Math 5111 (Algebra 1)

Lecture #4 $\sim$ September 21, 2020

Fields and Vector Spaces

- Fields + Basic Examples
- Vector Spaces
- Subfields and Field Extensions

This material represents §2.1.1-2.2.1 from the course notes.

Overview of §2: Fields and Field Extensions

Now that we have set the table, so to speak, by discussing the basics of rings and polynomials, we can now start our discussion of fields.

- We start (today) with some additional examples of fields, and then review vector spaces over an arbitrary field, which provide important tools for our later study.
- Then we discuss subfields and field extensions, and explore the deep connections between polynomials and fields.
- We will give a variety of applications of field theory, such as the impossibility of certain classical straightedge-and-compass constructions such as trisecting an arbitrary angle and doubling the cube.
- We will also discuss at length the structure of fields obtained by "adjoining" roots of polynomials, and in particular the (historically perilous) topic of establishing that every field has an algebraic closure.

Fields, I

Recall the definition of a field:

Definition

A field is any set F having two (closed) binary operations $+$ and $\cdot$ that satisfy the nine axioms [F1]-[F9]:

[F1] *$+$ is associative: $a+(b+c)=(a+b)+c$ for any a, b, c in F.*

[F2] *$+$ is commutative: $a+b=b+a$ for any a, b in F.*

[F3] *There is an additive identity 0 with $a+0=a$ for all $a \in F$.*

[F4] *Every $a \in F$ has an additive inverse $-a$ with $a+(-a)=0$.*

[F5] *$\cdot$ is associative: $a \cdot (b \cdot c)=(a \cdot b) \cdot c$ for any a, b, c in F.*

[F6] *$\cdot$ is commutative: $a \cdot b=b \cdot a$ for any a, b in F.*

[F7] *There is a mult. identity $1 \neq 0$ with $1 \cdot a=a$ for all $a \in F$.*

[F8] *Every nonzero $a \in F$ has an inverse a^{-1} satisfying $a \cdot a^{-1}=1$.*

[F9] *$\cdot$ distributes over $+$: $a \cdot (b+c)=a \cdot b+a \cdot c$ for all $a, b, c \in F$.*

Fields, II

We have previously mentioned some examples of fields:

1. The rational numbers $\mathbb{Q}$ are a field.
2. The real numbers $\mathbb{R}$ are a field.
3. The complex numbers $\mathbb{C}$ are a field.
4. If p is a prime number, then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field.
5. If F is any field and p is any irreducible polynomial in $F[x]$, then the ring $F[x]/p$ of residue classes modulo p is also a field.

Fields, III

Some additional examples of fields:

6. If F is a field, the collection of rational functions in t with coefficients in F, denoted $F(t)$, forms a field.
   - We use the letter t to denote the indeterminate rather than x, since we will later want to discuss polynomials in the context of this field of rational functions.
   - Explicitly, the elements of this field are quotients of polynomials $\frac{p}{q}$ where $p, q \in F[t]$ and $q \neq 0$, and where $\frac{p}{q} = \frac{r}{s}$ whenever $ps = rq$.
   - Addition and multiplication are defined in the same way as for fractions: $\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs}$ and $\frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$.
   - It is tedious (but straightforward) to verify that these operations are well-defined and satisfy the field axioms.
   - This field is the fraction field of the polynomial ring $F[t]$.

Fields, III

Some additional examples of fields:

7. The set $S = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ forms a field, denoted $\mathbb{Q}(\sqrt{2})$ (typically read as "$\mathbb{Q}$ adjoin $\sqrt{2}$").
   - The arithmetic in $\mathbb{Q}(\sqrt{2})$ is as follows: $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$, and $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$.
   - Since $\mathbb{Q}(\sqrt{2})$ is clearly closed under subtraction and multiplication, and contains $0 = 0 + 0\sqrt{2}$, it is a subring of $\mathbb{C}$ and hence an integral domain, since it contains 1.
   - To see that $\mathbb{Q}(\sqrt{2})$ is actually a field, we need to show that every element has a multiplicative inverse: this follows by "rationalizing the denominator", since we can write $(a + b\sqrt{2})^{-1} = \dfrac{a - b\sqrt{2}}{a^2 - 2b^2}$, and as long as one of a, b is nonzero the denominator is also nonzero because $\sqrt{2}$ is irrational.

Fields, IV

Some additional examples of fields:

8. The set $S = \{a + bi : a, b \in \mathbb{Q}\}$ forms a field, denoted $\mathbb{Q}(i)$. (As usual, i denotes the imaginary unit with $i^2 = -1$.)
   - The arithmetic in $\mathbb{Q}(i)$ is the same as for regular complex numbers: $(a + bi) + (c + di) = (a + c) + (b + d)i$, and $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.
   - Like with $\mathbb{Q}(\sqrt{2})$ we can see that every nonzero element has a multiplicative inverse, since $(a + bi)^{-1} = \dfrac{a - bi}{a^2 + b^2}$, so $\mathbb{Q}(i)$ is a field.

Fields, V

The last two examples are special cases of a more general class:

Definition

Let D be a squarefree integer not equal to 1. The quadratic field $\mathbb{Q}(\sqrt{D})$ is the set of complex numbers of the form $a + b\sqrt{D}$, where a and b are rational numbers.

