1: INTRODUCTION, FIELDS, VECTOR SPACES, BASES

STEVEN HEILMAN

Abstract. These notes are mostly copied from those of T. Tao from 2002, available here

Contents

1. Introductory Remarks 1
3. Fields and Vector Spaces 2
4. Three Fundamental Motivations for Linear Algebra 4
5. Subspaces, Linear independence 5
6. Bases, Spanning Sets 7
7. Subspaces and Dimension 13
8. Appendix: Notation 14

1. Introductory Remarks

1.1. **What will we be learning?** We will be learning linear algebra from an abstract perspective.

1.2. **Why so abstract?** The abstract approach to learning rigorous mathematics, can be a bit of a difficult adjustment. This approach uses an axiomatic presentation with complete proofs, as opposed to intuitive reasoning and sketches of proofs which are used in your lower division classes. You have probably seen rigorous proofs and the axiomatic method in a class in Euclidean geometry; we will be using this approach for linear algebra. The main proponents of this approach were the Bourbaki group of mainly French mathematicians, starting in the 1930s. The power of the abstract approach is that we can make statements about many examples, simultaneously. The difficulty of the abstract approach is that abstract thinking can require some adjustment for the learner. It is sometimes beneficial to keep some examples in mind to stay grounded, but sometimes these examples can be misleading.

2. A Brief History of Linear Algebra

Early antecedents for solving systems of linear equations go back at least to Leibniz and Newton. This theory along with matrix theory were developed through the 1800s. Essentially everything that we do in this course was known by the year 1900, though the presentation has been streamlined over the years, as we already discussed. By now matrices are ubiquitous in mathematics. And linear algebra serves as the foundation of quantum mechanics, functional analysis, Fourier analysis, probability theory, partial differential equations, computer science,

Date: April 6, 2015.

and several other fields. There is a very good reason that this class is required for all math majors.

3. Fields and Vector Spaces

In this course, we will be using arithmetic of vectors and fields at an abstract level. For the sake of basic intuition, we can think of a field as $\mathbf{R}$ or $\mathbf{C}$, and we can think of a vector space as $\mathbf{R}^2$ or $\mathbf{R}^n$ for any natural number n with $n \geq 1$. However, many of the statements that we will prove in this course will hold for all objects that satisfy the usual properties of arithmetic with which we are familiar. We formalize these properties below as abstract definitions, when we define both fields and vector spaces, which we will focus on throughout the course.

Definition 3.1 (**Binary Operation**)**.** Let F be a set. A **binary operation** is a function $F \times F \to F$.

Example 3.2. Addition on the real numbers is a binary operation. Two real numbers (x, y) are mapped to the real number $x + y$.

Definition 3.3 (**Field**)**.** A **field** is a set $\mathbf{F}$ with two binary operations $+$ and $\cdot$, such that the following properties hold.

(1) $\forall\ \alpha, \beta \in \mathbf{F}$, $\alpha + \beta = \beta + \alpha$ (commutativity of addition)
(2) $\forall\ \alpha, \beta, \gamma \in \mathbf{F}$, $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ (associativity of addition)
(3) $\forall\ \alpha, \beta \in \mathbf{F}$, $\alpha \cdot \beta = \beta \cdot \alpha$ (commutativity of multiplication)
(4) $\forall\ \alpha, \beta, \gamma \in \mathbf{F}$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ (associativity of multiplication)
(5) $\forall\ \alpha, \beta, \gamma \in \mathbf{F}$, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ (distributivity)
(6) $\exists\ 0 \in \mathbf{F}$ such that $\forall\ \alpha \in \mathbf{F}$, $0 + \alpha = \alpha$ (additive identity)
(7) $\forall\ \alpha \in \mathbf{F}$, $\exists\ -\alpha \in \mathbf{F}$ such that $\alpha + (-\alpha) = 0$ (additive inverse)
(8) $\exists\ 1 \in \mathbf{F}$ such that, $\forall\ \alpha \in \mathbf{F}$, $1 \cdot \alpha = \alpha$ (multiplicative identity)
(9) $\forall\ \alpha \in \mathbf{F}$, $\alpha \neq 0$, $\exists\ \alpha^{-1} \in \mathbf{F}$ such that $\alpha \cdot \alpha^{-1} = 1$ (multiplicative inverse)

Remark 3.4. Note that the integers satisfy properties (1) through (8), but not property (9). For all $x \in \mathbf{Z}$, $2x \neq 1$. So, the integers are not a field.

Example 3.5. The real numbers $\mathbf{R}$ are a field, with respect to the usual addition and multiplication of real numbers.

Example 3.6. The rational numbers $\mathbf{Q}$ are a field, with respect to the usual addition and multiplication of rational numbers.

Example 3.7. The set $\mathbf{F} = \{0, 1\}$ can be made into a field if we define addition and multiplication via the following addition and multiplication tables.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

With these definitions of addition and multiplication, $\mathbf{F}$ is referred to as the field of two elements.

Remark 3.8. The elements of a field are often called **scalars**.

Definition 3.9 (**Vector Space**)**.** A **vector space** V over a field $\mathbf{F}$ is a set V together with two functions $+\colon V \times V \to V$, $\cdot\colon \mathbf{F} \times V \to V$, such that the following properties hold.

(1) $\forall\ u, v \in V$, $u + v = v + u$ (commutativity of addition)
(2) $\forall\ u, v, w \in V$, $u + (v + w) = (u + v) + w$ (associativity of addition)
(3) $\exists\ 0 \in V$ such that $\forall\ u \in V$, $0 + u = u$ (additive identity)
(4) $\forall\ u \in V$, $\exists\ -u \in V$ such that $u + (-u) = 0$ (additive inverse)
(5) $\forall\ u \in V$, $\forall\ \alpha, \beta \in \mathbf{F}$, $\alpha \cdot (\beta \cdot u) = (\alpha\beta) \cdot u$ (associativity of multiplication)
(6) $\forall\ u \in V$, $\forall\ \alpha, \beta \in \mathbf{F}$, $(\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u$ (scalar distributivity)
(7) $\forall\ u, v \in V$, $\forall\ \alpha \in \mathbf{F}$, $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$ (vector distributivity)
(8) $\forall\ u \in V$, $1 \in \mathbf{F}$ satisfies $1 \cdot u = u$ (multiplicative identity)

Remark 3.10. Strictly speaking, the field element $0 \in \mathbf{F}$ is distinct from the vector $0 \in V$. However, we use the same notation for both objects, since there is usually no confusion that arises. Yet, at the stage of creating definitions, we should be aware of the difference between these two objects.

