1 Fields

1.1 The Definition of a Field

The basic objects of study in linear algebra are vector spaces over fields and linear maps between vector spaces and one of our first prices of business is to define all of these terms. If $\mathbf{R}$ is the set of real numbers then the basic example of a vector space is the set $\mathbf{R}^n$ of n-tuples $(x_1, \ldots, x_n)$ where each x_i is an element of $\mathbf{R}$. Actually we will usually write elements of $\mathbf{R}^n$ as column tuples:

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

as this is more consistent with doing matrix algebra. I am assuming all of you have seen some linear algebra at least in the form of doing matrix computations where the elements of the matrices are real or complex numbers. The matrix theory part of the class will look very much like what you have seen (but a large part of what we do will not evolve matrices) with the difference that the elements of the matrices are not restricted to being real or complex numbers, but can come from more general sets called fields. The basic idea is that a field $\mathbf{F}$ is a set with two operations ***addition*** (denoted by $+$) and ***multiplication*** (denoted by $\cdot$ or just concatenation (*i.e.* $a \cdot b = ab$)) that satisfy all the rules of high school algebra. More precisely

Definition 1.1 *A **field** $(\mathbf{F}, +, \cdot)$ is a set $\mathbf{F}$ with two binary operations $+$ and $\cdot$ so that*

1. *The operations $+$ and $\cdot$ are both commutative and associative:*

$$x + y = y + x, \quad x + (y + x) = (x + y) + x, \qquad xy = yx, \quad x(yz) = (xy)z.$$

2. *Multiplication distributes over addition:*

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

3. *There is a unique[1] element $0 \in \mathbf{F}$ so that for all $x \in \mathbf{F}$*

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

   *This element will be called the **zero** of $\mathbf{F}$.*

4. *There is a unique[2] element $1 \in \mathbf{F}$ so that for all $x \in \mathbf{F}$*

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

   *This element is called the **identity** of $\mathbf{F}$.*

5. *$0 \neq 1$. (This implies $\mathbf{F}$ has at least two elements.)*

[1] It is not hard to show the assumption of the uniqueness can be dropped. For if 0 and $0'$ are elements so that $x + 0 = x$ and $x + 0' = x$ then $0 = 0 + 0' = 0' + 0 = 0'$ which implies uniqueness.

[2] Again the assumption of uniqueness can be dropped.

6. *For any $x \in \mathbf{F}$ there is a unique*[3] $-x \in \mathbf{F}$ *so that*

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

(This element is called the ***negative*** *of x. And from now on we write $x + (-y)$ as $x - y$.)*

7. *If $0 \neq x \in \mathbf{F}$ there is a unique*[4] *element $x^{-1} \in \mathbf{F}$ so that*

$$xx^{-1} = x^{-1}x = 1.$$

(We will also denote x^{-1} by $1/x$ and yx^{-1} by y/x. The element x^{-1} is called the ***inverse*** *of x.)*

We will usually just refer to "the field $\mathbf{F}$" rather than "the field $(\mathbf{F}, +, \cdot)$". For any field $\mathbf{F}$ we can view the positive integer n as an element of $\mathbf{F}$ by setting

$$n := \underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}}$$

Then for negative n we can set $n := -(-n)$ where $-n$ is defined by the last equation. That is $-4 = -(1 + 1 + 1 + 1)$. In most respects all of the basic algebra you know works as usual in a field. As a sample of this

Proposition 1.2 *Let $\mathbf{F}$ be a field. Then for all $a, b \in \mathbf{F}$*

1. *$a \cdot 0 = 0$*
2. *$ab = 0$ if and only if $a = 0$ or $b = 0$.*
3. *$x^2 = a^2$ implies $x = a$ or $x = -a$.*
4. *If $ad - bc \neq 0$ then*

$$\begin{array}{rcl} ax + by & = & e \\ cx + dy & = & f \end{array} \qquad \text{implies} \qquad x = \frac{ed - fb}{ad - bc}, \quad y = \frac{af - ce}{ad - bc}$$

PROOF: An exercise you should do if you are not familiar with this circle of ideas. □

1.2 Examples of Fields

The rational numbers. This is the set of ratios a/b of integers a, b with $b \neq 0$. (Note that integers can be either positive or negative.) This is the most natural example of a field.

