Constructing $\mathbf{Q}$ from $\mathbf{Z}$

In these notes we will construct a set $\mathbf{Q}$ which has all the familiar properties the rational numbers. Assuming the Peano Axioms, we have already constructed the natural numbers $\mathbf{N}$ and the integers $\mathbf{Z}$, and have shown that these number systems have the properties we are accustomed to. Without further ado, we can henceforth make use of all the properties of integers that we're used to using.

The ordered-pair notation via which we constructed $\mathbf{Z}$ from $\mathbf{N}$ has served its purpose, and we will no longer use it. We simply regard $\mathbf{N}$ as a subset of $\mathbf{Z}$, by the identification of $\mathbf{N}$ with $\mathbf{Z}_+$. Thus for each $n \in \mathbf{N}$, the number that would have been denoted $f_+(n)$ in the "Constructing $\mathbf{Z}$ from $\mathbf{N}$" handout will henceforth simply be denoted n. Also, we will frequently omit the "dot" for multiplication; e.g. ab means $a \cdot b$.

Our construction of $\mathbf{Q}$ will mimic the construction of $\mathbf{Z}$. Recall that for $m, n \in \mathbf{N}$, we declared $n < m$ if there existed $p \in \mathbf{N}$ with $m = n + p$. The multiplicative analog of "n is less than m" is "n is a divisor of m". Specifically, we say n *divides* m, and write $n|m$, if there exists $p \in \mathbf{Z}$ such that $m = np$.

Exercises

1. Prove that every integer m is divisible by $1, -1, m$, and $-m$.
2. Prove that every integer divides 0, and that 0 does not divide any nonzero integer.
3. If $m \neq 0$ and $n|m$, then there is a unique $p \in \mathbf{Z}$ such that $m = np$.

Because of the uniqueness statement in exercise 3, given $n, m \in \mathbf{Z}$ such that $n \neq 0$ and $n|m$, we can unambiguously define an integer m/n by declaring m/n to be the unique integer p satisfying $m = np$. (Notice that if we remove the restriction $n \neq 0$, exercise 2 shows us why we get into trouble: "$m/0$" doesn't make sense if $m \neq 0$ because zero doesn't divide any nonzero integer, and doesn't make sense if $m = 0$ because there's no *unique* p such that $0 = 0 \cdot p$.)

Just as for $\mathbf{Z}$, where we introduced negative numbers by extending the notion of subtraction to handle the "smaller number minus bigger number" situation, we want now to develop a larger number system (larger than $\mathbf{Z}$, that is) in which we can extend the notion of division to cases in which the denominator is not a divisor of the numerator.

Let $Y = \{(m, n) \in \mathbf{Z} \times \mathbf{Z} \mid n \neq 0\}$. Define a relation $\sim$ on Y by

$$(m, n) \sim (m', n') \quad \text{iff } mn' = nm'.$$

The "thought process" is the following: thinking of (m, n) as m/n (not yet defined!), two fractions should be equal if, when you cross-multiply, you get equal integers.

Exercise

4. Prove that $\sim$ is an equivalence relation.

5. Prove that if $(m, n) \sim (m', n')$ and $m \neq 0$, then $m' \neq 0$.

We define $\mathbf{Q}$ to be the set of equivalence classes created by the above relation, and refer to the elements of $\mathbf{Q}$ as *rational numbers.*

Exercises

6. Prove that the map $g : \mathbf{Z} \to \mathbf{Q}$ defined by $g(n) = [(n, 1)]$ is injective but not surjective.

7. Prove that if $m, n \neq 0$ and $n|m$, then $[(m, n)] = g(m/n)$.

At this point we could change our notation, and define "m/n" (where n does not necessarily divide m) to mean $[(m, n)]$. However, using the more familiar notation at this point might lead us to make hidden assumptions, so we will stick to the clumsier notation for now.

8. Prove that the formula

$$[(m, n)] \cdot [(p, q)] = [(mp, nq)]$$

unambiguously defines an operation "$\cdot$" (henceforth called multiplication) on $\mathbf{Q}$. I.e., show that the "$[(mp, nq)]$" above is a rational number, and that this rational number depends only on the equivalence classes of (m, n) and (p, q), not on the specific choices of ordered pairs within the equivalence classes.

