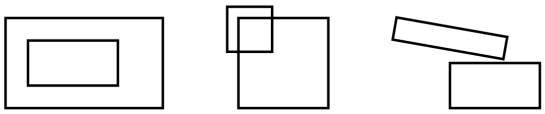
Mathematics Of Doing, Understand, Learning, and Educating Secondary Schools

MODULE(S^2): Algebra for Secondary Mathematics Teaching

Adapted for MODULE(S^2)

Version Spring 2018



The Mathematics Of Doing, Understand, Learning, and Educating Secondary Schools (MODULE(S^2)) project is partially supported by funding from a collaborative grant of the National Science Foundation under Grant Nos. DUE-1726707,1726804, 1726252, 1726723, 1726744, and 1726098. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Todo list

Contents

Part I

Introduction to Fields

1 Fields and Other Algebraic Structures

In this section we will begin our study of **fields**. You've already encountered fields in your mathematical studies: the set of rational numbers $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$ are fields, as is the set of complex numbers $\mathbb{C}$. The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are different in many ways, but here we will focus on the ways in which they are similar. We will also see that there are fields that are different from these three in some very important ways.

Consider the equation

$$3x + 8 = 14.$$

It's not hard to see that the solution to this equation is $x = 2$: $3(2) + 8 = 14$. Let's us solve this equation step-by-step, justifying each step along the way. First we will subtract 8 from both sides:

$$(3x + 8) - 8 = 14 - 8.$$

(Note that we could also view this as adding -8 to both sides. The number -8 is known as the **additive inverse** of 8.) Applying the associative law on the left-hand side gives

$$3x + (8 - 8) = 6.$$

We know that $8 - 8 = 0$ so we have

$$3x + 0 = 6.$$

The number 0 is an **additive identity**. That means adding 0 returns the value we added it to. So we have

$$3x = 6.$$

We now multiply each side by $1/3$ to obtain

$$\frac{1}{3}(3x) = \frac{1}{3} \cdot 6.$$

Multiplication is associative, so we can write this as

$$\left(\frac{1}{3} \cdot 3\right) x = 2.$$

The number $1/3$ is the **multiplicative inverse** of 3, meaning that $\frac{1}{3} \cdot 3$ is equal to the **multiplicative identity**; that is, $\frac{1}{3} \cdot 3 = 1$. Thus we have

$$1x = 2.$$

The number 1 is the **multiplicative identity** meaning that $1x = x$. So we conclude that

$$x = 2.$$

Let us analyze this situation more carefully. First note that the equation $3x + 8 = 14$ uses two operations, called addition and multiplication. (Subtraction can always be defined in terms of addition, and division can be defined in terms of multiplication.) We used some familiar properites of addition and multiplication such as associativity of addition and multiplication.

Above we multplied by $1/3$ at point in the solution. Since $1/3$ is a rational number, we say that we solved this equation "over the rationals." But, notice that in this example we didn't really need to do this. Next we give a solution to the equation $3x + 8 = 14$ "over the integers." We begin the same way:

$$\begin{aligned} 3x + 8 &= 14 \\ (3x + 8) - 8 &= 14 - 8 \\ 3x + (8 - 8) &= 6 \\ 3x + 0 &= 6 \\ 3x &= 6. \end{aligned}$$

Next we observe that $6 = 3(2)$ so we have

$$3x = 3(2).$$

One can prove that in the integers that if a, b, and c are integers and $ab = ac$ then $b = c$. Using just that fact, we can conclude that

$$x = 2.$$

- Prove that if a, b, and c are integers and $ab = ac$ then $b = c$. Remember - division is not allowed, we want to do this proof entirely in the integers.
- Can you solve the equation $3x + 8 = 14$ over the natural numbers? (Here you're not allowed to use additive inverses!)

We call 0 an additive identity because for any number n, $n + 0 = 0 + n = n$.

- Consider the collection of all 2×2 matricies whose entries are real numbers. Write down the additive identity of this set.
- How would you define the general notion of a **multiplicative identity**? What is a multiplicative identity in $\mathbb{Q}$?
- Is there a multiplicative identity for the set of all 2×2 matricies with real entries?

Once we have a notion of an additive identity, we can define the notion of an additive inverse. We say that a number b is an additive inverse of a number a if and only if $a + b = b + a = 0$. If b is an additive inverse of a we write $b = -a$. Note that $-a$ may be positive or negative. For example, the additive inverse of 4 is -4, but the additve inverse of -5 is 5.

How would you define the notion of a **multiplicative inverse**? Give an example of a number a and its multiplicative inverse b.

