Math 108a | Professor: Padraic Bartlett

Lecture 3: Vector Spaces

Week 1 | *UCSB 2013*

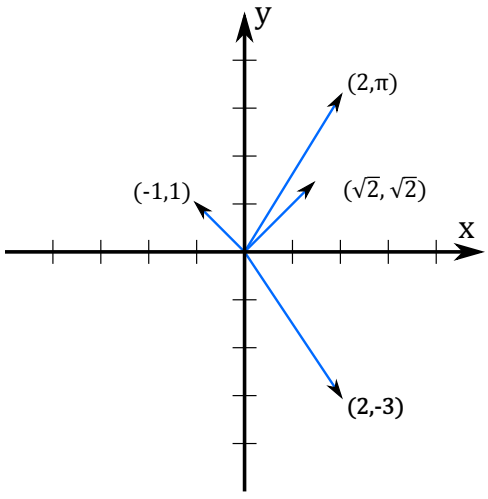
The main reason we studied fields in our first lecture is not because we're particularly interested in the definitions and concepts of fields themselves. (Which is not to say that fields are not interesting mathematical subjects; in fact, there is a remarkably large body of mathematical work devoted to studying fields and related algebraic objects!)

Instead, the main reason we're studying fields in a linear algebra class is because we want to study something built out of fields: **vector spaces**.

1 Vector Spaces, Informally

The two vector spaces you're probably the most used to working with, from either your previous linear algebra classes or even your earliest geometry/precalc classes, are the spaces $\mathbb{R}^2$ and $\mathbb{R}^3$. We briefly remind the reader about how these two vector spaces work here:

Definition. The **vector space** $\mathbb{R}^2$ consists of the collection of all pairs (a, b), where a, b are allowed to be any pair of real numbers. For example, $(2, -3), (2, \pi), (-1, 1)$, and $(\sqrt{2}, \sqrt{2})$ are all examples of vectors in $\mathbb{R}^2$. We typically visualize these vectors as arrows in the xy-plane, with the tail of the arrow starting at the origin[1] and the tip of the arrow drawn at the point in the plane with xy-coördinates given by the vector. We draw four such vectors here:

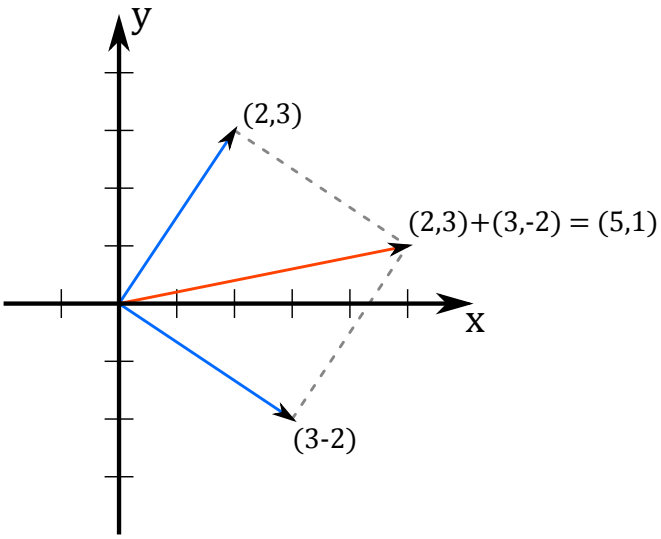


Given a pair of vectors in $\mathbb{R}^2$, we can **add** them together. We do this component-wise, i.e. if we have two vectors (a, b) and (c, d), their sum is the vector $(a+c, b+d)$. For example, the sum of the vectors $(3, -2)$ and $(2, 3)$ is the vector $(5, 1)$.

