Math From Scratch Lesson 40: Identifying New Algebras

W. Blaine Dowler

January 31, 2014

Contents

1 Purpose

In this lesson, we test the new sets of numbers that we have just defined (imaginary and complex) and determine which, if any, definitions of algebras they define.

2 Different Algebras

Different algebras are defined by the axioms they satisfy. Specifically, we have our axioms:

1. Closure under addition
2. Closure under multiplication

3. Commutativity under addition
4. Commutativity under multiplication
5. Associativity under addition
6. Associativity under multiplication
7. Additive identity
8. Multiplicative identity
9. Inverses under addition
10. Inverses under multiplication
11. Distributive property
12. Completeness Axiom
13. Existence of $i = \sqrt{-1}$, which is distributive such that $(a + b)\, i = ai + bi$ and $ai = ia$.

We can have the following different algebras if the listed properties hold:

- Magma or groupoid: Either property 1 or 2 holds.
- Semigroup: Either 1 and 5 or 2 and 6 hold.
- Monoid: Either 1, 5 and 7 or 2, 6 and 8 hold.
- Group: Either 1, 5, 7 and 9 or 2, 6, 8 and 10 hold.
- Abelian Group: Either 1, 3, 5, 7 and 9 or 2, 4, 6, 8 and 10 hold.
- Semiring: Properties 1, 2, 5, 6, 7 and 8 hold.
- Near-ring: Properties 1, 2, 5, 6, 7, 8 and 9 hold.
- Ring: Properties 1, 2, 3, 5, 6, 7, 8 and 9 hold.
- Field: Properties 1-11 hold.

Which definitions, if any, do the imaginary and complex sets of numbers satisfy?

3 Imaginary Numbers

The imaginary numbers are the set of numbers $\mathbb{I}$ such that $a \in \mathbb{I}$ if and only if $a = bi$ where $b \in \mathbb{R}$.

Let us test each of the first 11 properties individually.

1. By property 13, the definition of i, if $ai \in \mathbb{I}$ and $bi \in \mathbb{I}$, then $ai + bi = (a+b)\,i$ and the imaginary numbers are closed under addition.
2. If $ai \in \mathbb{I}$ and $bi \in \mathbb{I}$, then $ai \cdot bi = abi^2 = -ab \notin \mathbb{I}$. Without closure under multiplication, it is unlikely that any of the multiplication properties will hold.
3. If $ai \in \mathbb{I}$ and $bi \in \mathbb{I}$, then $ai + bi = (a+b)\,i = (b+a)\,i = bi + ai$ using the commutativity of addition of real numbers in the intermediate step.
4. If $ai \in \mathbb{I}$ and $bi \in \mathbb{I}$, then $ai \cdot bi = aibi = iabi = ibai = biai = bi \cdot ai$ and commutativity under multiplication holds insofar as closure holds. As multiplicative closure doesn't hold, neither does this.
5. If $ai \in \mathbb{I}$, $bi \in \mathbb{I}$ and $ci \in \mathbb{I}$, then $(ai + bi) + ci = ((a+b)\,i)\,i + ci = ((a+b)+c)\,i = (a+(b+c))\,i = ai + (b+c)\,i = ai + (bi + ci)$ and associativity under addition holds.
6. If $ai \in \mathbb{I}$, $bi \in \mathbb{I}$ and $ci \in \mathbb{I}$, then $(ai \cdot bi) \cdot ci = ((a \cdot b)\,i)\,i \cdot ci = ((a \cdot b) \cdot c)\,i = (a \cdot (b \cdot c))\,i = ai \cdot (b \cdot c)\,i = ai \cdot (bi \cdot ci)$ and associativity under multiplication holds insofar as multiplicative closure holds, meaning not at all.
7. If $ai \in \mathbb{I}$, then $ai + 0i = (a+0)\,i = ai$. Thus, $0i = 0$ is the identity element of the imaginary numbers under addition.
8. If $ai \in \mathbb{I}$, then we need a $bi \in \mathbb{I}$ such that $ai \cdot bi = ai \forall ai$ for the identity property to hold. By the restrictions on the definition of $bi \in \mathbb{I}$, we must have $b \in \mathbb{R}$. Yet, $aibi = abi^2 = -ab \notin \mathbb{I}$. Thus, we need to have $-ab = ai$ for every possible a, which only works if $b = -i \notin \mathbb{R}$, so there is no multiplicative identity in the set of imaginary numbers.
9. If $ai \in \mathbb{I}$ and $bi \in \mathbb{I}$, then $ai + bi = 0i$ if and only if $b = -a$. As the only restrictions on a and b are that they are both real numbers, this is satisfied, and additive inverses exist in the set of imaginary numbers.
10. As there is no multiplicative identity in the set of imaginary numbers, this set cannot possibly have a multiplicative identity.
11. If $ai \in \mathbb{I}$, $bi \in \mathbb{I}$ and $ci \in \mathbb{I}$, then $ai \cdot (bi + ci) = ai \cdot (b+c)\,i = a \cdot (b+c)\,i^2 = (a \cdot b + a \cdot c)\,i^2 = (a \cdot bi + a \cdot ci)\,i = a \cdot bii + a \cdot cii = ai \cdot bi + ai \cdot ci$ and the distributive property holds insofar as multiplicative closure holds. In

