Math 112 lecture for Monday, Week 4

FIELD AXIOMS

Our next goal is to make a short complete list of the rules governing real numbers. There will be three parts: (i) nine field axioms, (ii) four order axioms, and (iii) the completeness axiom.

Read our handout on the complete ordered field axioms. Some examples of fields are the real numbers, $\mathbb{R}$, the rational numbers, $\mathbb{Q}$, and the complex numbers, $\mathbb{C}$.

Examples of non-fields.

1. The natural numbers, $\mathbb{N} := \{0, 1, 2, \dots\}$ do not form a field. For instance, 1 has no additive inverse in $\mathbb{N}$. The number 2 has no multiplicative inverse in $\mathbb{N}$.

2. The integers, $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$, do not form a field. For instance, 2 has no multiplicative inverse in $\mathbb{Z}$.

3. $X := \mathbb{R} \setminus \mathbb{Q}$ is not a field. For instance, it do not contain 0. Even more fundamentally, we have π and $1/2 - \pi$ are in X, but $\pi + (1/2 - \pi) = 1/2$ is not. So we do not have an addition function $+ \colon X \times X \to X$. Similarly, $\sqrt{2} \in X$, but $\sqrt{2} \cdot \sqrt{2} = 2 \notin X$.

Fix $n \in \mathbb{Z}$, and recall $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n. Its elements are the equivalence classes for the equivalence relation $a \sim b$ if $a - b = kn$ for some $k \in \mathbb{Z}$. If $a \sim b$, we write $a = b \bmod n$. For example $2 = 12 \bmod 5$.

By elementary number theory, there are exactly n equivalence classes

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}.$$

(Each integer a has a unique remainder $r \in \{0, 1, \dots, n-1\}$ upon divison by n. Then $a = r + kn$, and $[a] = [r]$.)

It turns out (and we'll prove this below) that addition and multiplication of integers play very nicely with respect to this equivalence relation. To see an example of this, let's take $n = 5$. Then

$$2 + 4 = 1 \bmod 5 \quad \text{and} \quad 2 \cdot 4 = 3 \bmod 5.$$

Next we pick some random integers equivalent to 2 and 4 modulo 5. We have, for instance, $2 = 12 \bmod 5$ and $4 = 119 \bmod 5$. We find

$$12 + 119 = 131 = 1 \bmod 5 \quad \text{and} \quad 12 \cdot 119 = 1428 = 3 \bmod 5.$$

In other words, it doesn't matter which representatives we pick for equivalences classes when doing arithmetic modulo n. Here is another example: it turns out that $6^8 = 1 \bmod 5$. There are two ways to see this—one much harder than the other. The first way would be to multiply 6 by itself 8 times to find

$$6^{1234} = 1679616 = 1 \bmod 5.$$

The other is to first note that $6 = 1 \bmod 5$, and use the fact that multiplication "plays well" with equivalence modulo 5:

$$6^8 = 1^8 = 1 \bmod 5.$$

So, in fact, $6^{5439214392} = 1 \bmod 5$, too. Here is a similar example: since $4 = -1 \bmod 5$, we have

$$4^{1234567} = (-1)^{1234567} = -1 = 4 \bmod 5,$$

and

$$4^{1234568} = (-1)^{1234568} = 1 \bmod 5,$$

We now define addition and multiplication for $\mathbb{Z}/n\mathbb{Z}$.

Definition. For each $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, define

$$[a] + [b] := [a + b] \quad \text{and} \quad [a][b] = [ab].$$

The first thing to notice in the expression $[a] + [b] = [a + b]$ is that the $+$ on the left-hand side and the $+$ on the right-hand side are different. The $+$ on the right-hand side is ordinary addition of integers. The $+$ on the left-hand side is a new operation: it defines how to add not integers but equivalence classes of integers. The meaning of the $+$ on the left-hand side is a new thing which we are just now defining. It says this: to add two equivalence classes: (i) choose any representative integers for those classes, say a and b, (ii) add the representatives as integers, $a + b \in \mathbb{Z}$, and then (iii) take the equivalence class of the result, $[a + b]$. Similar remarks hold for multiplication.

Since addition and multiplication depend on the representative a and b that we choose for the equivalence classes, we need to make sure that the resulting sum $[a + b]$ does not depend on that choice. For instance, in $\mathbb{Z}/5\mathbb{Z}$, we have

$$[2] + [4] := [6] = [1].$$

On the other hand, since

$$[2] = [12] \quad \text{and} \quad [4] = [119],$$

we need

$$[2] + [4] = [12] + [119].$$

In fact, we're OK since

$$[12] + [119] := [12 + 119] = [131] = [1] = [6] =: [2] + [4]$$

in $\mathbb{Z}/5\mathbb{Z}$. Next time, we will show that addition an multiplication in $\mathbb{Z}/n\mathbb{Z}$ is well-defined (i.e., doesn't dependent on the choice of representatives) in general.