18.781 Problem Set 5 Solutions

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.

Any function f from R to $S_1 \times S_2$ is the same as a pair of functions f_i from R to S_i. This is just the definition of the set of $S_1 \times S_2$: giving an element (s_1, s_2) of $S_1 \times S_2$ is the same thing as giving an element s_1 of S_1 and an element s_2 of S_2. So suppose that $\phi = (\phi_1, \phi_2)$ is actually a homomorphism. This means three things:

$$\phi(r + r') = \phi(r) + \phi(r'), \quad \phi(r \cdot r') = \phi(r) \cdot \phi(r'), \quad \phi(1_R) = 1_S.$$

Let's write what those three things mean using the definition of $S_1 \times S_2$. On the left of the first equation we have

$$(\phi_1(r + r'), \phi_2(r + r'))$$

and on the right

$$(\phi_1(r), \phi_2(r)) + (\phi_1(r'), \phi_2(r')) = (\phi_1(r) + \phi_1(r'), \phi_2(r) + \phi_2(r)').$$

So the first equality means two equalities

$$\phi_1(r + r') = \phi_1(r) + \phi_1(r') \quad \text{and} \quad \phi_2(r + r') = \phi_2(r) + \phi_2(r') :$$

that each of ϕ_1 and ϕ_2 respects addition. In the same way, the second defining property means two equalities

$$\phi_1(r \cdot r') = \phi_1(r) \cdot \phi_1(r') \quad \text{and} \quad \phi_2(r \cdot r') = \phi_2(r) \cdot \phi_2(r') :$$

that each of ϕ_1 and ϕ_2 respects multiplication. Finally the third requirement means two requirements

$$\phi_1(1_R) = 1_{S_1} \quad \text{and} \quad \phi_2(1_R) = 1_{S_2} :$$

that each of ϕ_1 and ϕ_2 respects the multiplicative identity. This shows that **a ring homomorphism from R to $S_1 \times S_2$ is exactly the same thing as a pair of ring homomorphisms from R to S_i**, which is (slightly more than) what you were asked to show.

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

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

(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

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

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

The multiplicative identity of $\mathbb{Z}/n\mathbb{Z}$ is C_1^n. By definition, any ring homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ has to satisfy

$$\phi(C_1^n) = C_1^m.$$

If $1 \le x \le n$, then

$$C_x^n = \underbrace{C_1^n + \cdots + C_1^n}_{x \text{ summands}},$$

and therefore (since ϕ respects addition)

$$\begin{aligned} \phi(C_x^n) &= \phi\left(\underbrace{C_1^n + \cdots + C_1^n}_{x \text{ summands}}\right) \\ &= \underbrace{C_1^m + \cdots + C_1^m}_{x \text{ summands}} = C_x^m. \end{aligned}$$

So there is only one possible ring homomorphism, and (if it exists) it is onto. The only question is whether it exists; that is, whether the "definition"

$$\phi(C_x^n) = C_x^m$$

makes sense. "Makes sense" means that if $C_x^n = C_{x'}^n$, then $C_x^m = C_{x'}^m$. The first requirement is that n divides $x - x'$, and the second is that m divides $x - x'$. So "makes sense" means exactly

every integer divisible by n is also divisible by m.

This requirement is exactly the same as $m|n$.

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

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

What's shown in Problem 2 is that

$$\phi_n^m(C_x^n) = C_x^m,$$

and by definition this is $0 = C_0^m$ if and only if $m|x$.

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.)**

According to Problem 1, any homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to the product must be of the form

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

with $\phi_i\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$ a homomorphism. According to Problem 2, there is exactly one such homomorphism ϕ_i, namely

$$\phi_i(C_x^n) = C_x^{m_i}.$$

According to Problem 3,

$$\begin{aligned}
\phi(C_x^n) = 0 &\iff \phi_1(C_x^n) = 0 \quad \text{and} \quad \phi_2(C_x^n) = 0 \\
&\iff m_1|x \quad \text{and} \quad m_2|x \\
&\iff \operatorname{lcm}(m_1, m_2)|x \\
&\iff [n/\gcd(m_1, m_2)]|x.
\end{aligned}$$

We now look at two cases. Suppose first that $\gcd(m_1, m_2) = 1$. Then

$$\phi(C_x^n) = 0 \iff n|x \iff C_x^n = C_0^n = 0.$$

Furthermore

$$\begin{aligned}
\phi(C_x^n) = \phi(C_y^n) &\iff \phi(C_x^n - C_y^n) = 0 \\
&\iff \phi(C_{x-y}^n) = 0 \\
&\iff n|(x-y) \iff C_x^n = C_y^n;
\end{aligned}$$

so the homomorphism ϕ is one-to-one (distinct elements of $\mathbb{Z}/n\mathbb{Z}$ have distinct images). Because $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ both have exactly $n = m_1 \cdot m_2$

elements, the fact that ϕ is one-to-one means it must also be onto. So in this case ϕ is an isomorphism, as we wished to show.

For the second case, suppose that $\gcd(m_1, m_2) > 1$, so that

$$d =_{\text{def}} \operatorname{lcm}(m_1, m_2) = n/\gcd(m_1, m_2) < n.$$

According to what we proved above,

$$\phi(C_d^n) = 0 = \phi(C_0^n);$$

so the distinct elements C_d^n and C_0^n have the same image, so ϕ is not one-to-one. So ϕ is not an isomorphism, as we wished to show.