other words, the numbers will look right, but the result is not an imaginary number and is somewhat meaningless.

Thus, the imaginary numbers satisfy properties 1, 3, 5, 7 and 9 only. Thus, the set of imaginary numbers can be treated as a magma or groupoid, a semigroup, a monoid, a group and an Abelian group only. These may have their applications, but as this algebra behaves identically to that of the real numbers with an i attached, it is not a particularly useful revelation.

4 The Complex Numbers

The set of complex numbers $\mathbb{C}$ is defined such that $z \in \mathbb{C}$ if $z = x + iy$, $x, y \in \mathbb{R}$ and i is defined as per property 13 above. We now test each of properties 1-12 to see what type(s) of algebra this forms, if any. We must define what we mean by addition and multiplication for these numbers. We define the addition of $c = a+bi \in \mathbb{C}$ and $z = x+yi \in \mathbb{C}$ as $c+z = (a+x)+(b+y)\,i$ and $c \cdot z = (ax-by)+(ay+bx)\,i$. We will see that these definitions are consistent with the distributive property and the definition that $i^2 = -1$. In short, we have a choice: we may arbitrarily choose these definitions of addition and multiplication, or we may arbitrarily assume that the distributive property holds and then these simply apply. Either way, we must make an assumption. As defining our operations is part of all algebraic constructions on some level, that is the choice we make.

1. If $c = a + bi \in \mathbb{C}$ and $z = x + yi \in \mathbb{C}$, then $c + z = a + bi + x + yi = a + x + bi + yi = (a + x) + (b + y)\,i \in \mathbb{C}$, so the set of complex numbers is closed under addition.

2. If $c = a + bi \in \mathbb{C}$ and $z = x + yi \in \mathbb{C}$, then $c \cdot z = (a + bi) \cdot (x + yi) = ax + bxi + ayi + byi^2 = (ax - by) + (bx + ay)\,i$, so this is closed under multiplication.

3. If $c = a + bi \in \mathbb{C}$ and $z = x + yi \in \mathbb{C}$, then $c + z = a + bi + x + yi = a+x+bi+yi = (a + x) + (b + y)\,i = (x + a) + (y + b)\,i = x+a+yi+bi = x + yi + a + bi = z + c$, so commutativity holds.

4. If $c = a + bi \in \mathbb{C}$ and $z = x + yi \in \mathbb{C}$, then $c \cdot z = (a + bi) \cdot (x + yi) = ax+bxi+ayi+byi^2 = (ax - by) + (bx + ay)\,i = (xa - yb) + (xb + ya)\,i = xa - yb + xbi + yai = xa + xbi + yai + ybi^2 = (x + yi) \cdot (a + bi)$ and the set of complex numbers is commutative under multiplication.

