Math 112 lecture for Friday, Week 4

Field axioms

(Supplemental reading: Example 2.6 in Swanson.)

Our next goal is to make a short, complete list of the rules characterizing the real numbers. Anything that can be said about the real numbers will follow from these rules, and, roughly, the real numbers is the only object that satisfies these rules. There will be three parts: (i) the nine field axioms, (ii) the four order axioms, and (iii) the completeness axiom. For right now, we will concentrate on the field axioms.

Definition. A *field* is a set F with two operations[1]:

$$+ : F \times F \to F \text{ (addition)} \quad \text{and} \quad \cdot : F \times F \to F \text{ (multiplication)},$$

satisfying the following axioms:

A1. Addition is *commutative*. For all $x, y \in F$,

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

A2. Addition is *associative*. For all $x, y, z \in F$,

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

A3. There is an *additive identity*. There is an element of F, usually denoted 0, such that for all $x \in F$,

$$x + 0 = x.$$

A4. There are *additive inverses*. For all $x \in F$, there is an element $y \in F$ such that

$$x + y = 0.$$

The element y is denoted $-x$. Thus,$-x$ *is the element of* F *which when added to* x *yields* 0. (*Subtraction* is then defined by $x - y := x + (-y)$ for all $x, y \in F$.)

M1. Multiplication is *commutative*. For all $x, y \in F$,

$$xy = yx.$$

[1]In this context, "operation" is just another word for "function". Our functions take an ordered pair of elements of F and return another element of F.

M2. Multiplication is *associative*. For all $x, y, z \in F$,

$$(xy)z = x(yz).$$

M3. There is a *multiplicative identity*. There is an element, usually denoted 1, such that:

(a) $1 \neq 0$, and

(b) $1x = x$ for all $x \in F$.

M4. There are *multiplicative inverses*. For each *nonzero* $x \in F$, there is a $y \in F$ such that

$$xy = 1.$$

The element y is denoted $1/x$ or x^{-1}. Thus, $1/x$ *is the element of* F *which when multiplied by* x *yields* 1. (*Division* is then defined by $x/y := xy^{-1}$ for nonzero y.)

D. Multiplication *distributes* over addition. For all $x, y, z \in F$,

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

Thus, there are four field axioms governing addition, four governing multiplication, and one dictating how addition and multiplication interact.

Remark. The axioms for addition and multiplication are quite similar. Here are two subtle things to notice, however: (i) by definition, the additive and multiplicative identities are not equal ($0 \neq 1$), and (ii) only *nonzero* elements of a field are required to have multiplicative inverses.

Examples. The examples of fields with which you are most familiar are the rationals, $\mathbb{Q}$, and the reals, $\mathbb{R}$. Later in this course, we will consider the field of complex numbers, $\mathbb{C}$. It turns out that $\mathbb{Z}/n\mathbb{Z}$, with the addition and multiplication we defined earlier, is a field if and only if n is a prime number.[2] The only axiom that is not satisfied by $\mathbb{Z}/n\mathbb{Z}$ for general n is the existence of multiplicative inverses for nonzero elements (M4).

[2]Indeed, although $\mathbb{Z}/n\mathbb{Z}$ has many uses, the only two reasons it was introduced in this course is to help with the understanding of equivalence relations and field axioms.

Consider the addition and multiplication tables for $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$ (where we write k instead of $[k]$ for each equivalence class):

$\mathbb{Z}/5\mathbb{Z}$

$+$	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

$\mathbb{Z}/6\mathbb{Z}$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	5	2	0	4	2
5	0	5	4	3	2	1

.

The additive identity for $\mathbb{Z}/5\mathbb{Z}$ is $[0]$. Note that axiom A3 says the identity is usually denoted 0, and we will often do that in the case of $\mathbb{Z}/n\mathbb{Z}$, but note that in the case of $\mathbb{Z}/5\mathbb{Z}$, for instance, 0 is really $[0] = \{\dots, -10, -5, 0, 5, 10, \dots\}$. The additive identity for $\mathbb{Z}/6\mathbb{Z}$ is $[0] = \{\dots, -12, -6, 0, 6, 12, \dots\}$, again, an infinite set.

Commutativity of addition and multiplication for $\mathbb{Z}/n\mathbb{Z}$ can seen in the above examples via the symmetry of the addition and multiplication tables about the northwest-to-southeast diagonal.