Example 3.11. $\mathbf{R}$ is a vector space over $\mathbf{R}$.

Example 3.12. $\mathbf{R}^2$ is a vector space over $\mathbf{R}$. More generally, for any natural number n, $\mathbf{R}^n$ is a vector space over $\mathbf{R}$. More generally, for any field $\mathbf{F}$, and for any $n \in \mathbf{N}$, $\mathbf{F}^n$ is a vector space over $\mathbf{F}$.

Example 3.13. Let x be a real variable. The set $P_2(\mathbf{R})$ of all real polynomials in the variable x of degree at most 2 is a vector space over $\mathbf{R}$. More generally, the set $P(\mathbf{R})$ of all real polynomials in the variable x is a vector space over $\mathbf{R}$. More generally, the set $C^\infty(\mathbf{R})$ of all infinitely differentiable functions in the variable x is a vector space over $\mathbf{R}$.

Remark 3.14. Eventually, we will stop writing $\alpha \cdot u$, and we will just write αu, where $\alpha \in \mathbf{F}$ and $u \in V$. No confusion should arise from this change.

To get used to doing proofs, lets prove a fact that follows from the properties of a vector space (Definition 3.9).

Proposition 3.15 (**Vector Cancellation Law**). *Let V be a vector space over a field $\mathbf{F}$. Let $u, v, w \in V$ such that $u + v = u + w$. Then $v = w$.*

Proof. From property (4) in the Definition of a vector space, there exists $-u \in V$ such that $u + (-u) = 0$. So,

$$\begin{aligned}
v &= 0 + v && \text{, by Property (3) in Definition 3.9} \\
&= (u + (-u)) + v \\
&= ((-u) + u) + v && \text{, by Property (1) in Definition 3.9} \\
&= (-u) + (u + v) && \text{, by Property (2) in Definition 3.9} \\
&= (-u) + (u + w) && \text{, by assumption} \\
&= ((-u) + u) + w && \text{, by Property (2) in Definition 3.9} \\
&= (u + (-u)) + w && \text{, by Property (1) in Definition 3.9} \\
&= 0 + w \\
&= w && \text{, by Property (3) in Definition 3.9.}
\end{aligned}$$

□

After a while we won't do algebraic manipulations in this level of detail. The purpose of the above proof is to get used to justifying each step in our proofs. When doing homework problems, make sure to justify each step of your proof. If you cannot justify each step, then you may have a mistake in your proof!

Exercise 3.16. Let V be a vector space over a field $\mathbf{F}$. Using the same level of detail as the proof of Proposition 3.15, prove the following facts:

- $\forall\ v \in V$, $0 \cdot v = 0$.
- $\forall\ v \in V$, $(-1) \cdot v = -v$.
- $\forall\ \alpha \in F$, and for $0 \in V$, $\alpha \cdot 0 = 0$.
- $\forall\ \alpha \in \mathbf{F}$, $\forall\ v \in V$, $\alpha \cdot (-v) = (-\alpha) \cdot v = -(\alpha \cdot v)$.

4. Three Fundamental Motivations for Linear Algebra

We will now present three examples that should motivate the study of linear algebra. Consider the set $X := \{f \in C^\infty([0,1])\colon f(0) = f(1) = 0\}$. For any $f \in X$, define $Tf := -(d^2/dt^2)f(t)$, where $t \in [0,1]$. Note that X is a vector space over $\mathbf{R}$. We will see later that X is infinite dimensional, so to understand it, we cannot just use our intuition about finite dimensional vector spaces such as $\mathbf{R}^2$. Note that T is linear, in the sense that, for any $f, g \in X$ and for any $\alpha, \beta \in \mathbf{R}$, we have $T(\alpha f + \beta g) = \alpha T(f) + \beta T(g)$. Once again, since X is infinite dimensional, we cannot truly think about T as being a matrix, in the same way that we can understand a linear function on a finite dimensional vector space to be a matrix. However, there are some ways in which we can use our finite dimensional intuition even when X is infinite dimensional. For example, for any $k \geq 0$, $k \in \mathbf{Z}$, the functions $\sin(k\pi t)$ satisfy $T[\sin(k\pi t)] = k^2\pi^2 \sin(k\pi t)$. So, the functions $\sin(k\pi t)$ are eigenfunctions of T with eigenvalues $k^2\pi^2$. And understanding these eigenfunctions and eigenvalues leads us to an understanding of T. More general linear functions such as T are studied in partial differential equations, quantum mechanics, Fourier analysis, computer science, and so on. The theory of eigenfunctions and eigenvectors from linear algebra can in fact be extended to infinite dimensional vector spaces X. This is done in the mathematical subject of functional analysis. So, for now, we will mostly be studying finite dimensional spaces X, but there is still a lot more to be gained from this theory, as von Neumann and others found in the 1930s.

Linear algebra is also used in search technology, e.g. Google's PageRank algorithm. In this setting, it is desirable to design a large matrix A with very few entries. When we iterate A roughly thirty times to get the matrix A^{30}, then the largest entries of A^{30} give the most relevant websites for a search query. The specific choice of A relies on a linear algebraic interpretation of the set of all websites on the internet. In particular, we take x to be a real vector whose length is the number of websites on the internet, and then A is a square matrix whose side lengths are both the number of websites on the internet. Since A has very few entries, the matrix A^{30} can be computed rather quickly. When Google estimates the time it has taken to complete a search query, it is basically estimating the time it takes to iterate a certain matrix A around 30 times.

Lastly, in sampling and data compression (WAV files, cell phones, JPEG, MPEG, youtube videos,etc.), we once again want to *design* linear transformations which compress data as much as possible. In this setting, a vector x is an audio, image or video file, we design some

matrix A in a certain way, and the output Ax is a compressed file. The details of the design of A now come from Fourier analysis.

5. Subspaces, Linear independence

We are now going to make some definitions that will help us break apart vector spaces into sub-objects. Eventually, we will be able to treat certain vector spaces as sums of simpler pieces. And the simpler pieces (subspaces) will be easier to understand.

Definition 5.1 (**Subspace**)**.** Let V be a vector space over a field $\mathbf{F}$, and let $W \subseteq V$ with $W \neq \emptyset$. If W is closed under vector addition and scalar multiplication, we say that W is a **subspace** of V. So, $\forall\ u, v \in W$, we have $u + v \in W$, and $\forall\ u \in W$, for all $\alpha \in \mathbf{F}$, $\alpha u \in W$.