Remark: An integer is squarefree if it is not divisible by the square of any prime. We do not lose any generality by assuming that D is a squarefree integer (think about why this is).

- As in the two special cases $D = 2$ and $D = -1$ analyzed on the last two slides, $\mathbb{Q}(\sqrt{D})$ is a field because we can write $(a + b\sqrt{D})^{-1} = \dfrac{a - b\sqrt{D}}{a^2 - Db^2}$, and $a^2 - Db^2 \neq 0$ provided that a and b are not both zero because $\sqrt{D}$ is irrational (by the assumption that D is squarefree and not equal to 1).

Fields, VI

Here is an important quantity related to quadratic fields:

Definition

Let D be a squarefree integer not equal to 1. The quadratic field norm is the function $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ defined via $N(a + b\sqrt{D}) = a^2 - Db^2 = (a + b\sqrt{D})(a - b\sqrt{D})$.

- The fundamental property of this field norm is that it is multiplicative: $N(xy) = N(x)N(y)$ for two elements x and y in $\mathbb{Q}(\sqrt{D})$, as can be verified by writing out both sides explicitly and comparing the results.
- The field norm provides a measure of "size" of an element of $\mathbb{Q}(\sqrt{D})$, in much the same way that the complex absolute value measures the "size" of a complex number. In fact, if $D < 0$, then the field norm of an element $a + b\sqrt{D}$ is the same as the square of its complex absolute value.

Fields, VII

Fields inherit all of the properties of integral domains:

Proposition (Basic Field Arithmetic)

The following properties hold in any field F:

1. *0 and 1 are unique, as are additive and multiplicative inverses.*
2. *Addition has a cancellation law: $a + b = a + c$ implies $b = c$.*
3. *Multiplication has a cancellation law: if $a \neq 0$ then $ab = ac$ implies $b = c$. In particular, $ab = 0$ implies $a = 0$ or $b = 0$.*
4. *For any $a \in F$, $0 \cdot a = 0 = a \cdot 0$ and $(-1) \cdot a = -a$.*
5. *For any $a, b \in F$, $-(a + b) = (-a) + (-b)$, $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$, and $(-a) \cdot (-b) = a \cdot b$.*
6. *For any $m, n > 0$ and any $a \in F$, $ma + na = (m + n)a$, $m(na) = (mn)a$, $a^{m+n} = a^m a^n$, and $a^{mn} = (a^m)^n$.*

Fields, VIII

Another fundamental property of a field is its characteristic:

Definition

If F is a field, we say F has characteristic p if $p1_F = 0$, and no smaller positive integer multiple of 1 is 0. (Recall that $p1_F = \underbrace{1_F + 1_F + \cdots + 1_F}_{p \text{ times}}$.)

If $n1_F \neq 0$ for all $n > 0$, then we say F has characteristic 0.

- Example: The fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ have characteristic 0.
- Example: For a prime p, the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p.
- Any finite field necessarily has positive characteristic, although infinite fields with positive characteristic also exist, such as the function field $\mathbb{F}_p(t)$.

Fields, IX

The characteristic of a field is either 0 or a prime number:

Proposition (Positive Characteristic)

If the field F has characteristic $p > 0$, then p is a prime.

Proof:

- Suppose F has characteristic $m > 0$ and $m = ab$ for positive integers a, b: then $0 = m1_F = (a1_F) \cdot (b1_F)$.
- Since F is a field, this implies that one of $a1_F$ and $b1_F$ must be zero, but since m is minimal, the only possibility is that $a = m$ or $b = m$, meaning that m must be prime.

Vector Spaces, I

Vector spaces are a central ingredient for studying fields.

- We will not need very much of linear algebra in this course, so the goal is just to review some of the basic properties of vector spaces over an arbitrary field.
- However, please note that linear algebra is wonderful and, no matter how much linear algebra you have learned, you should learn more of it[1].

[1] Seriously, go learn more linear algebra. But not right now.

Vector Spaces, II

Definition

Let F be a field, and refer to the elements of F as scalars. A vector space over F is a collection V of vectors, together with two binary operations, addition of vectors $(+)$ and scalar multiplication of a vector by a scalar $(\cdot)$, satisfying the following axioms:

[V1] *$+$ is commutative: $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$ for any vectors $\mathbf{v}$ and $\mathbf{w}$.*

[V2] *$+$ is associative: $(\mathbf{u}+\mathbf{v})+\mathbf{w}=\mathbf{u}+(\mathbf{v}+\mathbf{w})$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$.*

[V3] *There exists a zero vector $\mathbf{0}$, with $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $v \in V$.*

[V4] *Every $\mathbf{v} \in V$ has an additive inverse $-\mathbf{v}$, with $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.*

[V5] $\alpha \cdot (\beta \cdot \mathbf{v}) = (\alpha\beta) \cdot \mathbf{v}$ *for any $\alpha, \beta \in F$ and $\mathbf{v} \in V$.*

[V6] $(\alpha + \beta) \cdot \mathbf{v} = \alpha \cdot \mathbf{v} + \beta \cdot \mathbf{v}$ *for any scalars α, β and vector $\mathbf{v}$.*

