Math From Scratch Lesson 24: The Rational Numbers

W. Blaine Dowler

May 23, 2012

Contents

1 Defining the Rational Numbers

Colloquially, the rational numbers are fractions. Mathematically, they are the result of extending the set of integers $\mathbb{Z}$ into a set of numbers $\mathbb{Q}$ which forms an algebraic field instead of just a ring. Thus, they satisfy both the ring axioms

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

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

and the two additional axioms

1. **Commutativity under $\cdot$:** $a \cdot b = b \cdot a \ \forall a, b \in \mathbb{Q}$
2. **Inverses under $\cdot$:** $\forall a \neq 0 \in \mathbb{Q} \exists a^{-1} \in \mathbb{Q} : a \cdot a^{-1} = 1$. Division is defined as $a \cdot b^{-1} = a \div b \forall b \neq 0$. Division by 0 is undefined, as 0 has no inverse.

Adding commutativity is relatively simple; for the case of the integers, we know this works. The difficulty is in defining formal inverses, and ensuring that they still conform to all of these axioms.

1.1 Defining inverses

We start by introducing the inverses, denoted by the $^{-1}$ superscript. At this stage; that is completely arbitrary, using what I like to refer to as "the method of wishful thinking." We assume the existence of exactly what we want, and then verify that everything works as expected. In fact, marking the inverse nature with an exponent is also wishful thinking. It is far from the first notation humanity developed, but it is the most useful in this context, for reasons that are not yet apparent. This will always be an assumption; it is entirely possible, as we have seen, to build algebras without these inverses. Thus, we have to assume their existence and then just verify that they behave as we want them to.

These inverses extend the set $\mathbb{Z}$ into the set $\mathbb{Q}$ such that

$$(x \in \mathbb{Q}) \Leftrightarrow \left(x = a \cdot b^{-1} : a \in \mathbb{Z}, b \neq 0 \in \mathbb{Z}\right)$$

Now we test all 11 axioms, with the implicit assumption that none of our inverses are meant to be the inverse of 0. We do not test them in the order we defined them, as some tests are easier if "later" axioms can be applied.

1. **Inverses under $\cdot$:**

   We have taken this as an assumption. With that assumption, and that one alone, we need to test the rest.

2. **Identity for $\cdot$:**

   This is one of the easiest to test. $a^{-1} \cdot 1 = a^{-1}$. Similarly, if $x = a \cdot b^{-1}$ then $x \cdot 1 = a \cdot b^{-1} \cdot 1 = a \cdot b^{-1} = x$

3. **Identity for $+$:**

   If $x = a \cdot b^{-1}$ then $x + 0 = a \cdot b^{-1} + 0 = a \cdot b^{-1} = x$

4. **Associativity under $\cdot$:**

   This one is true, by our definition of inverses. We can't calculate with specific inverses yet, but the property is automatically inherited from the ring algebra.

5. **Commutativity under $\cdot$:**

   This is similarly inherited given our definition. In other words, if we can find a structure to inverses that satisfies everything else on this list, it will also satisfy this.

6. **Closure under $\cdot$:**

   Before we can prove this, we must define a compound inverse. Let $x, y \in \mathbb{Q}$. Given the closure property, $x \cdot y \in \mathbb{Q}$. Given this, what is $(x \cdot y)^{-1}$?

   Well, we need $(x \cdot y) \cdot (x \cdot y)^{-1} = 1$. We can manually build a system with this property:

   $$x \cdot y \cdot y^{-1} \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1$$

   where we have used the associative property. Thus, $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. Note the reversed order of the letters: this is necessary for algebras that have (at least some) inverses but not the commutativity property. Since we have the commutative property, we can just as easily say $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1} = x^{-1} \cdot y^{-1}$

   Now all we need to do for the closure property is prove that, given $x = a \cdot b^{-1} \in \mathbb{Q}$ and $y = c \cdot d^{-1} \in \mathbb{Q}$, then $x \cdot y = z \in \mathbb{Q}$. We prove this by showing that z can be written in the form $z = e \cdot f^{-1} \in \mathbb{Q}$.

   $$x \cdot y = a \cdot b^{-1} \cdot c \cdot d^{-1} = a \cdot c \cdot b^{-1} \cdot d^{-1} = (a \cdot c) \cdot (d \cdot c)^{-1}$$

   In the last step, the terms in brackets are already known to be in the set. With our assumption of extending $\mathbb{Z}$ with inverses for every non-zero quantity, then this holds. $a \cdot c$ is in $\mathbb{Z}$, and $d \cdot c$ is in $\mathbb{Z}$, so $(a \cdot c) \cdot (d \cdot c)^{-1} \in \mathbb{Q}$ and the set $\mathbb{Q}$ is closed under multiplication, $\cdot$.

