mathscr{C}^1(I,\mathbb{R})$ have their own vector space structures defined using the operation inherited from this larger space of functions.

In such a case, one must check that the extra structure is preserved by vector addition and scaling, i.e. that the operations are closed on the subset.

This leads us naturally to the idea of *subspaces* of a vector space.

Defining a vector subspace

Definition

A subset W of an $\mathbb{F}$-vector space V is called an $\mathbb{F}$-vector subspace of V if $\mathbf{0} \in W$, and it is closed under vector addition and multiplication, that is, for all $\mathbf{v}, \mathbf{w} \in W$ and any scalar $s \in \mathbb{F}$:

- $\mathbf{v} + \mathbf{w} \in W$,
- $s\mathbf{v} \in W$.

If the base field is understood, one simply says W is/is not a vector subspace of V. In casual conversation, you can even omit the word "vector", so long as everyone knows what vector space structure you are working with on V.

Defining a vector subspace

Another way of defining a vector subspace is to say that a subset $W \subseteq V$ of a vector space V is a subset which is itself a vector space with the restricted operations it inherits from V and with the zero vector inherited from V as well.

It is immediate that these definitions are equivalent, for suppose $\mathbf{0} \in W \subset V$ and W. Then

- if W is a vector space with inherited operations, this necessitates closure under vector addition and scaling, and
- if W is closed with respect to the addition and scaling inherited from V, then these restrict to operations which are known to satisfy the requisite axioms of a vector space.

Testing if a set is a subspace

We now give an easy criterion to apply to determine whether a subset of a vector space is or is not a subspace.

Proposition

Let V be a vector space over a field $\mathbb{F}$. A nonempty subset $W \subseteq V$ is a vector subspace of V if and only if for all $\mathbf{v}, \mathbf{w} \in W$ and $s \in \mathbb{F}$, $s\mathbf{v} + \mathbf{w} \in W$.

Proof.

If W is a vector space it is immediate that for all $\mathbf{v}, \mathbf{w} \in W$ and $s \in \mathbb{F}$, $s\mathbf{v} + \mathbf{w} \in W$. Thus we prove the other direction, that if for all $\mathbf{v}, \mathbf{w} \in W$ and $s \in \mathbb{F}$, $s\mathbf{v} + \mathbf{w} \in W$, we can show W is a vector subspace.

Proof (Continued)

Proof.

First, since the condition holds for any $\mathbf{v}$ and $\mathbf{w}$ in W and any scalar, we may choose any $\mathbf{v} \in W$, and take $\mathbf{w} = \mathbf{v}$ and $s = -1$, to conclude that $-\mathbf{v} + \mathbf{v} = \mathbf{0} \in W$.

Taking $\mathbf{u}$ and $\mathbf{w}$ arbitrary and setting $s = 1$, we get that $\mathbf{u} + \mathbf{v} \in W$ so W is closed under vector addition.

Finally, taking $s \in \mathbb{F}$ and $\mathbf{v} \in W$ arbitrary and $\mathbf{w} = \mathbf{0}$, we get that $s\mathbf{v} \in W$, so W is closed under scaling. □

The Trivial and Improper Subspaces

Example

Let V be any $\mathbb{F}$-vector space. There are two subspaces that are obvious, important, and boring:

- the *trivial subspace* $\{\mathbf{0}\} \subseteq V$, and
- the *improper subspace* $V \subseteq V$.

It is easy to check with the above test that these are subspaces.

A subspace W is called *nontrivial* if it contains a nonzero vector, and is called *proper* if there is at least one vector in V that is not in W.

The Trivial and Improper Subspaces

Example

Note that $\mathbf{0}$ is contained in every subspace of V, whence every subspace of V also has a trivial subspace.

Indeed, $\{\mathbf{0}\}$ is the *intersection* of all nontrivial subspaces.

The improper subspace V is the *union* of all *proper* subspaces.

Example: $\mathbb{R}^2$, $\mathbb{R}^3$, and the *xy*-plane

Example

$\mathbb{R}^2$ is not a subspace of $\mathbb{R}^3$, since $\mathbb{R}^2 \not\subset \mathbb{R}^3$. However, there are many subsets of $\mathbb{R}^3$ that "look like" $\mathbb{R}^2$, e.g., the x_1x_2-plane.

