Homework #5 Solutions

p 298, #4 Case 1: char$R = 0$. In this case, given any $n \in \mathbb{Z}^+$ there is an $r \in R$ so that $n \cdot r \neq 0$. However, since R is a subring of $R[x]$, these elements suffice to show that there is no $n \in \mathbb{Z}^+$ so that $n \cdot f = 0$ for all $f \in R[x]$. That is, char$R[x] = 0 =$ char$R$.

Case 2: char$R \neq 0$. Let char$R = n \in \mathbb{Z}^+$ and $f(x) = a_m x^m + a_{m-1}x^{m-2} + \cdots a_0 \in R[x]$. Then we have $n \cdot a_i = 0$ for $i = 1, 2, \ldots, m$ and so

$$n \cdot f(x) = n \cdot a_m x^m + n \cdot a_{m-1}x^{m-2} + \cdots n \cdot a_0 = 0x^m + 0x^{m-2} + \cdots 0 = 0$$

proving that char$R[x] \leq n$. However, by the definition of characteristic, given $m \in \mathbb{Z}^+$ with $m < n$ there is an $r \in R$ so that $m \cdot r \neq 0$. But R is a subring of $R[x]$ so, as above, these elements suffice to show that the characteristic of $R[x]$ cannot be less than n. Hence, char$R[x] = n =$ char$R$.

p 299, #12 We perform long division, remembering to reduce our coefficients mod 7 at each stage.

$$\begin{array}{r|l}
 & 5x^2 + 6x + 6 \\
\hline
3x + 2 & x^3 + 2x + 4 \\
 & x^3 + 3x^2 \\
\hline
 & \quad 4x^2 + 2x + 4 \\
 & \quad 4x^2 + 5x \\
\hline
 & \qquad 4x + 4 \\
 & \qquad 4x + 5 \\
\hline
 & \qquad\qquad 6
\end{array}$$

The quotient is therefore $5x^2 + 6x + 6$ and the remainder is 6.

p 299, #16 Let R be a ring with zero divisors. Then there is a nonzero $a \in R$ so that $ab = 0$ for some nonzero $b \in R$. Let $f(x) = ax \in R[x]$. Since $a \neq 0$, $f(x)$ has degree 1. However, $f(b) = ab = 0 = f(0)$ so that both b and 0 are roots of $f(x)$. As $b \neq 0$, this disproves the statement in question.

p 299, #20 Let $h(x) = f(x) - g(x) \in F[x]$. Assume that $h(x) \neq 0$ and let $\deg h(x) = n \geq 0$. Then $n+1 \in \mathbb{Z}^+$ and so according to our hypothesis we can find distinct $a_1, a_2, \ldots, a_{n+1} \in F$ so that $f(a_i) = g(a_i)$ for all i. But then $h(a_i) = f(a_i) - g(a_i) = 0$ for $i = 1, 2 \ldots, n+1$. That is, $h(x)$ has degree n but at least $n + 1$ roots in F, contradicting Corollary 3 to Theorem 16.2. Having reached a contradiction we conclude that our original assumption is false, i.e. that we must have $f(x) - g(x) = h(x) = 0$. That is, $f(x) = g(x)$ as desired.

p 299, #24 Let $k \geq 1$ be the multiplicity of the root a of $f(x)$. Then, by definition, we can write $f(x) = (x-a)^k g(x)$ for some $g(x) \in \mathbb{R}[x]$. Differentiating we obtain $f'(x) = k(x-a)^{k-1}g(x) + (x-a)^k g'(x)$. If $k > 1$ then $k-1 > 0$ and so

$$f'(a) = k(a-a)^{k-1}g(x) + (a-a)^k g'(a) = 0 + 0 = 0$$

which contradicts our hypothesis. Thus it must be the case that $k = 1$, as claimed.

