Math 566 - Homework 7
SOLUTIONS
Prof Arturo Magidin

1. Let R be a ring with unity and let $I \triangleleft R$ be an ideal of R. Prove that $I[x]$ is an ideal of $R[x]$ and $R[x]/I[x] \cong (R/I)[x]$.

   Proof. The canonical projection $\pi\colon R \to R/I$, composed with the canonical inclusion $(R/I) \hookrightarrow (R/I)[x]$, defines a ring homomorphism $R \to (R/I)[x]$, sending $a \in R$ to the constant polynomial $a + I$ in $(R/I)[x]$. Then mapping $x \in R[x]$ to $x \in (R/I)[x]$ induces a ring homomorphism $f\colon R[x] \to (R/I)[x]$, by

   $$f(a_0 + a_1x + \cdots + a_nx^n) = (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n,$$

   which we are guaranteed is a ring homomorphism by the universal property. Invoking the universal property saves us a lot of verifications.

   We claim that $\ker(f) = I[x]$. Indeed, if $a_i \in I$ for $i = 0, \ldots, n$, then

   $$f(a_0 + a_1x + \cdots + a_nx^n = (a_0 + I) + \cdots + (a_n + I)x^n = 0 + 0x + \cdots + 0x^n = 0,$$

   so $I[x] \subseteq \ker(f)$. Conversely, if $a_0 + \cdots + a_nx^n \in \ker(f)$, then $a_i + I = 0 + I$ for each i, so $a_i \in I$ for each i; thus, $\ker(f) \subseteq I[x]$.

   Thus, $I[x] \triangleleft R[x]$. Finally, we show that f is surjective: given $b_0, \ldots, b_n \in R/I$, let $a_i \in R$ be such that $a_i + I = b_i$. Then

   $$f(a_0 + a_1x + \cdots + a_nx^n) = (a_0 + I) + \cdots + (a_n + I)x^n = b_0 + \cdots + b_nx^n.$$

   Thus, by the First Homomorphism Theorem, we have that $R[x]/I[x] \cong (R/I)[x]$, as desired. $\square$

2. Let R be the ring of 2×2 matrices with coefficients in $\mathbb{Z}$

   (i) Show that for all $A \in R$, $(x + A)(x - A) = x^2 - A^2$ holds in $R[x]$.
   Proof. This is just the definition of product in the polynomial ring. We have

   $$\begin{aligned}(x + A)(x - A) &= xx + x(-A) + Ax + A(-A) = x^2 - Ax + Ax - A^2\\ &= x^2 + (-A + A)x - A^2 = x^2 + 0x - A^2\\ &= x^2 - A^2,\end{aligned}$$

   because we know that in the polynomial ring $R[x]$ we have $Ax = xA$ for all $A \in R$, so $x(-A) = -Ax$. $\square$

   (ii) Show that there are matrices A and C in R such that

   $$(C + A)(C - A) \neq C^2 - A^2.$$

   Proof. There are, of course, many possible answers. Here's one. Take

   $$A = \left(\begin{array}{rr} 0 & 1\\ -1 & 0\end{array}\right), \qquad C = \left(\begin{array}{rr} 0 & 1\\ 1 & 0\end{array}\right).$$

   Then

   $$A^2 = \left(\begin{array}{rr} -1 & 0\\ 0 & -1\end{array}\right) \quad\text{and}\quad C^2 = \left(\begin{array}{rr} 1 & 0\\ 0 & 1\end{array}\right).$$

   Thus,

   $$C^2 - A^2 = \left(\begin{array}{rr} 2 & 0\\ 0 & 2\end{array}\right).$$

On the other hand,

$$\begin{aligned}(C+A)(C-A) &= \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right)\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right)\\ &= \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}\\ &\neq C^2 - A^2.\end{aligned}$$

This means that the "evaluation at C" map is *not* a ring homomorphism from $R[x]$ to R in this case (because R is not commutative, and C is not in the center of R). □

3. Let R be a commutative ring. Given $p \in R[x]$,

$$p = a_0 + a_1x + \cdots + a_nx^n,$$

we have a function $\mathbf{p}\colon R \to R$ given by

$$\mathbf{p}(r) = a_0 + a_1r + \cdots + a_nr^n.$$

The assignment $p \mapsto \mathbf{p}$ defines a ring homomorphism $\varphi\colon R[x] \to R^R$, the ring of all functions from R to itself with pointwise addition and product. (You may take this for granted).