Remark 5.2. If V is a vector space over a field $\mathbf{F}$, and if $W \subseteq V$ is a subspace of V, then W is a vector space over $\mathbf{F}$.

Remark 5.3. $C^\infty(\mathbf{R})$ is a subspace of the space of all functions from $\mathbf{R}$ to $\mathbf{R}$.

Remark 5.4. Every subspace W of a vector space V must satisfy $0 \in W$. (To see this, choose $\alpha = 0$ in the definition of a subspace.) Note that $\emptyset$ is not a subspace of V.

The book uses a different definition of a subspace, so let's show that our definition agrees with the definition in the book.

Proposition 5.5 (**Subspace Equivalence**)**.** *Let V be a vector space over a field $\mathbf{F}$, and let $W \subseteq V$ with $W \neq \emptyset$. Then W is closed under vector addition and scalar multiplication if and only if W is a vector space over $\mathbf{F}$ (with the operations of addition and scalar multiplication defined on V).*

Proof. We begin with the reverse implication. Suppose W is a vector space over $\mathbf{F}$. Then, from the definition of a vector space (Definition 3.9), the operations of addition and multiplication must satisfy $+\colon W \times W \to W$ and $\cdot\colon \mathbf{F} \times W \to W$. That is, W is closed under addition and scalar multiplication.

We now prove the forward implication. Suppose W is closed under vector addition and scalar multiplication. We need to show that W satisfies all of the properties in the definition of a vector space (Definition 3.9). Let $u, v, w \in W$, $\alpha, \beta \in \mathbf{F}$. Since $W \subseteq V$, $u, v, w \in V$. Since V is a vector space and $u, v, w \in V$, properties (1), (2), (5), (6), (7) and (8) all apply to u, v, w, α, β. That is, all properties except for properties (3) and (4) must hold for W. So, we will conclude once we show that W satisfies properties (3) and (4). (Note that it is not immediately obvious that $0 \in W$ or $-u \in W$.)

We now show that W satisfies properties (3) and (4). Let $u \in W$. Since $W \subseteq V$, $u \in V$. From Exercise 3.16 applied to V, $0 \cdot u = 0$ and $(-1) \cdot u = -u$. Since W is closed under scalar multiplication, we conclude that $0 \in W$ and $-u \in W$. From properties (3) and (4) of Definition 3.9 applied to V (recalling that V is a vector space and $u \in V$), we know that $0 + u = u$ and $u + (-u) = 0$. Combining these facts with $0 \in W$ and $-u \in W$, we know that properties (3) and (4) hold for W, as desired. □

Exercise 5.6. Show that the intersection of two subspace is also a subspace.

Definition 5.7 (**Linear combination**)**.** Let V be a vector space over a field $\mathbf{F}$. Let $u_1, \ldots, u_n \in V$ and let $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$. Then $\sum_{i=1}^n \alpha_i u_i$ is called a **linear combination** of the vector elements $u_1, \ldots, u_n$.

Definition 5.8 (**Linear dependence**)**.** Let V be a vector space over a field $\mathbf{F}$. Let S be a subset of V. We say that S is **linearly dependent** if there exists a finite set of vectors $u_1, \ldots, u_n \in S$ and there exist $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$ which are not all zero such that $\sum_{i=1}^{n} \alpha_i u_i = 0$.

Definition 5.9 (**Linear independence**)**.** Let V be a vector space over a field $\mathbf{F}$. Let S be a subset of V. We say that S is **linearly independent** if S is not linearly dependent.

Example 5.10. The set $S = \{(1,0),(0,1)\}$ is linearly independent in $\mathbf{R}^2$. The set $S \cup (1,1)$ is linearly dependent in $\mathbf{R}^2$, since $(1,0) + (0,1) - (1,1) = 0$.

Definition 5.11 (**Span**)**.** Let V be a vector space over a field $\mathbf{F}$. Let $S \subseteq V$ be a finite or infinite set. Then the **span** of S, denoted by $\operatorname{span}(S)$, is the set of all finite linear combinations of vectors in S. That is,

$$\operatorname{span}(S) = \left\{ \sum_{i=1}^{n} \alpha_i u_i \colon n \in \mathbf{N}, \alpha_i \in \mathbf{F}, u_i \in S, \forall\, i \in \{1, \ldots, n\} \right\}.$$

Remark 5.12. We define $\operatorname{span}(\emptyset) := \{0\}$.

Theorem 5.13 (**Span as a Subspace**)**.** *Let V be a vector space over a field $\mathbf{F}$. Let $S \subseteq V$. Then* $\operatorname{span}(S)$ *is a subspace of V such that $S \subseteq \operatorname{span}(S)$. Also, any subspace of V that contains S must also contain* $\operatorname{span}(S)$.

Proof. We first deal with the case that $S = \emptyset$. In this case, $\operatorname{span}(S) = \{0\}$, which is a subspace of V. Also, any subspace contains $\{0\}$, as shown in Remark 5.4. Below, we therefore assume that $S \neq \emptyset$.

We first show that $\operatorname{span}(S)$ is a subspace of V.

Step 1. We first show that $\operatorname{span}(S) \subseteq V$. Let $u \in \operatorname{span}(S)$. By the definition of span (Definition 5.11), $\exists\ n \in \mathbf{N}$, $\exists\ \alpha_1, \ldots, \alpha_n \in \mathbf{F}$ and $\exists\ u_1, \ldots, u_n \in S \subseteq V$ such that $u = \sum_{i=1}^{n} \alpha_i u_i$. Since V is closed under scalar multiplication and vector addition, we have $u \in V$. Since $u \in \operatorname{span}(S)$ is arbitrary, we conclude that $\operatorname{span}(S) \subseteq V$.

Step 2. We now show that $\operatorname{span}(S)$ is closed under vector addition. Let $v \in \operatorname{span}(S)$. By the definition of span (Definition 5.11), $\exists\ m \in \mathbf{N}$, $\exists\ \beta_1, \ldots, \beta_m \in \mathbf{F}$ and $\exists\ v_1, \ldots, v_m \in S \subseteq V$ such that $v = \sum_{i=1}^{m} \beta_i v_i$. So,

$$u + v = \alpha_1 u_1 + \cdots + \alpha_n u_n + \beta_1 v_1 + \cdots + \beta_m v_m.$$

Since $u_1, \ldots, u_n, v_1, \ldots, v_m \in S$, $u + v$ is a linear combination of elements of S. We conclude that $u + v \in \operatorname{span}(S)$. Since $u, v \in \operatorname{span}(S)$ were arbitrary, we have that $\operatorname{span}(S)$ is closed under vector addition.

