# Solutions to Homework 3

**1.** Let $R = \mathbb{Q}[x]$.

a. Let $I = \langle x^2 \rangle$. For $f, g \in R$, prove that $f \equiv g \pmod{I}$ if and only if $f(0) = g(0)$ and $f'(0) = g'(0)$.

**Solution:** By definition, $f \equiv g \pmod{I}$ if and only if $f - g \in I$, that is, $f - g$ is a multiple of $x^2$. If we write

$$f = a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0$$
$$g = b_n x^n + \cdots + b_2 x^2 + b_1 x + b_0,$$

then
$$f - g = \cdots + (a_2 - b_2)x^2 + (a_1 - b_1)x + (a_0 - b_0).$$

This is a multiple of $x^2$ if and only if the last two coefficients $a_1 - b_1$ and $a_0 - b_0$ are zero, which is true if and only $a_1 = b_1$ and $a_0 = b_0$. And we have

$$f(0) = a_0 \qquad f'(0) = 2a_1 \qquad g(0) = b_0 \qquad g'(0) = 2b_1,$$

so $a_0 = b_0$ if and only if $f(0) = g(0)$, and $a_1 = b_1$ if and only if $f'(0) = g'(0)$.

b. Let $J = \langle (x-5)^2 \rangle$. For $f, g \in R$, prove that $f \equiv g \pmod{J}$ if and only if $f(5) = g(5)$ and $f'(5) = g'(5)$.

**Solution:** It might be possible to manipulate the coefficients of $f$ and $g$, like the solution to part (a), but it would be very messy. Here's a cleaner approach using the root-factor theorem (§3.1 Corollary 1.5).

First suppose that $f \equiv g \pmod{J}$, so $f - g \in J$, so we can write

$$f - g = (x-5)^2 h$$

for some $h \in R$. Plugging in $x = 5$, we find that $f(5) = g(5)$. Taking derivatives, we get

$$f' - g' = 2(x-5)h + (x-5)^2 h',$$

and plugging in $x = 5$ again we find that $f'(5) = g'(5)$.

Conversely, suppose that $f(5) = g(5)$; then 5 is a root of $f - g$, so by the root-factor theorem we can write $f - g = (x - 5)k$ for some $k \in R$. Taking derivatives, we get

$$f' - g' = k + (x - 5)k',$$

and plugging in $x = 5$ we find that $k(5) = 0$, so by the root-factor theorem again we can write $k = (x - 5)\ell$ for some $\ell \in R$. Thus $f - g = (x - 5)^2\ell$, so $f - g \in J$, so $f \equiv g \pmod{J}$.

Yet another approach would be to apply part (a) to the polynomials $F(x) = f(x + 5)$ and $G(x) = g(x + 5)$, which satisfy $F(0) = G(0)$ and $F'(0) = G'(0)$.

c. Prove that the map $\phi\colon R \to \mathbb{Q} \times \mathbb{Q}$ given by $\phi(f) = (f(5), f(6))$ is a surjective homomorphism, and that $\ker \phi = \langle x^2 - 11x + 30\rangle$.

**Solution:** First we show that $\phi$ is a homomorphism. For $f, g \in R$ we have

$$\begin{aligned}
\phi(f + g) &= \Big((f + g)(5),\ (f + g)(6)\Big) \\
&= \Big(f(5) + g(5),\ f(6) + g(6)\Big) \\
&= \Big(f(5), f(6)\Big) + \Big(g(5), g(6)\Big) \\
&= \phi(f) + \phi(g).
\end{aligned}$$

Similarly, we find that $\phi(fg) = \phi(f)\phi(g)$. Finally, $\phi(1) = (1, 1)$, which is the multiplicative identity in $\mathbb{Q} \times \mathbb{Q}$.

Next we show that $\phi$ is surjective. Given some $(a, b) \in \mathbb{Q} \times \mathbb{Q}$, take

$$f = b(x - 5) - a(x - 6).$$

Then $f(5) = a$ and $f(6) = b$, so $\phi(f) = (a, b)$.