Show that if R is finite and nonzero, then φ is not one-to-one.

Proof. Because R is nonzero, the ring $R[x]$ is infinite: pick $a \in R$, $a \neq 0$; then $R[x]$ contains a, ax, $ax^2, \ldots, ax^n, \ldots$.

On the other hand, if R is finite, then $|R^R| = |R|^{|R|}$ is finite. So the function φ goes from an infinite set to a finite set, and hence is not one-to-one. □

4. Let D be an integral domain. Show that the morphism $\varphi\colon D[x] \to D^D$ from the previous problem is one-to-one if and only if D is infinite.

Proof. We saw above that if D is finite then φ is not one-to-one.

Now assume that D is infinite. If $\varphi(f) = \varphi(g)$, then $\varphi(f-g)$ is the zero function, and therefore $(f-g)(r) = 0$ for all $r \in D$.

Because D is an integral domain, a polynomial of degree n has at most n roots. Since $(f-g)(r) = 0$ for infinitely many r, it follows that $f-g$ must be the zero polynomial, so $f = g$, as desired. □

5. Show that if F is a field, then (x) is a maximal ideal of $F[x]$, but it is not the only maximal ideal of F.

Proof. The evaluation map $F[x] \to F$ given by $p(x) \mapsto p(0)$ is a ring homomorphism, which is surjective, and by the Factor Theorem its kernel is precisely the polynomials that are multiples of x, i.e. (x). Thus, (x) is maximal, since $F[x]/(x) \cong F$, a field.

The evaluation map $F[x] \to F$ given by $p(x) \mapsto p(1)$ is also a ring homomoprhism, which is surjective (constant polynomials suffice to ensure surjectivity) and its kernel is precisely the polynomials that are multiples of $x-1$, i.e., $(x-1)$. Thus, the ideal $(x-1)$ is also maximal, since $F[x]/(x-1) \cong F$, a field. Also, $(x) \neq (x-1)$, so (x) is not the only maximal ideal of F. □

6. Let D be an integral domain, and let $c \in D$ be an irreducible element. Prove that the ideal (x,c) of $D[x]$ is not principal.

Proof. Note that $(x,c) \neq (1)$. This follows because $D[x]/(x) \cong D$, so $D[x]/(x,c) \cong D/(c)$. Since c is assumed to be irreducible, it follows that it is not a unit, so $(c) \neq D$. Hence $D/(c)$ is not trivial, so $(x,c) \neq (1)$.

If $(x, c) \subseteq (a)$, then $a \mid x$ and $a \mid c$ in $D[x]$. Since D is an integral domain, if $a \mid c$ then $\deg(a) \leq \deg(d) = 0$, so a is constant. Thus, $a \mid c$ in D, and hence a is a unit or a is an associate of c, given that c is an irreducible element.

If a is an associate of c, then we have that $c \mid a$ and $a \mid x$, so $c \mid x$. But that means that there exists a polynomial of degree 1, $r + sx$, such that $c(r + sx) = x$. This means that $cr = 0$ and $cs = 1$. But the latter says that c is a unit, which is impossible since c is irreducible. Thus, a is a unit.

But if a is a unit, then $(x, c) \neq (1) = (a)$. Thus, if $(x, c) \subseteq (a)$, then $(x, c) \neq (a)$. This proves that (x, c) is not principal, as required. □

7. Let R be a commutative ring with unity, and let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. Define the *formal derivative* of $f(x)$ by $f'(x) = a_1 + 2a_2 x + \cdots + na_n x^{n-1}$. with $f'(x) = 0$ if $f = 0$.

   (i) Prove that $(f + g)' = f' + g'$, $(af)' = af'$, and $(fg)' = f'g + fg'$ for all $f, g \in R[x]$ and all $a \in R$.