Similarly, using the definitions in this course, $\mathbb{R}$ is not a subspace of $\mathbb{R}^2$, $\mathbb{R}^3$, or $\mathbb{R}^n$ for any $n > 1$.

However, it *is natural* to regard $\mathbb{R}$ as a subspace of $\mathbb{C}$ when $\mathbb{C}$ is given the structure of a *real vector space*.

A Subtly of Subfields

Example

Yet, $\mathbb{R}$ is not a *complex vector subspace of the complex vector space* $\mathbb{C}$, since scaling a real number by *i* produces an imaginary number.

Similarly, though $\mathbb{Q}$ is a subset of $\mathbb{R}$ which is closed under addition, it is not closed under scaling by a real number. E.g., $1/2 \in \mathbb{Q}$, but $\pi(1/2) = \pi/2 \notin \mathbb{Q}$.

On the other hand, $\mathbb{R}$ can be viewed as a vector space over $\mathbb{Q}$, and $\mathbb{Q}$ is a $\mathbb{Q}$-vector subspace of $\mathbb{R}$ with respect to the $\mathbb{Q}$-vector space structure on $\mathbb{R}$.

Thus there are examples of *subfields* of a field $\mathbb{F}$, that are *not* $\mathbb{F}$-vector *subspaces* of $\mathbb{F}$. The moral is, the choice of vector space structure matters when talking about subspaces!

Example: Lines and Planes through $\mathbf{0}$

Example

In any vector space $\mathbb{R}^n$, $n \geq 3$, there are many subspaces that "look like" $\mathbb{R}$ or $\mathbb{R}^2$, namely, lines and planes through $\mathbf{0}$.

Indeed, these can be defined as spans of one vector or two linearly independent vectors, respectively. From the definition of a span, it is easy to show that these are vector subspaces.

Example: Spans are Subspaces

Claim

We can in fact show that, given any $\mathbb{F}$-vector space V, and some elements $\mathbf{v}_1, \ldots, \mathbf{v}_k$, the set $\mathrm{Span}_{\mathbb{F}}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} \subseteq V$ consisting of all $\mathbb{F}$-linear combinations is a vector subspace.

Here, an $\mathbb{F}$-linear combination is just a linear combination $\sum_{i=1}^k a_i\mathbf{v}_i$ where each a_i is an element of $\mathbb{F}$.

Proof.

To prove this claim, let's apply the subspace test. For any $\mathbf{u}, \mathbf{w} \in \mathrm{Span}_{\mathbb{F}}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$, there are sets of scalars $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{F}$ such that $\mathbf{u} = \sum_{i=1}^k a_i\mathbf{v}_i$ and $\mathbf{w} = \sum_{i=1}^k b_i\mathbf{v}_i$.
Now let $s \in \mathbb{F}$ be any arbitrary scalar. Then

$$s\mathbf{u}+\mathbf{w} = s\sum_{i=1}^k a_i\mathbf{v}_i + \sum_{i=1}^k b_i\mathbf{v}_i = \sum_{i=1}^k (sa_i+b_i)\mathbf{v}_i \in \mathrm{Span}_{\mathbb{F}}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}.$$

□

Example: Even Polynomials

Example

The set of polynomials $\{p(x^2)\,|\,p(x) \in \mathscr{P}_n(\mathbb{F})\} \subset \mathscr{P}_{2n}(\mathbb{F})$ is a subspace of $\mathscr{P}_{2n}(\mathbb{F})$. This is just the set of even polynomials of degree less than or equal to $2n$.

It is clear that this set is closed under addition and scaling, as the constant zero polynomial is even, the sum of two even polynomials is even, and a constant multiple of an even polynomial is even.

What about the odd degree polynomials? Are they a subspace? No, since the zero polynomial is not odd.

Example: Differentiable functions are Continuous

Example

One can apply the result that any differentiable function is continuous, together with a subspace test, to show that the space of $\mathbb{R}$-valued differentiable functions on an interval is a subspace of $\mathscr{C}^0(I, \mathbb{R})$.

Similarly, the *continuously differentiable* functions $\mathscr{C}^1(I, \mathbb{R})$ form a subspace of the differentiable functions, and of the continuous functions.

