Abstract Fields

The computational and conceptual questions in the prior handout help us recall the following important culminating theorem.

Theorem 1. *$\mathbb{Z}_n$ with $+_n$ and $\cdot_n$ satisfies all twelve algebraic axioms if and only if $n \geq 2$ is a prime integer. Namely, every number in $\mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $n \geq 2$ is a prime integer.*

This means that $\mathbb{Z}_n$ satisfies all of the same algebraic axioms as $\mathbb{R}$ whenever $n \geq 2$ is prime. This encourages us to truly consider $\mathbb{Z}_n$ (for $n \geq 2$ prime) to be its own "number system". Of course, mathematicians have their own special name for this situation.

Definition 1. *Let $\mathbb{F}$ be any set of objects. Suppose we can add and multiply together the objects in $\mathbb{F}$, meaning there are binary operations $+$ and $\cdot$ on $\mathbb{F}$. If $\mathbb{F}$ with $+$ and $\cdot$ satisfies all twelve algebraic axioms, we call $\mathbb{F}$ a field.*

We usually call the additive identity of $\mathbb{F}$ zero and write $0_{\mathbb{F}}$ or 0 when the context is clear. Similarly, we usually call the multiplicative identity of $\mathbb{F}$ one and write $1_{\mathbb{F}}$ or 1 when the context is clear.

For x in $\mathbb{F}$, we usually write the additive inverse of x as $-x$. If $x \neq 0_{\mathbb{F}}$, we usually write the multiplicative inverse of x as x^{-1}.

Problem 1. *Rewrite Theorem 1 using the word "field".*

Problem 2. *Which of the types of numbers on the real number line are a field? Recall we discussed the naturals $\mathbb{N}$, the wholes $\mathbb{W}$, the integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, and the reals $\mathbb{R}$.*

Problem 3 (Extra Credit Challenge!). *You may recall our in-class discussion of the complex numbers $\mathbb{C}$ and quaternions $\mathbb{H}$. Only one of these two types of numbers is a field. Which one is not a field and which algebraic axiom does it not satisfy?*

The algebraic structure of fields is very strong. We can actually prove many facts about fields simply because of the algebraic axioms! Consider the following examples where $\mathbb{F}$ is a field with addition $+$ and multiplication $\cdot$. These rules should seem very familiar from the real numbers, although we will leave the proofs as completely optional extra credit challenges.

Example 1 (Cancellation laws). *Let x, y, z be in $\mathbb{F}$. If $x + y = x + z$, then $y = z$. Also, if $x \cdot y = x \cdot z$ and $x \neq 0_{\mathbb{F}}$, then $y = z$.*

Example 2 (Uniqueness of identity). *There is exactly one additive identity and exactly one multiplicative identity in $\mathbb{F}$.*

Example 3 (Uniqueness of inverses). *Let x be in $\mathbb{F}$. Then x has exactly one additive inverse which is equal to $-1 \cdot x$. If $x \neq 0_{\mathbb{F}}$, then x has exactly one multiplicative inverse.*

Example 4 (Multiplying by zero). $0_{\mathbb{F}}$ *does not have a multiplicative inverse since $0_{\mathbb{F}} \cdot x = 0_{\mathbb{F}}$ for all x in $\mathbb{F}$.*

Problem 4 (Super Extra Credit Challenge!). *Complete the following parts.*

(i) *Prove Example 1. Note that it is circular reasoning to just cancel out the left and right terms. Instead, try to use previous axioms and identities.*

This problem continues to the next page.

This is a continuation of the problem on the prior page.

(ii) *Prove Example 2. Remember that the two identity axioms for fields tell us that there is at least one additive identity and multiplicative identity, but it's actually true that there must be exactly one of each. Hint: use part (i) of this problem.*

(iii) *Prove Example 3. Remember that the two inverse axioms for fields tell us that there is at least one additive inverse for x in $\mathbb{F}$ and at least one multiplicative inverse for non-zero x in $\mathbb{F}$. It's actually true that there must be exactly one of each inverse. Hint: use part (i) of this problem.*

(iii) *Prove Example 4. You only need to show that $0_{\mathbb{F}} \cdot x = 0_{\mathbb{F}}$ for all x in $\mathbb{F}$. Hint: use part (i) of this problem.*