[V7] $\alpha \cdot (\mathbf{v} + \mathbf{w}) = \alpha \cdot \mathbf{v} + \alpha \cdot \mathbf{w}$ *for any $\alpha \in F$ and $\mathbf{v}, \mathbf{w} \in V$.*

[V8] *1 acts like the identity: $1 \cdot \mathbf{v} = \mathbf{v}$ for any $\mathbf{v} \in V$.*

Vector Spaces, III

Here are a few standard examples of vector spaces:

1. For any positive integer n, the set of all n-tuples of elements from F, denoted F^n, is an F-vector space under componentwise addition and scalar multiplication.
   - Explicitly, the operations in F^n are componentwise addition and scalar multiplication:
     $\langle a_1, a_2, \ldots, a_n \rangle + \langle b_1, b_2, \ldots, b_n \rangle =$
     $\langle a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n \rangle$ and
     $\alpha \cdot \langle b_1, b_2, \ldots, b_n \rangle = \langle \alpha b_1, \alpha b_2, \ldots, \alpha b_n \rangle$.
   - The additive identity is the zero vector $\langle 0, 0, \ldots, 0 \rangle$ and additive inverses are given by negating each component:
     $-\langle b_1, b_2, \ldots b_n \rangle = \langle -b_1, -b_2, \ldots, -b_n \rangle$.

Vector Spaces, III

Here are a few standard examples of vector spaces:

2. The zero space with a single element $\mathbf{0}$, with $\mathbf{0} + \mathbf{0} = \mathbf{0}$ and $\alpha \cdot \mathbf{0} = \mathbf{0}$ for every $\alpha \in F$, is an F-vector space.
3. Any field is a vector space over itself (with its own addition and multiplication operations).
4. The rings $F[x]$ and $F[x]/p$ for any polynomial p are F-vector spaces.
5. Under the normal addition and multiplication, $\mathbb{R}$ is a vector space over $\mathbb{Q}$.
6. Under the normal addition and multiplication, $\mathbb{C}$ is a vector space over $\mathbb{Q}$. $\mathbb{C}$ is also a vector space over $\mathbb{R}$.

Vector Spaces, IV

Like with rings and fields, vector spaces have some basic arithmetic properties that can be derived immediately from the axioms:

Proposition (Basic Arithmetic in Vector Spaces)

In any vector space V, the following are true:

1. *The additive identity 0 is unique, as are additive inverses.*
2. *Addition has a cancellation law: for any $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$, if $\mathbf{a} + \mathbf{b} = \mathbf{a} + \mathbf{c}$, then $\mathbf{b} = \mathbf{c}$.*
3. *For any $\mathbf{v} \in V$, $0 \cdot \mathbf{v} = \mathbf{0}$, and for any $\alpha \in F$, $\alpha \cdot \mathbf{0} = \mathbf{0}$.*
4. *For any $\mathbf{v} \in V$, $(-1) \cdot \mathbf{v} = -\mathbf{v}$, and $-(-\mathbf{v}) = \mathbf{v}$.*

Proofs: Straightforward from the axioms.

Vector Subspaces

Our interest is in studying the structure of vector spaces and using them to say things about fields. First, subspaces:

Definition

A subspace W of a vector space V is a subset of the vector space V which, under the same addition and scalar multiplication operations as V, is itself a vector space.

Examples:

- Any vector space V has two obvious subspaces: the zero space and V itself.
- As a $\mathbb{Q}$-vector space, $\mathbb{R}$ is a subspace of $\mathbb{C}$.

Linear Combinations and Span, I

Definition

Given a set $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ of vectors in a vector space V, we say a vector $\mathbf{w}$ in V is a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ if there exist scalars $a_1, \cdots, a_n$ such that $\mathbf{w} = a_1 \cdot \mathbf{v}_1 + a_2 \cdot \mathbf{v}_2 + \cdots + a_n \cdot \mathbf{v}_n$.

In other words, a vector $\mathbf{w}$ is a linear combination of other vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ if we can obtain $\mathbf{w}$ from the $\mathbf{v}_i$ using the basic vector space operations.

Linear Combinations and Span, II

Examples:

1. In $\mathbb{Q}^4$, the vector $\langle 4, 0, 5, 9\rangle$ is a linear combination of $\langle 1, 0, 0, 1\rangle$, $\langle 0, 1, 0, 0\rangle$, and $\langle 1, 1, 1, 2\rangle$, because $\langle 4, 0, 5, 9\rangle = 1 \cdot \langle 1, -1, 2, 3\rangle - 2 \cdot \langle 0, 1, 0, 0\rangle + 3 \cdot \langle 1, 1, 1, 2\rangle$.
2. In $\mathbb{F}_3^2$, the vector $\langle 1, 0, 2\rangle$ is a linear combination of $\langle 1, 1, 1\rangle$ and $\langle 2, 1, 0\rangle$, because $\langle 1, 2\rangle = 2 \cdot \langle 1, 1, 1\rangle + 1 \cdot \langle 2, 1, 0\rangle$.
3. In $\mathbb{R}^3$, the vector $\langle 0, 0, 1\rangle$ is not a linear combination of $\langle 1, 1, 0\rangle$ and $\langle 0, 1, 1\rangle$ because there exist no scalars a_1 and a_2 for which $a_1 \cdot \langle 1, 1, 0\rangle + a_2 \cdot \langle 0, 1, 1\rangle = \langle 0, 0, 1\rangle$: this would require a common solution to the three equations $a_1 = 0$, $a_1 + a_2 = 0$, and $a_2 = 1$, and this system has no solution.

