Math 721 - Homework 13 Solutions

1. Find generators for the kernels of the following ring homomorphisms: (a) $\phi : \mathbb{R}[x] \to \mathbb{C}$ defined by $\phi(f) = f(2+i)$. (b) $\phi : \mathbb{Z}[x] \to \mathbb{R}$ defined by $\phi(f) = f(1+\sqrt{2})$. (c) $\phi : \mathbb{C}[x,y,z] \to \mathbb{C}[t]$ defined by $\phi(f(x,y,z)) = f(t,t^2,t^3)$.

(a) Notice that $(2+i)^2 = 4+2i+i^2 = 4+2i+(-1) = 3+2i$. Thus, $(2+i)^2 - 2(2+i) - 1 = 0$ and so $x^2-2x-1 \in \ker\phi$.

Claim: We have $\ker\phi = (x^2-2x-1)$.

Proof: It is clear that since $x^2-2x-1 \in \ker\phi$, $(x^2-2x-1) \subseteq \ker\phi$. We will show that $\ker\phi \subseteq (x^2-2x-1)$.

If $p(x) \in \ker\phi$, we can write $p(x) = (x^2-2x-1)q(x) + r(x)$, where $r(x)$ has degree less than or equal to 1. (This is because x^2-2x-1 has nonzero, so we can use Proposition 11.2.9). Then since $p(x)$, (x^2-2x-1) are both in $\ker\phi$, $r(x) \in \ker\phi$. We have $r(x) = ax+b$ and so $r(2+i) = a(2+i)+b = (2a+b)+ai = 0$. Thus, $a=0$ and $2a+b=0$ and so $a=b=0$. Thus, $r=0$ and so $p(x) = (x^2-2x-1)q(x)$. Hence, $p(x) \in (x^2-2x-1)$.

(b) We have $(1+\sqrt{2})^2 = 2+2\sqrt{2}+2 = 4+2\sqrt{2}$, so $(1+\sqrt{2})^2 - 2(1+\sqrt{2}) - 2 = 0$. Thus, $x^2-2x-2 \in \ker\phi$.

Claim: We have $\ker\phi = (x^2-2x-2)$.

Proof: The same sort of argument that we gave above in (a) proves this. Notice that we can still apply Proposition 11.2.9 because the leading coefficient of x^2-2x-2 is a unit in $\mathbb{Z}$.

(c) Notice that $y-x^2$ and $z-x^3$ are in $\ker\phi$ since $\phi(y-x^2) = t^2-(t)^2 = 0$ and $\phi(z-x^3) = t^3-(t)^3 = 0$.

Claim: We have $\ker\phi = (y-x^2, z-x^3)$.

Proof: Again, it is clear that $(y-x^2, z-x^3) \subseteq \ker\phi$. We'll prove that $\ker\phi \subseteq (y-x^2, z-x^3)$. Let $p(x,y,z) \in \ker\phi$. We will think of $p(x,y,z)$ as a polynomial in the single variable z (with coefficients that are polynomials in x and y - we'll write this as $p(x,y,z) \in \mathbb{C}[x,y][z]$).

We can divide $p(x,y,z)$ by $z-x^3$. We can do this because the leading coefficient of z, which is 1 is a unit in $\mathbb{C}[x,y]$. The remainder will be zero, or have degree zero in z. Thus, we get

$$p(x,y,z) = (z-x^3)q(x,y,z) + r(x,y)$$

(I wrote the remainder as $r(x, y)$ to indicate that it is a "constant" in the polynomial ring $\mathbb{C}[x, y][z]$, namely a polynomial only in x and y.) It's not necessarily the case that $r(x, y) = 0$, but $r(x, y)$ is in the kernel (since $p(x, y, z)$ and $z - x^3$ are).

