Math From Scratch Lesson 23: The Field Axioms

W. Blaine Dowler

April 27, 2012

Contents

1 Recap

In previous lessons, we established the axioms of an algebraic ring. They are as follows:

1. **Closure under +:** $a + b \in R \; \forall a, b \in R$.
2. **Closure under $\cdot$:** $a \cdot b \in R \; \forall a, b \in R$.
3. **Commutativity under +:** $a + b = b + a \; \forall a, b \in R$
4. **Associativity under +:** $(a + b) + c = a + (b + c) \; \forall a, b, c \in R$.
5. **Associativity under $\cdot$:** $(a \cdot b) \cdot c = a \cdot (b \cdot c) \; \forall a, b, c \in R$.
6. **Identity for +:** $0 \in R$, and $a + 0 = a \; \forall a \in R$
7. **Identity for $\cdot$:** $1 \in R$, and $a \cdot 1 = a \; \forall a \in R$
8. **Inverses under +:** $\exists(-a)$ such that $a + (-a) = 0 \; \forall a \in R$. Subtraction is defined as $a + (-b) = a - b$.

9. **Distributive Property:** $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ $\forall a, b, c \in R$.

With two additions, we can create an algebraic field.

2 Our First New Axiom: The "Missing" Axiom Found

With the exception of the distributive property, each axiom deals with one operation or another. Also, every multiplication axiom to date has a similar addition axiom. There are two addition axioms which do not have matching multiplication axioms. Here, we introduce the first.

Commutativity under $\cdot$: $a \cdot b = b \cdot a$ $\forall a, b \in R$

With the "repeated addition" definition of multiplication we are accustomed to, this is a very natural axiom to include, and will not receive additional explanation.

3 Multiplicative Inverses

Our instinct to create a matching axiom for multiplicative inverses is doomed to failure. We must, however, see why it fails to prove that it does fail. We start as follows:

Inverses under $\cdot$ **(broken version):** $\exists a^{-1}$ such that $a \cdot a^{-1} = 1$ $\forall a \in R$. Division is defined as $a \cdot b^{-1} = a \div b$.

Let us explore this axiom.

The axioms of a ring ensure that $0 \cdot x = 0$ and $0 \cdot y = 0$ regardless of x and y. This means that

$$0 \cdot x = 0 \cdot y$$

as well. Now, what if the element 0 has an inverse? Then we get a logical inconsistency. Observe:

$$\begin{aligned} 0^{-1} \cdot 0 \cdot x &= 0^{-1} \cdot 0 \cdot y \\ 1 \cdot x &= 1 \cdot y \\ x &= y \end{aligned}$$

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Table 1: The multiplication table for $\mathbb{Z}_3$.

We did not require that $x = y$. We can find explicit, concrete examples where this is not the case, and yet the initial statement $0 \cdot x = 0 \cdot y$ is absolutely correct. The logical flaw is the existence of 0^{-1}. Let us drop the exponent to make this more obvious: let $a = 0^{-1}$. In that case, we have $a \cdot 0 = 1$ when we already know that $a \cdot 0 = 0$ regardless of a. Therefore, we cannot have the axiom in the form it was written. We modify it as follows:

Inverses under $\cdot$ (corrected version): $\exists a^{-1}$ such that $a \cdot a^{-1} = 1$ $\forall a \neq 0 \in R$. Division is defined as $a \cdot b^{-1} = a \div b$.

This now removes the only exception to the multiplicative rule. Going back to the axioms, if we did not already have a context for the symbols $0, 1, +$, and $\cdot$ then we would be unable to distinguish the axioms. It is this exception that formally distinguishes addition from multiplication and 0 from 1.

4 Example: Back To Modular Arithmetic

In our first volume, we looked at modular arithmetic. For example, $\mathbb{Z}_n$ means we look at the integers, but we truncate them as the remainder received when divided by n. For certain values of n, we produce algebraic fields. Let us prove that with a concrete example: $n = 3$. We have already seen that this is a ring, but need to verify that it is a field by testing the two new axioms. Examining the multiplication table will establish this; see table 1.

This table is symmetric about the diagonal running from the upper left corner to the lower right. This verifies the commutativity axiom: $x \cdot y = y \cdot x$. We can also see that every *nonzero* element has an inverse: each nonzero element's row or column contains a product of 1. This is a field. Let us now examine the multiplication table for $\mathbb{Z}_6$ as seen in table 2 on the next page.

This still is commutative: the symmetry about the main diagonal is there. There are, however, elements that do not have inverses. In fact, neither 2, 3 nor 4 have inverses. 1 does, but 1 always will as $1 \cdot 1 = 1$ in any ring, and therefore in any field. 5 serves as its own inverse.

·	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	4	2	0	4	2
5	0	5	4	3	2	1

Table 2: The multiplication table for $\mathbb{Z}_6$.

So, why is $\mathbb{Z}_n$ a field for some values of n and not others?

Let us look at this on a per element basis. If x has no inverse in $\mathbb{Z}_n$, then there are some values of $y \in \mathbb{Z}_n$ and $k \in \mathbb{Z}$ such that

$$x \cdot y = k \cdot n$$

The value of k is completely arbitrary. This is only true if $x \cdot y$ is a multiple of n. Now, if $\gcd(x, n) = 1$, then we could use the mechanisms of the Euclidean Algorithm and linear Diophantine equations to find $x \cdot m = 1 \, (mod \; n)$. Thus, $\gcd(x, n) \neq 1$. In other words, if x and n are not coprime, x cannot have an inverse. As *every* possible x must satisfy this condition for $\mathbb{Z}_n$ to be a field, then the only possible options for fields are those for which n is prime. This is a necessary condition, but is it a sufficient condition? Can you have a prime number p such that $\mathbb{Z}_p$ is not a field?

For that to happen, we must have $x, y \in \mathbb{Z}_p$ such that $x \cdot y = k \cdot p$. This is impossible: both x and y are less than p, and by the definition of prime numbers, $\gcd(x, p) = 1$ and $\gcd(y, p) = 1$. There is no value of k that satisfies this relation, as $(x \cdot y) \div p$ would need to have zero remainder, and that is impossible as neither x nor y nor their combination has a factor of p with which to apply the Fundamental Theorem of Arithmetic. Thus, for all cases, $\mathbb{Z}_p$ is a field.

5 Next Lesson

Our next lesson applies these axioms to create a new set of numbers: the rational numbers.