Step 3. We now show that $\operatorname{span}(S)$ is closed under scalar multiplication. Let $\gamma \in \mathbf{F}$. Recall that $u = \sum_{i=1}^{n} \alpha_i u_i$. Using properties (7) and (5) from the definition of a vector space (Definition 3.9),

$$\gamma \cdot u = \gamma \cdot \left(\sum_{i=1}^{n} \alpha_i u_i \right) = \sum_{i=1}^{n} (\gamma \alpha_i) \cdot u_i.$$

That is, $\gamma \cdot u$ is a linear combination of elements of S. Since $u \in \operatorname{span}(S)$ is artbirary, we conclude that $\operatorname{span}(S)$ is closed under scalar multiplication.

Combining Steps 1, 2 and 3 and applying Definition 5.1, we get that $\operatorname{span}(S)$ is a subspace of V.

We now show that $S \subseteq \text{span}(S)$. Let $u \in S$. In the definition of the span (Definition 5.11), choose $n = 1$, $\alpha_1 = 1$ to get $1 \cdot u \in \text{span}(S)$. By property (8) of the definition of a vector space (Definition 3.9), $u = 1 \cdot u \in \text{span}(S)$. Therefore, $S \subseteq \text{span}(S)$.

We now prove the final claim of the Theorem. Let $W \subseteq V$ be a subspace such that $S \subseteq W$. We want to show that $\text{span}(S) \subseteq W$ as well. So, let $n \in \mathbf{N}$, let $u_1, \ldots, u_n \in S$, and let $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$. Since $S \subseteq W$, $u_1, \ldots, u_n \in W$. Since W is a subspace of V, W is closed under scalar multiplication and under vector addition. So, $\sum_{i=1}^{n} \alpha_i u_i \in W$. Since $n \in \mathbf{N}$, $u_1, \ldots, u_n \in S$, and $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$ were arbitrary, we conclude that $\text{span}(S) \subseteq W$. □

6. Bases, Spanning Sets

Definition 6.1 (**Spanning Set**)**.** Let V be a vector space over a field $\mathbf{F}$. Let $S \subseteq V$. We say that S **spans** V if $\text{span}(S) = V$. In this case, we call S a **spanning set** for V. We can also say that S **generates** V, and S is a **generating set** for V.

Example 6.2. The set $\{(1, 0), (0, 1)\}$ is a spanning set for $\mathbf{R}^2$.

Spanning sets S are nice to have, since a spanning set S is sufficient to describe the vector space V (since $\text{span}(S) = V$). If we instead have a set S of linearly dependent vectors, then there is some redundancy in our description of V. To use an analogy, if we want to make a dictionary to describe a language, we want to just make a single entry for each word. It isn't very sensible to have multiple identical entries in our dictionary. The following Theorem then shows that we can remove redundancy in a linearly dependent set of vectors.

Theorem 6.3. *Let V be a vector space over a field $\mathbf{F}$. Let $S \subseteq V$ be finite and linearly dependent. Then there exists $u \in S$ such that*

$$\text{span}(S) = \text{span}(S \setminus \{u\}).$$

Conversely, if S is linearly independent and finite, then any proper subset $S' \subsetneq S$ satisfies

$$\text{span}(S') \subsetneq \text{span}(S).$$

Proof. We begin with the first claim. Let $S \subseteq V$ be linearly dependent. Write $S = \{u_1, \ldots, u_n\}$, with $u_i \in V$ for all $i \in \{1, \ldots, n\}$. Since S is linearly dependent, there exist $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$ such that

$$\sum_{i=1}^{n} \alpha_i u_i = 0. \qquad (*)$$

There also exists $i \in \{1, \ldots, n\}$ such that $\alpha_i \neq 0$. By rearranging the vectors $u_1, \ldots, u_n$, we may assume that $\alpha_1 \neq 0$. Then we can rearrange $(*)$ and solve for u_1 to get

$$u_1 = -\alpha_1^{-1} \sum_{i=2}^{n} \alpha_i u_i = \sum_{i=2}^{n} (-\alpha_1^{-1} \alpha_i) u_i. \qquad (**)$$

Since $(S \setminus \{u_1\}) \subseteq S$, $\text{span}(S \setminus \{u_1\}) \subseteq \text{span}(S)$. So, it remains to show that $\text{span}(S \setminus \{u_1\}) \supseteq \text{span}(S)$. To show this, let $w \in \text{span}(S)$. Then there exist $\beta_1, \ldots, \beta_n \in \mathbf{F}$ such that

$$w = \sum_{j=1}^{n} \beta_j u_j.$$

Substituting $(**)$ into this equation,

$$w = \beta_1 \sum_{i=2}^{n} (-\alpha_1^{-1}\alpha_i)u_i + \sum_{j=2}^{n} \beta_j u_j.$$

That is, $w \in \text{span}(S \setminus \{u_1\})$. In conclusion, $\text{span}(S \setminus \{u_1\}) \supseteq \text{span}(S)$, and so $\text{span}(S \setminus \{u_1\}) = \text{span}(S)$.

We now prove the second claim. Since $S' \subseteq S$, $\text{span}(S') \subseteq \text{span}(S)$. So, it remains to find $w \in \text{span}(S)$ such that $w \notin \text{span}(S')$. Since $S' \subsetneq S$, there exists $w \in S$ such that $w \notin S'$. We will show that $w \notin \text{span}(S')$. To show this, we argue by contradiction. Assume that $w \in \text{span}(S')$. Then, there exist $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$ and there exist $u_1, \ldots, u_n \in S' \subseteq S$ such that

$$w = \sum_{i=1}^{n} \alpha_i u_i.$$

That is,

$$0 = (-1)w + \sum_{i=1}^{n} \alpha_i u_i. \qquad (\ddagger)$$

Since $-1 \neq 0$ and $w \notin S'$, we have achieved an equality $(\ddagger)$ that violates the linear independence of S. (If we had $w \in S'$, then the -1 coefficient in front of w could possibly be cancelled by some α_i term in the sum in $(\ddagger)$. And then all coefficients in $(\ddagger)$ could be zero, so $(\ddagger)$ may not give us any linear dependence among elements of S. So, we are really using here that $w \notin S'$.) Since we have achieved a contradiction, we conclude that in fact $w \notin \text{span}(S')$, as desired. □

Exercise 6.4. Show that the assumption that S is finite can be removed from the statement of Theorem 6.3.

