Mathematics 4300 – Foundations of Algebra – Fall 1999

2. Next Stop on the Tour: The Rational Numbers: Let $\mathbf{Q}$ denote the set of rational numbers:

$$\mathbf{Q} = \{\text{points on the number-line corresponding to fractions}\}$$

(A fraction will be a/n where a is an integer and n is a natural number.)

Prescription for locating a/n on the number-line:

Step 1: Divide the number-line into intervals of size $1/n$ by subdividing the space between each a and $a+1$ into n equal intervals.

Step 2: Start at 0. If $a = m$, move m of these intervals to the right. If $a = -m$, move m of these intervals to the left. If $a = 0$, stay at 0.

Remark: Notice that many (in fact infinitely many) fractions give the same point on the number-line, and hence represent the same rational number. For example:

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{4}{8} = \dots \text{ and } \frac{-1}{2} = \frac{-2}{4} = \frac{-3}{6} = \frac{-4}{8} = \dots$$

and integers themselves are expressible as fractions by putting a "1" in the denominator, so that:

$$0 = \frac{0}{1} = \frac{0}{2} = \frac{0}{3} = \dots \text{ and } 1 = \frac{1}{1} = \frac{2}{2} = \frac{3}{3} = \dots$$

The cross multiplication rule: $a/n = b/m$ exactly when $am = bn$.

This rule is extremely useful for working with rational numbers!

Addition: To find $a/n+b/m$ on the number-line, move by the same amount in the same direction as in the prescription for locating b/m on the number-line, but start at the point represented by a/n instead of at 0. Notice that if we started with different fractions representing the same rational numbers, then the starting point and the movement would be the same, so that we would end up at the same location on the number-line. This prescription for the sum works best when the denominators are equal, since in that case the same subdivisions of the number-line may be used to locate $a/n, b/m$ and $a/n+b/m$. We can achieve this by using the cross-multiplication rule to put the fractions over a **common denominator**:

$$\frac{a}{n} = \frac{ma}{mn} \text{ and } \frac{b}{m} = \frac{bn}{mn}$$

Because the prescription for addition does not depend upon the fractions we use, we therefore have $a/n + b/m = ma/mn + bn/mn$ and the latter sum is obtained by the same rule which gave us $ma+bn$, only moving by intervals of $1/mn$ instead of 1. That is, we obtain the following formula:

$$\frac{a}{n} + \frac{b}{m} = \frac{ma+bn}{mn}$$

showing in particular that the sum of two rational numbers is again rational.

This formula is useful for checking the properties of addition:

Addition of rational numbers is commutative and associative,

Zero is the additive identity, and $a/n + -a/n = 0$ always.

For example, the last formula (which says that $-a/n$ is the additive inverse of a/n) is true because if we start at $-a/n$ and move by a/n units, we end up at zero (this should properly be done by considering the three cases $a = m, a = -m$ and $a = 0$). Or we can use the formula for addition without doing any thinking:

$$\frac{a}{n} + \frac{-a}{n} = \frac{an + (-a)n}{n^2} = \frac{0}{n^2} = 0$$

(Notice that we need the formula $(-a)n = -(an)$ from Exercise 1.7 to conclude that $an + (-a)n = an + -(an) = 0$.)

Subtraction. As with the integers, subtraction is defined by adding the additive inverse:

$$\frac{a}{n} - \frac{b}{m} := \frac{a}{n} + \frac{-b}{m}$$

(We use the notation ":=" to indicate that this is the **definition** of "$-$").

Relations. Since the rational numbers are located as points on the number-line, the relations are defined in the same way. It is convenient to define:

$$\mathbf{Q}^+ = \{\text{positive rational numbers}\}$$

Alternatively, $\mathbf{Q}^+$ is the set of rational numbers of the form m/n.

Multiplication. The product of rational numbers has an intuitive definition in terms of area. Namely, if m/n and k/l represent positive rational numbers, then $m/n \cdot k/l$ should be the area of the rectangle with sides of lengths m/n and k/l. (This is analogous to the "array" definition for natural numbers). One can pursue this train of thought to arrive at the following formula:

$$\frac{a}{n} \cdot \frac{b}{m} = \frac{ab}{mn}$$

for the product of rational numbers.

But let's not do that. Instead, let's take this formula as the **definition** of multiplication. But notice that something needs to be checked if we do this. Namely, we are after a definition of multiplication for rational numbers, not just for fractions. If a/n and b/m were replaced by different representatives for the same pair of rational numbers, say by $a/n = a'/n'$ and $b/m = b'/m'$, then we need to know that $ab/mn = a'b'/m'n'$. If this were not the case, then our definition would be **no good** as a product for **rational numbers**. (Think about this if it doesn't seem clear!) This same check could have been performed for the addition, but we knew in advance that addition was going to work because we were able to define the addition of two rational numbers in a way that obviously did not depend upon the fractions, and only later obtained the formula. Here, we are doing something different. We are using the formula as a definition.

