Mathematics 546 Homework.

Let us review what we should all know about polynomials. Let F be a field, which for the time being we can assume is one of the following:

$$\begin{aligned}\mathbb{Q} &= \text{The rational numbers,}\\ \mathbb{R} &= \text{The real numbers,}\\ \mathbb{C} &= \text{The complex numbers, or}\\ \mathbb{Z}_p &= \text{for } p \text{ a prime number.}\end{aligned}$$

You can find a formal definition of a field in Definition 4.1.1 on Page 191 of the text, but for the time being the above examples are plenty. Let $F[x]$ be the polynomials with coefficients from F. That is (See Definition 4.1.4 on Page 194 of the text) ***polynomials*** are expressions of the form

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

where the ***coefficients*** $a_0, a_1, \ldots, a_m$ are elements of the field F. In summation notation this is

$$f(x) = \sum_{j=0}^{m} a_j x^j$$

with the understanding that $x^0 = 1$. If $a_m \neq 0$, then

$$\deg(f(x)) = m.$$

For example

$$\begin{aligned}\deg(4x^3 - 9x^2 + 17x - 42) &= 3\\ \deg(x^n - x) &= n \qquad \text{When } n \text{ is an integer} \geq 2.\\ \deg(5) &= 0.\end{aligned}$$

In general if $a_0 \neq 0$ is a nonzero constant, then the constant polynomial $f(x) = a_0 = a_0 x^0$ has $\deg(f(x)) = 0$. The zero polynomial $f(x) = 0$ is not given a degree (or some people give it the degree $\deg(0) = -\infty$).

The basic rule for exponents

$$x^j x^k = x^{j+k}$$

and the distributive law tells us how to multiply polynomials. For example using the distributive law on the product $(a_2x^2 + a_1x + a_0)(b_3x^3 + b_2x^2 + b_1x + b_0)$ leads to $3 \times 4 = 12$ terms which can then be grouped by powers

of x:

$$\begin{aligned}
&(a_2x^2+a_1x+a_0)(b_3x^3+b_2x^2+b_1x+b_0)\\
&\quad=a_2x^2(b_3x^3+b_2x^2+b_1x+b_0)\\
&\qquad+a_1x(b_3x^3+b_2x^2+b_1x+b_0)\\
&\qquad+a_0(b_3x^3+b_2x^2+b_1x+b_0)\\
&\quad=a_2b_3x^5+a_2b_2x^4+a_2b_13+a_2b_0^2\\
&\qquad+a_1b_3x^4+a_1b_2x^3+a_1b_1x^2+a_1b_0x\\
&\qquad+a_0b_3x^3+a_0b_2x^2+a_0b_1x+a_0b_0\\
&\quad=a_2a_3x^5+(a_2b_2+a_1b_3)x^4+(a_2b_1+a_1b_2+a_0b_3)x^3\\
&\qquad+(a_2b_0+a_1b_1+a_0b_2)x^2+(a_1b_0+a_0b_1)x+a_0b_0.
\end{aligned}$$

In general if

$$\begin{aligned}
f(x)&=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0\\
g(x)&=b_nx^n+b_{n-1}x^{m-1}+\cdots+a_1x+b_0
\end{aligned}$$

then the product

$$f(x)g(x)=c_{m+n}x^{m+n}+c_{n+m-1}x^{m+n-1}+c_{m+n-2}x^{m_n-2}+\cdots+c_1x+c_0$$

$$\sum_{k=0}^{m+n}c_kx^k$$

where

$$\begin{aligned}
c_{m+n}&=a_mb_n\\
c_{m+n-1}&=a_mb_{m-1}+a_{m-1}b_n\\
c_{n+m-2}&=a_nb_{n-2}+a_{m-1}b_{n-1}+a_{n-2}b_n\\
&\vdots\qquad\vdots\\
c_k&=\sum_{\substack{i+j=k\\0\le i\le m\\0\le j\le n}}a_ib_j\\
&\vdots\qquad\vdots\\
c_2&=a_2b_0+a_1b_1+a_0b_2\\
c_1&=a_1b_0+a_0b_1\\
c_0&=a_0b_0.
\end{aligned}$$