7. **Distributive Property:**

   We wish to show that, with $x, y, z \in \mathbb{Q}$, we have $x \cdot (y + z) = x \cdot y + x \cdot z$. Let $x = a \cdot b^{-1}$ and $y = c \cdot d^{-1}$ where $a, b, c, d \in \mathbb{Z}$. $z = e \cdot f^{-1}$ with $e, f \in \mathbb{Z}$.

   $$\begin{aligned} x \cdot (y + z) &= a \cdot b^{-1} \cdot \left(c \cdot d^{-1} + e \cdot f^{-1}\right) \\ &= a \cdot \left(b^{-1} \cdot c \cdot d^{-1} + b^{-1} \cdot e \cdot f^{-1}\right) \\ &= a \cdot b^{-1} \cdot c \cdot d^{-1} + a \cdot b^{-1} \cdot e \cdot f^{-1} \\ &= x \cdot y + x \cdot z \end{aligned}$$

So the distributive property holds.

8. **Closure under $+$:**

   This is one of the more challenging ones, partly because the distributive property must be verified first. As a side effect of this one, though, we will actually demonstrate why fractions need to have common denominators before they can be added!

   Let $x = a \cdot b^{-1}$ and $y = c \cdot d^{-1}$ where $a, b, c, d \in \mathbb{Z}$. Can we show that $x + y = z$ where z is of the form $z = e \cdot f^{-1}$ with $e, f \in \mathbb{Z}$?

   We already know how to add something like $a + c$. We also know how to multiply inverses $\left(a^{-1} \cdot b^{-1} = (b \cdot a)^{-1}\right)$ but we haven't figured out how to add inverses. Oddly enough, we won't need to. What we will need to do, however, is recognize that $m \cdot m^{-1} = 1$ for any possible $m \neq 0$ and $m \in \mathbb{Q}$. I will make definitions for e and f that are informed by the final result now: $e = a \cdot d + b \cdot c \in \mathbb{Z}$ and $f = b \cdot d \in \mathbb{Z}$.

   $$\begin{aligned} x + y &= a \cdot b^{-1} + c \cdot d^{-1} \\ &= a \cdot d \cdot d^{-1} \cdot b^{-1} + c \cdot b \cdot b^{-1} \cdot d^{-1} \\ &= (a \cdot d + b \cdot c) \cdot \left(d^{-1} \cdot b^{-1}\right) \\ &= (a \cdot d + b \cdot c) \cdot (b \cdot d)^{-1} \\ &= e \cdot f^{-1} \\ &= z \end{aligned}$$

   Thus, the rational number set $\mathbb{Q}$ is closed under addition.

9. **Commutativity under $+$:**

   This now follows readily from the distributive property and commutativity under $\cdot$.

10. **Associativity under $+$:**

    This now follows readily from the distributive property, associativity under $\cdot$ and commutativity under $\cdot$.

11. **Inverses under $+$:**

    This is the final axiom needed to prove that the rational numbers $\mathbb{Q}$ as defined here form a field under normal circumstances. We need to show that, if $x = a \cdot b^{-1}$, then there is a number $y = -x$ such that $x + y = 0$.

    This is most easily done by the "guess and test" method of proof, in which we take an educated guess at what might work and show that our guess is correct or incorrect. We begin with an incorrect guess.

    Some might intuit that $y = -a \cdot (-b)^{-1}$ is the correct option. This is not actually the case. In fact, we can explicitly show that $-1 \cdot -1 = 1$, therefore $-1 = -1^{-1}$, which is equivalent so saying that -1 is its own inverse, or self-inverse. Thus, we can break down $-a \cdot (-b)^{-1}$ as follows:

$$\begin{aligned}
-a \cdot (-b)^{-1} &= -1 \cdot a \cdot (-1 \cdot b)^{-1} \\
&= -1 \cdot a \cdot (-1)^{-1} \cdot b^{-1} \\
&= -1 \cdot a \cdot -1 \cdot b^{-1} \\
-a \cdot (-b)^{-1} &= a \cdot b^{-1}
\end{aligned}$$

In other words, making both components of the rational number negative produces the identical rational number! Therefore, our second guess will be $y = -a \cdot b^{-1}$, which is identical to guessing $y = a \cdot (-b)^{-1}$ by logic similar to the above. Now we test this guess.

$$\begin{aligned}
x + y &= a \cdot b^{-1} + -a \cdot b^{-1} \\
&= (a + -a) \cdot b^{-1} \\
&= 0 \cdot b^{-1} \\
&= 0
\end{aligned}$$

which is exactly what we wanted. Therefore, for any given $x = a \cdot b^{-1}$, we can construct the additive inverse $-x = -a \cdot b^{-1}$, and the final required axiom is proven.

