Math 4000 – Solutions to practice problems for Exam #3

Here are some more problems to try.

4.1.5. a. First, suppose that $I = \langle f(x) \rangle \subseteq J = \langle g(x) \rangle$. Then

$$f(x) \in \langle f(x) \rangle \subseteq \langle g(x) \rangle.$$

Hence, $g(x) \mid f(x)$.

Now suppose that $f(x) \mid g(x)$. Then $f(x) \in \langle g(x) \rangle$. Since $\langle g(x) \rangle$ absorbs multiplication, $a(x)f(x) \in \langle g(x) \rangle$ for all $a(x) \in F[x]$. Letting $a(x)$ range over all elements of $F[x]$, it follows that $\langle f(x) \rangle \subseteq \langle g(x) \rangle$.

b. Since $F[x]$ is a PIR, an arbitrary ideal I has the form $\langle g(x) \rangle$. If $I = \langle g(x) \rangle$ contains $(x^2+x-1)^3(x-3)^2$, then $g(x)$ divides $(x^2+x-1)^3(x-3)^2$. Now x^2+x-1 and $x-3$ are irreducible in $\mathbf{Q}[x]$. So — up to nonzero constant factors (which are units in $\mathbf{Q}[x]$) — the possibilities for $g(x)$ are

$$(x^2+x-1)^a(x-3)^b, \quad \text{where} \quad a = 0, 1, 2, \text{ or } 3, \quad b = 0, 1, \text{ or } 2.$$

Thus, $I = \langle g(x) \rangle = \langle (x^2+x-1)^a(x-3)^b \rangle$ for some choice of a, b as above. Moreover, the $(3+1)(2+1) = 12$ ideals obtained in this way are distinct. This follows from the result in homework that two polynomials generate the same ideal of $F[x]$ if and only if they differ by nonzero constant factors.

4.1.8. First, we show that if the kernel is nonzero, then ϕ is not injective. Let $r \in R$ be a nonzero element of $\ker \phi$. Then $\phi(r) = \phi(0)$ despite the fact that $r \neq 0$. Thus, ϕ is not injective.

Now suppose that the kernel is $\langle 0 \rangle$. Whenever $\phi(r) = \phi(s)$, we have $\phi(r-s) = \phi(r) + \phi(-s) = \phi(r) - \phi(s) = 0$. So $r - s \in \ker \phi = \langle 0 \rangle$, forcing $r = s$. Thus, ϕ is injective.

4.1.16. a. We check that $\phi^{-1}(J)$ has the three definining properties of an ideal.

$0 \in \phi^{-1}(J)$: Since $\phi(0) = 0 \in J$, we have $0 \in \phi^{-1}(J)$.

$\phi^{-1}(J)$ is closed under $+$: Suppose $a, b \in \phi^{-1}(J)$. Then $\phi(a), \phi(b) \in J$. Since J is closed under $+$,

$$\phi(a+b) = \phi(a) + \phi(b) \in J,$$

and so $a + b \in \phi^{-1}(J)$.

$\phi^{-1}(J)$ absorbs multiplication: Suppose $a \in \phi^{-1}(J)$ and $r \in R$. Then $\phi(a) \in J$. Since J absorbs multiplication,

$$\phi(ra) = \phi(r)\phi(a) \in J,$$

so that $ra \in \phi^{-1}(J)$.

b. Suppose that ϕ maps onto S. We prove that $\phi(I)$ has the three defining properties of an ideal.

$0 \in \phi(I)$: Since $0 \in I$, we have $0 = \phi(0) \in \phi(I)$.