There are straightforward computational methods using row-reduction of matrices to determine whether a vector in F^n is a linear combination of other given vectors.

Linear Combinations and Span, III

Definition

If V is a vector space and S is a subset, the span of S is defined to be $\operatorname{span}(S) = \{a_1 \cdot \mathbf{v}_1 + \cdots + a_n \cdot \mathbf{v}_n : a_i \in F, \mathbf{v}_i \in S\}$, the set of all linear combinations of finitely many vectors in S. (Note that $\operatorname{span}(\emptyset) = \{\mathbf{0}\}$.)

- It is not hard to show that $\operatorname{span}(S)$ is the smallest subspace of V containing S.
- Another definition of the span is the intersection of all subspaces of V containing S.
- Example: The span of the set $\{1, x\}$ inside $F[x]$ is the set of linear polynomials (i.e., of the form $a + bx$ for $a, b \in F$).

Linear Combinations and Span, IV

Definition

If $\operatorname{span}(S) = V$*, we say that* S *is a spanning set for* V*: in other words, when every vector in* V *can be written as a linear combination of the vectors in* S*.*

Examples:

- The set $\{1, i\}$ is a spanning set for $\mathbb{C}$ as a vector space over $\mathbb{R}$.
- The set $\{\langle 1,0,0\rangle, \langle 0,1,0\rangle, \langle 0,0,1\rangle\}$ is a spanning set for F^3.
- The set $\{\langle 1,1\rangle, \langle 2,1\rangle, \langle 3,1\rangle\}$ is a spanning set for $\mathbb{Q}^2$.

For spanning sets, there is no requirement that vectors be uniquely representable as a linear combination (e.g., in the third example), only that there is at least one way.

Linear Independence, I

Definition

If V is a vector space, a subset S of V is linearly independent if, for any distinct vectors $\mathbf{v}_i \in S$ and any scalars $a_i \in F$, $a_1 \cdot \mathbf{v}_1 + \cdots + a_n \cdot \mathbf{v}_n = \mathbf{0}$ implies $a_1 = \cdots = a_n = 0$. Otherwise, S is linearly dependent.

For a finite set $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, S is linearly independent precisely when the only way to form the zero vector as a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is when all the scalar coefficients are zero (the "trivial" linear combination).

An infinite set is linearly independent when all its finite subsets are linearly independent.

The term "linear dependence" arises from the fact that if a set of vectors is linearly dependent, one of the vectors is necessarily a linear combination of the others (i.e., it "depends" on the others).

Linear Independence, II

Examples:

1. The vectors $\langle 1, 1, 0 \rangle$ and $\langle 0, 2, 1 \rangle$ in $\mathbb{R}^3$ are linearly independent, because $a \cdot \langle 1, 1, 0 \rangle + b \cdot \langle 0, 2, 1 \rangle = \langle 0, 0, 0 \rangle$ implies $a = 0$, $a + 2b = 0$, and $b = 0$, so that $a = b = 0$.
2. The set $\{1, x, x^2, x^3, \ldots, x^n\}$ is linearly independent in $F[x]$ because the only solution to $a_0 \cdot 1 + a_1 x + \cdots + a_n x^n = 0$ for scalars a_i is $a_0 = a_1 = \cdots = a_n = 0$.
3. The complex numbers $3 - 5i$, $3 - 4i$, and $1 - i$ are linearly dependent over $\mathbb{Q}$ because $1(3-5i) - 2(3-4i) + 3(1-i) = 0$.
4. The empty set is always linearly independent, in any vector space.
5. The set $\{\mathbf{v}\}$ is linearly independent if and only if $\mathbf{v} \neq \mathbf{0}$.
6. The set $\{\mathbf{v}, \mathbf{w}\}$ is linearly independent if and only if neither $\mathbf{v}$ nor $\mathbf{w}$ is a scalar multiple of the other.

Linear Independence, III

If a set of vectors is linearly independent, every vector in their span can be uniquely written as a linear combination:

Proposition (Characterization of Linear Independence)

A set S of vectors is linearly independent if and only if every vector $\mathbf{w}$ in $\operatorname{span}(S)$ may be uniquely written as a sum $\mathbf{w} = a_1 \cdot \mathbf{v}_1 + \cdots + a_n \cdot \mathbf{v}_n$ for unique scalars $a_1, a_2, \ldots, a_n$ and unique vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ in S (where we view sums as equivalent if additional terms with coefficient 0 are added or removed).

When $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is finite, this means every vector $\mathbf{w} \in \operatorname{span}(S)$ can be written as a linear combination $\mathbf{w} = a_1 \cdot \mathbf{v}_1 + \cdots + a_n \cdot \mathbf{v}_n$ where $a_1, \ldots, a_n$ are now unique.