Now, we will take $r(x, y)$ and think of it as an element of $\mathbb{C}[x][y]$ (polynomials in y with coefficients that are polynomials in x). We will divide $r(x, y)$ by $y - x^2$, and again get a remainder of degree zero in y (that is, a "constant", which means a polynomial only in x). Hence, we have

$$r(x, y) = (y - x^2)s(x, y) + u(x).$$

Since $r(x, y)$ and $y - x^2$ are in $\ker\phi$, so is $u(x)$. This means that $\phi(u(x)) = u(t) = 0$. This means that $u(x) = 0$. Putting all of this together we have

$$\begin{aligned} p(x, y, z) &= (z - x^3)q(x, y, z) + r(x, y) \\ &= (z - x^3)q(x, y, z) + (y - x^2)s(x, y) \end{aligned}$$

and so $p(x, y, z) \in (z - x^3, y - x^2) = \{(z - x^3)a_1(x, y, z) + (y - x^2)a_2(x, y, z) : a_1(x, y, z), a_2(x, y, z) \in \mathbb{C}[x, y, z]\}$ and thus, $\ker\phi \subseteq (z - x^3, y - x^2)$.

2. Let R be a ring of prime characteristic p (see the last paragraph of Section 11.3 for a review of this definition). Prove that the map $\phi : R \to R$ given by $\phi(x) = x^p$ is a ring homomorphism. (It is called the Frobenius map.)

Since R has prime characteristic,

$$p = \overbrace{1 + 1 + 1 + \cdots + 1}^{p \text{ times}} = 0.$$

Thus, for any $r \in R$, $px = 0x = 0$. Now, we have

$$\phi(a + b) = (a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

We have $\binom{p}{k} = \frac{p!}{k!(p-k)!} = p\frac{(p-1)!}{k!(p-k)!}$ is a multiple of p if $0 < k < p$ (for these values of k, $k!$ and $(p - k)!$ don't have any factors of p in them). Thus, $\binom{p}{k}a^k b^{p-k} = 0$ if $0 < k < p$ and so

$$\phi(a + b) = a^p + b^p = \phi(a) + \phi(b).$$

We have $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$, and $\phi(1) = 1^p = 1$. Thus, ϕ is a ring homomorphism.

3. Let I and J be ideals of a ring R. Prove that the intersection $I \cap J$ is an ideal. Show by example that the set of products $\{xy|x \in I, y \in J\}$

need not be an ideal, but that the set of finite sums $\sum_{v=1}^{k} x_v y_v$ of products of elements of I and J is an ideal. This ideal is called the *product ideal*, and is denoted IJ. Is there a relation between IJ and $I \cap J$?

If a and b are both in $I \cap J$, then $a+b \in I$ and $a+b \in J$ since I and J are ideals, and so $a+b \in I \cap J$. If $a \in I \cap J$ and $r \in R$, then $ar \in I$ and $ar \in J$ since I and J are ideals, and so $ar \in I \cap J$. This proves that $I \cap J$ is an ideal.

Let $R = \mathbb{Z}[x]$, $I = J = (2, x)$. Then, $\{yz | y \in I, z \in J\}$ contains x^2 and 4. However, x^2+4 is an irreducible polynomial. [If not, then any factor of it with degree less than 2 must have leading coefficient a unit, and so Proposition 11.2.9 implies that the factor must be a linear factor, and this means that x^2+4 has an integer root. This is impossible since $x^2+4 > 0$ for all $x \in \mathbb{Z}$.] This shows that x^2+4 is not in the set $\{yz | y \in I, z \in J\}$.

On the other hand, if $a = \sum_{v=1}^{k} x_v y_v$ and $b = \sum_{v=k+1}^{l} x_v y_v$ are both finite sums of products of elements of I and J, then

$$a + b = \sum_{v=1}^{l} x_v y_v$$

is also a finite sum of products, and so IJ is closed under addition. Also, if $r \in R$, then

$$ar = \sum_{v=1}^{k} x_v (y_v r)$$

is also a finite sum of products of elements in IJ because $y_v \in J$ implies that $y_v r \in J$. Hence, IJ is an ideal.