$\phi(I)$ is closed under $+$: Suppose $a, b \in \phi(I)$. Then $a = \phi(r)$ and $b = \phi(s)$, where $r, s \in I$. Since I is closed under $+$, we have $r + s \in I$, and hence

$$a + b = \phi(r) + \phi(s) = \phi(r + s) \in \phi(I).$$

$\phi(I)$ absords multiplication: Let $a \in \phi(I)$ and $s \in S$. Then $a = \phi(r_1)$ where $r_1 \in I$. Since ϕ is surjective, there is an $r_2 \in R$ with $\phi(r_2) = s$. Since I absorbs multiplication and $r_1 \in I$, we have $r_2 r_1 \in I$. Thus,

$$s \cdot a = \phi(r_2)\phi(r_1) = \phi(r_2 r_1) \in \phi(I).$$

To see that the surjectivity hypothesis is necessary, let $R = \mathbf{Z}$ and $S = \mathbf{Q}$. Let $\phi\colon \mathbf{Z} \to \mathbf{Q}$ be the identity map on $\mathbf{Z}$: that is, $\phi(n) = n$ for all $n \in \mathbf{Z}$. Then $I = \mathbf{Z}$ is an ideal of $\mathbf{Z}$, but $\phi(I) = \mathbf{Z}$ is not an ideal of $\mathbf{Q}$. (Make sure you see why!)

c. We show that $\phi(\langle a \rangle)$ both contains and is contained in $\langle \phi(a) \rangle$.

$\phi(\langle a \rangle) \subseteq \langle \phi(a) \rangle$: Let $x \in \langle a \rangle$. Then $x = ra$ for some $r \in R$. Hence, $\phi(x) = \phi(r)\phi(a)$, which is an element of $\langle \phi(a) \rangle$. So $\phi(\langle a \rangle) \subseteq \langle \phi(a) \rangle$.

$\langle \phi(a) \rangle \subseteq \phi(\langle a \rangle)$: Let $x \in \langle \phi(a) \rangle$. Then $x = s\phi(a)$ for some $s \in S$. Since ϕ is surjective, there is an $r \in R$ with $\phi(r) = s$. So

$$x = \phi(r)\phi(a) = \phi(ra) \in \phi(\langle a \rangle).$$

Thus, $\langle \phi(a) \rangle \subseteq \phi(\langle a \rangle)$.

4.1.20. Yes, I is the kernel of the homomorphism $\phi\colon R \to R/I$ sending a to $\overline{a}$.

We check this: If $\phi(r) = 0$, then $\overline{r} = \overline{0}$ in R/I. Now $\overline{r} = \overline{0}$ if and only if $r \equiv 0 \pmod{I}$; equivalently, $r \in I$. Thus, $\ker \phi = I$.

4.2.2(c). Assume first that R and S are not the zero ring. (Remember that this is part of the book's definition of a ring.) Then $R \times S$ is never an integral domain: the product of the nonzero elements $(1_R, 0_S)$ and $(0_R, 1_S)$ is $(0_R, 0_S)$.

On the other hand, if R is the zero ring, then it is easy to prove that $R \times S$ is a domain exactly when S is a domain.

4.2.11(a,b). a. Neither isomorphism holds.

In $\mathbf{Z}_2[x]/\langle x^2 \rangle$, every element when added to itself yields the additive identity. But this is not the case in $\mathbf{Z}_4$. So the first isomorphism fails.

In $\mathbf{Z}_2[x]/\langle x^2 \rangle$, there is a nonzero element whose square is zero, namely $\overline{x}$. But in $\mathbf{Z}_2 \times \mathbf{Z}_2$, there is no such element. So the second isomorphism also fails.

b. Working out the multiplication table for $\mathbf{Z}_2[x]/\langle x^2 + x \rangle$, one can see that no nonzero element squares to zero. But in $\mathbf{Z}_4$, there is such an element, namely $\overline{2}$. So the first isomorphism fails.

However, the second isomorphism holds. Namely, consider the map $\phi\colon \mathbf{Z}_2[x]/\langle x^2 + x \rangle \to \mathbf{Z}_2 \times \mathbf{Z}_2$ given by $\phi(\overline{f(x)}) = (f(\overline{0}), f(\overline{1}))$. It is straightforward to prove this is an isomorphism (compare with the proof of 5(d) below).

