18.781 Problem Set 5

Due Monday, March 18 in class.

First problems are about the idea of a *product* of two rings. Definition of a ring is in the text, except that you should *ignore* the requirement that the ring have at least two elements. (That won't really come up in the problem.)

Suppose S_1 and S_2 are rings. The *product ring* $S_1 \times S_2$ is the set of all ordered pairs

$$S_1 \times S_2 = \{(s_1, s_2) \mid s_1 \in S_1,\ s_2 \in S_2\},$$

with addition and multiplication defined "coordinate by coordinate:"

$$(s_1, s_2) + (s_1', s_2') = (s_1 + s_1', s_2 + s_2'), \qquad (s_1, s_2) \cdot (s_1', s_2') = (s_1 \cdot s_1', s_2 \cdot s_2').$$

You may assume that this definition makes $S_1 \times S_2$ a ring, with

$$0_{S_1 \times S_2} = (0_{S_1}, 0_{S_2}), \qquad 1_{S_1 \times S_2} = (1_{S_1}, 1_{S_2}).$$

Recall also (what I *hope* I mentioned in class) that an *isomorphism* of rings R and R' is a homomorphism $\phi\colon R \to R'$ which is one-to-one and onto: that is, every element of R' is the image ("onto") of a unique ("one-to-one") element of R.

1. Suppose that R is any ring. Explain why every homomorphism from R to $S_1 \times S_2$ must be of the form

$$\phi(r) = (\phi_1(r), \phi_2(r)),$$

with ϕ_i a homomorphism from R to S_i.

Suppose n is a positive integer. Recall that $\mathbb{Z}/n\mathbb{Z}$ means the ring of residue classes of integers modulo n: if x is any integer, then the residue class of x modulo n is

$$C_x^n = \{x + nb | b \in \mathbb{Z}\} = \{x' \in \mathbb{Z} | n | (x - x')\}.$$

There are n residue classes modulo n, and

$$\mathbb{Z}/n\mathbb{Z} = \{C_x^n \mid x \in \mathbb{Z}\} = \{C_0^n, C_1^n, \dots, C_{n-1}^n\}.$$

(These are all things you already know; I write them just to fix notation.)

2. Suppose m and n are positive integers. Prove that there is a ring homomorphism

$$\phi_n^m\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

if and only if $m|n$; that in this case there is exactly *one* such homomorphism; and that the homomorphism is *onto.*

3. Suppose $m|n$ are positive integers, and consider the ring homomorphism

$$\phi_n^m\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

from #2. Prove that

$$\phi_n^m(C_x^n) = 0 \iff m|x.$$

4. Suppose that n is a positive integer and that $n = m_1 \cdot m_2$, with m_i a positive integer. Prove that

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

if and only if $\gcd(m_1, m_2) = 1$. (You are asked whether the ring of integers modulo n is isomorphic to the product of these two smaller rings.)