5. If $c = a + bi \in \mathbb{C}$, $w = u + vi \in \mathbb{C}$ and $z = x + yi \in \mathbb{C}$, then $c + (w + z) = a + bi + (u + vi + x + yi) = a + bi + ((u + x) + (v + y)\,i) = a + (u + x) + bi + (v + y)\,i = (a + u) + x + (b + v)\,i + yi = (a + u) + (b + v)\,i + x + yi = (c + w) + z$ and the complex numbers are associative under addition.

6. If $c = a + bi \in \mathbb{C}$, $w = u + vi \in \mathbb{C}$ and $z = x + yi \in \mathbb{C}$, then $c \cdot (w \cdot z) = (a + bi) \cdot ((u + vi) \cdot (x + yi)) = (a + bi) \cdot (ux + xvi + uyi - yv) = aux + axvi + auyi - ayv + buxi - bxv - buy - byvi = (aux - ayv - bxv - buy) + (axv + auy + bux - byv)\, i = (au - bv)\, x + (av + bu)\, yi^2 + (av + bu)\, x + (au - bv)\, yi = (au - bv)\,(x + yi) + (av + bu)\, i\,(x + yi) = (au - bv + avi + bui)\,(x + yi) = \left(au + avi + bui + bvi^2\right)(x + yi) = ((a + bi)\,(u + vi))\,(x + yi)$, which (finally) shows that the complex numbers are associative under multiplication.

7. If $c = a + bi \in \mathbb{C}$, then $c + 0 = c$ for $0 = 0 + 0i \in \mathbb{C}$, so we have an additive identity.

8. If $c = a + bi \in \mathbb{C}$, then $c \cdot 1 = (a + bi) \cdot (1 + 0i) = a + bi + 0ai + 0bi^2 = a + bi = c$, so we have a multiplicative identity under multiplication.

9. If $c = a + bi \in \mathbb{C}$, then $-c = -a - bi$ and $c + (-c) = a + bi - a - bi = 0 + 0i = 0$ and we have inverses under addition.

10. Verifying inverses under multiplication is more challenging. We need to show that, for every possible $c = a + bi$, there is a matching $z = x + yi$ such that $(a + bi) \cdot (x + yi) = 1 + 0i$. Now we simply need to find definitions of x and y in terms of a and b that are always defined, regardless of a and b. By our definition of multiplication, $(a + bi) \cdot (x + yi) = (ax - by) + (ay + bx)\, i$. Thus, we need to find x and y such that $ax - by = 1$ and $ay + bx = 0$. Let us start by isolating y in the latter equation, giving us $y = -\frac{bx}{a}$. If we now substitute this into our former equation, we have $ax - b\left(-\frac{bx}{a}\right) = 1$. This simplifies to $ax + \frac{b^2}{a}x = 1$, or $\frac{a^2+b^2}{a}x = 1$, which leads us to $x = \frac{a}{a^2+b^2}$. Substituting this back into $y = -\frac{bx}{a}$ gives $y = -\frac{b}{a^2+b^2}$. These are defined any time $a^2 + b^2 \neq 0$, which is true for all cases save $a = b = 0$, which is the same sole exception we had for the real numbers or any other algebraic field. Thus, if $c = a + bi \in \mathbb{C}$, then $c^{-1} = \frac{1}{c} \in \mathbb{C}$ exists unless $c = 0$.

11. If $c = a + bi \in \mathbb{C}$, $w = u + vi \in \mathbb{C}$ and $z = x + yi \in \mathbb{C}$, then $c \cdot (w + z) = (a + bi) \cdot (u + vi + x + yi) = au + avi + ax + ayi + bui - bv + bxi - by = (au - bv) + (av + bu)\, i + (ax - by) + (ay + bx)\, i = c \cdot w + c \cdot z$, and the Distributive Property holds.