In general, if $a \in IJ$, then

$$a = \sum_{v=1}^{k} x_v y_v$$

for $x_v \in I$ and $y_v \in J$. Since $x_v y_v \in I$ for all v, it follows that $a \in I$. Similar reasoning shows that $a \in J$. Thus, $a \in I \cap J$ and so $IJ \subseteq I \cap J$. This is all one can say in general, for example, if $I = (2)$ and $J = (3)$, then $IJ = (6)$ and $I \cap J = (6)$. However, if $I = (2)$ and $J = (2)$, then $IJ = (4)$ and $I \cap J = (2)$. Here $I \cap J$ is strictly larger than IJ.

4. Identify the following rings: (a) $\mathbb{Z}[x]/(x^2-3, 2x+4)$ (b) $\mathbb{Z}[x]/(6, 2x-1)$ (c) $\mathbb{Z}[x]/(x^2+3, 5)$. [Here, I'm not necessarily asking you to give a simple name for the quotient ring, I'm asking you to describe the

ring as accurately as possible. You should also answer the following questions: Is it finite? Is it infinite? Is it a field?]

(a) Let $I = (x^2 - 3, 2x + 4)$ and let $f = x^2 - 3$ and $g = 2x + 4$. Then, $gx - 2f = 2x^2 + 4x - 2(x^2 - 3) = 4x + 6$. Thus, $2g - (gx - 2f) = (4x + 8) - (4x + 6) = 2 \in I$. Define $\phi : \mathbb{Z}[x] \to \mathbb{F}_2[x]$ by taking

$$p(x) = \sum_{n=0}^{k} c_n x^n$$

and letting

$$\phi(p(x)) = \sum_{n=0}^{k} (c_n \bmod 2) x^n \in \mathbb{F}_2[x].$$

It is straightforward to check that ϕ is a surjective homomorphism, and $\ker \phi = \{\sum_{n=0}^{k} c_n x^n : c_n \text{ is even for all } n\} = (2)$. Thus, if $R = \mathbb{Z}[x]$, $\mathcal{R} = \mathbb{F}_2[x]$ and $\mathcal{I} = \phi(I) = (x^2 - 3)$, then by the correspondence theorem, we have that $R/I \approx \mathcal{R}/\mathcal{I} \approx \mathbb{F}_2[x]/(x^2 - 3)$.

An arbitrary element of $\mathbb{F}_2[x]/(x^2 - 3)$ can be represented as $r(x) + \mathcal{I}$, and $r(x)$ is unique up to addition by a multiple of $x^2 - 3$. Since any polynomial $h(x) \in \mathbb{F}_2[x]$ can be represented uniquely in the form

$$h(x) = (x^2 - 3)q(x) + r(x)$$

where $r = 0$ or $\deg r \leq 1$, it follows that $\mathbb{F}_2[x]/(x^2 - 3)$ has four elements: $\mathcal{I}$, $1 + \mathcal{I}$, $x + \mathcal{I}$ and $x + 1 + \mathcal{I}$. This ring is not a field, since

$$(x + 1 + \mathcal{I})^2 = x^2 + 2x + 1 + \mathcal{I} = (x^2 - 3) + (2x + 4) + \mathcal{I} = \mathcal{I},$$

and so $(x + 1 + \mathcal{I})^2 = 0$ in $\mathcal{R}/\mathcal{I}$.

(b) If $I = (6, 2x - 1)$, we have that $6x - 3(2x - 1) = 3 \in I$. Thus, $I = (3, 2x - 1)$. A similar argument to the one in part (a) shows that $\mathbb{Z}[x]/I \approx \mathbb{F}_3[x]/(2x - 1)$. Now, 2 is a unit in $\mathbb{F}_3$, and so we can represent every element in $\mathbb{F}_3[x]/(2x - 1)$ as $a + \mathcal{I}$, where $\mathcal{I} = (2x - 1) \subseteq \mathbb{F}_3[x]$. This shows that $\mathbb{Z}[x]/I \approx \mathbb{F}_3[x]/\mathcal{I} \approx \mathbb{F}_3$, and so this ring is a field.