Linear Independence, IV

Proof:

- First suppose the decomposition is always unique.
- Then for any $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ in S, $a_1 \cdot \mathbf{v}_1 + \cdots + a_n \cdot \mathbf{v}_n = \mathbf{0}$ implies $a_1 = \cdots = a_n = 0$, because $0 \cdot \mathbf{v}_1 + \cdots + 0 \cdot \mathbf{v}_n = \mathbf{0}$ is by assumption the only decomposition of $\mathbf{0}$.
- Now suppose that $\mathbf{w} = a_1 \cdot \mathbf{v}_1 + \cdots + a_n \cdot \mathbf{v}_n = b_1 \cdot \mathbf{v}_1 + \cdots + b_n \cdot \mathbf{v}_n$ has two decompositions.
- Subtracting yields $(a_1 - b_1) \cdot \mathbf{v}_1 + \cdots + (a_n - b_n) \cdot \mathbf{v}_n = \mathbf{w} - \mathbf{w} = \mathbf{0}$, and since $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent, $a_1 - b_1, \cdots, a_n - b_n$ are all zero.

Bases and Dimension, I

Now we can get to the good part.

Definition

A linearly independent set of vectors that spans V is called a basis for V. (The plural of "basis" is "bases".)

From our characterization of linear independence above, we can see that S is a basis for V if and only if every vector in V can be written uniquely as a linear combination of vectors in S.

Bases and Dimension, II

Example:

1. The "standard basis" for F^n consists of the unit coordinate vectors $\langle 1, 0, \ldots, 0, 0\rangle$, $\langle 0, 1, \ldots, 0, 0\rangle$, ... , $\langle 0, 0, \ldots, 0, 1\rangle$.
2. The set $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$, as is the set $\{1 + i, 2 - 3i\}$.
3. If p has degree n, then the set $\{1, x, x^2, \ldots, x^{n-1}\}$ is a basis for $F[x]/p$.
4. The vectors $\langle 1, 1, 0\rangle$ and $\langle 1, 1, 1\rangle$ are not a basis for $\mathbb{Q}^3$ since they do not span $\mathbb{Q}^3$.
5. The vectors $\langle 1, 0, 0\rangle$, $\langle 0, 1, 0\rangle$, $\langle 0, 0, 1\rangle$, $\langle 1, 1, 1\rangle$ are not a basis for $\mathbb{Q}^3$ since they are not linearly independent.

Bases and Dimension, III

Theorem (Spanning Sets)

Any spanning set for a vector space V contains a basis of V.

- If the spanning set is finite, then the idea is to throw away linearly dependent vectors one at a time until the resulting set is linearly independent. The collection of elements which we have not thrown away will always be a spanning set (since removing a dependent element will not change the span).
- By an easy induction argument, this process will eventually terminate, and the end result will be a linearly independent spanning set.
- In the event that the spanning set is infinite, the argument relies on Zorn's lemma.

Interlude: Zorn's Lemma, I

Zorn's lemma is a useful tool for proving the existence of something when it seems like an inductive construction should work, but the underlying sets are too large. It is a general statement about partially-ordered sets. To review the ingredients:

Definition

A relation $\leq$ on a set S is a partial ordering if it is reflexive, antisymmetric, and transitive: that is, when $a \leq a$, when $a \leq b$ and $b \leq a$ imply $a = b$, and when $a \leq b$ and $b \leq c$ imply $a \leq c$.

Definition

If S is a partially ordered set, a chain is a totally-ordered subset: in other words, a subset in which any two elements are comparable, so that either $a \leq b$ or $b \leq a$ holds.

Interlude: Zorn's Lemma, II

Definition

If S is a partially ordered set, an upper bound for a subset X is an element $y \in S$ such that $x \leq y$ for all $x \in X$.

Definition

If S is a partially ordered set, a maximal element is an element $y \in S$ such that $x \leq y$ for all $x \in S$.

Example: Take the usual ordering $\leq$ on $\mathbb{R}$.

- Both 1 and 2 are upper bounds for the closed interval $[0, 1]$ and the open interval $(0, 1)$.
- The element 1 is a maximal element inside $[0, 1]$, while $(0, 1)$ has no maximal element.
- The set $\mathbb{R}$ has neither an upper bound nor a maximal element.

Interlude: Zorn's Lemma, III

Zorn's lemma provides a condition for the existence of a maximal element in a partially-ordered set:

Statement (Zorn's Lemma)

Suppose S is a nonempty partially-ordered set such that every chain has an upper bound in S. Then S contains a maximal element.

We will not prove Zorn's lemma. There is a good reason for this: it is actually equivalent to the axiom of choice. (If you are interested in such things, you can ponder how to show the equivalence.)

The purpose of Zorn's lemma, just as with the axiom of choice, is that it allows us to posit the existence of something in situations where there is no obstruction to the existence of the object, but it is not possible give an explicit recipe for a construction because the underlying sets are too large or too numerous.

Bases and Dimension, IV

Theorem (Spanning Sets)

Any spanning set for a vector space V contains a basis of V.