4.2.12. We are given that $I + \langle a \rangle = R$. Since $1 \in R$, it follows that there is a solution to

$$x + ar = 1,$$

where $x \in I$ and $r \in R$. Looking at this equation modulo I yields

$$\overline{x} + \overline{a} \cdot \overline{r} = \overline{1}.$$

Since $\overline{x} = \overline{0}$, we have $\overline{ar} = \overline{1}$, and so $\overline{a}$ has an inverse in R/I, namely $\overline{r}$.

1. Let R be a commutative ring. If I and J are two ideals of R, define

$$I + J = \{a + b : a \in I, b \in J\}.$$

Show that $I + J$ is an ideal of R and that $I + J$ contains both I and J.

Proof. We first check that $I + J$ is an ideal by verifying the three definining properties:

$0 \in I + J$: This is clear, since $0 \in I, 0 \in J$, and $0 = 0 + 0$.

$I + J$ is closed under $+$: Let a_1, a_2 be arbitrary elements of $I + J$. By the definition of $I + J$, we can write $a_1 = \alpha_1 + \beta_1$, where $\alpha_1 \in I$ and $\beta_1 \in J$, and $a_2 = \alpha_2 + \beta_2$, where $\alpha_2 \in I$ and $\beta_2 \in J$. Thus,

$$a_2 + b_2 = (\alpha_1 + \alpha_2) + (\beta_1 + \beta_2).$$

The first parenthesized term on the right is in I, since I is closed under $+$, while the second is in J, since J is closed under $+$. Thus, $a_2 + b_2 \in I + J$.

Absorbs multiplication: Let $a \in I + J$. Then $a = \alpha + \beta$, where $\alpha \in I$ and $\beta \in J$. For any $r \in R$,

$$ra = r\alpha + r\beta.$$

Now $r\alpha \in I$, since I absorbs multiplication, and $r\beta \in J$, since J absorbs multiplication. So $ra \in I + J$.

It remains to show that $I + J$ contains both I and J. But this is easy: Since $0 \in J$, for each $\alpha \in I$ we have $\alpha = \alpha + 0 \in I + J$. Thus, $I \subseteq I + J$. Similarly, $J \subseteq I + J$. $\square$

Follow-up: If $R = \mathbf{Z}$, $I = \langle a \rangle$, and $J = \langle b \rangle$, where a, b are positive integers, which ideal is $I + J$? e.g., what is $\langle 19 \rangle + \langle 133 \rangle$?

Solution. Notice that $\langle a \rangle + \langle b \rangle$ consists of all integers of the form $ax + by$, where $x, y \in \mathbf{Z}$; in other words, $\langle a \rangle + \langle b \rangle = \langle a, b \rangle$. As you showed in homework, $\langle a, b \rangle = \langle d \rangle$, where d is the gcd of a and b. Hence, $\langle 19 \rangle + \langle 133 \rangle = \langle \gcd(19, 133) \rangle = \langle 19 \rangle$. $\square$

2. Suppose that m and n are relatively prime positive integers. Define a map $\phi \colon \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by

$$\phi(\overline{a}) = (\overline{a}, \overline{a}).$$

   (a) Check that ϕ is well-defined.

Proof. We must show that if $\overline{a} = \overline{a'}$ in $\mathbf{Z}_{mn}$, then $\overline{a} = \overline{a'}$ in both $\mathbf{Z}_m$ and $\mathbf{Z}_n$. If $\overline{a} = \overline{a'}$ in $\mathbf{Z}_{mn}$, then $a \equiv a' \pmod{mn}$. Thus,

$$mn \mid a - a'.$$

Since $m, n \mid mn$, it follows that $m \mid a - a'$ and $n \mid a - a'$. Thus, $a \equiv a' \pmod{m}$ and $a \equiv a' \pmod{n}$, so that $\overline{a} = \overline{a'}$ in $\mathbf{Z}_m$ and $\overline{a} = \overline{a'}$ in $\mathbf{Z}_n$. □

(b) Prove that ϕ is a homomorphism.