Remark 6.5. If we begin with a finite, linearly dependent set of vectors S, then we can apply Theorem 6.3 multiple times to eliminate more and more vectors from S to get a linearly independent set.

Definition 6.6 (**Basis**)**.** Let V be a vector space over a field $\mathbf{F}$. Let $S \subseteq V$. We say that S is a basis of V if S is a linearly independent set such that $\text{span}(S) = V$.

Example 6.7. The set $\{(1,0),(0,1)\}$ is a basis of $\mathbf{R}^2$.

Example 6.8. The set $\{1, x, x^2\}$ is a basis of $P_2(\mathbf{R})$.

Example 6.9. The set $\{1, x, x^2, x^3, \ldots\}$ is a basis of $P(\mathbf{R})$.

Remark 6.10. Bases are the building blocks of a vector space.

Bases are nice for many reasons. One such reason is that they have the following uniqueness property.

Theorem 6.11 (**Existence and Uniqueness of Basis Coefficients**)**.** *Let $\{u_1, \ldots, u_n\}$ be a basis for a vector space V over a field $\mathbf{F}$. Then for any vector $u \in V$, there exist unique scalars $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$ such that*

$$u = \sum_{i=1}^{n} \alpha_i u_i.$$

Proof. Let $u \in V$. Since $\{u_1, \ldots, u_n\}$ spans V, there exist scalars $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$ such that

$$u = \sum_{i=1}^{n} \alpha_i u_i. \qquad (*)$$

It remains to show that these scalars are unique. To prove the uniqueness, let $\beta_1, \ldots, \beta_n \in \mathbf{F}$ such that

$$u = \sum_{i=1}^{n} \beta_i u_i. \qquad (**)$$

Subtracting $(*)$ from $(**)$, we get

$$0 = \sum_{i=1}^{n} (\beta_i - \alpha_i) u_i.$$

Since $\{u_1, \ldots, u_n\}$ are linearly independent, we conclude that $(\alpha_i - \beta_i) = 0$ for all $i \in \{1, \ldots, n\}$. That is, $\alpha_i = \beta_i$ for all $i \in \{1, \ldots, n\}$. That is, the scalars $\alpha_1, \ldots, \alpha_n$ are unique. □

Theorem 6.12. *Let V be a vector space over a field $\mathbf{F}$. Let S be a linearly independent subset of V. Let $u \in V$ be a vector that does not lie in S.*

(a) *If $u \in \operatorname{span}(S)$, then $S \cup \{u\}$ is linearly dependent, and $\operatorname{span}(S \cup \{u\}) = \operatorname{span}(S)$.*
(b) *If $u \notin \operatorname{span}(S)$, then $S \cup \{u\}$ is linearly independent, and $\operatorname{span}(S \cup \{u\}) \supsetneq \operatorname{span}(S)$.*

Proof of (a). Let $u \in \operatorname{span}(S)$. Then there exist $u_1, \ldots, u_n \in S$, $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$ such that $u = \sum_{i=1}^{n} \alpha_i u_i$. That is,

$$0 = (-1) \cdot u + \sum_{i=1}^{n} \alpha_i u_i.$$

Since $u_i \in S$ for all $i \in \{1, \ldots, n\}$, we conclude that $S \cup \{u\}$ is a linearly dependent set (since $-1 \neq 0$).

Since $S \subseteq S \cup \{u\}$, we know that $\operatorname{span}(S \cup \{u\}) \supseteq \operatorname{span}(S)$. So, it remains to show that $\operatorname{span}(S \cup \{u\}) \subseteq \operatorname{span}(S)$. To this end, let $v \in \operatorname{span}(S \cup \{u\})$. Then there exist $v_1, \ldots, v_m \in S$, $\beta_0, \ldots, \beta_n \in \mathbf{F}$ such that $v = \beta_0 u + \sum_{i=1}^{m} \beta_i v_i$. Since $u = \sum_{i=1}^{n} \alpha_i u_i$, we conclude that

$$v = \beta_0 (\sum_{i=1}^{n} \alpha_i u_i) + \sum_{i=1}^{m} \beta_i v_i.$$

That is, v is a linear combination of elements in S. So, $v \in \operatorname{span}(S)$. In conclusion, $\operatorname{span}(S \cup \{u\}) \subseteq \operatorname{span}(S)$, so $\operatorname{span}(S \cup \{u\}) = \operatorname{span}(S)$. □

Proof of (b). Let $u_1, \ldots, u_n \in S$, and let $\alpha_0, \ldots, \alpha_n \in \mathbf{F}$. Assume that

$$\alpha_0 u + \sum_{i=1}^{n} \alpha_i u_i = 0. \qquad (*)$$

We need to show that $\alpha_0 = \cdots = \alpha_n = 0$. We split into two cases, depending whether or not α_0 is zero. If $\alpha_0 = 0$, then $(*)$ becomes

$$\sum_{i=1}^{n} \alpha_i u_i = 0.$$

And then $\alpha_1 = \cdots = \alpha_n = 0$, since S is linearly independent. On the other hand, if $\alpha_0 \neq 0$, then $(*)$ says

$$u = -\alpha_0^{-1}\left(\sum_{i=1}^{n} \alpha_i u_i\right) = \sum_{i=1}^{n}(-\alpha_0^{-1}\alpha_i)u_i.$$

That is, $u \in \text{span}(S)$, contradicting our assumption that $u \notin \text{span}(S)$. So, we must have $\alpha_0 = 0$, and therefore (as we showed), $\alpha_0 = \alpha_1 = \cdots = \alpha_n = 0$, as desired. Therefore, $S \cup \{u\}$ is linearly independent.

We now prove the second claim of part (b). Since $S \subseteq S \cup \{u\}$, $\text{span}(S \cup \{u\}) \supseteq \text{span}(S)$. Finally, by assumption, $u \notin \text{span}(S)$, so $\text{span}(S \cup \{u\}) \supsetneq \text{span}(S)$, as desired. □

The following theorem elaborates on the previous theorem.