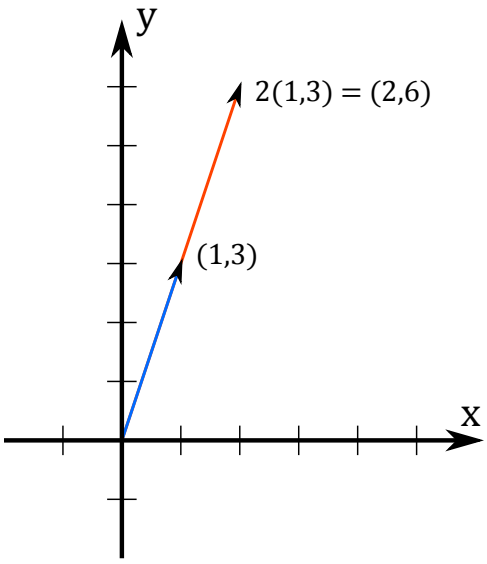
You can visualize this by taking the arrow corresponding to the first vector that we add, and "translating" this arrow over to the start of the second vector; if you travel along the

[1] The origin is the point $(0, 0)$ in the plane.

first vector and then continue along this second translated vector, you arrive at some point in the plane. The arrow connecting the origin to this point is the vector given by the sum of these two vectors! If this seems hard to understand, the diagram below may help some:



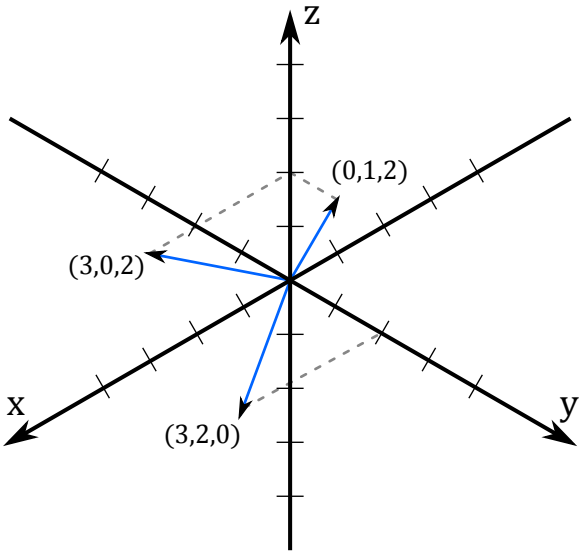
We can also **scale** a vector in $\mathbb{R}^2$ by any real number a. Intuitively, this corresponds to the concept of "stretching:" the vector (x, y) scaled by a, denoted $a(x, y)$, is the quantity (ax, ay). For example, $2(1, 3) = (2, 6)$, and is essentially what happens if we "double" the vector $(1, 3)$. We illustrate this below:



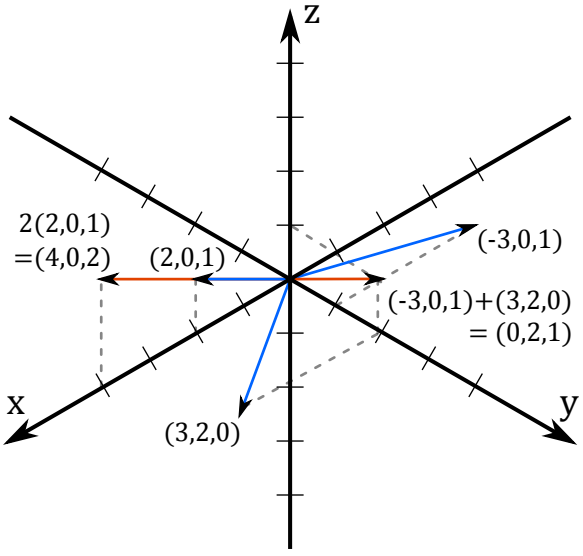
We can define $\mathbb{R}^3$ in a similar fashion:

Definition. The **vector space** $\mathbb{R}^3$ consists of the collection of all pairs (a, b, c), where a, b, c are allowed to be any triple of real numbers. For example, $(0, 1, 2), (3, 0, 2)$, and $(3, 2, 0)$ are all examples of vectors in $\mathbb{R}^3$. We typically visualize these vectors as arrows in three-dimensional xyz-space, with the tail of the arrow starting at the origin and the tip of the

arrow drawn at the point in the plane with xyz-coördinates given by the vector. We draw three such vectors here:



