# Final Exam Solutions

1. Let $\varphi\colon R \to S$ be a homomorphism, let $I \subset R$ be an ideal, and let

$$J = \varphi(I) = \{j \in S : j = \varphi(i) \text{ for some } i \in I\}.$$

   (a) Show that if $\varphi$ is surjective then $J$ is an ideal.

   **Solution:** Let $j_1, j_2 \in I$, and write $j_1 = \varphi(i_1)$ and $j_2 = \varphi(i_2)$ for some $i_1, i_2 \in I$. Then $i_1 + i_2 \in I$, so

$$j_1 + j_2 = \varphi(i_1) + \varphi(i_2) = \varphi(i_1 + i_2) \in J.$$

   Next let $j \in I$ and $s \in S$, and write $j = \varphi(i)$ for some $i \in I$ and, because $\varphi$ is surjective, write $s = \varphi(r)$ for some $r \in R$. Then $ri \in I$, so

$$sj = \varphi(r)\varphi(i) = \varphi(ri) \in J.$$

   (b) Give an example to show that if $\varphi$ is not surjective then $J$ need not be an ideal.

   **Solution:** There are many possibilities of course. Here's one: let $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ be the inclusion, and let $I = (2)$. Then

$$J = \{0, \pm 2, \pm 4, \pm 6, \dots\} \subset \mathbb{Q}$$

   is not an ideal, because $\frac{1}{2} \in \mathbb{Q}$ and $2 \in J$ but $\frac{1}{2} \cdot 2 = 1 \notin J$.

2. Let $S \subset \mathbb{Q}$ be the set of numbers of the form $m/2^n$, where $m \in \mathbb{Z}$ and $n \in \{0, 1, 2, \dots\}$.

   (a) Show that $S$ is a subring of $\mathbb{Q}$.

   **Solution:** The set $S$ is closed under addition:

$$\frac{m_1}{2^{n_1}} + \frac{m_2}{2^{n_2}} = \frac{m_1 2^{n_2} + m_2 2^{n_1}}{2^{n_1+n_2}}.$$

It is closed under multiplication:

$$\frac{m_1}{2^{n_1}} \cdot \frac{m_2}{2^{n_2}} = \frac{m_1 m_2}{2^{n_1+n_2}}.$$

It contains opposites:

$$-\frac{m}{2^n} = \frac{-m}{2^n}.$$

It contains 1:

$$1 = \frac{1}{2^0}.$$

Thus $S$ is a subring.

(b) Show that $S/5 \cong \mathbb{Z}/5$.

Hint: Of course you want a homomorphism $\varphi\colon S \to \mathbb{Z}/5$ with $\ker\varphi = (5)$; the main question is where to send $\frac{1}{2}$. Observe that $2 \cdot 3 = 1$ in $\mathbb{Z}/5$.

**Solution:** Define a map $\varphi\colon S \to \mathbb{Z}/5$ by

$$\varphi\left(\frac{m}{2^n}\right) = m \cdot 3^n \pmod 5.$$

First I claim that $\varphi$ is well-defined. Suppose that $m_1/2^{n_1} = m_2/2^{n_2}$. Without loss of generality we can assume that $m_1 \leq m_2$. Then $m_2 = m_1 \cdot 2^k$ and $n_2 = n_1 + k$ for some non-negative integer $k$, so

$$m_2 \cdot 3^{n_2} = m_1 \cdot 2^k \cdot 3^{n_1+k} \equiv m_1 \cdot 3^{n_1} \pmod 5,$$

where we have used the fact that $2 \cdot 3 \equiv 1 \pmod 5$.