12. If we define an infinite series of $c_n = a_n + b_n i$ termwise as $\sum c_n = \sum a_n + i \sum b_n$, then completeness is inherited from the fact that $a_n, b_n \in \mathbb{R}$.

Thus, the complex numbers are a complete set of numbers which satisfy all of the axioms of the algebraic structures we have examined thus far.

5 Conjugates, Denominators and Absolute Values

In the past, it has proven useful to denote multiplicative inverses not only with negative exponents, but as denominators in fractions. Is it possible to maintain that same convenience here? If so, we would need to find a meaningful interpretation of

$$c^{-1} = \frac{1}{a+bi}$$

with i in the denominator. Thus far, we have only defined i in a complex number in numerators, where we can distinguish between a "real" part $a = \Re(c)$ and the "imaginary" part $b = \Im(c)$ such that $c = \Re(c) + i\Im(c)$. We have a goal in that we have found the general form of the multiplicative inverse of c, but it would be nice to "derive" such a form for general use.

Let us start by defining the complex conjugate of c as the number $c^* = a - bi = \Re(c) - i\Im(c)$, sometimes denoted $c^\dagger$. We use the former notation here, as the latter is primarily used for a more general class of algebraic objects that we are not ready to define yet. Rest assured, once we get to that definition, you will be able to see (possibly because I will explicitly demonstrate it) that inverses of complex numbers are really special cases of the more general class of objects. We shall now demonstrate that these conjugates may be used to transform an unclear denominator into a real denominator in a fraction with a complex numerator. As we can break up a fraction according to terms being added in its numerator, this will allow us to transform the result into something more familiar.

We begin by reviewing the idea of equivalent fractions:

$$\frac{f}{g} = \frac{f}{g} \cdot \frac{h}{h} = \frac{fh}{gh}$$

In other words, fractions are defined in such a way that common factors between numerator and denominator do not impact the value of the fraction. Let us now look at the same notion in terms of complex numbers.

$$\frac{1}{c} = \frac{1}{c} \cdot \frac{c^*}{c^*} = \frac{c^*}{cc^*}$$

Writing this with explicit substitution of $c = a + bi$ and $c = a - bi$, we have

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2 + abi - abi - b^2 i^2} = \frac{a-bi}{a^2+b^2}$$

This allows us a simple interpretation of imaginary and complex denominators. Thus, we won't always apply the conjugate during the algebra, and may simply leave complex denominators as written, but we will always understand what is intended by such a fraction.

Finally, we may also use the complex conjugates to define the absolute value of a complex number. As you may recall, for a real number x, we have defined

$$|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$$

How would this definition work for complex numbers? The axiom of inequality no longer applies, so we can't necessarily compare the numbers to 0 in this sense. We will take a close look at the product cc^* to help us in this quest. For any $c = a + bi$, we have $c^* = a - bi$, and thus

$$cc^* = (a + bi)\,(a - bi) = a^2 + abi - abi - b^2 i^2 = a^2 + b^2 \in \mathbb{R}$$

Thus, the combination cc^* will always be a real number. Ideally, we would find a way to map cc^* into a real number in such a way that we can define the absolute value in a way that the absolute value of real number x would have the same absolute value as the complex number $x + 0i$. We already have the framework in place, ready to be applied: $|c| = \sqrt{cc^*} = \sqrt{a^2 + b^2}$. If $b = 0$, then $|c| = |a|$, and if $a = 0$ then $|c| = |b|$. Thus, even if we treat the real numbers as a subset of the complex numbers (as we could) we can define the absolute value of a number as

$$|c| = \sqrt{cc^*}$$

and we can then do everything with it that we used to do before.

6 Next Lesson

We start to use the complex numbers to generalize the idea of numbers and mathematical objects that can't be placed on a number line, as our next step towards graphing and algebra.