Nesting Spaces of Functions

The subspace structures of function spaces are very rich and complex; there are many more interesting subspaces of the function spaces we've encountered.

For example, you can consider k-times continuously differentiable functions $\mathscr{C}^k(I,\mathbb{R})$, infinitely differentiable functions $\mathscr{C}^\infty(I,\mathbb{R})$, or *analytic functions* $\mathscr{C}^\omega(I,\mathbb{R})$ (which possess convergent power series over the interval I).

How are these subspaces nested?

$$\mathscr{C}^\omega(I,\mathbb{R}) \subsetneq \mathscr{C}^\infty(I,\mathbb{R}) \subsetneq \mathscr{C}^k(I,\mathbb{R}) \subsetneq \mathscr{C}^0(I,\mathbb{R})\,.$$

Definition of a Linear Map between $\mathbb{F}$-Vector Spaces

Definition

Given two $\mathbb{F}$-vector spaces V and W, a function $T : V \to W$ is said to be a *linear transformation*, a *linear map*, or a *linear function* if for all $\mathbf{u}, \mathbf{v} \in V$ and any scalar $s \in \mathbb{F}$

- $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$, and
- $T(s\mathbf{u}) = sT(\mathbf{u})$.

Remark

As with the subspace test, one can show that to check a given map $T : V \to W$ is linear, it suffices to check that for any $\mathbf{u}, \mathbf{v} \in V$ and a scalar $s \in \mathbb{F}$, $T(s\mathbf{u} + \mathbf{v}) = sT(\mathbf{u}) + T(\mathbf{v})$.

The Usual Suspects

Example

All of the previous linear maps $T : \mathbb{R}^n \to \mathbb{R}^m$ we've considered are linear maps between $\mathbb{R}$-vector spaces in the sense of the above definition.

Another example is the transpose map ${}^{\mathrm{t}} : \mathbb{R}^{m\times n} \to \mathbb{R}^{n\times m}$.

We'll now consider some examples of linear maps that involve spaces other than the familiar $\mathbb{R}^n$, and matrix spaces.

Example: d/dx is a Linear Operator

Proposition

Let $I \subset \mathbb{R}$ be an interval. Then the map $\mathrm{d}/\mathrm{dx} : \mathscr{C}^1(I, \mathbb{R}) \to \mathscr{C}^0(I, \mathbb{R})$ is a linear operator from continuously differentiable $\mathbb{R}$-valued functions on I to continuous $\mathbb{R}$-valued functions on I.

Proof.

Let $c \in \mathbb{R}$ be any constant, and $f, g \in \mathscr{C}^1(I, \mathbb{R})$ any $\mathbb{R}$-valued continuously differentiable functions on I. Then by elementary properties of the derivative

$$\frac{\mathrm{d}}{\mathrm{dx}}\left(cf(x) + g(x)\right) = c\frac{\mathrm{d}f}{\mathrm{dx}} + \frac{\mathrm{d}g}{\mathrm{dx}} \in \mathscr{C}^0(I, \mathbb{R})\,.$$

□

Example: Evaluation Maps

Example

For any field $\mathbb{F}$, regard $\mathbb{F}$ as an $\mathbb{F}$-vector space in the usual way, and consider the $\mathbb{F}$-vector space of polynomials $\mathscr{P}(\mathbb{F})$. For any fixed $\alpha \in \mathbb{F}$, there is a map $\mathrm{ev}_\alpha : \mathscr{P}(\mathbb{F}) \to \mathbb{F}$ which maps a polynomial $p(x)$ to it's *evaluation* $p(\alpha) \in \mathbb{F}$.

One can check that ev_α is a linear map. More generally, one can define evaluation maps for any function space V^X, and they always provide a linear map from V^X to V.

The Image and Kernel of a Map

Throughout our definitions and theorems, fix a field $\mathbb{F}$ and a pair of $\mathbb{F}$-vector spaces V and W. If it helps, just imagine $\mathbb{F} = \mathbb{R}$, and then consider what, if anything crucial, might change if instead you used $\mathbb{C}$, $\mathbb{Q}$, or $\mathbb{F}_p$.