Next I claim that $\varphi$ is a homomorphism. Clearly $\varphi(1) = 1$ and $\varphi(ab) = \varphi(a)\varphi(b)$, so it remains to show that $\varphi(a+b) = \varphi(a) + \varphi(b)$. For this we have

$$\begin{aligned}
\varphi\left(\frac{m_1 2^{n_2} + m_2 2^{n_1}}{2^{n_1+n_2}}\right) &= (m_1 2^{n_2} + m_2 2^{n_1}) 3^{n_1+n_2} \pmod 5 \\
&= m_1 2^{n_2} 3^{n_1+n_2} + m_2 2^{n_1} 3^{n_1+n_2} \pmod 5 \\
&= m_1 3^{n_2} + m_2 3^{n_2} \pmod 5 \\
&= \varphi\left(\frac{m_1}{2^{n_1}}\right) + \varphi\left(\frac{m_2}{2^{n_2}}\right)
\end{aligned}$$

where in the third line we have used the fact that $2 \cdot 3 \equiv 1 \pmod 5$.

Clearly $\varphi$ is surjective, and $\varphi(5) = 0$, so $(5) \subset \ker\varphi$. For the reverse inclusion, suppose that $\varphi(m/2^n) = 0$. Then $m \cdot 3^n \equiv 0 \pmod 5$, so 5 divides $m \cdot 3^n$. Since 5 is prime and does not divide $3^n$, we see that $5 \mid m$. Writing $m = 5k$, we have $m/2^n = 5 \cdot k/2^n$, so $m/2^n \in (5)$.

Now by the first isomorphism theorem, $\varphi$ induces an isomorphism $S/5 \cong \mathbb{Z}/5$.

(c) Let $f \in \mathbb{Z}[x]$. Show that if $f(\frac{1}{2}) = 0$ then $2x - 1 \mid f$.

**Solution:** We know that $(2x - 1) \mid f$ in $\mathbb{Q}[x]$. If you want to give the details, by polynomial long division we can write $f = (2x - 1)q + r$ for some $q, r \in \mathbb{Q}[x]$ with $\deg r \leq 1$; that is, $r$ is a constant. Plugging in $x = \frac{1}{2}$ we find that $r = 0$.

So we have $f = (2x - 1)q$ with $q \in \mathbb{Q}[x]$. By Gauss's Lemma, there is an $a \in \mathbb{Q}$ such that $a(2x - 1) \in \mathbb{Z}[x]$ and $a^{-1}q \in \mathbb{Z}[x]$. But $a(2x - 1) = 2ax - a$, so $a \in \mathbb{Z}$, so $q = a \cdot a^{-1}q \in \mathbb{Z}[x]$.

Alternatively, for a non-zero polynomial

$$f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x],$$

we can consider the *reverse* of $f$,

$$\operatorname{rev} f = x^n f(1/x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n.$$

We verify that $\operatorname{rev}(fg) = \operatorname{rev} f \cdot \operatorname{rev} g$: if $\deg g = m$ then

$$\begin{aligned}\operatorname{rev}(fg) &= x^{m+n} f(1/x) g(1/x) \\ &= x^m f(1/x) \cdot x^n g(1/x) = \operatorname{rev} f \cdot \operatorname{rev} g.\end{aligned}$$

Thus $2x - 1$ divides $f$ if and only if $\operatorname{rev}(2x - 1) = -x + 2$ divides $\operatorname{rev} f$, which is true if and only if $x - 2$ divides $\operatorname{rev} f$. Also, $f(1/2) = 0$ if and only if $(\operatorname{rev} f)(2) = 0$: we have

$$(\operatorname{rev} f)(2) = 2^n f(1/2).$$

Now $x - 2$ is a monic, so we can use polynomial long division in $\mathbb{Z}[x]$ to say that $x - 2 \mid \operatorname{rev} f$ if and only if $(\operatorname{rev} f)(2) = 0$.

(d) Show that $S \cong \mathbb{Z}[x]/(2x-1)$.

Hint: Consider an appropriate homomorphism $\varphi\colon \mathbb{Z}[x] \to \mathbb{Q}$.