Last we show that $\ker \phi = \langle x^2 - 11x + 30\rangle$. We have $\phi(x^2 - 11x + 30) = (0, 0)$, so $x^2 - 11x + 30 \in \ker \phi$, so $\langle x^2 - 11x + 30\rangle \subset \ker \phi$ by problem 1 of homework 1. For the reverse inclusion, suppose that $f \in \ker \phi$, so $\phi(f) = (0, 0)$, so $f(5) = 0$ and $f(6) = 0$. By the root-factor theorem, the first implies that $x - 5 \mid f$, and the second implies that $x - 6 \mid f$. Because $\gcd(x - 5, x - 6) = 1$, these imply that $(x - 5)(x - 6) \mid f$, so $f \in \langle (x - 5)(x - 6)\rangle$ as desired.

d. Prove that the map $\psi\colon R \to \mathbb{Q} \times \mathbb{Q}$ given by $\psi(f) = (f(5), f'(5))$ is not a homomorphism.

**Solution:** Let $f = g = x$. Then $\psi(f) = \psi(g) = (5, 1)$ so $\psi(f)\psi(g) = (25, 1)$, but $\psi(fg) = \psi(x^2) = (25, 10)$.

Or you could just you say that $\psi(1) = (1, 0) \neq (1, 1)$.

**2.** Continued from Worksheet 6: Let $R = \mathbb{Z}[x]$, and let $I = \langle 2, x^2+5\rangle$.

a. Prove that $(x+1)(x-1) \in I$.

**Solution:** We have

$$(x+1)(x-1) = x^2 - 1 = (x^2+5) - 3\cdot 2,$$

which is an element of $I$.

b. Prove that $x+1 \notin I$, as follows. If $x+1$ were in $I$ then we could write

$$x+1 = 2f + (x^2+5)g$$

for some $f, g \in R$. Consider the reduction homomorphism $\rho\colon R \to \mathbb{Z}_2[x]$ from example 1(d) on page 115, which takes a polynomial $a_nx^n + \cdots + a_0 \in R$ to $\bar{a}_nx^n + \cdots + \bar{a}_0 \in \mathbb{Z}_2[x]$. Apply $\rho$ to the displayed equation above to get a contradiction.

(Notice that $\rho(2) = \bar{0}$, so $\rho(2f) = \bar{0}$.)

**Solution:** Suppose we could write $x+1 = 2f + (x^2+5)g$. Applying $\rho$ to both sides and using the fact that $\rho$ is a homomorphism, we would get

$$\rho(x+1) = \rho(2)\rho(f) + \rho(x^2+5)\rho(g),$$

which becomes

$$x + \bar{1} = (x^2 + \bar{1})\rho(g),$$

so $x^2+\bar{1}$ would divide $x+\bar{1}$ in $\mathbb{Z}_2[x]$. But this is impossible, because $x^2+\bar{1}$ has degree 2 and $x+\bar{1}$ has degree 1; note that the degree of a polynomial in $\mathbb{Z}_2[x]$ is well-behaved because $\mathbb{Z}_2$ is a field (§3.1, Proposition 1.2).

c. Write "Similarly, $x-1 \notin I$. Thus $I$ is not a prime ideal."

**Solution:** Similarly, $x-1 \notin I$. Thus $I$ is not a prime ideal.

**3.** Based on §4.2 #4:

a. Prove that if $\phi\colon R \to S$ and $\psi\colon S \to T$ are ring homomorphisms, then so is their composition $\psi \circ \phi\colon R \to T$.

**Solution:** For $a, b \in R$, we have

$$\psi(\phi(a + b)) = \psi(\phi(a) + \phi(b)) = \psi(\phi(a)) + \psi(\phi(b)),$$

where the first equality uses the fact that $\phi$ is a homomorphism and the second uses the fact that $\psi$ is a homomorphism. Similarly,

$$\psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)),$$

and

$$\psi(\phi(1_R)) = \psi(1_S) = 1_T.$$

b. Prove that if $\phi\colon R \to S$ is a ring isomorphism, then so is its inverse $\phi^{-1}\colon S \to R$.

**Solution:** We know from basic set theory that if $\phi$ is a bijection then $\phi^{-1}$ is too, so it remains to check that $\phi^{-1}$ is a homomorphism. Given two elements $s_1, s_2 \in S$, let $r_1 = \phi^{-1}(s_1)$ and $r_2 = \phi^{-1}(s_2)$. Because $\phi$ is a homomorphism, we have

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = s_1 + s_2.$$

Applying $\phi^{-1}$, we get

$$\phi^{-1}(s_1 + s_2) = r_1 + r_2 = \phi^{-1}(s_1) + \phi^{-1}(s_2).$$

Similarly we find that $\phi^{-1}(s_1 s_2) = \phi^{-1}(s_1)\phi^{-1}(s_2)$.

Lastly we have $\phi(1_R) = 1_S$, so $\phi^{-1}(1_S) = 1_R$.