Chapter 7

Fields

Math 4520, Fall 2017

If there is any lesson that we have learned about geometry in the last five hundred years, it is that it really works best when it is friendly with, and even intimate with, algebra. One of the most productive objects in algebra for geometry is the concept of a field. You have probably seen several fields, perhaps not knowing that they were called fields. For example, the real numbers, the rational numbers, and complex numbers are fields. Roughly speaking, fields are things where you can add, subtract, multiply and divide, but not divide by zero. The ordinary rules of arithmetic apply.

7.1 Definition of a field

Here is a more careful definition of a field. (A good introduction to fields is in Chapter 8 of "A Concrete Introduction to Higher Algebra" by Lindsay N. Childs, which is used in Math 3360.) A Field $\mathbf{F}$ is a set, where, for any two elements $a, b \in \mathbf{F}$, the elements $a + b$ and $a \cdot b = ab$ are also in $\mathbf{F}$. Furthermore, there are two special elements in $0, 1 \in F$, called the additive and multiplicative identities, respectively. Here are the axioms/properties that define a field: Suppose that $a, b, c \in \mathbf{F}$ are any three elements in $\mathbf{F}$.

1.) $0 + a = a + 0 = a$ (0 is the identity for addition.)

2.) $1 \cdot a = a \cdot 1 = a$ (1 is the identity for multiplicaton.)

3.) $(a + b) + c = a + (b + c)$ (Associativity for additon.)

4.) $a + b = b + a$ (Commutativity for addition.)

5.) There is an element $-a$ such that $a + (-a) = 0$ ($-a$ is the additive inverse of a.)

6.) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associativity of multiplication.)

7.) $a \cdot (b + c) = a \cdot b + a \cdot c$ (The distributive law.)

8.) If $a \neq 0$ there is an element $a^{-1} \in \mathbf{F}$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (a^{-1} is the multiplicative inverse of a.)

9.) $a \cdot b = b \cdot a$ (Commutativity of multiplication.)

Yetch! Nine axioms are more than a third of the way toward Hilbert's twenty some axioms for the Euclidean plane. On top of that, there are two points 0 and 1 that are somehow different from the others. How is that like the plane, where all the points look like all the other points? What's geometric about all of this?

Answer Number 1: They have proven their worth over the last one or two hundred years.

Answer Number 2: There are lots of examples, in addition to the real numbers, the rational numbers, and even the complex numbers, and they each have their own special virtues that we have come to appreciate.

Answer Number 3: These properties all correspond to geometric straightedge constructions in a projective plane. You just need a couple extra properties of that projective plane, the Desargues property, or better the Pappus property, and you can create a corresponding field and vice-versa. Section 7.2 shows how addition and multiplication can be defined with a projective plane, and gives a hint about how the algebra can be extracted from the geometry.

7.2 Addition and multiplication with a straightedge

Here we indicate how we can define addition and multiplication in any projective plane. Choose a line, which we call the *x-axis*, in the projective plane. Choose two points on the x-axis, which we call 0 and X_∞, respectively. Choose a line incident to 0, which we call the *y-axis*, not the x-axis. Choose another point Y_∞ on the y-axis. Call the line incident to X_∞ and Y_∞ the *line at infinity.* Let L be another line that is incident to X_∞ not the x-axis and not the line at infinity. We simply take L to be the line $y = 1$ in the Euclidean representation.

Notice that this terminology is meant to be similar to the points and lines that we defined for the extended Euclidean plane. But these definitions work in any projective plane. We will define the "field" **F** to be the x-axis minus X_∞. So we choose two points a and b in **F** in the x-axis. We will show how to add and multiply these two points to get $a + b$ and ab. Figure 7.1 shows how addition is defined in the Euclidean plane, where coordinates are used to show what is going on, but again all the constructions work in any projective plane. Verifying the axioms for a field are another matter.