Proof:

- We use Zorn's lemma. Let $\mathcal{F}$ be the collection of all linearly-independent subsets of V, partially ordered by inclusion, and note that $\mathcal{F} \neq \emptyset$ since $\emptyset \in \mathcal{F}$.
- If $\mathcal{C}$ is any chain in $\mathcal{F}$, then the union of all the elements of $\mathcal{C}$ is an upper bound for $\mathcal{C}$ and is linearly independent.
- Specifically, any linear dependence in the union would imply a linear dependence in one of the elements in the chain: linear dependences involve only finitely many vectors, so we may take the maximum of the subsets in which all vectors appear.
- Thus, by Zorn's lemma, $\mathcal{F}$ contains a maximal element.
- Finally, a maximal linearly-independent subset is a basis: otherwise, we could adjoin an element not in the span.

Bases and Dimension, V

We can also construct a basis from the other direction by building up from a linearly independent set:

Theorem (Building-Up Theorem)

Given any linearly independent set of vectors in a vector space V, there exists a basis of V containing those vectors. In short, any linearly independent set of vectors can be extended to a basis.

Proof:

- The idea (roughly speaking) is to start with the given linearly independent set, and then append linearly independent vectors to S one at a time until a basis for V is obtained.
- If V is finite-dimensional (i.e., has a finite spanning set), this procedure will always terminate in a finite number of steps.
- In the case where V is infinite-dimensional, the argument again relies on Zorn's lemma.

Bases and Dimension, VI

Using either approach, we see that every vector space has a basis:

Theorem (Bases of Vector Spaces)

Every vector space has a basis, and any two bases have the same number of elements.

- The existence of bases follows from either of the theorems given above.
- As another fun note, it has been proven that the statement "every vector space has a basis" is actually equivalent to the axiom of choice (under the Zermelo-Frankel axioms of set theory), so in fact appealing to the axiom of choice, or equivalently Zorn's lemma, is necessary to establish this theorem.

Bases and Dimension, VII

To show that any two bases have the same number of elements is more difficult, and can be done by first proving the following "replacement theorem":

Theorem (Replacement Theorem)

Suppose that $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ *is a basis for* V *and* $\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m\}$ *is a linearly independent subset of* V*. Then there is a reordering of the basis* S*, say* $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ *such that for each* $1 \leq k \leq m$*, the set* $\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k, \mathbf{a}_{k+1}, \mathbf{a}_{k+2}, \ldots, \mathbf{a}_n\}$ *is a basis for* V*. Equivalently, the elements* $\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m\}$ *can be used to successively replace the elements of the basis, with each replacement remaining a basis of* V*.*

This is just an explicit calculation (it really is just an application of row-reducing an appropriate matrix).

Bases and Dimension, VIII

An easy corollary of the replacement theorem:

Corollary

Suppose V has a basis with n elements. If $m > n$, then any set of m vectors of V is linearly dependent. In particular, any two bases must have the same number of elements.

Definition

If V is an F-vector space, the number of elements in any basis of V is called the dimension of V and is denoted $\dim_F(V)$. If $\dim_F(V)$ is finite, V is finite-dimensional; otherwise, V is infinite-dimensional.

We will not concern ourselves with the cardinality of the basis for an infinite-dimensional vector space, and merely refer to all of these infinite cardinalities as ∞. (But if you care, the cardinalities of any two bases are necessarily the same.)

Bases and Dimension, IX

Examples:

1. $\dim_F(F^n) = n$, since the standard unit vectors form a basis.
2. $\dim_F(F[x]) = \infty$ since the set $\{1, x, x^2, \dots\}$ is a basis.
3. $\dim_F(F[x]/p) = \deg(p)$ since the set $\{1, x, x^2, \dots, x^{\deg(p)-1}\}$ is a basis.
4. The dimension of the zero space is 0, because the empty set (containing 0 elements) is a basis.
5. $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ since the set $\{1, i\}$ is a basis.
6. $\dim_{\mathbb{C}}(\mathbb{C}) = 2$ since the set $\{1\}$ is a basis.

Bases and Dimension, IX

Examples:

5. $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ since the set $\{1, i\}$ is a basis.
6. $\dim_{\mathbb{C}}(\mathbb{C}) = 2$ since the set $\{1\}$ is a basis.
7. $\dim_{\mathbb{Q}}(\mathbb{C}) = \infty$ since any finite-dimensional vector space over $\mathbb{Q}$ necessarily has only countably many elements, and $\mathbb{C}$ is uncountable. Alternatively, $\mathbb{C}$ contains a transcendental number π, so the set $\{1, \pi, \pi^2, \pi^3, \dots\}$ is $\mathbb{Q}$-linearly independent since otherwise π would be a root of a polynomial with rational coefficients.

As these examples show, the dimension of a vector space depends intrinsically on its associated field of scalars.

Linear Transformations, I

We can also study the structure-preserving maps on vector spaces, which are the vector-space equivalent of homomorphisms:

Definition

If V and W are vector spaces having the same scalar field F, we say a function $T : V \to W$ is a linear transformation if it respects addition of vectors and scalar multiplication: in other words, if $T(\mathbf{v}_1 + \mathbf{v}_2) = T(\mathbf{v}_1) + T(\mathbf{v}_2)$ and $T(\alpha\mathbf{v}) = \alpha T(\mathbf{v})$ for any vectors $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in V$ and any scalar $\alpha \in F$.