Again, given a pair of vectors in $\mathbb{R}^3$, we can **add** them together. We do this component-wise, i.e. if we have two vectors (a, b, c) and (d, e, f), their sum is the vector $(a+d, b+e, c+f)$. For example, the sum of the vectors $(3, -2, 0)$ and $(2, 1, 2)$ is the vector $(5, -1, 2)$. We can also **scale** a vector in $\mathbb{R}^3$ by any real number a: the vector (x, y, z) scaled by a, denoted $a(x, y, z)$, is the quantity (ax, ay, az). These operations can be visualized in a similar fashion to the pictures we drew for $\mathbb{R}^2$:



You can generalize this discussion to $\mathbb{R}^n$, the vector space made out of n-tuples of real numbers: i.e. elements of $\mathbb{R}^4$ would be things like $(\pi, 2, 2, 1)$ or $(-1, 2, 1, -1)$.

2 Vector Spaces, Formally

In general, there are many other kinds of vector spaces — essentially, anything with the two operations "addition" and "scaling" is a vector space, provided that those operations are well-behaved in certain specific ways. Much like we did with $\mathbb{R}$ and the field axioms, we can generate a list of "properties" for a vector space that seem like characteristics that will insure this "well-behaved" nature. We list a collection of such properties and use them to define a vector space here:

Definition. A **vector space** V over a field F is a set V along with the two operations addition and scalar multiplication, such that the following properties hold:

- **Closure(+)**: $\forall \vec{v}, \vec{w} \in V$, we have $v + w \in V$.
- **Identity(+)**: $\exists \vec{0} \in V$ such that $\forall \vec{v} \in V$, $\vec{0} + \vec{v} = \vec{v}$.
- **Commutativity(+)**: $\forall \vec{v}, \vec{w} \in V, \vec{v} + \vec{w} = \vec{w} + \vec{v}$.
- **Associativity(+)**: $\forall \vec{u}, \vec{v}, \vec{w} \in V, (\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$.
- **Inverses(+)**: $\forall \vec{v} \in V, \exists$ some $-\vec{v} \in V$ such that $\vec{v} + (-\vec{v}) = 0$.
- **Closure($\cdot$)**: $\forall a \in F, \vec{v} \in V$, we have $a\vec{v} \in V$.
- **Identity($\cdot$)**: $\forall \vec{v} \in V$, we have $1\vec{v} = \vec{v}$.
- **Compatibility($\cdot$)**: $\forall a, b \in F$, we have $a(b\vec{v}) = (a \cdot b)\vec{v}$.
- **Distributivity($+, \cdot$)**: $\forall a \in F, \vec{v}, \vec{w} \in V, a(\vec{v} + \vec{w}) = a\vec{v} + a\vec{w}$.

As with fields, there are certainly properties that $\mathbb{R}^n$ satisfies that are not listed above. For example, consider the following property:

- **New property?(+)**: The additive identity, $\vec{0}$, is unique in any vector space. In other words, there cannot be two distinct vectors that are both the additive identity for a given vector space.

Just like before, this property turns out to be redundant: in other words, this property is implied by the definition of a vector space! We prove this here:

Claim. In any vector space, the additive identity is unique.

Proof. Take any two elements $\vec{0}, \vec{0'}$ that are both additive identities. Then, by definition, we know that because $\vec{0}$ is an additive identity, we have

$$\vec{0'} = \vec{0} + \vec{0'}.$$

Similarly, because $\vec{0'}$ is an additive identity, we have

$$\vec{0} = \vec{0'} + \vec{0}.$$

If we use commutativity to switch the $\vec{0}$ and $\vec{0'}$, we can combine these two equalities to get that

$$\vec{0} = \vec{0'} + \vec{0} = \vec{0} + \vec{0'} = \vec{0'}.$$

Therefore, we have shown that $\vec{0}$ and $\vec{0'}$ are equal. In other words, we've shown that all of the elements that are additive identities are all equal: i.e. that they're all the same element! Therefore, this additive identity element is **unique**: there is no other element that is somehow an additive identity that is different from $\vec{0}$. □

As we did with fields, there are a number of other properties that $\mathbb{R}^n$ possesses that you can prove that any vector space must have: in your textbook, there are proofs that every vector has a unique additive inverse, that $0\vec{v}$ is always $\vec{0}$, that $-1\vec{v} = -\vec{v}$, and other such things.

