Math 3613
Homework Problems from Chapter 4

§4.1

4.1.1. Perform the indicated operations in $\mathbb{Z}_6[X]$ and simply your answer.

(a) $(3x^4 + 2x^3 - 4x^2 + x - 4) + (4x^3 + x^2 + 4x + 3)$

(b) $(x + 1)^3$

4.1.2. Which of the following subsets of $\mathbb{R}[x]$ are subrings of $\mathbb{R}[x]$? Justify your answer.

(a) $S = \{$All polynomials with constant term $0_R\}$.

(b) $S = \{$Alll polynomials of degree 2 $\}$.

(c) $S = \{$All polynomials of degree $\leq k \in \mathbb{N}$, where $0 < k\}$.

(d) $S = \{$All polynomials in which odd powers of x have zero coefficients$\}$.

(e) $S = \{$All polynomials in which even powers of x have zero coefficients$\}$.

4.1.3. List all polynomials of degree 3 in $\mathbb{Z}_2[x]$.

4.1.4. Let F be a field and let f be a non-zero polynomial in $F[x]$. Show that f is a unit in $F[x]$ if and only if $\deg f = 0$.

§4.2

4.2.1. If $a, b \in F$ and $a \neq b$, show that $x + a$ and $x + b$ are relatively prime in $F[x]$.

• Proof by contradiction.

4.2.2. Let $f, g \in F[x]$.

(a) If $f \mid g$ and $g \mid f$, show that $f = cg$ for some non-zero $c \in F$.

• Observe that $\deg(f) \leq \deg(g)$, $\deg(g) \leq \deg(f)$ and $\deg(f) = \deg(c) + \deg(g)$.

(b) If f and g are monic and $f \mid g$ and $g \mid f$, show that $f = g$.

• Show f and g have same leading term to if $f = cg$ then $c = 1$.

4.2.3. Let $f \in F[x]$ and assume $f \mid g$ for every nonconstant $g \in F[x]$. Show that f is a constant polynomial.

• Show that $\deg(f) \leq \deg(g)$ for **every** polynomial g (forcing $\deg(f) = 0$).

4.2.4. Let $f, g \in F[x]$, not both zero, and let $d = GCD(f, g)$. If h is a common divisor of f and g of highest possible degree, then prove that $h = cd$ for some nonzero $c \in F$.

• Use uniqueness of GCD and the fact that every nonzero polynomial has a monic associate.

4.2.5. If f is relatively prime to 0_F, what can be said about f.

• Note $CGD(f, 0_F) = 1_F$ is the monic common divisor of greatest possible degree, and every polynomial divides 0_F.

4.2.6. Let $f, g, h \in F[x]$, with f and g relatively prime. If $f \mid h$ and $g \mid h$, prove that $fg \mid h$.

• Write $h = qf = rg$. Then multiply the relation $1_F = uf + vg$ by h, and then replace ufh with $uf(rg)$ and vg with $v(qf)$ on the right hand side.

4.2.7. Let $f, g, h \in F[x]$, with f and g relatively prime. If $h \mid f$, prove that h and g are relatively prime.

• Write $1_F = uf + vg$ and then replace f by qh, and note that any polynomial that divides h and g must divide 1_F.

4.2.8. Let $f, g, h \in F[x]$, with f and g relatively prime. Prove that the GCD of fh and g is the same as the GCD of h and g.

• Show that the sets of common divisors of f and g is the same as the set of common divisors of fh and g and then conclude since the sets of common divisors are the same, their monic elements of highest degree (the corresponding GCD's) must coincide.

§4.3

4.3.1 Prove that f and g are associates in $F[x]$ if and only if $f \mid g$ and $g \mid f$.

• See problem 4.2.2.

4.3.2 Prove that f is irreducible in $F[x]$ if and only if its associates are irreducible.

• Proof by contradiction.

4.3.3. If p and q are nonassociate irreducibles in $F[x]$, prove that p and q are relatively prime.

• List possible monic divisors of p and q and compare.

§4.4

4.4.1. Verify that every element of $\mathbb{Z}_3$ is a root of $f = x^3 - x \in \mathbb{Z}_3$.

4.4.2. Use the Factor Theorem to show that $f = x^7 - x$ factors in $\mathbb{Z}_7$ as

$$f = x(x - [1]_7)(x - [2]_7)(x - [3]_7)(x - [4]_7)(x - [5]_7)(x - [6]_7) \quad .$$

4.4.3. If $a \in F$ is a nonzero root of

$$f = c_n x^n + \ldots + c_1 x + c_0 \in F[x] \quad ,$$

show that a^{-1} is a root of

$$g = c_0 x^n + c_1 x^{n-1} + \cdots + c_n \quad .$$

4.4.4. Prove that $x^2 + 1$ is reducible in $\mathbb{Z}_p[x]$ if and only if there exists integers a and b such that $p = a + b$ and $ab \equiv 1 \ (mod\ p)$.

• If $x^2 = 1$ is reducible, it must be factorizable in terms of degree 1 polynomials, and, moreover, by Corollary 4.10 it must have a root in $\mathbb{Z}_p$. (N.B., $\mathbb{Z}_p$ is a field whenever p is prime, as we are assuming here.) Thus, $x^2 + 1$ must factorize as

$$x^2 + 1 = (x - a)\, q$$

with $a \in \mathbb{Z}_p$ satisfying $a^2 + [1]_p = [0]_p$. It follows easily that the other factor q must be of the form $q = x - b$. So we have

$$x^2 + 1 = (x - a)(x - b) = x^2 + (a + b)x + ab$$

Comparing coefficients on both sides we conclude

$$\begin{aligned} (a+b) &= [0]_p \\ ab &= [1]_p \end{aligned}$$

4.4.5. Find a polynomial of degree 2 in $\mathbb{Z}_6[x]$ that has four roots in $\mathbb{Z}_6$. Does this contradict Corollary 4.13?