A **field** $\mathbb{F}$ is a collection of mathematical objects (possibly numbers, matrices, functions, etc.) with two operations, called addition $(+)$ and multiplication $(\cdot)$, in which we can always solve an equation of the form

$$ax + b = c$$

where $a, b, c\mathbb{F}$ and $a \neq 0$. The properties we need to make this happen are given in the following definition.

Definition 1.1. A field $\mathbb{F}$ is a nonempty set together with two operations addition $+$ and multiplication $\cdot$ which satisfy the following properties, called the field axioms:

1. If $a, b \in \mathbb{F}$, there is a unique $a + b \in \mathbb{F}$.
2. Addition is associative. That is, if $a, b, c \in \mathbb{F}$, then
$$(a + b) + c = a + (b + c).$$
3. Addition is commutative. That is, if $a, b \in \mathbb{F}$, then
$$a + b = b + a.$$
4. There is an additive identity in $\mathbb{F}$.
5. If $a \in \mathbb{F}$, then a has an additive inverse in $\mathbb{F}$.
6. If $a, b \in \mathbb{F}$, then there is a unique $a \cdot b \in \mathbb{F}$.
7. Multiplication is associative.
8. Multiplication is commutatitive.
9. There is a multiplicative identity in $\mathbb{F}$.
10. If $a \in \mathbb{F}$ and $a \neq 0$, then there is a multiplicative inverse of a in $\mathbb{F}$.

11. Multiplication distributes over addition. That is, if $a, b, c \in \mathbb{F}$, then
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$
12. The additive identity does not equal the multiplicative identity.

Of course, you have seen fields before: the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$ are both fields under their usual operations of addition and multplication. In fact, $\mathbb{Q}$ is a **subfield** of $\mathbb{R}$.

More on Identities and Inverses

We all know that in the rational numbers there is only one additive identity: the number 0. But could it be that there is a field with more than one additive identity? We have the following proposition:

Proposition 1.2. *In any field $\mathbb{F}$, then additive identity is unique.*

Proof. Suppose that we have additive identities 0 and z in $\mathbb{F}$. Since 0 is an additive identity, we know that
$$0 + z = z.$$
But since z is also an additive identity, we also know that
$$0 + z = 0.$$
So, we have that
$$z = 0 + z = 0.$$
This proves that the additive identity in any field is unique. □

There are a couple of observations to make about this prove. First, a good general strategy for proving that something is unique is to assume that there are two of them and then prove that they are equal. If needed, you can also assume that your two proposed objects are not equal and derive a contraticton, but notice that we did not need to do that in the proof above. Second, observe that besides using the definition of an additive identity, the only other property we used to prove the proposition above is that addition is commutatitive.

Since the additive identity in any field is unique, we will almost always use the usual symbol 0 to represent it, unless we have reason not to.

> Use the proof above as a model to show that in any field the multiplicative identity is unique.

Similarly, since the multplicative identity in any field is unique, we will almost always use the usual symbol 1 to represent it.

There is a similar fact to observe with respect to additive and multiplicative inverses. For example, there is only one rational number whose sum with $-\frac{1}{2}$ is 0, namely $\frac{1}{2}$. Similarly, there is only one rational number whose product with $-\frac{1}{2}$ is 1, namely -2. We have:

Proposition 1.3. *If $\mathbb{F}$ is a field and $a \in \mathbb{F}$, then its additive inverse is unique to it.*

Proof. Suppose that $\mathbb{F}$ is a field and that $a \in \mathbb{F}$. We want to prove that there is only one element $b \in \mathbb{F}$ so that
$$a + b = b + a = 0.$$
To this end, suppose that there are two such elements $b, c \in \mathbb{F}$. Then we have both:
$$a + b = b + a = 0$$
$$a + c = c + a = 0$$
Consider the sum $b + a + c$. On one hand we have
$$b + a + c = (b + a) + c = 0 + c = c.$$
On the other hand we have
$$b + a + c = b + (a + c) = b + 0 = b.$$
Thus we conclude that $c = b$ and that every element in a field has a unique additive inverse. □

Proposition 1.4. *If $a \in \mathbb{F}$, then $a \cdot 0 = 0 \cdot a = 0$.*

Proposition 1.5. *Suppose $a, b \in \mathbb{F}$. Then*

1. $-(-a) = a$
2. $-a = (-1)a$
3. $-(a + b) = (-a) + (-b)$
4. $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$.

Ordered Fields

Part II

Constructible Numbers

Part III

Three Famous Problems