6. Fields and Subspaces

Since linear algebra is such a powerful tool and it appears in so many places, we want to take as much advantage of this as possible. The idea then is to abstract many of the techniques we used in the previous lectures.

The first thing to generalise is the notion of scalar. We need to be able to add, subtract, multiply and divide.

Definition 6.1. *A **field** F is a set with two operations addition and multiplication,*

$$+\colon F \times F \longrightarrow F \qquad \text{and} \qquad \cdot\colon F \times F \longrightarrow F,$$

*which obey the following axioms. $(F, +)$ is an **abelian group** under addition:*

(1) *Addition is **associative**. That is for every x, y and $z \in F$,*

$$(x + y) + z = x + (y + z).$$

(2) *There is an **identity** element under addition. This element is often denoted $0 \in F$ and for every element $x \in F$,*

$$0 + x = x + 0 = x.$$

(3) *Every element has an additive **inverse**. That is given $x \in F$ there is an element $-x \in F$ and*

$$x + (-x) = -x + x = 0.$$

(4) *Addition is **commutative**. That is given x and $y \in F$,*

$$x + y = y + x.$$

Let $F^* = F - \{0\}$. Then $(F^*, \cdot)$ is an abelian group under multiplication:

(5) *Multiplication is associative. That is for every x, y and $z \in F$,*

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

(6) *There is an identity element under addition. This element is often denoted $1 \in F$ and for every element $x \in F$,*

$$1 \cdot x = x \cdot 1 = x.$$

(7) *Every element has a multiplicative inverse. That is given $x \in F$ there is an element $x^{-1} \in F$ and*

$$x \cdot x^{-1} = x^{-1} \cdot x = 0.$$

(8) *Multiplication is commutative. That is given x and $y \in F$,*

$$x \cdot y = y \cdot x.$$

Finally we require that addition and multiplication are compatible,

(9) *F satisfies the* ***distributive*** *law. That is given x, y and $z \in F$,*

$$x(y+z) = xy + xz.$$

We will often be sloppy and write $x - x = 0$, $x \cdot y = xy$ and $x^{-1} = 1/x$. Note that $(F, \cdot)$ is never a group under multiplication ("you cannot divide by zero"). The axioms have certain consequences. For example

Lemma 6.2. *Let $(F, +, \cdot)$ be a field.*
Then for every $x \in F$, $0 \cdot x = x \cdot 0 = 0$.

Proof. $0+0 = 0$ as 0 is the identity under addition. By the distributive law

$$x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0.$$

So

$$x \cdot 0 = x \cdot 0 + x \cdot 0.$$

Subtract $x \cdot 0$ (or better add the additive inverse of $x \cdot 0$) from both sides,

$$0 = x \cdot 0.$$

As multiplication is commutative, $0 \cdot x = 0$ as well. □

So what are examples of fields? Certainly the real numbers $\mathbb{R}$ are a field, with the usual rules for addition and multiplication. Also the complex numbers $\mathbb{C}$. The only slightly tricky thing is to write down the multiplicative inverse of any non-zero complex number. If $a + bi \in \mathbb{C}$ is a complex number, so that a and b are two real numbers, not both zero, then

$$(a+bi)(a-bi) = a^2 + b^2 \neq 0.$$

It follows then that $c + di$ is the multiplicative inverse of $a + bi$ where

$$c = \frac{a}{a^2+b^2} \qquad \text{and} \qquad d = \frac{-b}{a^2+b^2}.$$

In fact the rational numbers form a field

$$\mathbb{Q} = \{\, p/q \,|\, p \in \mathbb{Z}, q \in \mathbb{N} - \{0\} \,\}.$$

Note that the integers are not a field. 2 does not have a multiplicative inverse (it does as a rational number of course). The natural numbers are not even a group under addition 1 does not have an additive inverse (again, it does as an integer). There are some more quixotic examples

$$\mathbb{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} \,|\, a, b \in \mathbb{Q} \,\}.$$

Again all of the axioms are pretty much clear except finding a multiplicative inverse. Given a and $b \in \mathbb{Q}$, we have

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 + 2b^2.$$

So $c + d\sqrt{2}$ is the multiplicative inverse of $a + b\sqrt{2}$, where

$$c = \frac{a}{a^2 + 2b^2} \qquad \text{and} \qquad d = \frac{-b}{a^2 + 2b^2}.$$

Let F be a field and let $F[x]$ denote all polynomials $p(x)$ in x with coefficients in F. This is not a field but it is pretty easy to make it into one. Let $F(x)$ denote all rational functions in x, that is the quotient of two polynomials $p(x)/q(x)$ where $q(x)$ is not the zero polynomial. In other words the rational numbers are to the integers as the rational functions are to polynomials.

