Math From Scratch Lesson 10: One Algebra to Rule Them All

W. Blaine Dowler

January 12, 2011

Contents

1 Rings

To this stage, our formal studies of algebra have been limited to a single operation at a time. Noncommutative groups have used the operation of multiplication, $\cdot$, while commutative or abelian groups have used the operation of addition. With the definition of an algebraic ring, we can move into more complex systems. We begin with the axioms for an abelian group, and add new axioms in addition to them.

1.1 Review: Abelian Group Axioms

The five axioms of an abelian group, originally defined in lesson four, are as follows, for a group $(R, +)$ where $a, b, c \in G$.

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

It is property two which allows us to use the customary trick of dropping the brackets around sums of three or more items. After all, the operation $+$ is defined as a *binary* operation, meaning it is defined only in terms of adding two numbers at a time. $a+b+c$ is not technically defined, but given the associativity from property 2, we often omit the brackets as it does not matter whether the reader interprets the sum as $(a + b) + c$ or $a + (b + c)$.

1.2 The New Axioms

The transformation of our group into a ring is performed by adding a second binary operation, denoted $\cdot$, which is subject to the axioms of a monoid, as defined in lesson four, as well as an additional pair of axioms related to the interaction of the two operations. Our ring, now denoted $(R, +, \cdot)$, must also satisfy the following:

1. **Closure:** $a \cdot b \in R \ \forall a, b \in R$.
2. **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c) \ \forall a, b, c \in R$.
3. **Identity:** $1 \in R$, and $a \cdot 1 = a \ \forall a \in R$

This defines much of what we need. There is still one burning question here, though: how do we mix the operations? That aspect is defined through the distributive property axiom:

1. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c \ \forall a, b, c \in R$.

The distributive property is very powerful when determining properties of an algebra. For example, it can be used to prove that $a \cdot 0 = 0$ for every possible a as follows:

$$\begin{aligned} a \cdot b &= a \cdot (b + 0) \\ &= a \cdot b + a \cdot 0 \end{aligned}$$

If the left hand side equals the right hand side, regardless of the specific values of a and b, then $a \cdot 0$ *must* be the additive identity, so $a \cdot 0 = 0$. (Remember, we proved that the identity element for either operation must be unique back in lesson four.)

These axioms combine to define an algebraic ring.

2 Integers

We have already defined the set of whole numbers, back in lesson three. We may now define the integers in the context in the whole numbers.

Definition The set of integers, denoted $\mathbb{Z}$, are the set which extends the whole numbers so that it is possible to act as the basis of a ring. Formally, $x \in \mathbb{Z}$ if either $x \in \mathbb{W}$ or $-x \in \mathbb{W}$.

2.1 An Author's Rant

Note that, contrary to the insistence of public school teachers and textbooks throughout the English speaking world, the symbol $\mathbb{I}$ most emphatically does ***not*** represent the integers. This seems to be a holdover from the early twentieth century. The symbol $\mathbb{Z}$ derives from the German word "Zahlen," which translates as "numbers." The author has heard rumours that he has yet to substantiate indicating that there was a push to reduce the German influence in North American youth, and so the symbol was changed in public schools to something that was easier to remember for the novice student. However, the symbol $\mathbb{I}$ stands for the imaginary numbers, a set of numbers not yet defined in these lessons. As a result of the need for international collaboration in research, plus resistance to local politically driven stupidity, professional mathematicians did not change their notations. As a result, many North American public school teachers and textbooks teach students incorrect notation that doesn't cause problems in public school, but which leads to massive confusion in the first few weeks of post-secondary education when students have no idea

what that $\mathbb{Z}$ thing means when their professors use it, nor why it is written with double lines on the blackboard,[1] while the professors are equally confused by the insistence of their students that "1" is somehow imaginary. End rant.

3 Axiom of Inequality

Before moving on, we must prove that any given ring (or group, for that matter) has only one multiplicative identity. The proof is surprisingly simple. Assume a and b are both identities in the ring $(R, +, \cdot)$. Then,

$$a = a \cdot b = b$$

Thus, there is only one multiplicative identity. If we have two labels which satisfy the property of the identity, then they must be two labels for exactly the same thing.

This introduces an asymmetry in our ring. 1 is special, in that it is the multiplicative identity, yet -1 is not the multiplicative identity. There must be some specific property which distinguishes 1 from -1, indicating that there are (at least) two types of numbers. We can define this property through the following recursive definition:

Definition A finite sum or product of *positive* numbers is a *positive* number.