The real numbers. For lack of a shorter definition this is the collection of all decimal numbers $\mathbf{R}$. I am assuming that you know the basic properties of the real numbers, or are at least learning about them in Math 703. One advantage of the real numbers over the rational numbers

[3] Again the assumption of uniqueness can be dropped: If $x+y = 0$ and $x+z = 0$ then $y = y+0 = y+(x+z) = (x + y) + z = 0 + z = z$.

[4] And yet again the assumption of uniqueness can be dropped.

is that every positive real number has a real numbers as a square root, while not every rational number has a rational number as a square root.

The complex numbers. Let $i = \sqrt{-1}$ so that $i^2 = -1$. Then the complex numbers $\mathbf{C}$ is the set of all numbers $x + iy$ where x and y are real numbers and addition and multiplication are done in the natural way. That is

$$(x_1+y_1i)+(x_2+y_2i) = (x_1+x_2)+(y_1+y_2)i \qquad (x_1+y_1i)(x_2+y_2i) = (x_1x_2-y_1y_2)+(x_1y_2+x_2y_1)i.$$

(The rule for multiplication is what is obtained by expanding the product $(x_1 + y_1i)(x_2 + y_2i)$, using that $i^2 = -1$ and grouping the terms with an i together.) What is not quite obvious if you have not seen it before is that if $x + iy$ is a nonzero complex number that it has an inverse. To get the inverse of $x + iy$ we use the trick of "rationalizing the denominator" by multiplying by $x - iy$ (call the ***complex conjugate*** of $x + iy$). That is

$$\frac{1}{x+iy} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x-iy}{x^2+y^2} = \frac{x}{x^2+y^2} + i\frac{-y}{x^2+y^2}.$$

Note that $x + iy \neq 0$ means that $x \neq 0$ or $y \neq 0$ so that $x^2 + y^2 > 0$ and therefore the above calculation works for any nonzero complex number. The importance of the complex numbers is that not only does every complex number z have a square root that is also a complex number, but if $p(z) = a_nz^n + a_{n-1}z^{n-1} + \cdots a_0$ is a polynomial with complex coefficients and $a_n \neq 0$ then the equation $p(z) = 0$ will always have at least one complex solution. This fact is referred to as the ***fundamental theorem of algebra***.

Quadratic number fields. This is not anything that we will use other than in passing, but it is interesting to see examples that are not as familiar as the ones above. Let n be an integer (either positive or negative) that does not have a rational square root. That is $x^2 = n$ does not have a solution with $x = a/b$ a rational number. This implies that if a and b are rational numbers then $a^2 - b^2n \neq 0$ unless both a and b are zero. Let $\mathbf{F} := \{a + b\sqrt{n} : a, b \in \mathbf{Q}\}$. Multiplication and addition are done as usual (that is this just viewing them as complex numbers.) The only thing that might keep $\mathbf{F}$ from being a field is that the inverse of a member of $\mathbf{F}$ might not be in $\mathbf{F}$. Again rationalizing the denominator saves the day:

$$\frac{1}{a+b\sqrt{n}} = \frac{a-b\sqrt{n}}{(a+b\sqrt{n})(a-b\sqrt{n})} = \frac{a-b\sqrt{n}}{a^2-b^2n} = \frac{a}{a^2-b^2n} + \frac{-b}{a^2-b^2n}\sqrt{n}$$

and as remarked above $a^2 - b^2n \neq 0$ unless $a + b\sqrt{n} = 0$.