Given any axioms describing an algebraic system one can always try to understand the axioms by becoming a minimalist. What is the smallest set which can be turned into a field? The emptyset? No, we are forced to put at least one element into F and call it zero. Okay, how about the set $F = \{0\}$ with one element? No, F^* should contain one element, which we call 1. Okay, how about the set $F = \{0, 1\}$?

The surprising thing is that we can make this into a field. It is convenient to make addition and multiplication tables. In fact the axioms force both addition and multiplication:

$+$	0	1
0	0	1
1	1	0

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

One can check that all the axioms are satisfied.

Okay, how about a field with three elements? Let us call the third element 2.

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

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1.

It is not so obvious anymore but again we do get a field.

Definition 6.3. *Let $a \in \mathbb{Z}$ be an integer and let m be a natural number. Then are always integers q and r, called the **quotient** and **remainder** where $0 \leq r \leq m - 1$ and*

$$a = mq + r.$$

*The number r is called the **residue** of a modulo m.*

Definition 6.4. *Let p be a prime number. Let $\mathbb{F}_p$ be the set of numbers between 0 and $p-1$. Define a law of addition by adding the two numbers i and j the usual way and then taking the residue modulo p. Define a law of mutiplication by multiplying i and j the usual way and then taking the residue modulo p.*

Lemma 6.5. *$(\mathbb{F}_p, +, \cdot)$ is a field.*

Note again that most axioms are not hard to check. If $i \in \mathbb{F}_p$ then $p - i$ is the additive inverse. The only tricky thing is to define the multiplicative inverse. To do this we need to use the fact that if two integers a and b are coprime (that is they have no common factors) then we may find two other integers x and y such that

$$xa + by = 1.$$

(In fact this follows from Euclid's algorithm and "backwards substitutiob"). On the other hand, if $0 < a < p$ and p is prime, then a and p are automatically prime. So we may find x and y such that

$$xa + bp = 1.$$

Modulo p we then we get

$$xa \equiv 1 \mod p.$$

So x is the multiplicative inverse of a. Perhaps an example will help. Consider $\mathbb{F}_7$. Pick $a = 4$. $2 \cdot 4 = 8$. So $2 \cdot 4 \equiv 1 \mod 7$. Thus 2 is the inverse of 4 in $\mathbb{F}_7$.

Perhaps more surprisingly, there is only one field $\mathbb{F}_p$ with p elements, for every prime. The point is that $2 = 1 + 1$, $3 = 1 + 1 + 1$, up to $p - 1$ and $p = 0$. So to calculate

$$\begin{aligned} 2 \cdot 3 &= (1 + 1)(1 + 1 + 1) \\ &= 1 + 1 + 1 + 1 + 1 + 1. \end{aligned}$$

This obviously generalises. It follows that every sum and product is determined.

Definition 6.6. *Let F be a field and let d be a positive integer.*

$$F^d = \{ (a_1, a_2, \ldots, a_d) \mid a_i \in F \}.$$

*d is called the **dimension**.*

We have already seen $\mathbb{R}^d$. At the other extreme, $\mathbb{F}_p^d$ is a finite set with p^d elements. We call the elements of F^d vectors. We can add vectors component by component and multiply them by scalars. It

might seem strange at first, by it makes sense to do geometry in F^d even using unusual fields.

Definition 6.7. *Let $v_1, v_2, \ldots, v_k$ be vectors and let $r_1, r_2, \ldots, r_k$ be scalars. We say that v is a **linear combination** of $v_1, v_2, \ldots, v_k$ if*

$$v = r_1 v_1 + r_2 v_2 + \cdots r_k v_k.$$

*The **span** of $v_1, v_2, \ldots, v_k$ is the set of all linear combinations of $v_1, v_2, \ldots, v_k$. It is denoted by* $\text{span}\{v_1, v_2, \ldots, v_k\}$.

The span of a single non-zero vector in $\mathbb{R}^3$ is the line through the origin containing this vector. The span of two non-zero vectors in $\mathbb{R}^3$ is either the plane containing the vectors or in the degenerate case when one vector is a multiple of the other, the line through the origin containing both.