The problem with a recursive definition is that it is recursive. Positive numbers and negative numbers are typically defined for students on their first exposure in terms of a number line, but one cannot draw a number line without the axiom of inequality. As we shall soon see, the axiom of inequality requires positive and negative numbers to already be defined. We need a new approach.

As we know we have at least two types of numbers, let us the types Type A and Type B. We must now try to determine which is positive and which is negative. We use the distributive property to make our first observation (given $a, b \in R$, where a and b are both numbers of Type A such that their inverses a^* and b^* are both Type B):

$$0 = a \cdot 0 = a \cdot (b + (b^*)) = a \cdot b + a \cdot (b^*)$$

[1] Originally, standard sets were noted with bold faced characters. However, bold face is hard to write on the blackboard, so a double lined letter was used as an in-class substitute. Printing technology "improved" over the years in ways that made it difficult to reproduce math, so math texts reverted to hand written reproductions. When more advanced typefaces became available once more, entire generations had grown up with the double line version, and that became the new de facto standard. We now return you to your regularly scheduled rant.

As the entire expression must equal 0, $a \cdot (b^*)$ must be the inverse of $a \cdot b$. Thus, $a \cdot (b^*) = (a \cdot b)^*$. In other words, when we multiply a Type A number by a Type B number, the result is a Type B number. As our definition of positive numbers requires a product of numbers of the same type, this does not appear to be useful. Its usefulness comes into play in our second application of the distributive property:

$$0 = a^* \cdot 0 = (a^*) \cdot (b + (b^*)) = (a^*) \cdot b + (a^*) \cdot (b^*)$$

By our first application, we know that $(a^*) \cdot b = (a \cdot b)^*$, a Type B number. As the entire right hand side must equal zero, the combination $(a^*) \cdot (b^*)$ must be a Type A number. As we have shown (back in lesson four again) that each element has a unique inverse, and given that $a \cdot b$ is known to be the inverse of $(a \cdot b)^*$, we must have that $(a^*) \cdot (b^*) = a \cdot b$. Thus, the product of two Type B numbers is a Type A number. *Now* we know how to identify the positive numbers; they are Type A. The product of two negative numbers is a positive number, while the product of two negatives is *also* a positive number. One only gets a negative product when multiplying one number of each type.

The only element whose product with other elements can be determined with certainty for all rings is the multiplicative identity 1. By the very definition of the multiplicative identity, we know that $1 \cdot 1 = 1$. Thus, the multiplicative identity multiplied by itself is itself; the type did not change. As we now know a Type B number multiplied by itself is a Type A number, 1 cannot be Type B. Thus, 1 is a positive number, and -1 is a negative number. We can also prove that $-1 \cdot a = -a$ in a similar manner, now that we know $-a \cdot (-b) = a \cdot b$ for any possible a and b, including $b = -1$:

$$0 = -1 \cdot 0 = -1 \cdot (a + (-a)) = -1 \cdot a + (-1) \cdot (-a) = -1 \cdot a + 1 \cdot a = -1 \cdot a + a$$

As the right hand side must still equal 0, we have $-1 \cdot a = -a$.

What of 0? Well, $0 + 0 = 0$, by definition of the additive identity, so 0 is its own inverse. So, then, is 0 positive or negative? It is actually neither; it marks the division between the positive and negative numbers, as seen in the Axiom of Inequality:

Axiom of Inequality: For any element $a \in R$, at least one of the following conditions holds:

- a is positive
- $a = 0$
- $-a$ is positive

To see how the third item may be true, take $a = -1$. In this case $-a$ is the inverse of -1, which is 1. Thus, $-(-1) = 1$, or in general (by similar logic) $-(-a) = a$. It is also important to note that, while all rings satisfy this axiom, there are some rings in which both a and $-a$ are positive numbers. More on that in a later lesson.

4 Ordering $\mathbb{Z}$

We now have almost everything we need to impose an order on the integers.[2] We have positive numbers. We haven't formally defined negative numbers, but we can quite quickly:

Definition A number a is *negative* if $-a$ is positive.

We also have a definition for subtraction: $a - b = a + (-b)$. Now, we can create a relation between any two elements $a, b \in R$ for a ring $(R, +, \cdot)$ which is a transitive relation (as defined in lesson one).

Definition For any two elements $a, b \in R$, we say that a is *greater than* b if and only if $a - b$ is positive. This is denoted $a > b$. This relation is the lowest priority when performing computations: thus $x - y > 0$ is to be read as $(x - y) > 0$.