Theorem 6.13 (**The Replacement Theorem**). *Let V be a vector space over a field $\mathbf{F}$. Let $S \subseteq V$ be a finite spanning set (i.e. such that $\text{span}(S) = V$). Assume that S has exactly n elements. Let L be a finite subset of V which is linearly independent. Assume that L has exactly m elements. Then $m \leq n$. Moreover, there exists a subset S' of S containing exactly $n - m$ vectors such that $S' \cup L$ spans V.*

Proof. We use induction on m. The base case is $m = 0$, and in this case it is true that $n \geq 0 = m$. Since $\text{span}(S) = V$, we then define $S' := S$, completing the proof.

We now prove the inductive step. Let $m > 0$. Assume that the theorem is true for $m - 1$. Since L has m elements, we can write $L = \{v_1, \ldots, v_m\}$, where $v_i \in V$ for all $i \in \{1, \ldots, m\}$. Since L is linearly independent, the set $\{v_2, \ldots, v_m\}$ is also linearly independent, by the definition of linear independence. So, by the inductive hypothesis, we apply the theorem to the set of vectors $\{v_2, \ldots, v_m\}$. Then $m - 1 \leq n$, and there exists a subset S'' of S containing exactly $n - m + 1$ vectors such that $S'' \cup \{v_2, \ldots, v_m\}$ spans V.

Write $S'' = \{w_1, \ldots, w_{n-m+1}\}$, where $w_i \in V$ for all $i \in \{1, \ldots, n - m + 1\}$. We now prove that $n \geq m$. We know $n \geq m - 1$, so we need to exclude the case $n = m - 1$. Since $S'' \cup \{v_2, \ldots, v_m\} = \{w_1, \ldots, w_{n-m+1}, v_2, \ldots, v_m\}$ spans V and $v_1 \in V$, there exist $\alpha_1, \ldots, \alpha_{n-m+1}, \beta_2, \ldots, \beta_m \in \mathbf{F}$ such that

$$v_1 = \alpha_1 w_1 + \cdots + \alpha_{n-m+1} w_{n-m+1} + \beta_2 v_2 + \cdots + \beta_m v_m. \qquad (*)$$

We now argue by contradiction to show that $n \neq m - 1$. So, assume to the contrary that $n = m - 1$. Then S'' is empty, and $(*)$ becomes

$$v_1 = \beta_2 v_2 + \cdots + \beta_m v_m. \qquad (**)$$

That is,

$$0 = (-1)v_1 + \beta_2 v_2 + \cdots + \beta_m v_m.$$

But $\{v_1, \ldots, v_m\} = L$ is a linearly independent set, so we get a contradiction, since $-1 \neq 0$. We therefore conclude that $n \neq m - 1$. Since $n \geq m - 1$ also, we conclude that $n \geq m$.

We will now conclude the proof. Since $n \geq m$, and S'' has $n - m + 1$ elements, we know that S'' is nonempty. Recall that the set

$$\{w_1, \ldots, w_{n-m+1}, v_2, \ldots, v_m\}$$

spans V, so by adding one vector, we still span V. That is, the set

$$\{w_1, \ldots, w_{n-m+1}, v_1, \ldots, v_m\}$$

spans V. To conclude the proof, we need to remove one of the w_i from this set, and still retain the spanning property.

In equation $(*)$, at least one element of $\alpha_1, \ldots, \alpha_{n-m+1}$ must be nonzero, otherwise we would get $(**)$ and obtain a contradiction. Since the ordering of the vectors in $(*)$ does not matter, we may assume that $\alpha_1 \neq 0$. So, rewriting $(*)$ and solving for w_1,

$$w_1 = v_1 - \alpha_1^{-1}\alpha_2 w_2 - \cdots - \alpha_1^{-1}\alpha_{n-m+1} w_{n-m+1} - \alpha_1^{-1}\beta_2 v_2 - \cdots - \alpha_1^{-1}\beta_m v_m.$$

That is, w_1 is a linear combination of $\{w_2, \ldots, w_{n-m+1}, v_1, \ldots, v_m\}$.

So, define $S' := \{w_2, \ldots, w_{n-m+1}\}$. Then w_1 is a linear combination of elements of $S' \cup L$. By Theorem 6.12(a),

$$\operatorname{span}(S' \cup L) = \operatorname{span}(S' \cup L \cup \{w_1\}).$$

But $S' \cup L \cup \{w_1\} = S'' \cup L$, so

$$\operatorname{span}(S' \cup L) = \operatorname{span}(S'' \cup L).$$

Since $S'' \cup \{v_2, \ldots, v_m\}$ spans V and $S'' \cup L \supseteq S'' \cup \{v_2, \ldots, v_m\}$, we conclude that $S'' \cup L$ spans V, so $\operatorname{span}(S' \cup L) = V$. Finally, S' has exactly $n - m$ elements, as desired. □

The Replacement Theorem will allow us to finally start talking about the dimension of finite vector spaces. We now collect some consequences of the Replacement Theorem, some of which will help us in constructing bases of vector spaces.

Corollary 6.14. *Let V be a vector space over a field $\mathbf{F}$. Assume that B is a finite basis of V, and B has exactly d elements. Then*

(a) *Any set $S \subseteq V$ containing less than d elements cannot span V. (That is, any spanning set must contain at least d elements.)*
(b) *Any set $S \subseteq V$ containing more than d elements must be linearly dependent. (That is, any linearly independent set in V must contain at most d elements.)*
(c) ***Any basis of V must contain exactly d elements.***
(d) *Any spanning set of V with exactly d elements is a basis of V.*
(e) *Any set of d linearly independent elements of V is a basis of V.*
(f) *Any set of linearly independent elements of V is contained in a basis of V.*
(g) *Any spanning set of V contains a basis.*

Proof of (a). We argue by contradiction. Suppose S spans V, and S has $d' < d$ elements. Since B is linearly independent, the Replacement Theorem (Theorem 6.13) implies that $d' \geq d$. But $d' < d$ by assumption. Since we have arrived at a contradiction, we conclude that S cannot span V. □

Proof of (b). First, assume that S is finite. We argue by contradiction. Suppose S is linearly independent, and S has $d' > d$ elements. Since B spans V, the Replacement Theorem (Theorem 6.13) implies that $d \geq d'$. But $d' > d$ by assumption. Since we have arrived at a contradiction, we conclude that S is linearly dependent.