Note that if we take $r_1 = r_2 = \cdots = r_k = 0$, then $v = 0$. That is the zero vector is a linear combination of any non-empty collection of vectors and the zero vector always belongs to the span. For this reason we adopt the convention that the span of the empty set is $\{0\}$.

$(4, 3, -1)$ is a linear combination of $(3, 4, -2)$ and $(-2, -1, 1)$, since

$$(4, 7, -3) = 2(3, 4, -2) + 1(-2, -1, 1)$$

Here is a key result:

Proposition 6.8. *Let A be the $m \times n$ matrix whose columns are the n vectors $v_1, v_2, \ldots, v_n$ in F^m.*

Then the vector v is a linear combination of $v_1, v_2, \ldots, v_n$ if and only if the equation $Ax = b$ has a solution.

Proof. Suppose that v is a linear combination of $v_1, v_2, \ldots, v_n$. Then there are scalars $r_1, r_2, \ldots, r_n \in F$ such that $v = \sum r_i v_i$. Let $w = (r_1, r_2, \ldots, r_n) \in F^n$. Then Aw is the vector obtained by summing the columns of A together, that is $Aw = v$. Then w is a solution to the the equation $Ax = v$.

Conversely suppose that w is a solution of the equation $Ax = v$. Suppose that $w = (r_1, r_2, \ldots, r_n) \in F^n$. Then

$$v = \sum r_i v_i,$$

so that v is a linear combination of $v_1, v_2, \ldots, v_n$. □

Let us see an easy example. Is $(1, 1, 3)$ a linear combination of $(-1, 2, 1)$ and $(1, 3, 1)$? Let A be the matrix

$$\begin{pmatrix} -1 & 1 \\ 2 & 3 \\ 1 & 1 \end{pmatrix}$$

We try to solve the linear equation $Ax = b$. We first form the augmented matrix

$$\left(\begin{array}{ccc} -1 & 1 & 1 \\ 2 & 3 & 1 \\ 1 & 1 & 3 \end{array}\right).$$

Now we apply Gaussian elimination. We multiply the first row by -1.

$$\left(\begin{array}{ccc} 1 & -1 & -1 \\ 2 & 3 & 1 \\ 1 & 1 & 3 \end{array}\right).$$

Next we multiply the first row by -2 and -1 and add it to the second row and third rows

$$\left(\begin{array}{ccc} 1 & -1 & -1 \\ 0 & 5 & 3 \\ 0 & 2 & 4 \end{array}\right).$$

It is convenient to swap the second and third rows,

$$\left(\begin{array}{ccc} 1 & -1 & -1 \\ 0 & 2 & 4 \\ 0 & 5 & 3 \end{array}\right).$$

Now multiply the second row by $1/2$,

$$\left(\begin{array}{ccc} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 5 & 3 \end{array}\right).$$

Finally multiply the second row by -5 and add it to the third row,

$$\left(\begin{array}{ccc} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & -7 \end{array}\right).$$

This clearly an inconsistent set of equations. Therefore $(1, 1, 3)$ is not a linear combination of of $(-1, 2, 1)$ and $(1, 3, 1)$. But suppose that we began with $(1, 8 = 7 + 1, 3)$. If we apply Gaussian elimination then at every stage the second (until it becomes the third) row is greater by 7. Thus we end up with

$$\left(\begin{array}{ccc} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{array}\right).$$

Solving by back subsitution gives $r_2 = 2$ and $r_1 - 2 = -1$ so that $r_1 = 1$. Thus

$$(1, 8, 3) = (-1, 2, 1) + 2(1, 3, 1),$$

which is indeed correct.

We give some provisional definitions:

Definition 6.9. *Let $V \subset F^d$ be any subset. We say that V is **closed under addition** if whenever v and w are in V then so is $v+w$. We say that V is **closed under scalar multiplication** if whenever $v \in V$ and $\lambda \in F$ then $\lambda v \in V$.*

Definition 6.10. *Let F be a field and let $V \subset F^d$ be a subset.*
*We say that V is a **subspace** of F^d if*

(1) *V is not empty.*
(2) *V is closed under addition.*
(3) *V is closed under scalar multiplication.*

There are two "classic" ways to generate subspaces. Here is the first:

Lemma 6.11. *Let F be a field and let $v_1, v_2, \ldots, v_k \in F^d$ be a sequence of vectors.*
If $V = \text{span}\{v_1, v_2, \ldots, v_k\}$ then V is a subspace of F^d.