Here is an **important point**: if x is an element of a field, then $-x$ is *defined* to be the additive inverse of x, i.e., the field element which when added to x gives the additive identity, 0. Similarly, if x is nonzero, then $1/x$ is *defined* to be the multiplicative inverse of x, i.e., the field element which when multiplied by x gives the multiplicative identity 1. For instance, since $[2][3] = [1]$ in $\mathbb{Z}/5\mathbb{Z}$, we have that

$$\frac{1}{[2]} = [3] \quad \text{and} \quad \frac{1}{[3]} = [2].$$

If we know that we are working in $\mathbb{Z}/5\mathbb{Z}$, we might abbreviate these to $1/2 = 3$ and $1/3 = 2$.

Note that every nonzero element of $\mathbb{Z}/5\mathbb{Z}$ has a multiplicative inverse. (It turns out that $\mathbb{Z}/5\mathbb{Z}$ satisfies all of the field axioms.) On the other hand, the only nonzero elements of $\mathbb{Z}/6\mathbb{Z}$ with multiplicative inverses are 1 and 5. You can see this in the

multiplication table, above: only the columns for 1 and 5 contain 1s. (In general, the nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ with multiplicative inverses turn out to be $[k]$ such that k and n share no prime factors in common.)

A final fun fact: the smallest field is $\mathbb{Z}/2\mathbb{Z}$. Every field needs an additive identity, 0 and a distinct multiplicative identity 1, and $\mathbb{Z}/2\mathbb{Z}$ has no elements besides these.

Non-examples.

- The set of natural numbers, $\mathbb{N} = \{0, 1, 2, \dots\}$ with its usual addition and multiplication does not form a field. It violates axioms A4 and M4 (the existence of additive and multiplicative inverses). For instance, no natural number besides 0 has an additive inverse (0 is its own additive inverse), and no natural number besides 1 has a multiplicative inverse.
- The set of integers, $\mathbb{Z}$, satisfies all of the axioms except M4: no integers besides ± 1 have multiplicative inverses.
- Consider the set $X := \mathbb{R} \setminus \mathbb{Q}$ with ordinary addition and multiplication. Then X is not a field. For instance, it does not have an additive or a multiplicative identity since both 0 and 1 are elements of $\mathbb{Q}$. There is another serious problem. Consider the elements $\pm\sqrt{2} \in X$. We have $-\sqrt{2} + \sqrt{2} = 0 \notin X$. So addition is not defined for X (recall that addition for X would be a function $X \times X \to X$, so the result of the sum of two elements of X must be an element of X).

As said earlier, everything that can be known about the real numbers follows from the fact that the reals satisfy the field axioms (along with the order axioms and the completeness axiom, which we will examine later). For instance, we all know that if x is a real number then $x \cdot 0 = 0$. But why is that? Can you prove it? Note that it is not one of the field axioms. The following proposition shows that this result holds in any field (including, for example, $\mathbb{Z}/5\mathbb{Z}$). One may think of this as a game: the nine field axioms are the rules, and you need to use them to show $x \cdot 0 = 0$. It is surprisingly tricky (see the first displayed line of the proof—how could one know that's a reasonable first step?)!

Proposition. Let F be a field, and let $x \in F$. Then $x \cdot 0 = 0$.

Proof. We have

$$\begin{aligned} x \cdot 0 &= x(0 + 0) && \text{(since 0 is the additive identity)} \\ &= x \cdot 0 + x \cdot 0 && \text{(distributivity).} \end{aligned}$$

Since F is a field, we know $x \cdot 0 \in F$ and hence has an additive inverse $-(x \cdot 0)$. Continuing from above,

$$
\begin{aligned}
& x \cdot 0 = x \cdot 0 + x \cdot 0 \\
\Rightarrow \quad & -(x \cdot 0) + x \cdot 0 = -(x \cdot 0) + (x \cdot 0 + x \cdot 0) && \\
\Rightarrow \quad & 0 = -(x \cdot 0) + (x \cdot 0 + x \cdot 0) && \text{(definition of additive inverse)} \\
\Rightarrow \quad & 0 = (-(x \cdot 0) + x \cdot 0) + x \cdot 0 && \text{(associativity of addition)} \\
\Rightarrow \quad & 0 = 0 + x \cdot 0 && \text{(definition of additive inverse)} \\
\Rightarrow \quad & 0 = x \cdot 0 && \text{(0 is the additive identity).}
\end{aligned}
$$

□