Math From Scratch Lesson 4: The Group Axioms

W. Blaine Dowler

December 1, 2010

Contents

1 What Are Axioms?

Axioms are rules that are chosen arbitrarily. We work with them because it makes sense that they are true. Of course, because the application of the rules is made by human choice, we cannot guarantee that they always apply. What we *can* do is clearly define which arbitrary assumptions are being made, and explore the consequences both with and without these rules. If we have different options for different sets of axioms, it would be best if we had terminology to describe them.

2 What Are Algebras?

Normally when we think of "algebra," we think of math that includes letters as constants and variables. While this is true, it's actually a much more limiting

definition than necessary. For one, it implies there is only one type of algebra, when in practice, there are many.

An algebra[1] is a combination of three things:

1. A list of axioms.
2. A set A consisting of members of some kind.
3. An operation $\cdot$ which is defined using members of the set A.

We denote the algebra by $(A, \cdot)$. Note that $\cdot$ can represent either addition or multiplication, and the conventional definition for the one we choose is best left for later.

3 The Group Axioms

An algebra is a group if it satisfies the above three conditions with the following list of axioms.

3.1 Axiom 1: Closure Under $\cdot$

To qualify as a group, an algebra must be *closed under* $\cdot$. Defined mathematically:

Definition An algebra $(A, \cdot)$ is closed under $\cdot$ if and only if, for all $a, b \in A$, then $(a \cdot b) \in A$.

In other words, if the operation $\cdot$ represents multiplication, you cannot multiply two members of A to get a result which is not a member of A. For example, if A were the set of all even numbers, then closure holds: the product of two even numbers is always an even number. However, if A were the set of all prime numbers, then closure does *not* hold: the product of two prime numbers is never prime.[2] The set of all prime numbers combined with multiplication still forms an algebra, but that algebra cannot be a group. An algebra which is subject to this axiom and this axiom alone is known as a *magma* or *groupoid*.

[1] Historical sidenote: the word "algebra" derives from the Arabic "al jebr," which means "reunion of broken parts," according to `http://www.etymonline.com/index.php?term=algebra`. It was adopted by the English speaking world after the publication and popularization of "Kitab al-Jabr w'al-Muqabala," which introduced the Western world to the Arabic number system we still use today.

[2] Prime and even numbers will both be formally defined in a later lesson.

3.2 Axiom 2: Associative Under $\cdot$

To qualify as a group, an algebra must also be *associative under* $\cdot$. Defined mathematically:

Definition An algebra $(A, \cdot)$ is associative under $\cdot$ if and only if, for all $a, b, c \in A$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

In other words, when combining three elements with the group's operation, it does not matter which two are combined first. Therefore, we often drop the brackets, and simply state $(a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c$ for simplicity.[3] Note that the order *does* matter: we did not require that $(a \cdot b) \cdot c = (b \cdot a) \cdot c$. Again, this distinction will be important later.

Now, if we were to stop at this point, we would have a *semigroup* algebra.

3.3 Axiom 3: Existence of Identity

The third axiom required for a group algebra is the existence of an identity element e.

Definition An algebra $(A, \cdot)$ has an identity element e if, for every $x \in A$, we have $x \cdot e = e \cdot x = x$.

In other words, there is an element in A which, when paired with a member x through the operation $\cdot$, does not change the identity of x. If the operation is addition, we call this identity 0, but if the operation is multiplication, we call this identity 1. The identity must be unique. For example, if both a and b were identity elements with operation $\cdot$, then $a = a \cdot b = b$ follows immediately.

An algebra with these three axioms only is called a *monoid*.

3.4 Axiom 4: Existence of Inverses

The fourth and final axiom of a group is the existence of inverses. It is through this axiom that subtraction and division are defined.

[3] This is another example of the special type of laziness that was mentioned in an earlier lesson: associativity is formally defined, instead of simply being assumed, and as a result, we can get lazy and stop writing many of our brackets.

Definition Let $(A, \cdot)$ be an algebra, and $x \in A$. If x has an inverse in $(A, \cdot)$, which we will denote x^{-1}, then $x \cdot x^{-1} = x^{-1} \cdot x = e$. To satisfy this axiom and qualify as a group algebra, then $(A, \cdot)$ must contain an element x^{-1} for every possible x in A. Note that the identity element e is its own inverse: $e \cdot e = e$. The reason for the notation x^{-1} will have to wait for a later lesson.

If our operation is addition, then we denote the inverse of x as $-x$. Subtraction is then simply a shorthand instead of a complete operation in and of itself: $a - b$ is nothing more than a shorthand for $a + (-b)$. Similarly, when the operation is multiplication, and the identity is 1, the inverse of x is denoted by either x^{-1} or $\frac{1}{x}$. Again, division is just a shorthand rather than a formally defined operation: $a \div b$ simply means $a \times b^{-1}$. There are some subtle aspects of this definition that will lead to a surprising result when we deal with modular algebras: under certain circumstances, fractions can equal whole numbers.

Finally, the inverse of a given element x is unique. We can prove as follows: assume a and b are both inverses of x. Then,

$$a = a \cdot e = a \cdot (x \cdot b) = (a \cdot x) \cdot b = e \cdot b = b$$

Thus, $a = b$, and the inverse is unique.

3.5 A Missing Axiom: Commutativity

At no point did we require that $a \cdot b = b \cdot a$. The reason for this is surprisingly simple: in some algebras, it simply isn't true. We will see explicit examples of this counterintuitive notion in our next few lessons. If this is true, we typically label our group operation as addition. If it is not, we typically call it multiplication. Groups which possess this property are also known as *abelian* groups, as Niels Henrik Abel's work in this field was quite extensive.

4 Upcoming Lessons

The next few lessons will deal with rudimentary group theory. Once that is complete, we will add more axioms and operations to our algebras to create rings and play with those. After that, we will add some final axioms to create algebraic fields, which are the class of algebras most people are familiar with.