Homework 12: Due Friday, December 6

Our field of fractions construction provides a way to define the rational numbers from the integers. In the first three 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 two elements $0, 1 \in \mathbb{N}$ such that the following properties hold:

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. $n + 0 = n$ for all $n \in \mathbb{N}$.
6. $n \cdot 1 = n$ for all $n \in \mathbb{N}$.
7. $k \cdot (m + n) = k \cdot m + k \cdot n$ for all $k, m, n \in \mathbb{N}$.
8. If $k, m, n \in \mathbb{N}$ and $k + m = k + n$, then $m = n$.
9. If $k, m, n \in \mathbb{N}$ and $k \cdot m = k \cdot n$, then either $k = 0$ or $m = n$.

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 its 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 $\mathbb{N} \times \mathbb{N}$. Use only the above properties of $\mathbb{N}$.

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

Problem 2: Explain how to define addition on $\mathbb{Z}$ and verify that your definition is well-defined. Also, explain how to define multiplication on $\mathbb{Z}$ (you need not verify that it is well-defined).

Problem 3: Determine, with proof, the additive and multiplicative identities in $\mathbb{Z}$.

One then goes on to use the above properties of $\mathbb{N}$ to prove that $\mathbb{Z}$ is an integral domain. Many of the proofs are completely straightforward (there are a couple of annoying ones), but we will not pursue that goal here. Instead, we move on to four different problems.

Problem 4: Let $C[0,1]$ be the set of all continuous functions $f\colon [0,1] \to \mathbb{R}$. Define $+$ and $\cdot$ on $C[0,1]$ to be the usual addition and multiplication of functions. That is, we define

$$(f+g)(x) = f(x) + g(x) \qquad \text{and} \qquad (f \cdot g)(x) = f(x) \cdot g(x)$$

With these operations, $C[0,1]$ is a ring (the additive identity is the constant function 0, and the multiplicative identity is the constant function 1). Let

$$I = \{f \in C[0,1] : f(0) = 0 = f(1)\}.$$

a. Show that I is an ideal of $C[0,1]$.
b. Show that I is not a prime ideal of $C[0,1]$.

Problem 5: Let R be an integral domain. Suppose that p is an irreducible element of R. Show that if $q \in R$ is an associate of p, then q is irreducible.

Problem 6:
a. Find, with proof, all irreducible polynomials in $\mathbb{Z}/2\mathbb{Z}[x]$ of degree 2 or 3.
b. Show that $x^5 + x^2 + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[x]$ is irreducible.

Problem 7: Determine whether the following polynomials are irreducible in $\mathbb{Q}[x]$.
a. $x^4 - 5x^3 + 3x - 2$.
b. $x^4 - 2x^3 + 2x^2 + x + 4$.