So we have to do the following:

Check that the formula for multiplication is "well-defined": If $a/n = a'/n'$ and $b/m = b'/m'$, then by the cross-multiplication rule,

$$(1) \quad an' = a'n \quad \text{and} \quad (2) \quad bm' = b'm.$$

Multiplying equation (1) with equation (2) gives us:

$$(3) \quad (ab)(m'n') = (a'b')(mn)$$

(I have reordered the terms on each side...see Exercise 2.4).

But equation (3) and the cross-multiplication rule tell us that:

$$\frac{ab}{mn} = \frac{a'b'}{m'n'}$$

which is **exactly** what we needed to know.

With this formula in hand, it is now easy to check that:

Multiplication is commutative, associative and distributive and

One is the multiplicative identity.

With all this work under our belts, we need a bonus property for rational numbers to make it all worthwhile. The bonus is, as we all know, that (precise) division is now possible. For that, by analogy with subtraction, one needs a multiplicative inverse. This is always possible, but with one exception of course, since we **can't divide by zero!**

n/m **is the multiplicative inverse (or reciprocal) of** m/n and

$-n/m$ **is the multiplicative inverse of** $-m/n$**.**

Proof: The formula allows us to easily check:

$$\frac{n}{m} \cdot \frac{m}{n} = \frac{mn}{mn} = 1 \quad \text{and} \quad \frac{-n}{m} \cdot \frac{-m}{n} = \frac{(-m)(-n)}{mn} = 1$$

Division by anything other than zero is now defined as multiplication by the multiplicative inverse:

$$\frac{a}{n} \div \frac{l}{m} := \frac{a}{n} \cdot \frac{m}{l} \quad \text{and} \quad \frac{a}{n} \div \frac{-l}{m} := \frac{a}{n} \cdot \frac{-m}{l}$$

From the point of view of algebra, the rational numbers satisfy all the properties we could ever hope for. They are the first example of a **field**, which we now define in an abstract way.

Definition: Suppose F is a set, with a notion of "+" and "·" such that:

(a) Addition is associative.

(b) F has an additive identity (call it 0).

(c) Every element of F has an additive inverse (so subtraction works).

(d) Addition is commutative.

(e) Multiplication is associative.

(f) Multiplication distributes with addition.

(g) F has a multiplicative identity (call it 1).

(h) Every element other than 0 has a multiplicative inverse.

(i) Multiplication is commutative.

then we will say that F (together with its "+" and "·") is a **field**.

$\mathbf{N}$ and $\mathbf{Z}$ are not fields because they fail to have properties (b) and (h), respectively. (Property (h) is the only property that $\mathbf{Z}$ fails to have!)

Exercises: Using the formulas for addition and multipication, the cross multiplication rule and any property of the integers from §1, prove the following:

2.1 Addition of rational numbers is commutative.

2.2 Addition of rational numbers is associative.

2.3 Multiplication of rational numbers distributes with addition.

Example: Proof that multiplication of rational numbers is associative:

Let $a/n, b/m$ and c/l represent rational numbers. Then:

$$\left(\frac{a}{n} \cdot \frac{b}{m}\right) \frac{c}{l} = \frac{ab}{nm} \cdot \frac{c}{l} = \frac{(ab)c}{(nm)l},$$

$$\frac{a}{n} \left(\frac{b}{m} \cdot \frac{c}{l}\right) = \frac{a}{n} \cdot \frac{bc}{ml} = \frac{a(bc)}{n(ml)}.$$

But $(ab)c = a(bc)$ and $(nm)l = n(ml)$ because multiplication of integers is associative, so:

$$\frac{(ab)c}{(nm)l} = \frac{a(bc)}{n(ml)}$$

which gives us the desired equality of rational numbers.

2.4. If a, b, c, d are integers, prove that:

$$(ab)(cd) = (ad)(bc)$$

(we used this to prove multiplication of rational numbers is well-defined).

2.5. The Smallest Field! Suppose $F = \{0, 1\}$ with addition:

$$0 + 0 = 0,\ 0 + 1 = 1,\ 1 + 0 = 1,\ 1 + 1 = 0$$

and multiplication:

$$0 \cdot 0 = 0,\ 0 \cdot 1 = 0,\ 1 \cdot 0 = 0,\ 1 \cdot 1 = 1$$

Show that F (with this addition and multiplication) is a field!

Food for Thought: How would you prove the cross-multiplication rule?