The formula for c_k can be simplified if we set $a_i=0$ for $i>m$ and $b_j=0$ for $j>n$. Then

$$c_k=\sum_{i+j=k}a_jb_j=\sum_{i=0}^{k}a_ib_{k-i}=\sum_{j=0}^{k}a_{k-j}b_j.$$

Proposition 1. *If $f(x), g(x) \in F[x]$ are not the zero polynomial, then*

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

Proof. Let $\deg(f(x)) = m$ and $\deg(g(x)) = n$ then

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_n x^n + b_{n-1}x^{m-1} + \cdots + a_1 x + b_0$$

where $a_m \neq 0$ and $b_n \neq 0$. Then

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1 x + c_0.$$

where $c_{m+n} = a_m b_n \neq 0$. Thus $\deg(f(x)g(x)) = m + n = \deg(f(x)) + \deg(g(x))$ as required. □

Problem 1. This problem is just a bit of practice (or review) in basic operations with polynomials. Let

$$f(x) = 3x^2 - 4x + 1$$
$$g(x) = x^3 + 2x^2 - x + 5.$$

Compute the following

(a) $f(x) + g(x)$ (or just write "Oh come on, you know we can all add polynomials".)
(b) $f(x)^2$
(c) $f(x)g(x)$. □

Problem 2. Let $a \in F$ and compute the following

(a) $(x - a)(x + a)$
(b) $(x - a)(x^2 + ax + a^2)$
(c) $(x - a)(x^3 + ax^2 + a^2x + a^3)$
(d) $(x - a)(x^4 + ax^3 + a^2x^2 + a^3x + a^4)$
(e) At this point you should have seen a pattern. What is it? □

We will also want to do long division with polynomials. For example if we divide $f(x) = x^4 + 4x^3 + 3x^2 + 2x - 1$ by $g(x) = x^2 + 2x - 3$:

$$\begin{array}{r} x^2 + 2x + 2 \\ x^2 + 2x - 3 \,\overline{)\, x^4 + 4x^3 + 3x^2 + 2x - 1} \\ \underline{x^4 + 2x^3 - 3x^2} \\ 2x^3 + 6x^2 + 2x - 1 \\ \underline{2x^3 + 4x^2 - 6x} \\ 2x^2 + 8x - 1 \\ \underline{2x^2 + 4x - 6} \\ 4x + 5 \end{array}$$

we get a quotient of $q(x) = x^2 + 2x - 3$ and a remainder of $r(x) = 4x + 5$. This means

$$f(x) = q(x)g(x) + r(x).$$

Problem 3. Find the quotient and remainder when $g(x)$ is divided into $f(x)$ in the following cases.

(a) $g(x) = x - 5$ and $f(x) = 4x^2 - 3x + 7$.
(b) $g(x) = x^2 + 2x + 3$ and $f(x) = 3x^4 - 2x^3 + x^2 - 5x + 1$.
(c) $g(x) = x - s$ and $f(x) = ax^2 + bx + c$ where s, a, b, c are constants (that is elements of the field F.)

The next result just says that we can always do long division. If you look closely at a long division problem at the same time you are doing the proof, you will see that the induction step is just the same as one of the usual steps in doing the division.

Theorem 2 (The division algorithm)**.** *Let $f(x), g(x) \in F[x]$ be polynomials over the field F with $g(x)$ not the zero polynomial. Then there are unique polynomials $q(x)$ (the **quotient**) and $r(x)$ (the **remainder**) such that*

$$f(x) = q(x)g(x) + r(x) \quad \textit{with } r(x) = 0 \textit{ or } \deg(r(x)) < \deg(g(x)).$$

Problem 4. Prove this. *Hint:* Fist show the existence of $q(x)$ and $r(x)$. First note if $\deg(g(x)) = 0$, then $g(x) = c$ is a constant in which case

$$f(x) = \left(\frac{1}{c}f(x)\right) g(x) + 0$$

and so the result holds with $q(x) = \frac{1}{c}f(x)$ and $r(x) = 0$. So we assume that $\deg(g(x)) \geq 1$. Let $\deg(g(x)) = m$, then $g(x)$ is of the form

$$g(x) = b_m x^m + g_1(x) \quad \text{where } b_m \neq 0 \text{ and } \deg(g_1(x)) < m.$$

and prove the result by induction on $\deg(f(x))$.