**Solution:** Define $\varphi\colon \mathbb{Z}[x] \to \mathbb{Q}$ by $\varphi(f) = f(1/2)$.

First I claim that $\operatorname{im}\varphi = S$. Clearly $\operatorname{im}\varphi \subseteq S$, and for the reverse inclusion we have $m/2^n = \varphi(mx^n)$.

Next I claim that $\ker\varphi = (2x-1)$. Clearly $2x-1 \in \ker\varphi$, so $(2x-1) \subset \ker\varphi$, and the reverse inclusion is part (c).

Now by the first isomorphism we have $\mathbb{Z}[x]/\ker\varphi \cong \operatorname{im}\varphi$.

This suggests another approach to part (b):

$$\begin{aligned} S/5 &\cong \mathbb{Z}[x]/(2x-1)/5 \\ &\cong \mathbb{Z}[x]/(2x-1,5) \\ &\cong \mathbb{Z}_5[x]/(2x-1) \\ &= \mathbb{Z}_5[x]/(x-3) \\ &\cong \mathbb{Z}_5. \end{aligned}$$

In the fourth line we have used the fact that $3(2x-1) = x-3$, and 3 is a unit in $\mathbb{Z}_5$.

3. Recall that $\mathbb{Q}[[x]]$ is the ring of formal power series

$$f = a_0 + a_1x + a_2x^2 + \cdots$$

where $a_i \in \mathbb{Q}$, and infinitely many $a_i$ may be non-zero. It does not make sense to talk about the *degree* of $f$, but for $f \neq 0$ we define the *order* of $f$ to be the smallest $i$ such that $a_i \neq 0$. For example, $\operatorname{ord}(1+x+x^2) = 0$ and $\operatorname{ord}(x+x^2) = 1$.

(a) Show that $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.

**Solution:** Let $n = \operatorname{ord}(f)$ and $m = \operatorname{ord}(g)$, so we can write

$$\begin{aligned} f &= a_nx^n + a_{n+1}x^{n+1} + \cdots \\ g &= b_mx^m + b_{m+1}x^{m+1} + \cdots \end{aligned}$$

with $a_n \neq 0$ and $b_m \neq 0$. Then $a_nb_m \neq 0$, and

$$fg = a_nb_mx^{m+n} + (a_nb_{m+1} + a_{n+1}b_m)x^{m+n+1} + \cdots,$$

so $\operatorname{ord}(fg) = m+n$.

(b) Let
$$f = a_0 + a_1 x + a_2 x^2 + \cdots \in \mathbb{Q}[[x]].$$
Show that if $f$ is a unit then $a_0 \neq 0$.

**Solution:** Suppose there is a $g \in \mathbb{Q}[[x]]$ with $fg = 1$, and write
$$g = b_0 + b_1 x + b_2 x^2 + \cdots .$$
Then
$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots ,$$
so $a_0 b_0 = 1$, so $a_0 \neq 0$.

Another possibility: Suppose there is a $g \in \mathbb{Q}[[x]]$ with $fg = 1$. Then $\mathrm{ord}(f) + \mathrm{ord}(g) = \mathrm{ord}(1) = 0$, and $\mathrm{ord}(f)$ and $\mathrm{ord}(g)$ are non-negative integers, so $\mathrm{ord}(f) = 0$, so $a_0 \neq 0$.

(c) Show that if $a_0 = 1$ then $f$ is a unit.

Hint: Think about the geometric series:
$$\frac{1}{1 + \text{stuff}} = 1 - \text{stuff} + \text{stuff}^2 - \text{stuff}^3 + \cdots .$$
But make sure that your argument doesn't accidentally prove that $1 + (x - 1)$ is a unit.

**Solution:** Following the hint, we write $f = 1 + h$ with $\mathrm{ord}(h) \geq 1$, and let
$$g = 1 - h + h^2 - h^3 + h^4 - \cdots .$$
This is an infinite sum, but it is nonetheless well-defined: for each $i$, only finitely many terms of the sum contribute to the coefficient of $x^i$ in $g$, namely
$$1 - h + h^2 - \cdots \pm h^i,$$
and the later terms all have order $> i$ because $\mathrm{ord}(h) \geq 1$.