   Proof. Let $f = a_0 + \cdots + a_n x^n$ and $g = b_0 + \cdots + b_n x^n$. Then for the sum, we have:

$$\begin{aligned}(f+g)' &= \left(\sum_{i=0}^{n}(a_i + b_i)x^i\right)' = \sum_{i=1}^{n} i(a_i + b_i)x^{i-1} = \sum_{i=1}^{n} ia_i x^{i-1} + \sum_{i=1}^{n} ib_i x^{i-1} \\ &= \left(\sum_{i=0}^{n} a_i x^i\right)' + \left(\sum_{i=0}^{n} b_i x^i\right)' = f' + g'.\end{aligned}$$

   Next,

$$\begin{aligned}(af)' &= \left(a\sum_{i=0}^{n} a_i x^i\right)' = \left(\sum_{i=0}^{n} aa_i x^i\right)' \\ &= \sum_{i=1}^{n} iaa_i x^{i-1} = a\sum_{i=1}^{n} ia_i x^{i-1} = af'.\end{aligned}$$

   For the product, we first prove that for $r \geq 0$, $(x^r g)' = rx^{r-1}g + x^r g'$. Indeed, for $r = 0$ this just says $g' = g'$. For $r > 0$, we have

$$\begin{aligned}(x^r g)' &= \left(\sum_{j=0}^{n} b_j x^{j+r}\right)' = \sum_{j=0}^{n}(j + r)b_j x^{j+r-1}. \\ rx^{r-1}g + x^r g' &= \left(\sum_{j=0}^{n} rb_j x^{j+r-1}\right) + x^r\left(\sum_{j=0}^{n-1}(j+1)b_{j+1}x^j\right) \\ &= \sum_{j=0}^{n} rb_j x^{j+r-1} + \sum_{j=0}^{n-1}(j+1)b_{j+1}x^{r+j} \\ &= \sum_{j=0}^{n} rb_j x^{j+1-1} + \sum_{j=1}^{n} jb_j x^{r+j-1} \\ &= \sum_{j=0}^{n}(rb_j + jb_j)x^{r+j-1} \\ &= \sum_{j=0}^{n}(j + r)b_j x^{r+j-1} = (x^r g)'.\end{aligned}$$

Now applying the formulas for addition and multiplication by a constant, we have:

$$\begin{aligned}
(fg)' &= \left(\left(\sum_{i=0}^{n} a_i x^i\right) g\right)' = \sum_{i=0}^{n} a_i \left(x^i g\right)' \\
&= \sum_{i=0}^{n} a_i (i x^{i-1} g + x^i g') = \left(\sum_{i=0}^{n} i a_i x^{i-1} g\right) + \left(\sum_{i=0}^{n} a_i x^i g'\right) \\
&= \left(\sum_{i=0}^{n} i a_i x^{i-1}\right) g + \left(\sum_{i=0}^{n} a_i x_i\right) g' \\
&= f'g + fg',
\end{aligned}$$

as claimed. □

(ii) Prove that if R is an integral domain, $\deg(f) > 0$, and $\mathrm{char}(R) = 0$, then $f' \neq 0$.
Proof. Let $f(x) = a_0 + \cdots + a_n x^n$ with $n > 0$ and $a_n \neq 0$. Then

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Since $n - 1 \geq 0$ and $na_n \neq 0$, then $f'(x) \neq 0$. □

(iii) Prove that if R is an integral domain, $\deg(f) > 0$, and $\mathrm{char}(R) = p$, then $f' = 0$ if and only if f is a polynomial in x^p. That is,

$$f = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{mp} x^{mp}, \qquad a_i \in R.$$

Proof. For f a polynomial in x^p, we have

$$(a_0 + a_p x^p + \cdots a_{mp} x^{mp})' = p a_p x^{p-1} + \cdots p m a_{mp} x^{mp-1} = 0,$$

since all coefficients are 0 (because $pa = 0$ for all $a \in R$).
Conversely, assume that $f' = 0$. Write $f = a_0 + a_1 x + \cdots + a_n x^n$. We show that if $p \nmid i$, then $a_i = 0$. Indeed, if $p \nmid i$ then $i > 0$, and the coefficient of x^{i-1} in f' is ia_i. Since $f' = 0$, then $ia_i = 0$. This is equal to

$$(\underbrace{1_R + \cdots + 1_R}_{i \text{ summands}}) a_i = 0,$$

which can only happen if either $1_R + \cdots + 1_R = 0$ (which only occurs if the number of summands is a multiple of p, which in this case it is not), or if $a_i = 0$. Thus, we must have $a_i = 0$, as desired. □