Homework 28: Due Monday, December 7

In the first four problems below, we outline the beginnings of a construction of the integers from the natural numbers. For these purposes, suppose that we've defined $\mathbb{N}$ equipped with two binary operations $+$ and $\cdot$ on $\mathbb{N}$ and an element $1 \in \mathbb{N}$ such that

1. $k + (m + n) = (k + m) + n$ for all $k, m, n \in \mathbb{N}$.
2. $m + n = n + m$ for all $m, n \in \mathbb{N}$.
3. $k \cdot (m \cdot n) = (k \cdot m) \cdot n$ for all $k, m, n \in \mathbb{N}$.
4. $m \cdot n = n \cdot m$ for all $m, n \in \mathbb{N}$.
5. $n \cdot 1 = n$ for all $n \in \mathbb{N}$.
6. $k \cdot (m + n) = k \cdot m + k \cdot n$ for all $k, m, n \in \mathbb{N}$.
7. If $k, m, n \in \mathbb{N}$ and $k + m = k + n$, then $m = n$.
8. If $k, m, n \in \mathbb{N}$ and $k \cdot m = k \cdot n$, then $m = n$.

We want to define the integers (including the operations of addition and multiplication on them) using what we've assumed above. Perhaps the following is the most natural idea. Take two "copies" of the natural numbers (one to represent the positive integers and one to represent the negative inters) and add a new element which we denote 0. This definition is straightforward, but when it comes time to define addition and multiplication (and verify their basic properties), it becomes necessary to break things into many annoying cases.

There is a more elegant way to construct the integers from the natural numbers along the lines of how we constructed the rationals from the integers. If our whole goal in passing from the natural numbers to the integers is to allow the taking of "differences" so that we can always find a solution to the equation $x + n = m$, why not build this idea right into the definition. We don't yet have the notion of a "difference", so we instead use an ordered pair to take it's place. Thus, we think of (m, n) as representing the magical "difference" of m take away n. Of course, this introduces the problem that one integer will have many different representations. For instance, $(1, 4)$ and $(5, 8)$ should be the same integer (intuitively they are both -3). This isn't really a problem because we can just define an equivalence relation.

Problem 1: Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by letting $(k, \ell) \sim (m, n)$ if $k + n = \ell + m$. Show that $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

Definition: We define $\mathbb{Z}$ to be the set of equivalence classes of $\mathbb{N} \times \mathbb{N}$ under $\sim$, i.e. $\mathbb{Z} = \{[(n, m)] : n, m \in \mathbb{N}\}$.

We now want to define $+$ on $\mathbb{Z}$. Suppose that we have two elements $a = [(k, \ell)]$ and $b = [(m, n)]$ of $\mathbb{Z}$. Intuitively, a should represent $k - \ell$ and b should represent $m - n$. Thus, it seems that we should define $a + b$ to be $[(k + m, \ell + n)]$ (which should represent $(k + m) - (\ell + n)$). In order to make this definition work, we need to verify that it doesn't matter which representatives we choose.

Problem 2: Suppose that $(k_1, \ell_1) \sim (k_2, \ell_2)$ and $(m_1, n_1) \sim (m_2, n_2)$. Show that $(k_1 + m_1, \ell_1 + n_1) \sim (k_2 + m_2, \ell_2 + n_2)$.

Problem 2 now allows us to define addition on $\mathbb{Z}$.

Definition: We define + on $\mathbb{Z}$ by letting $[(k,\ell)] + [(m,n)] = [(k+m, \ell+n)]$.

Definition: $0 = [(1,1)]$.

Problem 3: Verify the following:
a. $a + b = b + a$ for all $a, b \in \mathbb{Z}$.
b. $a + 0 = a$ for all $a \in \mathbb{Z}$.
c. For all $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ with $a + b = 0$.

We want to define $\cdot$ on $\mathbb{Z}$. Suppose that $a = [(k,\ell)]$ and $b = [(m,n)]$ are elements of $\mathbb{Z}$. Intuitively, a represents $k - \ell$ and b represents $m - n$. Thus, in the end we want $a \cdot b$ to represent $(k-\ell)(m-n) = km + \ell n - kn - \ell m = (km + \ell n) - (kn + \ell m)$, so it seems that we should define $a \cdot b$ to be $[(km + \ell n, kn + \ell m)]$. In order to make this definition work, we need to verify that it doesn't matter which representatives we choose.

Problem 4: Show that if $(k_1, \ell_1) \sim (k_2, \ell_2)$ and $(m_1, n_1) \sim (m_2, n_2)$, then $(k_1 m_1 + \ell_1 n_1, k_1 n_1 + \ell_1 m_1) \sim (k_2 m_2 + \ell_2 n_2, k_2 n_2 + \ell_2 m_2)$.

Now for something completely different. Let R be a commutative ring with identity. We define a ring $R[[x]]$ as follows. The elements of $R[[x]]$ are all expressions of the form

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots$$

where it is possible that infinitely many a_i are nonzero. Just like our definition of $R[x]$, do not think of these as functions, and in particular there is no convergence or anything you need to worry about because we are not "plugging in" value for x. Define addition and multiplication in the natural way, so

$$(\sum_{n=0}^{\infty} a_n x^n) + (\sum_{n=0}^{\infty} b_n x^n) = \sum_{n=1}^{\infty} (a_n + b_n) x^n$$

$$(\sum_{n=0}^{\infty} a_n x^n) \cdot (\sum_{n=0}^{\infty} b_n x^n) = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k b_{n-k}) x^n$$

It is straightforward (but a bit painful) to check that $R[[x]]$ is a commutative ring with identity containing $R[x]$ as a subring. $R[[x]]$ is called the *power series ring* over R.

Now consider the case when F is a field and we are looking at $F[[x]]$. There are many more units in $F[[x]]$ aside from the nonzero constants. For example

$$(1 - x)(1 + x + x^2 + \dots) = 1$$

so both of the elements on the left above are units in $F[[x]]$.

Problem 5: Let F be a field. Show that

$$\sum_{n=0}^{\infty} a_n = a_0 + a_1 x + a_2 x^2 + \dots$$

is a unit in $F[[x]]$ if and only if $a_0 \neq 0$.