

CLASSICAL GEOMETRIES

8. Some examples of fields

We have seen the definition of a field. We present here some examples of fields that are useful for our geometric point of view.

8.1 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

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

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

$$i^2 = -I.$$

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. Since we take the determinant of a matrix in \mathbf{C} we have

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

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* . The following are some basic easily verifiable properties for complex conjugation. Let z and w be complex numbers.

- a. $\overline{z + w} = \bar{z} + \bar{w}$
- b. $\overline{(zw)} = \bar{z}\bar{w}$
- c. $z\bar{z} \geq 0$, and $z\bar{z} = 0$ if and only if $z = 0$
- d. $\overline{\bar{z}} = z$.

8.2 The quaternions

We now extend what was done in Section 8.1. We start with \mathbf{C} instead of \mathbf{R} the reals. We will end up defining the quaternions \mathbf{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 c, this shows that every element of H is invertible except the matrix of all 0's, which is the zero element of the 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*.

8.3 Finite fields

Let p be any prime integer, $p = 2, 3, 5, 7, 11, 13, \dots$. 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 $[0]$,

$[1], [2], \dots, [p-1]$ 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 .

8.4 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 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 .

$$\begin{array}{cc} [0] & [1] \\ [x] & [x + 1] \end{array}$$

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 the 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 (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 $f : \mathbf{F} \rightarrow \mathbf{F}'$ such that for every x, y in \mathbf{F}

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

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.

Exercises:

1. Find an explicit expression for the inverse of a quaternion and show that it is again a quaternion.
2. Construct \mathbf{F}_8 and \mathbf{F}_9 .
3. 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.
4. If x is in \mathbf{F}_q a finite field, show that $x^q = x$.
5. Show that the following subset of the real numbers is a field:

$$\{a + b\sqrt{2} \mid a \text{ and } b \text{ are rational numbers}\}.$$