Proof. If $k > 0$ then V is clearly not empty and if $k = 0$ then $0 \in V$ by convention. In particular V is not empty. Thus (1) of (6.10) holds.

Suppose that v and $w \in V$. Then v and w are linear combinations of $v_1, v_2, \ldots, v_k$. It follows that there are scalars $r_1, r_2, \ldots, r_k$ and $s_1, s_2, \ldots, s_k$ such that

$$v = r_1v_1 + r_2v_2 + \cdots + r_kv_k \qquad \text{and} \qquad w = s_1v_1 + s_2v_2 + \cdots + s_kv_k.$$

But then

$$\begin{aligned} v + w &= r_1v_1 + r_2v_2 + \cdots + r_kv_k + s_1v_1 + s_2v_2 + \cdots + s_kv_k \\ &= (r_1 + s_1)v_1 + (r_2 + s_2)v_2 + \cdots + (r_k + s_k)v_k. \end{aligned}$$

Hence $v + w$ is a linear combination of $v_1, v_2, \ldots, v_k$ and so $v + w \in V = \text{span}\{v_1, v_2, \ldots, v_k\}$. Thus V is closed under addition. Thus (2) of (6.10) holds.

Now suppose that $v \in V$ and $\lambda \in F$. As before we may find scalars $r_1, r_2, \ldots, r_k$ such that

$$v = r_1v_1 + r_2v_2 + \cdots + r_kv_k.$$

But then

$$\begin{aligned} \lambda v &= \lambda(r_1v_1 + r_2v_2 + \cdots + r_kv_k) \\ &= (\lambda r_1)v_1 + (\lambda r_2)v_2 + \cdots + (\lambda r_k)v_k. \end{aligned}$$

Hence λv is a linear combination of $v_1, v_2, \ldots, v_k$ and so $\lambda v \in V = \text{span}\{v_1, v_2, \ldots, v_k\}$. Thus V is closed under multiplication. Thus (3) of (6.10) holds.

As we have checked (1-3) of (6.10) it follows that V is a subspace. $\square$

Definition 6.12. *Let A be a $m \times n$ matrix with entries in a field. The* ***kernel*** *(also known as the* ***nullspace****) of A, denoted* $\operatorname{Ker} A$*, is the set of solutions to the homogeneous equation $Ax = 0$.*

Here is the other way to generate subspaces:

Lemma 6.13. *Let F be a field and let A be a $m \times n$ matrix whose entries belong to F.*

Then $V = \operatorname{Ker} A$ is a subspace of F^d.

Proof. As 0 is a solution of $Ax = 0$, $0 \in V$. In particular V is not empty.

Suppose that v and $w \in V$. Then v and w are both solutions of $Ax = 0$. It follows that

$$\begin{aligned} A(v + w) &= Av + Aw \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Hence $v + w$ is a solution of $Ax = 0$ and so $v + w \in V$. Thus V is closed under addition.

Finally suppose that $v \in V$ and $\lambda \in F$. Then v is a solution of $Ax = 0$. But then

$$\begin{aligned} A(\lambda v) &= \lambda(Av) \\ &= \lambda 0 \\ &= 0. \end{aligned}$$

Thus λv is a solution to $Ax = 0$ and so $\lambda v \in V$. But then V is closed under scalar multiplication.

As V is non-empty, and closed under addition and scalar multiplication it follows that V is subspace of F^d. □

There are two trivial subspaces of any vector space. The subset consisting of only the origin and the whole space F^d. One can check the axioms directly or appeal to either of (6.11) or (6.13).

$\{0\}$ is the span of the empty set and V is the span of the vectors $e_1, e_2, \ldots, e_d$, where e_i is the vector with a 1 in the ith place and zero everywhere else. Given $v = (r_1, r_2, \ldots, r_d) \in F^d$ then

$$v = r_1 e_1 + r_2 e_2 + \cdots + r_d e_d.$$

Hence every vector in F^d is a linear combination of $e_1, e_2, \ldots, e_d$.

On the other hand, V is the set of solutions to be the empty set of equations (that is take A to a $0 \times n$ matrix). If you don't like that possibility one can also take A to be the zero $m \times n$ matrix, any m.

At the other extreme, let $A = I_n$. The only solution to the equation $I_n x = 0$ is clearly the zero vector.