The field of rational functions. Let $\mathbf{F}$ be any field. Then we will use the notation $\mathbf{F}[x]$ for the set of all polynomials $p(x) = a_nx^n + \cdots a_0$ with coefficients $a_k \in \mathbf{F}$. Denote by $\mathbf{F}(x)$ the set of rational functions $p(x)/q(x)$ where $p(x), q(x) \in \mathbf{F}[x]$ are polynomial and $q(x)$ is not the zero polynomial. (It is standard to denote the set polynomials $\mathbf{F}[x]$ with the square bracket and the field of rational functions $\mathbf{F}(x)$ with the round bracket.) If addition and multiplication are defined by the usual rules i.e.

$$\frac{p_1(x)}{q_1(x)} + \frac{p_2(x)}{q_2(x)} = \frac{p_1(x)q_2(x) + p_2(x)q_1(x)}{q_1(x)q_2(x)}, \qquad \frac{p_1(x)}{q_1(x)} \cdot \frac{p_2(x)}{q_2(x)} = \frac{p_1(x)p_2(x)}{q_1(x)q_2(x)}$$

this becomes a field.

Finite fields. These will not come up often, but you should be aware they exist. Moreover in certain parts of mathematics (number theory, combinatorics, finite group theory) they quite important. Here are the basic examples. Let p be a prime number and let $\mathbf{Z}/p$ be the integers reduced modulo p. That is we consider two integers n and m to be "equal" (really congruent modulo p) if and only if they have the same remainder when divided by p in which case we write $m \equiv n \bmod p$. Therefore $m \equiv n \bmod p$ if and only if $m - n$ is evenly divisible by p. It is easy to check that

$$\begin{aligned} m_1 \equiv n_1 \bmod p \qquad &\text{and} \quad m_2 \equiv n_2 \bmod p \quad \text{implies} \\ &m_1 + m_2 \equiv n_1 + n_2 \bmod p \quad \text{and} \quad m_1 m_2 \equiv n_1 n_2 \bmod p. \end{aligned}$$

Then $\mathbf{Z}/p$ is the set of congruence classes modulo p. It only takes a little work to see that with the "obvious" choice of addition and multiplication that $\mathbf{Z}/p$ satisfies all the conditions of a fields except the existence of inverses of elements $n \not\equiv 0 \bmod p$. (In fact this much is true even when p in not prime, finding inverses is the only place where p being prime is used.) Using that p is prime it is possible to show that if $m \not\equiv 0 \bmod p$ that there is a m so that $mn \equiv 0 \bmod p$. (This is not all that hard and you might want to try to show it your self as an exercise.) This is exactly what is needed to show that inverses exist. To make this more concrete we work out the case of $p = 5$ in detail. The possible remainders when a number is divided by 5 are 0, 1, 2, 3, 4. Thus we can use for the elements of $\mathbf{Z}/5$ the set $\{0, 1, 2, 3, 4\}$. Addition works like this. $2 + 4 = 1$ in $\mathbf{Z}/5$ as the remainder of $4 + 2$ when divided by 5 is 1. Likewise $2 \cdot 4 = 3$ in $\mathbf{Z}/5$ as the remainder of $2 \cdot 4$ when divided by 5 is 3. Here are the addition and multiplication tables for $\mathbf{Z}/5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

and in this case one can see directly that each element has an inverse. Note that in this field we have $5 = 0$ which seems rather jarring at first. Finally I remark that there are lots of finite fields that are not of the form $\mathbf{Z}/p$ for any prime p. To give an easy example of this note that my looking at the multiplication table for $\mathbf{Z}/5$ we see that 2 has no square root in $\mathbf{Z}/5$. Therefore we can form a quadratic number field $\mathbf{F} := \{a + b\sqrt{2} : a, b \in \mathbf{Z}/p\}$ just as we did over the the rational numbers above. Then $\mathbf{F}$ is also a finite field and it has 25 elements and is not equal to $\mathbf{Z}/25$.