Instead of focusing on more of these proofs, we shift our attention instead to actually describing some vector spaces!

A few of these are relatively simple to come up with:

- $\mathbb{R}^n$, the example we used to come up with these properties, is a vector space over the field $\mathbb{R}$.
- $\mathbb{C}^n$ is similar. Specifically: $\mathbb{C}^n$ is the set of all n-tuples of complex numbers: i.e.

  $$\mathbb{C}^n = \{(z_1, \dots z_n) | z_1, \dots z_n \in \mathbb{C}\}.$$

  Just like with $\mathbb{R}^n$, we can add these vectors together and scale them by arbitrary complex numbers, while satisfying all of the vector space properties. We leave the details for the reader to check, but this is a vector space over the complex numbers $\mathbb{C}$.
- Similarly, $\mathbb{Q}^n$, the set of all n-tuples of rational numbers

  $$\mathbb{Q}^n = \{(q_1, \dots q_n) | q_1, \dots q_n \in \mathbb{Q}\},$$

  is a vector space over the field $\mathbb{Q}$.
- In general, given any field F, we can form the vector space F^n by taking our set to be

  $$F^n = \{(f_1, \dots f_n) | f_1, \dots f_n \in F\}.$$

  We can add these vectors pairwise: i.e. for any $\vec{f} = (f_1, \dots f_n), \vec{g} = (g_1, \dots g_n) \in F^n$, we can form

  $$(f_1, f_2, \dots f_n) + (g_1, g_2, \dots g_n) = (f_1 + g_1, f_2 + g_2 + \dots f_n + g_n).$$

  We can also scale them: for any $\vec{f} \in F^n, a \in F$, we can form the vector

  $$a(f_1, f_2, \dots f_n) = (a \cdot f_1, a \cdot f_2, \dots a \cdot f_n).$$

  It is not hard to check that because F is a field, F^n is forced to satisfy all of the vector space axioms:

  - **Closure(+)**: Immediate. Because F is a field and is closed under addition, the pairwise sums performed in vector addition must create another vector.

- **Identity(+)**: Because F is a field, it has an additive identity, 0. The vector $\vec{0} = (0, 0, \ldots 0)$ is consequently the additive identity for our vector space, as pairwise adding this vector to any other vector does not change any of the other vector's coördinates.
- **Commutativity(+)**: Again, this is a consequence of F being a vector space. Because addition is commutative in F, the pairwise addition in our vector space is commutative.
- **Associativity(+)**: Once more, this is a consequence of F being a vector space. Because addition is associative in F, the pairwise addition in our vector space is associative.
- **Inverses(+)**: Take any $\vec{f} = (f_1, \ldots f_n) \in F^n$. Because F is a field, we know that $(-f_1, \ldots - f_n)$ is a vector in F^n as well. Furthermore, the pairwise addition of these two vectors clearly yields the additive identity $\vec{0}$; therefore, our vector space has inverses.
- **Closure($\cdot$)**: This is a consequence of F being closed under multiplication.
- **Identity($\cdot$)**: Because F is a field, it has a multiplicative identity 1. This 1, when used to scale a vector, does not change that vector at any coördinate because of this multiplicative identity property; therefore 1 is also the scalar multiplicative identity for our vector space.
- **Compatibility($\cdot$)**: This is an immediate consequence from F's multiplication being associative, as for any $a, b \in F$, we have

$$\begin{aligned} a(b(f_1 \ldots f_n) =& a(b \cdot f_1, \ldots b \cdot f_n) = (a \cdot (b \cdot f_1), \ldots a \cdot (b \cdot f_n)) \\ =& (a \cdot b) \cdot f_1, \ldots (a \cdot b) \cdot f_n) = (a \cdot b)(f_1, \ldots f_n). \end{aligned}$$

- **Distributivity($+, \cdot$)**: This is a consequence of F being a vector space. Because multiplication and addition are distributive in F, their combination in our vector space is distributive as well.