We also have vector space isomorphisms:

Definition

If T is a linear transformation that is also a bijection, then T is a (vector space) isomorphism.

Linear Transformations, II

Examples:

1. If A is any $m \times n$ matrix, then the map $T : F^m \to F^n$ given by $T(\mathbf{v}) = A\mathbf{v}$ is a linear transformation.
2. If V is the vector space of differentiable functions and W is the vector space of real-valued functions, the derivative map D sending a function to its derivative is a linear transformation from V to W.
3. If V is the vector space of all continuous functions on $[a, b]$, then the integral map $I(f) = \int_a^b f(x)\,dx$ is a linear transformation from V to $\mathbb{R}$.
4. The transpose map is a linear transformation from $M_{m\times n}(F)$ to $M_{n\times m}(F)$ for any field F and any positive integers m, n: in fact, it is an isomorphism.

Linear Transformations, III

Examples:

5. For any $a \in F$, the evaluation at a map on $F[x]$, defined by $T(p) = p(a)$, is a linear transformation from $F[x]$ to F.
6. If V and W are any vector spaces, the zero map sending all elements of V to the zero vector in W is a linear transformation from V to W.
7. If V is any vector space, the identity map sending all elements of V to themselves is a linear transformation from V to V. The identity map is an isomorphism of V with itself.

Linear Transformations, III

We have the natural notion of kernel and image for linear transformations:

Definition

If $T : V \to W$ is a linear transformation, then the kernel of T, denoted $\ker(T)$, is the set of elements $\mathbf{v} \in V$ with $T(\mathbf{v}) = \mathbf{0}$, and the image of T, denoted $\mathrm{im}(T)$, is the set of elements $\mathbf{w} \in W$ such that there exists $\mathbf{v} \in V$ with $T(\mathbf{v}) = \mathbf{w}$.

- It is easy to verify from the definitions that the kernel and image are subspaces of V and W, respectively.
- Like with ring homomorphisms, it is also true that $\ker(T) = \{\mathbf{0}\}$ if and only if T is one-to-one.
- Thus, T is an isomorphism if and only if $\ker(T) = \{\mathbf{0}\}$ and $\mathrm{im}(T) = W$.

Linear Transformations, IV

Proposition (Properties of Linear Transformations)

If $T : V \to W$ is linear, then the following hold:

1. *$T(\mathbf{0}_V) = \mathbf{0}_W$ and for any $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ and $a_1, \ldots, a_n \in F$, $T(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) = a_1T(\mathbf{v}_1) + \cdots + a_nT(\mathbf{v}_n)$.*
2. *$T : V \to W$ is linear if and only if for any $\mathbf{v}_1$ and $\mathbf{v}_2$ in V and any scalar α, $T(\mathbf{v}_1 + \alpha\mathbf{v}_2) = T(\mathbf{v}_1) + \alpha T(\mathbf{v}_2)$.*
3. *T is characterized by its values on a basis of V: for any basis $B = \{\mathbf{v}_i\}$ of V and any $\{\mathbf{w}_i\} \in W$, there exists a unique linear $T : V \to W$ such that $T(\mathbf{v}_i) = \mathbf{w}_i$ for each i.*
4. *If T is an isomorphism, then T preserves linear independence and span (i.e., if S is a linearly independent set then so is $T(S)$, and likewise for a spanning set).*
5. *Two vector spaces V and W are isomorphic if and only if they have the same dimension. In particular, any finite-dimensional vector space V with scalar field F is isomorphic to $F^{\dim_F V}$.*

Linear Transformations, V

Proofs:

1. $T(\mathbf{0}_V) = \mathbf{0}_W$ and for any $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ and $a_1, \ldots, a_n \in F$, $T(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) = a_1T(\mathbf{v}_1) + \cdots + a_nT(\mathbf{v}_n)$.
2. $T : V \to W$ is linear if and only if for any $\mathbf{v}_1$ and $\mathbf{v}_2$ in V and any scalar α, $T(\mathbf{v}_1 + \alpha\mathbf{v}_2) = T(\mathbf{v}_1) + \alpha T(\mathbf{v}_2)$.
   - (1) and (2) are straightforward from the definition.
3. For any basis $B = \{\mathbf{v}_i\}$ of V and any $\{\mathbf{w}_i\} \in W$, there exists a unique linear $T : V \to W$ such that $T(\mathbf{v}_i) = \mathbf{w}_i$ for each i.
   - The values of T are determined by its values on the basis by (1) above, since any any vector $\mathbf{v}$ in V can be written as $\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$ for (unique) vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ in B and scalars $a_1, \ldots, a_n$.
   - Conversely, if we are given the values $T(\mathbf{v}_i) = \mathbf{w}_i$ for each $\mathbf{v}_i \in B$, then the map $T : V \to W$ defined by setting $T(a_1\mathbf{v}_{i_1} + a_2\mathbf{v}_{i_2} + \cdots + a_n\mathbf{v}_{i_n}) = a_1\mathbf{w}_{i_1} + \cdots + a_n\mathbf{w}_{i_n}$ is a well-defined linear transformation from V to W.