Here are the details you should supply:

(a) *Base case:* If $f(x) = 0$ or $\deg(f(x)) < \deg(g(x))$, then show the result holds with quotient $q(x) = 0$ and remainder $r(x) = f(x)$.
(b) *Induction step:* Here we have $\deg(f(x)) \geq m = \deg(g(x))$. Our induction hypothesis is that the result holds for any polynomial with degree $\leq n$. Let $\deg(f(x)) = n + 1$. Then $f(x)$ is of the form

$$f(x) = a_{n+1}x^{n+1} + f_1(x) \quad \text{where } a_{m+1} \neq 0 \text{ and } \deg(f_1(x)) \leq n$$

Now show that

$$f(x) - \frac{a_{n+1}}{b_m}x^{n-m+1}g(x) = f_1(x) - \frac{a_{n+1}}{b_m}x^{n+1-m}g_1(x)$$

and that this has degree $\leq n$. Therefore by the induction hypothesis there are polynomials $q_1(x)$ and $r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$ and

$$f(x) - \frac{a_{n+1}}{b_m}x^{n-m+1}g(x) = q_1(x)g(x) + r(x).$$

Show this can be rewritten as

$$f(x) = \left(\frac{a_{n+1}}{b_m}x^{n-m+1} + q_1(x)\right) g(x) + r(x)$$

and explain why this completes the proof of existence of the quotient and remainder.

(c) Prove uniqueness. That is show that if

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_1(x)$$

where each of $r_1(x)$ and $r_2(x)$ is either 0 of ha degree $< \deg(g(x))$ then show $r_1(x) = r_2(x)$ and $q_1(x) = q_2(x)$. *Hint:* Rewrite $q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_1(x)$ as

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$$

and compare degrees of both sides to get a contradiction if $r_1(x) \neq r_2(x)$. □

Definition 3. A nonempty subset $I \subseteq F[x]$ is an ***ideal*** in $F[x]$ if and only if

(a) I is closed under addition. That is if $f(x), g(x) \in I$ then $f(x)+g(x) \in I$.
(b) I is closed under multiplication by elements of $F[x]$. That is if $f(x) \in I$ and $h(x) \in F[x]$ then $h(x)f(x) \in I$. □

Proposition 4. *Let I be an ideal in $F[x]$. Then I is closed under linear combinations with coefficients form $F[x]$. That is if $f(x), g(x) \in I$ and $A(x), B(x) \in F[x]$, then $A(x)f(x) + B(x)g(x) \in I$.*

Problem 5. Prove this. □

Definition 5. If $g(x) \in F[x]$, then the ***principle ideal*** generated by $g(x)$ is

$$\langle g(x) \rangle = \{h(x)g(x) : h(x) \in F[x]\}.$$

That is $\langle g(x) \rangle$ is the set of all multiples of $g(x)$ where the multipliers are polynomials in $F[x]$. □

Proposition 6. *For any $g(x) \in F[x]$ the set $\langle g(x) \rangle$ is an ideal in $F[x]$.*

Problem 6. Prove this. □

The following is one of the most important facts about the ring $F[x]$ of polynomials.

Theorem 7 (Polynomial rings are principal ideal domains)**.** *Let I be an ideal in $F[x]$. Then $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$.*

Problem 7. Prove this. *Hint:* If I is just the one element set $I = \{0\}$ then the result is true with $g(x) = 0$. So assume that $I \neq \{0\}$. Let $g(x)$ be a nonzero element of I of smallest degree and show that $I = \langle g(x) \rangle$. As a start on this let $f(x) \in I$ and divide $g(x)$ into $f(x)$

$$f(x) = q(x)g(x) + r(x) \quad \text{where } r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)).$$

and show that $g(x)$ having smallest degree forces $r(x) = 0$. □