Definition

- The *image or range of a linear transformation* $T : V \to W$ is the subset $T(V) := \{T(\mathbf{v}) \,|\, v \in V\} \subseteq W$.
- The *kernel of the linear transformation* $T : V \to W$ is the subset $\ker T := \{\mathbf{v} \in V \mid T(\mathbf{v}) = \mathbf{0}\} \subseteq V$.

Images and Kernels are Subspaces

Proposition

Let $T : V \to W$ be a linear transformation. Then

- *$T(V)$ is a subspace of W, and*
- *$\ker T$ is a subspace of V.*

Proof.

We prove that the kernel $\ker T$ is a subspace of V, and leave the proof that the image $T(V)$ is a subspace of W as an exercise.

Let $\mathbf{u}, \mathbf{v} \in \ker T$, and $s \in \mathbb{F}$ be any scalar. We wish to apply the subspace test. To do this, compute $T(s\mathbf{u} + \mathbf{v})$ using linearity:

$$T(s\mathbf{u}+\mathbf{v}) = sT(\mathbf{u}) + T(\mathbf{v}) = s\mathbf{0} + \mathbf{0} = \mathbf{0} \implies s\mathbf{u} + \mathbf{v} \in \ker T. \qquad \square$$

Example

Example

The kernel of the derivative map $\mathrm{d}/\mathrm{d}x : \mathscr{C}^1(I, \mathbb{R}) \to \mathscr{C}^0(I, \mathbb{R})$ is the set of constants $c \in \mathbb{R}$. Thus $\mathbb{R}$ may be regarded naturally as a subspace of $\mathscr{C}^1(I, \mathbb{R})$.

Similarly, the image of any evaluation map $\mathrm{ev}_t : \mathscr{C}^0(I, \mathbb{R}) \to \mathbb{R}$ for $t \in \mathbb{R}$ is all of $\mathbb{R}$, and $\mathbb{R} \subset \mathscr{C}^0(I, \mathbb{R})$ is a subspace.

Definitions of Column Space and Null Space

Definition

In the case of a linear map $T : \mathbb{R}^n \to \mathbb{R}^m$, there is a matrix A such that $T(\mathbf{x}) = \mathrm{A}\mathbf{x}$, we have special names for the associated kernel and image subspaces:

- The image $T(\mathbb{R}^n)$, being the subspace of $\mathbb{R}^m$ spanned by the columns of A, is called the *column space of* A, and is denoted $\mathrm{Col}\,\mathrm{A}$. Equivalently, if $\mathrm{A} = \left[\begin{array}{ccc} \mathbf{a}_1 & \ldots & \mathbf{a}_n \end{array}\right]$ then $\mathrm{Col}\,\mathrm{A} = \mathrm{Span}\,\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbb{R}^m$
- The kernel of T is also called the *nullspace of* A, and is denoted $\mathrm{Nul}\,\mathrm{A}$. It can also be defined as the set of solutions $\mathbf{x} \in \mathbb{R}^n$ to the homogeneous equation $\mathrm{A}\mathbf{x} = \mathbf{0}$.

Example

Let

$$W = \left\{ \begin{bmatrix} 2c - b \\ a - c \\ 3b - 2a \end{bmatrix} \middle| a, b, c \in \mathbb{R} \right\} \subset \mathbb{R}^3 .$$

(a) Find a matrix A such that $W = \mathrm{Col}\,\mathrm{A}$.

(b) For the matrix A from (a), describe the nullspace $\mathrm{Nul}\,\mathrm{A}$ as a span.

Solution: First, rewrite the elements of W as a span:

Solution: First, rewrite the elements of W as a span:

$$W = \left\{ \begin{bmatrix} 2c - b \\ a - c \\ 3b - 2a \end{bmatrix} \middle| a, b, c \in \mathbb{R} \right\}$$

Solution: First, rewrite the elements of W as a span:

$$W = \left\{ \begin{bmatrix} 2c-b \\ a-c \\ 3b-2a \end{bmatrix} \middle| a,b,c \in \mathbb{R} \right\}$$

$$= \left\{ a\begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix} + b\begin{bmatrix} -1 \\ 0 \\ 3 \end{bmatrix} + c\begin{bmatrix} 2 \\ -3 \\ 0 \end{bmatrix} \middle| a,b,c \in \mathbb{R} \right\}$$