Proof. First, we check that ϕ sends the multiplicative identity to the multiplicative identity:

$$\phi(1_{\mathbf{Z}_{mn}}) = \phi(\overline{1}) = (\overline{1}, \overline{1}) = 1_{\mathbf{Z}_m \times \mathbf{Z}_n}.$$

Now we check that ϕ preserves operations. We have

$$\phi(\overline{a}) + \phi(\overline{b}) = (\overline{a}, \overline{a}) + (\overline{b}, \overline{b}) = (\overline{a} + \overline{b}, \overline{a} + \overline{b}) = (\overline{a+b}, \overline{a+b}) = \phi(\overline{a+b}) = \phi(\overline{a} + \overline{b}).$$

This shows that ϕ preserves addition. The proof that ϕ preserves multiplication is entirely analogous. □

(c) Prove that $\ker(\phi) = \{\overline{0}\}$ and conclude that ϕ is injective.

Proof. Suppose that $\phi(\overline{a}) = (\overline{0}, \overline{0})$. Then $\overline{a} = \overline{0}$ in both $\mathbf{Z}_m$ and $\mathbf{Z}_n$. Hence, $m \mid a$ and $n \mid a$. Since m and n are relatively prime, $mn \mid a$. Hence, $\overline{a} = \overline{0}$ in $\mathbf{Z}_{mn}$. Since the kernel is trivial, ϕ is injective. □

(d) By comparing the sizes of the domain and target, deduce that ϕ is surjective. Thus, ϕ is an isomorphism.

Proof. We have already shown that ϕ is injective. Since both the domain and target have mn elements, ϕ must also be surjective. Since ϕ is a one-to-one, onto homomorphism, ϕ is an isomorphism. □

3. Show that if F is a field and $f(x) \in F[x]$ is an irreducible polynomial of degree 2, then f splits over $K = F[x]/\langle f(x) \rangle$. (From class, you already know that K contains one root of f. The point of this problem is for you to show that K contains both roots.)

Proof. From class, we know that $f(X)$ has a root in K, namely $\alpha = \overline{x}$. By the root-factor theorem,

$$f(X) = (X - \alpha)g(X)$$

for some $g(X) \in K[X]$. Since $f(X)$ is quadratic, $g(X)$ has degree 1. Thus, $f(X)$ factors as a product of linear factors over K, as so $f(X)$ splits over K. □

4. (a) Given rings R and S, which elements of the direct product $R \times S$ are units?

Proof. We claim that the units in $R \times S$ are precisely those elements of $R \times S$ of the form (u, v), where u is a unit in R and v is a unit in S.

First, suppose (u, v) is a unit in $R \times S$. Since $1_{R \times S} = (1_R, 1_S)$, there is an element of $R \times S$, say (u', v'), with $(u, v)(u', v') = (1_R, 1_S) = (u', v')(u, v)$. Hence,

$$uu' = 1_R = u'u, \quad vv' = 1_S = v'v.$$

Thus, u' is an inverse of u in R, and v' is an inverse of v in S. So u, v are units in R and S respectively, as claimed.

Conversely, if u and v are units of R and S, with respective inverses u' and v', then $(u, v)(u', v') = (1_R, 1_S) = (u', v')(u, v)$. Thus, (u, v) is a unit in $R \times S$ (with inverse (u', v')). □

(b) Let $\varphi(n)$ denote the number of units in $\mathbf{Z}_n$; for example, $\varphi(6) = 2$, since the units in $\mathbf{Z}_6$ are $\overline{1}$ and $\overline{5}$.