p 300, #26 Let D be an integral domain and let $f(x) \in D[x]$ be nonzero. Let $n = \deg f(x)$ and suppose that $f(x)$ has m roots (counting multiplicities) in D. Let F denote the quotient field of D. Then D is a subring of F and so $D[x]$ is a subring of $F[x]$. Let k be the number of roots of $f(x)$ (counting multiplicities) in F. Then $k \geq m$, and Corollary 3 gives $n \geq k \geq m$. That is, the number of roots of $f(x)$ in D cannot exceed the degree of $f(x)$.

p 300, #30 Let $h(x) = x(x-1)(x-2) = x^3 - x \in \mathbb{Z}_3[x]$. Clearly $h(a) = 0$ for all $a \in \mathbb{Z}_3$. Moreover, for any $g(x) \in F[x]$, $f(x) = g(x)h(x)$ has the same property. Since there are infinitely many choices for $g(x)$ and $F[x]$ is an integral domain, there are infinitely many such polynomials $f(x)$.

p 301, #42 ***I* is an ideal in *F*[*x*]:** I is nonempty since the zero polynomial obviously belongs to I. Let $f(x), g(x) \in I$ and $h(x) \in F[x]$. Then for any $a \in F$ we have

$$\begin{aligned} f(a) - g(a) &= 0 - 0 = 0 \\ h(a)f(a) &= h(a) \cdot 0 = 0 \end{aligned}$$

proving that $f(x) - g(x), h(x)f(x) \in I$. Since $F[x]$ is commutative this proves that I is an ideal.

Now suppose that F is finite of order n. According to exercise 54 in chapter 13, $a^{n-1} = 1$ for all nonzero $a \in F$. It easily follows that $a^n = a$ for *all* $a \in F$ and hence that every element in F is a root of $f(x) = x^n - x$. Thus $f(x) \in I$ and, as I is an ideal, $\langle f(x) \rangle \subset I$. However, since $F[x]$ is an infinite domain, $\langle f(x) \rangle$ is also infinite, which implies that I is infinite as well.[1]

If F is infinite then any element in I has infinitely many roots. Arguing as in exercise 20, we find that the only such polynomial is $f(x) = 0$ and hence $I = \{0\}$.

p 301, #44 We argue by contradiction. That is, we assume that there *is* such an element in $F(x)$, i.e. an $r(x) \in F(x)$ so that $r(x)^2 = x$. By definition of the quotient field, we must have $r(x) = f(x)/g(x)$ for some $f(x), g(x) \in F(x)$, $g(x) \neq 0$. Therefore, we have

$$x = r(x)^2 = \frac{f(x)^2}{g(x)^2}.$$

Cross-multiplying gives $xg(x)^2 = f(x)^2$. Since $x, g(x) \neq 0$ we see that $f(x) \neq 0$ and so we may take the degree of both sides. Using the fact that $\deg a(x)b(x) = \deg a(x) + \deg b(x)$

[1] It is not hard to show that, in fact, $I = \langle x^n - x \rangle$ in this case. This is left as an additional exercise.

for all $a(x), b(x) \in F[x]$ we immediately find that

$$1 + 2 \deg g(x) = 2 \deg f(x)$$

which is impossible since both $\deg g(x)$ and $\deg f(x)$ are integers. Having reached a contradiction we conclude that our assumption that $r(x)$ exists is false, and conclude therefore that no such $r(x)$ exists.

p 301, #48 According to the division algorithm

$$x^{51} = q(x)(x + 4) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg(x + 4) = 1$. That is, $r(x)$ must be a constant $r \in \mathbb{Z}_7$. Substituting 3 for x we obtain

$$3^{51} = q(3)(3 + 4) + r = r$$

in $\mathbb{Z}_7$. Since $a^7 = a$ for all $a \in \mathbb{Z}_7$ we have

$$r = 3^{51} = 3^{49}3^2 = (3^7)^7 3^2 = 3^7 3^2 = 3 \cdot 3^2 = 3^3 = 27 = 6$$

in $\mathbb{Z}_7$.