1.2 Alternative Definition of Rational Numbers

In the above verifications, we indicated that $-a \cdot b^{-1} = a \cdot (-b)^{-1}$. With this equivalence, we can make a slightly more efficient definition of rational numbers. Instead of

$$(x \in \mathbb{Q}) \Leftrightarrow \left(x = a \cdot b^{-1} : a \in \mathbb{Z}, b \neq 0 \in \mathbb{Z}\right)$$

we can write

$$(x \in \mathbb{Q}) \Leftrightarrow \left(x = a \cdot b^{-1} : a \in \mathbb{Z}, b \in \mathbb{N}\right)$$

where the restriction of b to the set of natural numbers automatically includes the $b \neq 0$ criterion without impacting the possible values of x.

1.3 Axiom of Inequality

We know how to compare integers with the axiom of inequality. Recall that the axiom of inequality effectively says that all integers can be put on a number line, as the concept of "greater than" or "less than" can be formally defined for all integers in a consistent way. We imposed this axiom arbitrarily, although it has held so far.[1] Can we establish something similar for rational numbers?

We can, indeed, establish this. We say that $x > y$ if and only if $x + (-y)$ is a positive number. Given $x = a \cdot b^{-1}$ and $y = c \cdot d^{-1}$, with $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{N}$, we have

$$\begin{aligned} x + (-y) &= a \cdot b^{-1} + (-c) \cdot d^{-1} \\ &= a \cdot d \cdot d^{-1} \cdot b^{-1} + (-c) \cdot b \cdot b^{-1} \cdot d^{-1} \\ &= (a \cdot d + (-c) \cdot b) \cdot (b \cdot d)^{-1} \end{aligned}$$

By our definition above, we know that $(b \cdot d)^{-1}$ is a positive number. (b and d were chosen to be members of $\mathbb{N}$, all of which are positive. If the product of two numbers is positive, the original numbers must both be either positive or negative. As $b \cdot b^{-1} = 1$ with b and 1 both positive, it must be true that b^{-1} is also positive. Similar logic can be followed to show that d^{-1} is also positive.) Thus, $x + (-y) > 0$ if and only if $a \cdot d + (-c) \cdot b > 0$. By the closure of integers, we know that this is a perfectly valid test, so the axiom of inequality still holds.

2 Fractions and Negative Exponents

Fractions can now be completely defined as another type of notation for rational numbers. The rational number $x = a \cdot b^{-1}$ can be written in two ways:

$$x = a \cdot b^{-1} = \frac{a}{b}$$

The latter is known as the fractional form. So, why do the two forms exist? The fractional form shown here is the older notation. Why did a new notation become popular? It allows us to deal with fractions using our established exponent rules. We already know that

$$x^m \cdot x^n = x^{m+n}$$

is true. Let us examine this property in the context of inverses by calculating $a^3 \cdot a^{-1}$.

$$\begin{aligned} a^3 \cdot a^{-1} &= a \cdot a \cdot a \cdot a^{-1} \\ &= a \cdot a \cdot 1 \\ &= a^2 \\ &= a^{3+(-1)} \end{aligned}$$

[1]We will eventually have to abandon this axiom in order to establish the Fundamental Theorem of Algebra, but that is still a long way off.

so that we see our notation is consistent with our exponent rules. Similarly, $\left(x^{-1}\right)^m = x^{-m}$. There is a final, counterintuitive process that we can now prove.

By our exponent rules,

$$x \cdot x^{-1} = x^1 \cdot x^{-1} = x^0$$

But, by our definition of inverses,

$$x \cdot x^{-1} = 1$$

Therefore, comparing the two statements, we find

$$x^0 = 1$$

for every $x \neq 0$. Why do we have the restriction that $x \neq 0$ in place? Because the above logic is valid if, and only if, x^{-1} exists. There is no number 0^{-1}, so we cannot verify that $0^0 = 1$. In fact, this is the ambiguous case, as $0^n = 0 \forall n \in \mathbb{N}$, so one could argue for either case. If one needs to use 0^0, one must be extraordinarily careful. We will return to this example after dealing with limits.

3 Next Lesson

In the next lesson, we establish infinite processes, which is the next step in connecting fractions to decimal representations.