- A specific consequence of the above result is that something like $(\mathbb{Z}/5\mathbb{Z})^n$ is a vector space. This is a somewhat strange-looking beast: it's a vector space over a finite-sized field! In particular, it's a vector space with only finitely many elements, which is weird.

  To understand this better, we look at some examples. Consider $(\mathbb{Z}/5\mathbb{Z})^2$. This is the vector space consisting of elements of the form

$$(a, b),$$

  where $a, b \in \{0, 1, 2, 3, 4\}$. We add and scale elements in this vector space using mod-5 modular arithmetic: for example,

$$(2, 3) + (4, 4) = (1, 2),$$

  because $2 + 4 \equiv 1 \mod 5$ and $3 + 4 \equiv 2 \mod 5$. Similarly,

$$2(3, 1) = (1, 2),$$

because $2 \cdot 3 \equiv 1 \mod 5$ and $2 \cdot 1 \equiv 2 \mod 5$.

Perhaps surprisingly, these odd-looking vector spaces are some of the most-commonly used spaces in the theoretical computer science/cryptographic settings. In particular, they come up very often in the field of elliptic curve cryptography, and are instrumental to how a number of modern cryptographic schemes work.

There are some odder examples of vector spaces:

- Polynomials! Specifically, let $\mathbb{R}[x]$ denote the collection of all finite-degree polynomials in one variable x with real-valued coefficients. In other words,

$$\mathbb{R}[x] = \{a_0 + a_1 x + \dots a_n x^n | a_0, \dots a_n \in \mathbb{R}, n \in \mathbb{N}\}.$$

  Verifying that this is a vector space is not very difficult:

  - **Closure**$(+)$: Adding two polynomials together clearly gives us another polynomial.
  - **Identity**$(+)$: Adding 0 to any polynomial doesn't change it, and 0 is a polynomial itself (simply pick $a_0 = 0$ and $n = 0$.)
  - **Commutativity**$(+)$: We can add polynomials in any order that we want, and we'll always get the same answer. (This is because addition in $\mathbb{R}$ is commutative, and we just add polynomials by grouping common powers of x and adding their real-valued coefficients together!)
  - **Associativity**$(+)$: Holds for the precise same reason that commutativity holds.
  - **Inverses**$(+)$: Given any polynomial $a_0 + \dots a_n x^n$, the polynomial $-a_0 + \dots - a_n x^n$ is its additive inverse, as summing these two polynomials gives us 0.
  - **Closure**$(\cdot)$: Multiplying a polynomial by a real number clearly gives us another polynomial.
  - **Identity**$(\cdot)$: Multiplying a polynomial by 1 clearly gives us the same polynomial back.
  - **Distributivity**$(+, \cdot)$: Holds for the precise same reason that commutativity holds.

- Matrices! Specifically, let $M_{\mathbb{R}}(n, n)$ denote the set of $n \times n$ matrices with real-valued entries. For example

$$M_{\mathbb{R}}(3,3) = \left\{ \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \;\middle|\; a, b, c, d, e, f, g, h, i \in \mathbb{R} \right\}.$$

  If we define matrix addition as simply entrywise addition: i.e.

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \dots & a_{nn} + b_{nn} \end{bmatrix},$$

and scalar multiplcation as simply entrywise multiplication, i.e.

$$c\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} = \begin{bmatrix} ca_{11} & ca_{12} & \dots & ca_{1n} \\ ca_{21} & ca_{22} & \dots & ca_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ ca_{n1} & ca_{n2} & \dots & ca_{nn} \end{bmatrix},$$

then this is a vector space! Specifically, it's a vector space for precisely the same reasons that $\mathbb{R}^n$ is a vector space: if you just think of a $n \times n$ matrix as a very oddly-written vector in $\mathbb{R}^{n^2}$, then every argument for why $\mathbb{R}^{n^2}$ is a vector space carries over to $M_{\mathbb{R}}(n, n)$.

It might seem odd to think of matrices as a vector space, but if you go further in physics or pure mathematics, this is an incredibly useful and common construction.