110A HW7

Warren Kim

Winter 2024

Throughout this section, F is a field and $F[x]$ is the ring of polynomials with F coefficients.

Question 1

Let $f, g, h \in F[x]$, and suppose f and g are relatively prime. Show that if $f|h$ and $g|h$, we have $fg|h$.

Response

Proof: Let $f, g, h \in F[x]$ and suppose f and g are coprime. If $f \mid h$ and $g \mid h$, then $h = fa$ for some $a \in F[x]$. Then we have $g \mid h = fa$, and since $(f, g) = 1$, we necessarily have that $g \mid a$; that is, $a = gb$ for some $b \in F[x]$. Then we have $h = fa = fgb$, so $fg \cdot b = h$ and by definition, this means that $fg \mid h$. $\square$

Question 2

Let $a, b \in F$ be distinct (i.e., $a \neq b$). Show that $x - a$ and $x - b$ (viewed as elements of $F[x]$) are relatively prime.

Response

Proof: Let $d = (x - a, x - b)$. Then by definition, we have that $d \mid (x - a)$ and $d \mid (x - b)$; that is, $x - a = dp$ and $x - b = dq$ for some $p, q \in F[x]$. Then

$$\begin{aligned}
(x - a) - (x - b) &= dp - dq \\
a - b &= dp - dq \\
a - b &= d(p - q)
\end{aligned}$$

Now since $a \neq b$, we have that $a - b \neq 0$, so $a - b$ is a unit; i.e. it has an inverse. Then

$$\begin{aligned}
d(p - q) \cdot (a - b)^{-1} &= (a - b) \cdot (a - b)^{-1} \\
d(p - q) \cdot (a - b)^{-1} &= 1 \\
d\left((p - q)(a - b)^{-1}\right) &= 1
\end{aligned}$$

so $d \mid 1$. This implies that $d = 1$, so $(x - a, x - b) = 1$. $\square$

Question 3

Let $f, g \in F[x]$ and suppose $g \neq 0$. Consider the set $S = \{f - gs | s \in F[x]\}$. Let $r \in S$ be of lowest degree. Show that $\deg(r) < \deg(g)$. (yes, we did this in class.)

Response

Proof: Let $f, g \in F[x]$ and suppose $g \neq 0$. Consider the set $S = \{f - gs : s \in F[x]\}$. Let $r \in S$ be of lowest degree. Then we can write $r = f - gs$. Suppose for the sake of contradiction that $\deg(r) \geq \deg(g)$. Then $r = \sum_{i=0}^{n} r_i x^i$ and $g = \sum_{i=0}^{m} g_i x^i$ where $n \geq m$. Since $\deg(r) = n, \deg(g) = m$, we have that $r_n \neq 0$ and $g_m \neq 0$; i.e. they are units. Now consider $t := r_n x^n \cdot (g_m x^m)^{-1} = r_n g_m^{-1} x^{n-m}$. Then

$$tg = \left(r_n g_m^{-1} x^{n-m}\right) \cdot \left(\sum_{i=0}^{m} g_i x^i\right) = \left(\sum_{i=0}^{m-1} r_n g_m^{-1} g_i x^{n-m+i}\right) + r_n x^n$$

so

$$\begin{aligned} r - tg &= \left(\sum_{i=0}^{n-1} r_i x^i\right) + r_n x^n - \left(\left(\sum_{i=0}^{m-1} r_n g_m^{-1} g_i x^{n-m+i}\right) + r_n x^n\right) \\ &= \left(\sum_{i=0}^{n-1} r_i x^i\right) - \sum_{i=0}^{m-1} r_n g_m^{-1} g_i x^{n-m+i} \end{aligned}$$

so $\deg(r - tg) \leq n - 1 < n = \deg(r)$. But we have that $r = f - gs$, so we get

$$r - tg = (f - gs) - tg = f - g(s + t)$$

Since $s + t \in F[x]$, we have that $r - tg \in S$, but r was chosen to have the lowest degree and $\deg(r - tg) < \deg(r)$, a contradiction. Therefore, $\deg(r) < \deg(g)$. $\square$

Question 4

Let $f \in F[x]$, $a \in F$, and suppose $f(a) = 0$ (that is, when plugging in a for x in f, we obtain 0). Show that $x - a$ divides f.

Response

Proof: Let $f, \in F[x], a \in F$, and suppose that $f(a) = 0$. We can write $f = (x-a)q + r$ for unique $q, r \in F[x]$ where $\deg(r) < \deg(x - a) = 1$, which implies r is a constant. Then since $r = f(a) = 0$, we get $f = (x - a)q + 0 = (x - a)q$, so $(x - a) \mid f$. $\square$

Question 5

Let $p \in F[x]$, and suppose whenever $p = ab$ for $a, b \in F[x]$, we either have $p|a$ or $p|b$. Show that p is irreducible (i.e., its only factors are units and associates).

Response

Proof: Let $p \in F[x]$ and $a \in F[x]$ a divisor of p. Then $a \mid p$, so $p = ab$ for some $b \in F[x]$. There are two cases:

Case 1: If $p \mid a$, then $a = pq$ for some $q \in F[x]$, so we get $p = ab = (pq)b$. Since $F[x]$ is an integral domain, we apply the cancellation property to the equation $p = p(qb)$ to get $1 = qb$. So, q, b are units, which implies that a and p are associates.

Case 2: If $p \mid b$, then $b = pr$ for some $r \in F[x]$. But we have that $p = ab$ since $a \mid p$, so $p = ab = a(pr)$. Since $F[x]$ is an integral domain, we apply the cancellation property to the equation $p = (ar)p$ to get $1 = ar$, so a is a unit.

In either case, the only factors of p are units and associates, so p is irreducible. $\square$