(c) If $I = (x^2 + 3, 5)$, then as in part (a), we have $\mathbb{Z}[x]/I \approx \mathbb{F}_5[x]/(x^2 + 3)$. The polynomial $x^2 + 3$ is irreducible in $\mathbb{F}_5[x]$. [If it wasn't, it would have a linear factor, and hence have a root in $\mathbb{F}_5$. However, if $f(x) = x^2 + 3$, then $f(0) = 3$, $f(1) = 4$, $f(2) = 2$, $f(3) = 2$, $f(4) = 4$.] So $\mathcal{I} = (x^2 + 3) \subseteq \mathbb{F}_5[x]$, is an ideal generated by an irreducible polynomial. Thus, $\mathcal{I}$ is a maximal ideal of $\mathbb{F}_5[x]$, and so $\mathbb{F}_5[x]/\mathcal{I}$ is a field. Every element of $\mathbb{F}_5[x]/\mathcal{I}$ can be represented in the form $a + bx + \mathcal{I}$ (from the division algorithm, since $\mathcal{I}$ is generated by a polynomial of degree 2). Thus, $\mathbb{F}_5[x]/\mathcal{I}$ is a field of order 25.

5. Are the rings $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ isomorphic?

I gave one argument for this in class. I'll give a different one here, based on the units in the two rings. If we let $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-7}]$ be given by $\phi(p(x)) = p(\sqrt{-7})$, then ϕ is a surjective ring homomorphism, and $x^2+7 \in \ker\phi$. Let $I = (x^2+7)$. If we take $p(x) \in \ker\phi$, we can write

$$p(x) = (x^2+7)q(x) + r(x)$$

where $r = 0$ or $\deg r \leq 1$, and we have $r(x) \in \ker\phi$ (since $r(x) = p(x) - (x^2+7)q(x)$ is the difference of two things in the kernel). Now, if

$$r(x) = ax + b$$

then $r(\sqrt{-7}) = a\sqrt{-7} + b$, and this equals zero if and only if $a = b = 0$. Hence, $\ker\phi = (x^2+7)$. The first isomorphism theorem for rings then guarantees that $\mathbb{Z}[x]/(x^2+7) \cong \mathbb{Z}[\sqrt{-7}]$. Note that 2 is NOT a unit in $\mathbb{Z}[\sqrt{-7}]$ since $\frac{1}{2} \notin \mathbb{Z}[\sqrt{-7}]$.

On the other hand, 2 is a unit in the ring $\mathbb{Z}[x]/(2x^2+7)$ since if $J = (2x^2+7)$, then

$$\alpha = (x^2+4) + J \in \mathbb{Z}[x]/J$$

has $2\alpha = (2x^2+8) + J = (1+J) + (2x^2+7) + J = 1 + J$. Since $1+J$ is the multiplicative identity in $\mathbb{Z}[x]/J$, it follows that 2 is a unit in $\mathbb{Z}[x]/J$.

Finally, we will show that if two rings R_1 and R_2 are isomorphic, and 2 is a unit in R_1, then 2 must be a unit in R_2. This is because if $2a = 1$ in R_1, and $\phi : R_1 \to R_2$ is an isomorphism, then if we let $b = \phi(a)$, we have

$$2b = b + b = \phi(a) + \phi(a) = \phi(2a) = \phi(1) = 1$$

and so $2b = 1$ in R_2 as well. Thus, 2 is a unit in R_2.

Since 2 is not a unit in $\mathbb{Z}[x]/(x^2+7)$ and 2 is a unit in $\mathbb{Z}[x]/(2x^2+7)$, these two rings cannot be isomorphic.