Now, assume that S is infinite. Let S' be any subset of S with $d+1$ elements. From what we just proved, we know that S' is linearly dependent. Since $S' \subseteq S$, we conclude that S is linearly dependent. □

Proof of (c). Let $S \subseteq V$ be any basis. Suppose S has d' elements. Since S spans V, $d' \geq d$ by part (a). Since S is linearly independent, $d' \leq d$ by part (b). Therefore $d' = d$. □

Proof of (d). Let $S \subseteq V$ be a spanning set with d elements. It suffices to show that S is linearly independent. To show this, we argue by contradiction. Assume that S is linearly dependent. From Theorem 6.3, there exists $u \in S$ such that $S \setminus \{u\}$ is also a spanning set. But $S \setminus \{u\}$ has $d-1$ elements, contradicting part (a). We therefore conclude that S is linearly independent, as desired. □

Proof of (e). Let $S \subseteq V$ be a set of d linearly independent elements. It suffices to show that S is a spanning set. To show this, we argue by contradiction. Suppose S does not span V. Then there exists $u \in V$ such that $u \notin \text{span}(S)$. By Theorem 6.12(b), $S \cup \{u\}$ is linearly independent, and it has $d+1$ elements, contradicting part (b) of the present Theorem. We therefore conclude that S is a spanning set. □

Proof of (f). Let $L \subseteq V$ be a set of exactly d' linearly independent elements. By the Replacement Theorem (Theorem 6.13), there exists a subset B' of B with exactly $d-d'$ elements such that $L \cup B'$ spans V. Then $L \cup B'$ has at most $(d-d')+d' = d$ elements. Since $L \cup B'$ spans V, $L \cup B'$ must have exactly d elements, by part (a). It remains to show that $L \cup B'$ is linearly independent. This follows from part (d). □

Proof of (g). Let $S \subseteq V$ be a spanning set of V. From part (e), it suffices to find a subset of S of d linearly independent elements. To find such a subset, we argue by contradiction. Suppose every subset of S with d elements has at most $d' < d$ linearly independent elements. Suppose we have d' linearly independent elements $S' := \{u_1, \ldots, u_{d'}\} \subseteq V$. Let $u \in S$ with $u \notin S'$. Then u must be a linear combination of elements of S'. Otherwise, $S \cup \{u\}$ would be a linearly independent set of $d'+1$ elements, by Theorem 6.12(b). In conclusion, every element of S is a linear combination of elements of S'. So, $\text{span}(S') = \text{span}(S) = V$. So, S' is a basis of V with d' elements. But this fact contradicts part (c), since $d' < d$, and B is a basis of V with d elements. Since we have reached a contradiction, we conclude that there exists a subset S of V with d linearly independent elements, as desired. □

Definition 6.15 (**Dimension**)**.** Let V be a vector space over a field $\mathbf{F}$. We say that V is **finite-dimensional** if there exists $d \in \mathbf{N}$ such that V contains a basis with d elements. By Corollary 6.14(c), the number d does not depend on the choice of basis of V. We therefore call d the **dimension** of V, and we write $\dim(V) = d$. If the vector space V is not finite-dimensional, we say that V is **infinite-dimensional**, and we write $\dim(V) = \infty$.

Remark 6.16. From Corollary 6.14(c), we see that a given finite-dimensional vector space V over a field $\mathbf{F}$ has exactly one $d \in \mathbf{N}$ such that V has dimension d. That is, the notion of the dimension of a vector space V over a field $\mathbf{F}$ is well-defined.

Example 6.17. $\mathbf{R}^3$ has dimension 3.

Example 6.18. $P_2(\mathbf{R})$ has dimension 3.

Example 6.19. The vector space $M_{m\times n}(\mathbf{R})$ of $m \times n$ matrices over $\mathbf{R}$ has dimension mn.

Example 6.20. $P(\mathbf{R})$ is infinite dimensional.

Example 6.21. The complex numbers $\mathbf{C}$ viewed as a vector space over the field $\mathbf{C}$ have dimension 1.

Example 6.22. The complex numbers $\mathbf{C}$ viewed as a vector space over the field $\mathbf{R}$ have dimension 2. So, changing the field can change our notion of dimension.

7. Subspaces and Dimension

Theorem 7.1. *Let V be a finite-dimensional vector space over a field $\mathbf{F}$. Let W be a subspace of V. Then W is also finite-dimensional, and $\dim(W) \leq \dim(V)$. Moreover, if $\dim(W) = \dim(V)$, then $W = V$.*

Proof. We will build a basis for W. We begin with the zero vector $\{0\}$. If $W = \{0\}$, we stop building the basis. Otherwise, let $u_1 \in W$ be a nonzero vector. If $W = \text{span}(u_1)$, then the basis for W is $\{u_1\}$. Otherwise, let $u_2 \in W$ such that $u_2 \notin \text{span}(u_1)$. By Theorem 6.12(b), $\{u_1, u_2\}$ is a linearly independent set. If $W = \text{span}(u_1, u_2)$, then $\{u_1, u_2\}$ is a basis for W, by the definition of basis. Otherwise, let $u_3 \in W$ such that $u_3 \notin \text{span}(u_1, u_2)$. We continue in this way, building this list of vectors. Since V is finite-dimensional, it has a basis consisting of d elements for some $d \in \mathbf{N}$. So, by Corollary 6.14(b), we must stop building our list of vectors after at most d steps. Suppose that when this procedure stops, we have n vectors $\{u_1, \ldots, u_n\}$. Then $W = \text{span}(u_1, \ldots, u_n)$, so W is finite-dimensional, $\dim(W) = n$, and $n \leq d$. In the case $n = d$, then $W = \text{span}(u_1, \ldots, u_n)$, and $\{u_1, \ldots, u_n\}$ is a linearly independent set. So, by Corollary 6.14(e), $\{u_1, \ldots, u_n\}$ is a basis for V. So, $\text{span}(u_1, \ldots, u_n) = V$, i.e. $W = V$. □

The following result concerning polynomials may appear entirely unrelated to linear algebra. However, if we look at the problem in the right way, the uniqueness statement becomes a relatively easy consequence of the general theory we have developed above.

Theorem 7.2 (**Lagrange Interpolation Formula**). *Let $x_1, \ldots, x_n$ be distinct real numbers, and let $y_1, \ldots, y_n \in \mathbf{R}$. Then, there exists a unique polynomial $f \in P_{n-1}(\mathbf{R})$ such that $f(x_i) = y_i$ for all $i \in \{1, \ldots, n\}$. Moreover, for any $x \in \mathbf{R}$, f can be written as*

$$f(x) = \sum_{j=1}^{n} \frac{\prod_{1 \leq k \leq n:\ k \neq j} (x - x_k)}{\prod_{1 \leq k \leq n:\ k \neq j} (x_j - x_k)} \cdot y_j. \qquad \forall\, x \in \mathbf{R} \qquad (*)$$

Proof. We first show that f is unique. This uniqueness will come from writing f in a suitable basis of $P_{n-1}(\mathbf{R})$, and then applying Theorem 6.11.