This not only imposes an order on the elements of R, but it can be used to prove many of the common statements about positive numbers that we take for granted. For example, if a is positive, then $a > 0$, as $a - 0 = a + (-0) = a + 0 = a$ which is positive. The order is imposed by the demand of transitivity for the operation: if $a > b$ and $b > c$ for some $a, b, c \in R$, then $a > c$ follows.[3] For brevity, we can also define a *less than* relation denoted $<$, such that if $a > b$ then $b < a$.

Some quick consequences, given appropriately defined a, b, c:

- Any positive number is greater than any negative number: let $a > 0$ and $b < 0$. Then $-b$ is a positive number, so $a - b = a + (-b)$ is a finite sum of positive numbers, which is by definition positive.
- If $a > b$ then $-b > -a$: if $a > b$ is positive, then $a + (-b) > 0$. Well $a + (-b) = (-b) + a = (-b) - (-a)$, so if $a > b$ then $-b > -a$ automatically.

[2] Note that this will *not* be possible for all rings in general, as we will see in a future lesson.
[3] So, one cannot impose a transitive order on the set $\{rock, paper, scissors, lizard, Spock\}$.

- $-(b+c) = -b + (-c)$: by an earlier result this lesson, $-a = (-1) \cdot (a)$. Thus, $-b + (-c) = (-1) \cdot b + (-1) \cdot c = (-1) \cdot (b+c) = -(b+c)$.
- If $a > b$, then $a + c > b + c$: if $a > b$, then $a - b$ is positive. Well, we have $a-b = a+(-b) = a+0+(-b) = a+c+(-c)+(-b) = (a+c)+(-b+(-c)) = (a+c) - (b+c)$, which must also be positive by equality.
- If $a > b$, then $a - c > b - c$: if $a > b$, then $a - b$ is positive. Well, we have $a-b = a+(-b) = a+0+(-b) = a+(-c)+c+(-b) = (a-c)+(-b+c) = (a-c) - (b-c)$, which must also be positive by equality.
- If $a \cdot b = 0$, then either $a = 0$ or $b = 0$. This follows as 0 is neither positive nor negative. If neither a nor b is zero, then both are either positive or negative. We have now seen that every defined product of negative and positive elements is itself either negative or positive. As 0 is neither, it is not a possible product of nonzero elements.

5 Cancelable Elements

In an algebraic ring based on the integers, we have no multiplicative inverses. In other words, we cannot take $2 \cdot 3$ and cancel the 2 by multiplying by its inverse in the same way we can take $2 + 3$ and add -2 to cancel the 2. Therefore, we need to seek out a justification for reducing a statement such as $a \cdot d = (b+c) \cdot d$ to $a = b+c$. In other words, we need to either prove that $a \cdot d = b \cdot d$ is equivalent to $a = b$, or at least determine conditions under which this is the case.

So, to analyze, what is a situation in which $a \cdot d = b \cdot d$ does *not* imply that $a = b$? We can always define a function f such that $f(a) = a \cdot d$. In that case, we will find that $a \cdot d = b \cdot d$ implies $a = b$ any time f is *injective*, as defined in lesson eight. In other words, $a \cdot d = b \cdot d$ implies $a = b$ any time the products $a \cdot d$ and $b \cdot d$ are unique for a given d. Let us introduce a new integer c such that $a \neq c$. If we can prove that $a \cdot d \neq c \cdot d$, then we are done; the product must be unique.

As $a \neq c$, we know that $a - c \neq 0$. This follows from the uniqueness of the additive inverse; i.e. if $a \neq c$ then $-a \neq -c$. We now examine the construction $a \cdot d - c \cdot d$ for some d. We soon find the following:

$$a \cdot d - c \cdot d = (a - c) \cdot d$$

This is either zero, or not zero. We know that $a-c \neq 0$, so if the construction equals 0, then $d = 0$. Thus, we cannot have unique products if $d = 0$; $a \cdot 0 = b \cdot 0$ regardless of the specific values of a and b. Thus, 0 is not a cancelable element. If, however, $d \neq 0$, then we have the product of two positive or negative elements

$(a - c)$ and d. As shown in lesson ten, the product of two positive or negative elements is itself positive or negative, and thus cannot be zero.

Note that this entire argument hinges on the axiom of inequality. We will see in an upcoming lesson that there are algebraic rings which are *not* subject to the axiom of inequality, and for which there are nonzero elements which are not cancelable elements, as the terms "positive" and "negative" have no practical meaning.

6 Upcoming Lessons

In our next lessons, we define the idea of representing numbers with standard symbols, including base ten notation and other bases. We also demonstrate how to represent and computer the results of addition and multiplication without going through half a page of set theory.