9. Similarly, prove that the formula

$$[(m, n)] + [(p, q)] = [(mq + np, nq)]$$

unambiguously defines an operation "+" (henceforth called addition) on $\mathbf{Q}$.

10. Prove that for all $m, n \in \mathbf{Z}$, $g(m + n) = g(m) + g(n)$ and $g(mn) = g(m) \cdot g(n)$.

Remark. Combining the results of exercises 6 and 10, we see that g "embeds" $\mathbf{Z}$ in $\mathbf{Q}$ similarly to the way the map f_+ of the "Constructing $\mathbf{Z}$ from $\mathbf{N}$" handout embeds $\mathbf{N}$ in $\mathbf{Z}$. The map g preserves all the arithmetical operations; e.g. if we add two integers and then think of the result as an element of $\mathbf{Q}$ (by taking g of the result) we get the same answer as if we first regard the integers as elements of $\mathbf{Q}$ (by taking g of them) and then adding.

11. Prove that $\mathbf{Q}$ is a field (see the textbook, p. 16). Hence the properties F1 through F10 listed on pp. 17-19 hold with $\mathbf{R}$ replaced by $\mathbf{Q}$.

12. Let $\mathbf{Z}_- = \{n \in \mathbf{Z} \mid -n \in \mathbf{Z}_+\}$. For nonzero $m, n \in \mathbf{Z}$, say that m and n *have the same sign* if both $m, n \in \mathbf{Z}_+$ or both $m, n \in \mathbf{Z}_-$; say that the *have the opposite sign* if one lies in $\mathbf{Z}_+$ and the other in $\mathbf{Z}_-$. Let $(m, n), (m', n') \in Y$, $m \neq 0$, and $(m, n) \sim (m', n')$; note that $m' \neq 0$ by exercise 5. Show that m' and n' have the same sign if and only if m and n have the same sign.

13. Define $\mathbf{Q}_+ = \{q \in \mathbf{Q} \mid q = [(m, n)]$ for some nonzero m, n having the same sign$\}$. Prove that $\mathbf{Q}$, with this choice of $\mathbf{Q}_+$, satisfies the order property on p. 19 of the textbook. (I.e. replace all the book's $\mathbf{R}_+$'s by $\mathbf{Q}_+$'s and show that conditions (1) and (2) in what the book calls Property VI hold.) Hence the properties O1 through O8 listed (for $\mathbf{R}$) on pp. 19-20 hold for $\mathbf{Q}$.

14. (This exercise should have been included in the "Constructing $\mathbf{Z}$ from $\mathbf{N}$ handout".) Given $x, y \in \mathbf{Z}$, declare $x < y$ if and only if $y - x \in \mathbf{Z}_+$. Prove that this order relation is consistent with the order relation "<" on $\mathbf{N}$. I.e., temporarily reverting to the notation of the previous handout, where $f_+ : \mathbf{N} \to \mathbf{Z}$ is the map that embeds $\mathbf{N}$ in $\mathbf{Z}$, show that for $m, n \in \mathbf{N}$ we have $m < n$ in $\mathbf{N}$ if and only if $f_+(m) < f_+(n)$ in $\mathbf{Z}$.

15. Prove that the order relation "<" on $\mathbf{Q}$ is consistent with the order relation "<" on $\mathbf{Z}$. I.e. show that for $m, n \in \mathbf{Z}$ we have $m < n$ in $\mathbf{Z}$ if and only if $g(m) < g(n)$ in $\mathbf{Q}$.

Having now proven all the properties of $\mathbf{Q}$ that we're accustomed to, and the consistency of these properties with the properties of $\mathbf{Z}$, we can henceforth identify $\mathbf{Z}$ with $g(\mathbf{Z})$, and thereby think of $\mathbf{Z}$ itself as a subset of $\mathbf{Q}$. Similarly, it is now safe to write m/n in place of $[(m, n)]$ for arbitrary $m, n \in \mathbf{Z}$ with $n \neq 0$. (Initially this notation could mean two things if $n|m$, since we have already given a meaning to the notation "m/n" in this special case. But exercise 7 shows that the two possible meanings are equivalent: $g($"old" $m/n) =$ "new"m/n.)