Linear Transformations, VI

Proofs:

4. If T is an isomorphism, then T preserves linear independence and span (i.e., if S is a linearly independent set then so is $T(S)$, and likewise for a spanning set).
   - For independence, note $a_1 T(\mathbf{v}_1) + \cdots + a_n T(\mathbf{v}_n) = \mathbf{0}$ implies $T(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) = \mathbf{0}$ implies $a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$. So if the $\mathbf{v}_i$ are independent, so are their images.
   - For span, if $\mathbf{w} \in W$ then $\mathbf{w} \in \mathrm{im}(T)$ so $\mathbf{w} = T(\mathbf{v})$. Since $\mathbf{v}$ is in the span of a spanning set, $T(\mathbf{v})$ is in the span of its image.

Linear Transformations, VII

Proofs:

5. Two vector spaces V and W are isomorphic if and only if they have the same dimension. In particular, any finite-dimensional vector space V with scalar field F is isomorphic to F^n, where $n = \dim_F V$.
   - By (4), isomorphisms preserve linear independence, so two vector spaces can only be isomorphic if they have the same dimension.
   - For the other direction, choose a basis $\{\mathbf{v}_i\}_{i \in I}$ for V and a basis $\{\mathbf{w}_i\}_{i \in I}$ for W. Then by (3), there exists a unique linear transformation $T : V \to W$ with $T(\mathbf{v}_i) = \mathbf{w}_i$ for each $i \in I$. It is then a straightforward check that T is an isomorphism.

Linear Transformations, VIII

There is a well-defined notion of a quotient vector space, but we will not bother to develop this notion since it is rarely very useful by itself.

However, we can still give the analogue of the first isomorphism theorem, which is extremely important:

Theorem (Nullity-Rank)

For any linear transformation $T : V \to W$,
$\dim(\ker(T)) + \dim(\mathrm{im}(T)) = \dim(V)$.

The dimension of the kernel is called the nullity, while the dimension of the image is called the rank (whence the name "nullity-rank theorem").

Linear Transformations, IX

Proof:

- Let $\beta = \{\mathbf{w}_i\}_{i \in I}$ be a basis for $\mathrm{im}(T)$ in W.
- By definition, there exist $\{\mathbf{v}_i\}_{i \in I}$ in V such that $T(\mathbf{v}_i) = \mathbf{w}_i$ for each $i \in I$.
- Also, let $\alpha = \{\mathbf{a}_j\}_{j \in J}$ be a basis for $\ker(T)$.
- We claim that the set of vectors $S = \{\mathbf{v}_i\}_{i \in I} \cup \{\mathbf{a}_j\}_{j \in J}$ is a basis for V.

Linear Transformations, X

Proof (continued):

- To see that S spans V, let $\mathbf{v}$ be an element of V.
- Since $T(\mathbf{v}) \in \mathrm{im}(T)$, there exist scalars $b_1, \ldots, b_k$ and $\mathbf{v}_1, \ldots, \mathbf{v}_k$ such that $T(\mathbf{v}) = \sum_{j=1}^{k} b_j \mathbf{w}_j$.
- Then $T\left[\mathbf{v} - \sum_{j=1}^{k} b_j \mathbf{v}_j\right] = T(\mathbf{v}) - \sum_{j=1}^{k} b_j T(\mathbf{v}_j) = \sum_{j=1}^{k} b_j \mathbf{w}_j - \sum_{j=1}^{k} b_j \mathbf{w}_j = \mathbf{0}$.
- This means $\mathbf{v} - \sum_{j=1}^{k} b_j \mathbf{v}_j$ is in $\ker(T)$, so it can be written as a sum $\sum_{i=1}^{l} c_i \mathbf{a}_i$ for some scalars c_i and some $\mathbf{a}_1, \ldots, \mathbf{a}_l \in \alpha$.
- Then $\mathbf{v} = \sum_{j=1}^{k} b_j \mathbf{v}_j + \sum_{i=1}^{l} c_i \mathbf{a}_i \in \mathrm{span}(S)$, so S spans V.

Linear Transformations, XI

Proof (continued more):

- To see that S is linearly independent, suppose we had a dependence $\mathbf{0} = \sum_{j=1}^{k} b_j \mathbf{v}_j + \sum_{i=1}^{l} c_i \mathbf{a}_i$.
- Applying T to both sides yields $\mathbf{0} = T(\mathbf{0}) = \sum_{j=1}^{k} b_j T(\mathbf{v}_j) + \sum_{i=1}^{l} c_i T(\mathbf{a}_i) = \sum_{j=1}^{k} b_j \mathbf{w}_j$.
- Since the $\mathbf{w}_j$ are linearly independent, all the coefficients b_j must be zero.
- Then $\mathbf{0} = \sum_{i=1}^{l} c_i \mathbf{a}_i$, but now since the $\mathbf{a}_i$ are linearly independent, all the coefficients c_i must also be zero.

Summary

We discussed fields and gave a number of basic examples.

We discussed vector spaces, span, independence, bases, and dimension.

We discussed linear transformations.

Next lecture: Subfields and field extensions, properties of subfields, simple extensions.