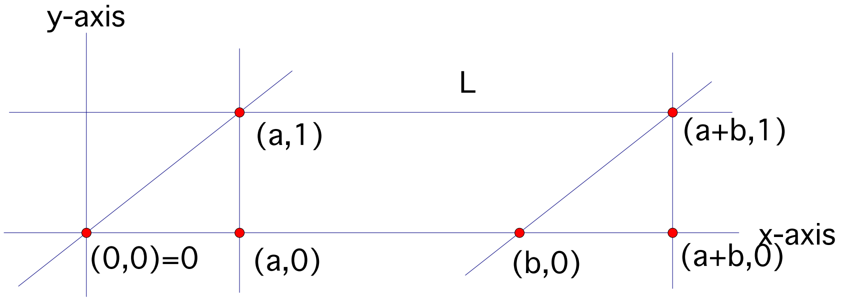

Figure 7.1

The construction goes as follows: From Y_∞ project a $(= (a, 0)$ in the Figure) into $(a, 1)$ in the line L, which we are taking to be the line $y = 1$ in the Figure. The line incident to 0 and $(a, 1)$ is incident to the line at infinity at the point say $P(a)$. From $P(a)$ project the point b $(= (b, 0)$ in the Figure) to the point $(a + b, 1)$ in L. Then from Y_∞, again, project $(a + b, 1)$ back to the x-axis. This is the point designated at the sum $a + b$ in $\mathbf{F}$.

For multiplication we describe a similar construction. Start with the x-axis, y-axis, an "origin" 0, X_∞, and Y_∞ as before. We must also choose a point on $\mathbf{F}$ that will play the role of 1, the additive identity, which in coordinates is $(1, 0)$. It also helps to choose another point on the y-axis, not 0 and not Y_∞ which we call $(0, 1)$. Call the point on the line at infinity (the line incident to X_∞ and Y_∞), incident to the line through $(0, 1)$ and $(1, 0)$, $P(45°)$. From $P(45°)$ project a $(= (a, 0)$) to $(0, a)$ on the y-axis. From X_∞ project $(0, a)$ onto $(1, a)$ on the line through $(1, 0)$ and Y_∞. From Y_∞ project b $(= (b, 0)$) onto (b, ab) on the line through 0 and $(1, a)$. From X_∞ project (b, ab) onto $(0, ab)$ in the y-axis. From $P(45°)$ project $(0, ab)$ onto ab $(= (ab, 0))$ in the x-axis. This is the definition of the product ab. Figure 7.2 shows this.

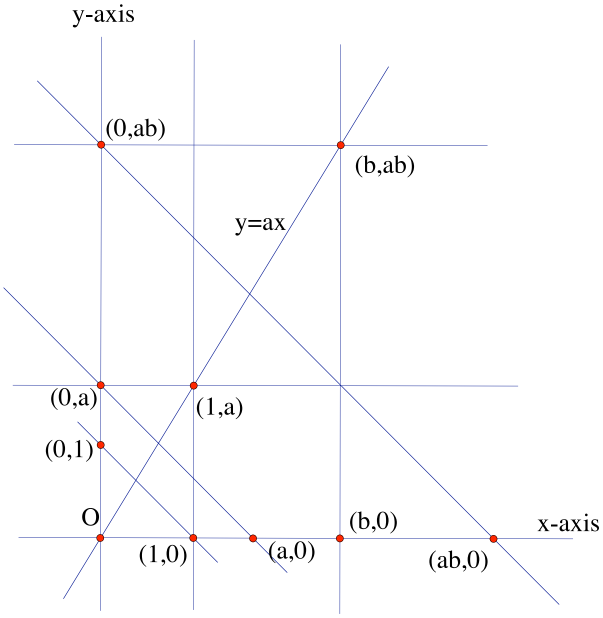

Figure 7.2

Theorem 7.2.1. *If a projective plane is such that the Desargues property holds, then the addition and multiplication operations defined above on the set* $\mathbf{F}$ *have properties* $(1), \ldots, (8)$. *If, instead, the Pappus property holds, then all nine properties for a field hold and* $\mathbf{F}$ *is field.*

A proof of Theorem 7.2.1 can be found in the book "A Modern View of Geometry" by Leonard M. Blumenthal. If a set $\mathbf{F}$ has an addition and multiplication defined where properties $(1), \ldots, (8)$ hold but not the multiplicative commutativity property (9), then $\mathbf{F}$ is called a *skew field* or a *division algebra*. An example of such a skew field will be given in Section 7.4.

We next present here some examples of fields, which can be used construct a corresponding projective plane later.