Solution: First, rewrite the elements of W as a span:

$$\begin{aligned} W &= \left\{ \begin{bmatrix} 2c-b \\ a-c \\ 3b-2a \end{bmatrix} \middle| a,b,c\in\mathbb{R} \right\} \\ &= \left\{ a\begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix} + b\begin{bmatrix} -1 \\ 0 \\ 3 \end{bmatrix} + c\begin{bmatrix} 2 \\ -3 \\ 0 \end{bmatrix} \middle| a,b,c\in\mathbb{R} \right\} \\ &= \mathrm{Span}\left\{ \begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ -3 \\ 0 \end{bmatrix} \right\}. \end{aligned}$$

Solution: First, rewrite the elements of W as a span:

$$W = \left\{ \begin{bmatrix} 2c-b \\ a-c \\ 3b-2a \end{bmatrix} \middle| \, a,b,c \in \mathbb{R} \right\}$$

$$= \left\{ a\begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix} + b\begin{bmatrix} -1 \\ 0 \\ 3 \end{bmatrix} + c\begin{bmatrix} 2 \\ -3 \\ 0 \end{bmatrix} \middle| \, a,b,c \in \mathbb{R} \right\}$$

$$= \mathrm{Span}\left\{ \begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ -3 \\ 0 \end{bmatrix} \right\}.$$

Thus the matrix $\mathrm{A} = \begin{bmatrix} 0 & -1 & 2 \\ 1 & 0 & -3 \\ -2 & 3 & 0 \end{bmatrix}$ has $\mathrm{Col}\,\mathrm{A} = W$.

Solution (continued): To describe the nullspace, we solve the homogeneous system $\mathrm{A}\mathbf{x} = \mathbf{0}$, the solution set of which is $\mathrm{Nul}\,\mathrm{A}$. Row reduction yields

$$\mathrm{RREF}\left(\left[\mathrm{A} \mid \mathbf{0}\right]\right) = \left[\begin{array}{ccc|c} 1 & 0 & -3 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right],$$

whence a solution $\mathbf{x}$ to the homogeneous equation has the form

$$\mathbf{x} = t\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} \implies \mathrm{Nul}\,\mathrm{A} = \mathrm{Span}\left\{\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}\right\}.$$

Some remarks about this example:

(1) Observe that our solution to the homogeneous equation implies a dependence relation in the columns $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$ of A. In particular, $3\mathbf{a}_1 + 2\mathbf{a}_2 + \mathbf{a}_3 = \mathbf{0} \implies \mathbf{a}_3 = -3\mathbf{a}_1 - 2\mathbf{a}_2$. We can then rewrite $\mathrm{Col\,A} = \mathrm{Span}\,\{\mathbf{a}_1, \mathbf{a}_2\}$. Since there were pivot positions in the first two columns of $\mathrm{RREF(A)}$, we can deduce that $\mathbf{a}_1$ and $\mathbf{a}_2$ are linearly independent, so this is the "smallest" description of $\mathrm{Col\,A}$ we can produce.

(2) The matrix A is called a *skew-symmetric matrix*, since $\mathrm{A}^{\mathrm{t}} = -\mathrm{A}$. Such matrices are connected to cross products: if $\mathbf{v} = v_1\mathbf{e}_1 + v_2\mathbf{e}_2 + v_3\mathbf{e}_3$ and $\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + x_3\mathbf{e}_3$, then

$$\begin{bmatrix} 0 & -v_3 & v_2 \\ v_3 & 0 & -v_1 \\ -v_2 & v_1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \mathbf{v} \times \mathbf{x}\,.$$

Since $\mathbf{v} \times \mathbf{x} = \mathbf{0} \iff \mathbf{v} \parallel \mathbf{x}$, it follows that $\mathbf{v}$ generates the nullspace.

(3) A final remark: it is not a coincidence that $\mathrm{Col}\, A$ can be written as a span of two elements, while $\mathrm{Nul}\, A$ can be written as the span of one element.

We will soon define *dimension*, and see that, since $\mathrm{Col}\, A$ is the span of a pair of linearly independent vectors, $\mathrm{Col}\, A$ is a 2-dimensional subspace of $\mathbb{R}^3$. Similarly, $\mathrm{Nul}\, A$ is a 1-dimensional subspace.

