Math 113 **Fall 2015**

Homework #10

Nikhil Unni

1. For all problems, $R = \mathbb{Z}_3[x]$.

   (a) Let I be the subset of R consisting of the zero polynomial, plus the polynomials for which every nonzero term has degree at least 2. Prove that I is an ideal of R.

   First, we have to show that I is a valid additive subgroup of R. We know that 0 is in I, so it's nonempty. Next, for any $a, b \in I$ then $a + b^{-1}$ is the sum of many nonzero and non-one power monomials. Terms may cancel out, since elements have additive inverses. But since we can never degrade in power, there's no way to get any power 1 terms. Similarly, we can get a zero power term, but it is only the result of there being no higher power terms at all, making it 0, which is a valid element in I as well. Thus, $a + b^{-1}$ must be in I.

   Next, we can show it's an ideal. For some $i \in I, r \in R$, then $ir = ri \in I$ as well. $ir = ri$ because the ring is commutative. So for some:

   $$ir = (a_2x^2 + a_3x^3 + \ldots)(b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots)$$

   Looking at the lowest terms of i and r, we see that the lowest term in ir has to be from multiplying the lowest terms. **Worst case**, this would be $a_2b_0x^2$, which is power 2, meaning that $ir \in I$. If a_2 or b_0 are 0, then the power of our lowest term only increases, but it's still in I.

   (b) The factor ring R/I consists of (additive) cosets of the form $f(x)+I$, where $f(x) \in \mathbb{Z}_3[x]$. Prove that two polynomials in $\mathbb{Z}_3[x]$ belong to the same coset of I if and only if they have the same remainder after division by the polynomial x^2, as prescribed by the Division Algorithm.

   By the Division Algorithm, if dividing some polynomial $f(x)$ by another polynomial $g(x)$, the result is that $f(x) = g(x)q(x) + r(x)$, where the degree of $r(x)$ is less than the degree of $g(x)$. So if we have some $m(x), n(x) \in R$, then:

   $$m(x) = x^2 * q_1(x) + r_1(x)$$

$$n(x) = x^2 * q_2(x) + r_2(x)$$

And we know that $deg(r_1(x)) < 2$ and $deg(r_2(x)) < 2$. So they can only contain power 0 and power 1 terms.
So the problem can be restated as: for two polynomials, $(a_0 + a_1x + a_2x^2 + \ldots), (b_0 + b_1x + b_2x^2 + \ldots) \in R$, they are in the same coset iff $a_0 = b_0$ and $a_1 = b_1$. This is because the division by x^2 leaves only the first two terms for equality checking.

If $a, b \in R$ are in the same coset, then their coset can be uniquely represented by their lowest term + I. This is some $(a_0 + a_1x + a_2x^2 + \ldots) + I$. However, we know this is not the lowest term, since all terms power 2 and above can be "absorbed" by I. If you add a singular term of power 2 or above to I, you'll land in another term in I, because it is a valid additive subgroup. So the lowest representation becomes $a_0 + a_1x + I$ when you absorb all the higher terms away. Since they both have the same lowest representation, both of their power 0 and power 1 terms must equate, i.e. $a_0 = b_0$ and $a_1 = b_1$.

If $a, b \in R$ have the same power 0 and power 1 terms, then their cosets are just $a_0 + a_1x + I$ and $b_0 + b_1x + I$, for the reason we just mentioned. Because $(a_0 + a_1x = b_0 + b_1x)$, they are referring to the same coset, meaning that a and b share the same coset.

(c) How many elements are in the ring R/I?

There are 9 elements in R/I. As we described in part (b), the unique "lowest" representation of a coset is its power 0 term + its power 1 term + I. So each coset is represented by some $a_0 + a_1x + I$. And since there are only 3 possible values for a_0 and a_1, and the values are independent, we have $3 * 3 = 9$ total choices.

2. This problem is a continuiation of problem 1, so $R = \mathbb{Z}_3[x]$, and I is the same ideal as above.

   (a) Write out the multiplication table for R/I.

	I	1+I	2+I	x+I	1+x+I	2+x+I	2x+I	1+2x+I	2+2x+I
I	I	I	I	I	I	I	I	I	I
1+I		1+I	2+I	x+I	1+x+I	2+x+I	2x+I	1+2x+I	2+2x+I
2+I			1+I	2x+I	2+2x+I	1+2x+I	x+I	2+x+I	1+x+I
x+I				I	x + I	2x + I	I	x + I	2x + I
1+x+I					1+2x+I	2+I	2x+I	1+I	2+x+I
2+x+I						1+x+I	x+I	2+2x+I	1+I
2x+I							I	2x+I	x + I
1+2x+I								1+x+I	2+I
2+2x+I									1+2x+I

(b) Determine whether each element of R/I is a unit, a zero divisor, or neither.

I – Neither, it is the 0 element
$1 + I$ – Unit
$2 + I$ – Unit
$x + I$ – Zero divisor
$1 + x + I$ – Unit
$2 + x + I$ – Unit
$2x + I$ – Zero divisor
$1 + 2x + I$ – Neither
$2 + 2x + I$ – Neither

All of these were obtained by just looking at the multiplication table, and searching for I or $1 + I$ in the rows.

3. Prove that R/I and $\mathbb{Z}_3 \times \mathbb{Z}_3$ are isomorphic as additive groups, but not as rings.

Let $\phi : \mathbb{Z}_3 \times \mathbb{Z}_3 \to R/I$ be a homomorphism where:

$$\phi((\bar{a}, \bar{b})) = a + bx + I$$

It's a valid homomorphism because:

$$\phi((a_1, b_1)) + \phi((a_2, b_2)) = (a_1 + b_1x + I) + (a_2 + b_2x + I)$$

$= a_1 + a_2 + b_1x + b_2x + I = (a_1 + a_2) + (b_1 + b_2)x + I = \phi((a_1, b_1) + (a_2, b_2))$

Because our polynomial ring is based on $\mathbb{Z}_3$, the modulo arithmetic still holds properly, as expected.

Also, $ker\phi$ is just $\{(0, 0)\}$, since no other element can map to $0 + 0x + I$. And the mapping is one-to-one and onto, because every element in R/I

can be mapped to – just pick the right $a, b \in \mathbb{Z}_3$. And those a and b are unique because both sides are mod 3. If both sides have 9 elements, and every element in R/I is being mapped to, by the Pidgeonhole Principle every mapping must be unique. Thus, the two rings are isomorphic as additive groups.

However, they are not isomorphic as rings, because the multiplication properties are completely different. $\mathbb{Z}_3$ has no zero divisors, and so $\mathbb{Z}_3 \times \mathbb{Z}_3$ has no zero divisors either. If you take the only two nonzero terms ($\bar{1}$ and $\bar{2}$) and multiply them, they don't yield 0, and since multiplication is done component-wise, there can't be any zero divisors in $\mathbb{Z}_3 \times \mathbb{Z}_3$. However, as we've shown in 2b, there are zero divisors in R/I. Thus, the two cannot be isomorphic rings.