(This is the thing that doesn't work if $h = x - 1$. In that case the constant term of $g$ would have to be $1 + 1 + 1 + \cdots$, which is nonsense, the linear term would be $0 - x - 2x - 3x - \cdots$, etc.)

Then we have
$$\begin{aligned} fg &= (1 + h)(1 - h + h^2 - \cdots) \\ &= (1 - h + h^2 - \cdots) + (h - h^2 + h^3 - \cdots) = 1. \end{aligned}$$

(d) Show more generally that if $a_0 \neq 0$ then $f$ is a unit.

Hint: Factor $a_0$ out of $f$, and note that the product of two units is a unit.

**Solution:** Write

$$f = a_0 \cdot (1 + \tfrac{a_1}{a_0}x + \tfrac{a_2}{a_0}x^2 + \cdots).$$

Then $a_0$ is a unit, and the thing in parentheses is a unit by part (c), so $f$ is a unit.

(e) Let $f \in \mathbb{Q}[[x]]$ be non-zero, and let $n = \operatorname{ord}(f)$. Show that the ideal $(f) = (x^n)$.

Hint: Factor $x^n$ out of $f$; then what's left is a unit.

**Solution:** Since $\operatorname{ord} f = n$, we have

$$f = a_n x^n + a_{n+1}x^{n+1} + a_{n+2}x^{n+2} + \cdots$$

with $a_n \neq 0$. Then we can write

$$f = x^n \cdot (a_n + a_{n+1}x + a_{n+2}x^2 + \cdots),$$

and the thing in parentheses is a unit by part (d), so we can write

$$x^n = f \cdot (a_n + a_{n+1}x + a_{n+2}x^2 + \cdots)^{-1}.$$

Thus $f \in (x^n)$ and $x^n \in (f)$, so $(f) = (x^n)$.

(f) Show that every non-zero ideal $I \subset \mathbb{Q}[[x]]$ is of the form $(x^n)$ for some $n$.

Hint: Choose an $f \in I$ of minimal order. Do not assume that $I$ is finitely generated.

Remarks: Thus we have proved that $\mathbb{Q}[[x]]$ is a principal ideal domain, and that it has only one maximal ideal. A ring with a unique maximal ideal is called a *local ring*. A local PID is called a *discrete valuation ring*; in this example the valuation is what we've been calling the order of $f$.

**Solution:** Choose a non-zero $f \in I$ such that $\operatorname{ord} f \leq \operatorname{ord} g$ for all non-zero $g \in I$. Let $n = \operatorname{ord} f$. In part (d) we saw that there is a unit $u \in \mathbb{Q}[[x]]$ such that $f = x^n u$, so $x^n = fu^{-1}$. Thus $x^n \in I$, so $(x^n) \subset I$. For the reverse inclusion, let $g \in I$. If $g = 0$ then of course $g \in (x^n)$. If $g \neq 0$ then $\operatorname{ord} g \geq n$, so $x^n$ divides $g$, so again $g \in (x^n)$.

(g) Which of the ideals $(0), (x), (x^2), (x^3), \ldots$ are prime ideals?

**Solution:** The ideal $(0)$ is prime because $\mathbb{Q}[[x]]$ is an integral domain.

The ideal $(x)$ is prime because the quotient is $\mathbb{Q}$, which is an integral domain. Put another way, if $x \mid fg$ then $\operatorname{ord}(fg) \geq 1$, so $\operatorname{ord} f \geq 1$ or $\operatorname{ord} g \geq 1$, so $x \mid f$ or $x \mid g$.

For $n \geq 2$, the ideal $(x^n)$ is not prime: we have $x \cdot x^{n-1} = x^n$, but neither $x$ nor $x^{n-1}$ is in $(x^n)$.

You might also mention that $(1)$ is not prime by definition.