We'll prove that the sum of the dimension of the column space of a matrix (the *rank*) and the dimension of the nullspace of the matrix (the *nullity*) is equal to the number of columns of the matrix.

Example

Let A be the matrix

$$\mathrm{A} = \begin{bmatrix} 2 & -4 & -2 & 6 \\ -1 & 3 & 2 & -3 \\ 3 & -2 & 1 & 9 \end{bmatrix},$$

and let $\mathbf{u} = \begin{bmatrix} 3 \\ -6 \\ 6 \\ -3 \end{bmatrix}$ and $\mathbf{v} = \begin{bmatrix} 7 \\ 8 \\ 14 \end{bmatrix}$.

(a) Determine if $\mathbf{u}$ is in $\operatorname{Nul}\mathrm{A}$.

(b) Determine if $\mathbf{v}$ is in $\operatorname{Col}\mathrm{A}$.

(c) Express $\operatorname{Nul}\mathrm{A}$ as a span of a collection of vectors.

Solution:

(a) To check if **u** is in $\mathrm{Nul}\,\mathrm{A}$, we only have to compute $\mathrm{A}\mathbf{u}$ and see if it is **0**. Indeed

$$\begin{bmatrix} 2 & -4 & -2 & 6 \\ -1 & 3 & 2 & -3 \\ 3 & -2 & 1 & 9 \end{bmatrix} \begin{bmatrix} 3 \\ -6 \\ 6 \\ -3 \end{bmatrix} = \begin{bmatrix} 6+24-12-18 \\ -3-18+12+9 \\ 9+12+6-27 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

(b) To check if $\mathbf{v} \in \mathrm{Col}\,\mathrm{A}$ we need to check if **v** is a linear combination of the columns of A, which entails determining if the system $\mathrm{A}\mathbf{x} = \mathbf{v}$ has a solution.

Solution (continued):

(b) We need to compute $\mathrm{RREF}\left(\left[\mathrm{A} \mid \mathbf{v}\right]\right)$. You should check that

$$\mathrm{RREF}\left(\left[\mathrm{A} \mid \mathbf{v}\right]\right) = \left[\begin{array}{cccc|c} 1 & 0 & 1 & 3 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Thus, the matrix-vector equation $\mathrm{A}\mathbf{x} = \mathbf{v}$ is inconsistent, and so $\mathbf{v} \notin \mathrm{Col}\,\mathrm{A}$.

(c) Using the same row operations as in part (b):

$$\mathrm{RREF}\left(\left[\mathrm{A} \mid \mathbf{0}\right]\right) = \left[\begin{array}{cccc|c} 1 & 0 & 1 & 3 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right],$$

whence we find that there are two free variables, say s and t, with $x_1 = -s - 3t$, $x_2 = -s$, $x_3 = s$ and $x_4 = t$.

Solution (continued):

(c) Thus a solution to the homogeneous equation $\mathrm{A}\mathbf{x} = \mathbf{0}$ has form

$$\mathbf{x} = \begin{bmatrix} -s-3t \\ -s \\ s \\ t \end{bmatrix} = s\begin{bmatrix} -1 \\ -1 \\ 1 \\ 0 \end{bmatrix} + t\begin{bmatrix} -3 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

It follows that the nullspace can be described as a span of two vectors

$$\mathrm{Nul}\,\mathrm{A} = \mathrm{Span}\left\{\begin{bmatrix} -1 \\ -1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 0 \\ 1 \end{bmatrix}\right\}.$$

Homework

- Please read sections 4.1, 4.2 and 4.3 of the textbook by Friday, 3/23.
- Homework in MyMathLab for section 4.1 on Vector Spaces is due Thursday, 3/22.
- Homework in MyMathLab for section 4.2 on Column and Null Spaces, Images/Ranges and Kernels is due Tuesday, 3/27.
- **Exam 2 will be held Tuesday, April 4/10/18, 7:00PM-9:00PM, location TBA.**
  The syllabus for the second midterm is the following sections of the textbook: 2.2, 2.3, 3.1, 3.2, 3.3, 4.1, 4.2, 4.3, 4.4, 4.5.