For each $i \in \{1, \ldots, n\}$, define

$$f_i(x) := \prod_{1 \leq k \leq n:\ k \neq i} \frac{x - x_k}{x_i - x_k}.$$

Note that f_i is a degree $(n-1)$ polynomial,

$$f_i(x_i) = 1, \quad f_i(x_j) = 0 \ \forall\, j \in \{1, \ldots, n\} \setminus \{i\}. \qquad (**)$$

We claim that the set $\{f_i\}_{i=1}^n$ is a basis of $P_{n-1}(\mathbf{R})$. We know that $B := \{1, x, x^2, \ldots, x^{n-1}\}$ is a basis for $P_{n-1}(\mathbf{R})$ with n elements. So, to show that $\{f_i\}_{i=1}^n$ is a basis of $P_{(n-1)}(\mathbf{R})$, it suffices to show that $\{f_i\}_{i=1}^n$ is a linearly independent set, by Corollary 6.14(e).

We show that $\{f_i\}_{i=1}^n$ is a linearly independent set by contradiction. Suppose $\{f_i\}_{i=1}^n$ is not linearly independent. Then, there exist $\alpha_1, \ldots, \alpha_n \in \mathbf{R}$ such that

$$\sum_{i=1}^{n} \alpha_i f_i(x) = 0, \quad \forall\, x \in \mathbf{R}, \qquad (\dagger)$$

and there exists $j \in \{1, \ldots, n\}$ such that $\alpha_j \neq 0$. However, using $x = x_j$ in $(\dagger)$, and then applying $(**)$, we get from $(\dagger)$ that $\alpha_j = 0$, a contradiction. We conclude that $\{f_i\}_{i=1}^n$ is

a linearly independent set. So, by Theorem 6.11, for any $f \in P_{n-1}(\mathbf{R})$, there exist unique scalars $\beta_1, \ldots, \beta_n \in \mathbf{R}$ such that

$$f = \sum_{j=1}^{n} \beta_j f_j. \qquad (\ddagger)$$

If $f \in P_{n-1}(\mathbf{R})$ satisfies $f(x_j) = y_j$ for all $j \in \{1, \ldots, n\}$, we will show that $\beta_j = y_j$ for all $j \in \{1, \ldots, n\}$ in $(\ddagger)$. Fix $j \in \{1, \ldots, n\}$. Using x_j in $(\ddagger)$ and applying $(**)$, we get $f(x_j) = \beta_j$. If $f(x_j) = y_j$ for all $j \in \{1, \ldots, n\}$, we must therefore have $\beta_j = y_j$ in $(\ddagger)$. That is, we exactly recover formula $(*)$.

$$f = \sum_{j=1}^{n} y_j f_j.$$

Finally, note that f defined by the formula $f = \sum_{j=1}^{n} y_j f_j$ does satisfy $f \in P_{n-1}(\mathbf{R})$ and $f(x_j) = y_j$ for all $j \in \{1, \ldots, n\}$. □

Remark 7.3 (An Application to Cryptography.)**.** The following application of Theorem 7.2 is known as **Shamir's Secret Sharing**. Suppose I want to have a secret piece of information shared between n people such that all n people can together verify the secret, but any set of $(n-1)$ of the people cannot verify the secret. The following procedure allows us to share the secret in this way. We label the people as integers $i \in \{1, \ldots, n\}$. Let $x_1, \ldots, x_n$ be distinct, nonzero integers, and let $y_1, \ldots, y_n$ be any integers. Each person $i \in \{1, \ldots, n\}$ keeps a value (x_i, y_i). By Theorem 7.2, let $f \in P_{n-1}(\mathbf{R})$ be the unique polynomial such that $f(x_i) = y_i$ for all $i \in \{1, \ldots, n\}$. Then the secret information is $f(0)$. To see that the secret cannot be found by $n-1$ people, suppose we only knew the values $\{(x_i, y_i)\}_{i=1}^{n-1}$. Then there would be infinitely many polynomials f such that $f(x_i) = y_i$ for all $i \in \{1, \ldots, n-1\}$ by Theorem 7.2. So, the secret $f(0)$ could not be found by $n-1$ people.

8. Appendix: Notation

Let A, B be sets in a space X. Let m, n be a nonnegative integers. Let $\mathbf{F}$ be a field.

$\mathbf{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, the integers

$\mathbf{N} := \{0, 1, 2, 3, 4, 5, \ldots\}$, the natural numbers

$\mathbf{Q} := \{m/n \colon m, n \in \mathbf{Z}, n \neq 0\}$, the rationals

$\mathbf{R}$ denotes the set of real numbers

$\mathbf{C} := \{x + y\sqrt{-1} : x, y \in \mathbf{R}\}$, the complex numbers

$\emptyset$ denotes the empty set, the set consisting of zero elements

$\in$ means "is an element of." For example, $2 \in \mathbf{Z}$ is read as "2 is an element of $\mathbf{Z}$."

$\forall$ means "for all"

$\exists$ means "there exists"

$\mathbf{F}^n := \{(x_1, \ldots, x_n) \colon x_i \in \mathbf{F}, \forall\, i \in \{1, \ldots, n\}\}$

$A \subseteq B$ means $\forall\ a \in A$, we have $a \in B$, so A is contained in B

$A \smallsetminus B := \{x \in A \colon x \notin B\}$

$A^c := X \smallsetminus A$, the complement of A

$A \cap B$ denotes the intersection of A and B

$A \cup B$ denotes the union of A and B

$C(\mathbf{R})$ denotes the set of all continuous functions from $\mathbf{R}$ to $\mathbf{R}$

$P_n(\mathbf{R})$ denotes the set of all real polynomials in one real variable of degree at most n

$P(\mathbf{R})$ denotes the set of all real polynomials in one real variable

$M_{m\times n}(\mathbf{F})$ denotes the vector space of $m \times n$ matrices over the field $\mathbf{F}$

UCLA Department of Mathematics, Los Angeles, CA 90095-1555
E-mail address: heilman@math.ucla.edu