7.3 The complex numbers

The following is a way of defining the complex numbers

$$\mathbf{C} = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \text{ real} \right\},$$

where $\mathbf{C}$ is regarded as a subset of the set of real two by two matrices. Let

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + y \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and

$$i^2 = -I.$$

Thus using the usual rules for matrix multiplication and addition, we see that $\mathbf{C}$ is closed under addition, subtraction, and matrix multiplication. Furthermore, by the associativity of matrix multiplication, we see that multiplication is associative. Since the generators I and i commute, multiplication is commutative as well. We take the determinant of the matrix in $\mathbf{C}$ to get

$$\det \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x^2 + y^2.$$

Thus every non-zero element of $\mathbf{C}$ has a multiplicative inverse which is again in $\mathbf{C}$. Explicitly,

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}^{-1} = \frac{1}{x^2 + y^2} \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

It is easy to check the other axioms of a field, and we can see that this is just another way to think of the complex numbers, where

$$x + yi = xI + yi.$$

We can also continue and define complex conjugation in $\mathbf{C}$. Namely, if $z = x + yi$, then define $\bar{z} = x - yi$, called the *conjugate of z*. We see that the conjugate is just the transpose operation, when we think of complex numbers as matrices. The following are some basic easily verifiable properties for complex conjugation. Let z and w be complex numbers.

1.) $\overline{z + w} = \bar{z} + \bar{w}$

2.) $\overline{(xw)} = \bar{z}\bar{w}$

3.) $z\bar{z} \geq 0$, and $z\bar{z} = 0$ if and only if $z = 0$

4.) $\bar{\bar{z}} = z$.

7.4 The quaternions

We now extend what was done in Section 7.3. We start with **C** instead of **R** the reals. We will end up defining the quaternions **H**. Let

$$\mathbf{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \text{ in } \mathbf{C} \right\}.$$

It is clear when we take determinants that

$$\det \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} = z\bar{z} + w\bar{w} \geq 0.$$

Using property (3), this shows that every element of H is invertible except the matrix of all 0's, which is the zero element of the skew field H. We make the following identifications:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Thus every element of H is a real linear combination of the four matrices above. It is easy to check that H is closed under addition, subtraction, multiplication, and taking inverses of non-zero elements. Associativity of multiplication follows from the associativity of multiplication for matrices. Thus H satisfies all the axioms of a field except possibly commutativity of multiplication. However, we see that $ij = k$ and $ji = -k$. So H is definitely a *non-commutative* field or a *skew field*.

7.5 Finite fields

Let p be any prime integer, $p = 2, 3, 5, 7, 11, 13, \ldots$. We define an equivalence relation on the set of all integers by saying that the integers n and m are equivalent (where we write $n \equiv m \pmod{p}$) if $n - m$ is exactly divisible by p. We say n is congruent to m modulo p. Let $[n]$ represent the unique equivalence class containing n. It is easy to see that [0], [1], [2],. . . , $[p-1]$ represents all the equivalence classes for our equivalence relation. We denote the set of these equivalence classes by $\mathbf{Z}_p$. We define addition and multiplication of these equivalence classes in the following natural way:

$$[n] + [m] = [n + m]$$
$$[n][m] = [nm],$$

where n and m are integers. Of course, we must check that the above definition is "well-defined." In other words, we must check that it does not matter which representative of the equivalence class is chosen to define the addition and multiplication. The same equivalence class for the sum or product will be defined independent of the representatives chosen.

It is clear that the additive identity is $0 = [0]$, and the multiplicative identity is $1 = [1]$. It is easy to check that all the axioms of a field hold for $\mathbf{Z}_p$, except possibly for the existence of multiplicative inverses for non-zero elements. But recalling the Euclidean algorithm, we see that if the prime p does not divide the integer n, then there are integers a and b such that $na + pb = 1$. So $[n][a] = [1]$ in $\mathbf{Z}_p$, and $[a]$ is the multiplicative inverse for $[n]$. Thus $\mathbf{Z}_p$ is a field for any prime p.

7.6 More finite fields

There are more finite fields in addition to $\mathbf{Z}_p$. Let $q = p^n$, where p is a prime and n is a positive integer. We will sketch how to construct a finite field $\mathbf{F}_q$ with q elements. To demonstrate the idea we show how to define the finite field $\mathbf{F}_4$.

Start with $\mathbf{Z}_2$. Consider the polynomial $p_0(x) \equiv x^2 + x + 1$. We regard $p_0(x)$ as an abstract form, not necessarily as a function. If we did regard $p_0(x)$ as a function, then $p_0(0) = p_0(1) = 1$. But we do not regard our $p_0(x)$ as the same as the constant polynomial 1. When we add and multiply such polynomial forms we do this with the usual rules of such arithmetic. Note that our form $p_0(x)$ is *irreducible* in the sense that it cannot be written as the product of polynomial forms of lower degree, which in the case of $p_0(x)$ must be forms of degree 1. The *degree* of a polynomial form is the largest exponent of x that appears with a non-zero coefficient.