Prove that if a and b are relatively prime positive integers, then

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Proof. We know that $\mathbf{Z}_{ab} \cong \mathbf{Z}_a \times \mathbf{Z}_b$. Now recall that isomorphic rings have the same number of units. The number of units in $\mathbf{Z}_{ab}$ is $\varphi(ab)$, while part (a) implies that the number of units in $\mathbf{Z}_a \times \mathbf{Z}_b$ is $\varphi(a)\varphi(b)$. □

5. Use the Fundamental Homomorphism Theorem to establish the following ring isomorphisms.

(a) $\mathbf{R}[x]/\langle x^2 + 6\rangle \cong \mathbf{C}$.

Proof. Let $\sqrt{-6}$ denote the complex number $i\sqrt{6}$. We consider the map ϕ sending $f(x)$ to $f(\sqrt{-6})$. This is a homomorphism for reasons already discussed in class (see Example 1(e) on p.115).

Moreover, ϕ is onto: Given $a + bi \in \mathbf{C}$, we have $a + bi = f(a + \frac{b}{\sqrt{6}}x)$.

To determine $\ker(\phi)$, first observe that $\ker(\phi)$ contains $\langle x^2 + 6\rangle$. Since $x^2 + 6$ is a quadratic polynomial without roots in $\mathbf{R}$, it is irreducible in $\mathbf{R}[x]$. So the kernel is either $\langle x^2 + 6\rangle$ or $\mathbf{R}[x]$. But the kernel clearly does not contain 1, and so $\ker(\phi) = \langle x^2 + 6\rangle$.

The desired result now follows from the fundamental ring homomorphism theorem. □

(b) $R[x]/\langle x\rangle \cong R$ for every commutative ring R.

Proof. We consider the map ϕ sending $f(x)$ to its constant term $f(0)$. As in (a), this is a homomorphism.

It is onto, since given $r \in R$, we have $\phi(r) = r$.

Since the polynomials with constant term 0 are exactly those divisible by x, we have $\ker(\phi) = \langle x\rangle$. The result follows. □

(c) $\mathbf{Z}_{18}/\langle\overline{6}\rangle \cong \mathbf{Z}_6$.

Proof. (This is essentially the same as Example 4(c) on p. 128.) Consider the map ϕ taking $\overline{a}$ to $\overline{a}$. This is clearly an onto homomorphism. Moreover, $\overline{a}$ is in the kernel if and only if $6 \mid a$; hence, $\ker(\phi) = \langle \overline{6} \rangle$. The result follows. $\square$

(d) $\mathbf{Q}[x]/\langle x^2 - 1\rangle \cong \mathbf{Q} \times \mathbf{Q}$.

Proof. Consider the map $\phi\colon \mathbf{Q}[x] \to \mathbf{Q}\times\mathbf{Q}$ given by sending $f(x)$ to $(f(1), f(-1))$. This is easily seen to be a homomorphism. It is also onto, since any $(a,b) \in \mathbf{Q}\times\mathbf{Q}$ can be written as $\phi(\frac{a-b}{2}x + \frac{a+b}{2})$. (This was discovered by finding the equation of the straight line through the points $(1,a)$ and $(-1,b)$.)

The kernel consists of those $f(x) \in \mathbf{Q}[x]$ with $f(1) = 0$ and $f(-1) = 0$. The first condition corresponds to $x-1$ dividing $f(x)$, and the latter to $x+1$ dividing $f(x)$. By unique factorization in $\mathbf{Q}[x]$,

$$x - 1,\ x + 1 \text{ both divide } f(x) \Longleftrightarrow x^2 - 1 \mid f(x).$$

Hence, $\ker(\phi) = \langle x^2 - 1\rangle$. $\square$

6. Prove that if $\phi\colon R \to S$ is a homomorphism of (commutative, nonzero) rings, and R is a field, then ϕ is injective.

Proof. The kernel of ϕ must be an ideal of R. Since R is a field, the only ideals of R are $\langle 0\rangle$ and R. If $\ker(\phi) = R$, then ϕ sends all elements of R to 0_S. But $\phi(1_R) = 1_S$, and $1_S \neq 0_S$. So $\ker(\phi)$ cannot be all of R, and so must be $\langle 0\rangle$ — thus, ϕ is injective. $\square$