Let $\mathbf{Z}_2[x]$ be the collection of all such polynomial forms with coefficients in $\mathbf{Z}_2$. One can add, subtract, multiply, but not divide these polynomial forms in $\mathbf{Z}[x]$, so they are not quite a field. (They are called a *ring* though.). However, $\mathbf{Z}_2[x]$ will play a role similar to the role played by the integers in the construction of the field $\mathbf{Z}_p$. We define the following equivalence relation in $\mathbf{Z}_2[x]$. We say that $p(x)$ is equivalent to $q(x)$ if the polynomial form $p(x) - q(x)$ is exactly divisible by $p_0(x)$. We write this as $p(x) \equiv q(x) \pmod{p_0(x)}$. It is easy to check that this is indeed an equivalence relation. We define $\mathbf{F}_4$ as the set of these equivalence classes.

We define addition and multiplication in $\mathbf{F}_4$ in the following natural way.

$$[p(x)] + [q(x)] = [p(x) + q(x)]$$

$$[p(x)][q(x)] = [p(x)q(x)],$$

which is easily seen to be well-defined. Note that if $p(x)$ has degree greater than one, then we can divide $p(x)$ by $p_0(x)$ and get a remainder $r(x)$, whose degree is 0 or 1. In other words,

$$p(x) = q(x)p_0(x) + r(x),$$

for some polynomial form $q(x)$. So $[p(x)] = [r(x)]$, and each equivalence class has a representative of degree 0 or 1. So the following represent the four elements of $\mathbf{F}_4$

$$[0], \quad [1], \quad [x], \quad [x+1].$$

Addition and multiplication is now easy to work out. For example,

$$[x] + [x+1] = [x + x + 1] = [1] \quad \text{and} \quad [x][x+1] = [x^2 + x] = [1].$$

It is easy to check that the axioms of a field hold for $\mathbf{F}_4$. The zero element, the additive identity, is $[0]$, and the multiplicative identity is $[1]$, of course. The only part that might cause difficulty is how to find multiplicative inverses. But $p_0(x)$, since it is irreducible, behaves like the prime p in the construction of $\mathbf{Z}_p$. The Euclidean algorithm still works for polynomial forms (in one variable), and we can repeat the same argument to find inverses.

It turns out that the above method can be generalized to give a finite field with $q = p^n$ elements for any prime p and any positive integer n. The only difficulty is to find an irreducible polynomial form that plays the role of $p_0(x)$. In any case, we state, without proof, the following very basic algebraic theorem.

Theorem 7.6.1 (Wedderburn)**.** *For every $q = p^n$, where p is a prime number and n is a positive integer, there is a finite field $\mathbf{F}_q$ with q elements. Furthermore, if $\mathbf{F}$ is any other finite field (even possibly non-commutative), then $\mathbf{F}$ must have q elements, where $q = p^n$, p is a prime number and n is a positive integer, and $\mathbf{F}$ is isomorphic to $\mathbf{F}_q$.*

We say that a field $\mathbf{F}$ is *isomorphic* to a field $\mathbf{F}'$ if there is a one-to-one onto correspondence $f : \mathbf{F} \to \mathbf{F}'$ such that for every x, y in $\mathbf{F}$

$$\begin{aligned} f(x+y) &= f(x) + f(y) \quad \text{and} \\ f(xy) &= f(x)f(y). \end{aligned}$$

It turns out that Wedderburn's Theorem has an equivalent formulation in terms of finite projective planes. However, there is no known proof that uses a purely geometric approach. All known proofs use the algebraic structure only.

7.7 Exercises:

1. Find a projective construction for finding a^{-1}, when $a \neq 0$, similar to the constructions for defining addition multiplication in Section 7.2.

2. Find an explicit expression for the inverse of a quaternion and show that it is again a quaternion.

3. Construct the multiplication table for $\mathbf{F}_4$.

4. Without appealing to Wedderburn's Theorem, show directly that any finite commutative field must have p^n elements, where p is a prime number and n is a positive integer. (Hint: Use linear algebra over the field.)

5. If x is in $\mathbf{F}_q$ a finite field, show that $x^q = x$.

6. The following subset $\mathbb{Q}(\sqrt{2})$ of the real numbers is a field. Write down the inverse of a non-zero element of $\mathbb{Q}(\sqrt{2})$ and show that it lies in $\mathbb{Q}(\sqrt{2})$.

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a \text{ and } b \text{ are rational numbers}\}.$$

7. Find an irreducible polynomial in the field with 4 elements.