**Spring 2019, Math 320: Week 9 Problem Set**
**Due: Tuesday, April 9, 2019**
**Polynomial Rings and Divisibility**

**Discussion problems.** The problems below should be worked on in class.

(D1) *Divisibility in* $\mathbb{Q}[x]$ *and* $\mathbb{Z}_p[x]$.

(a) First, divide $a(x) = 2x^5 - x^4 + 3x^3 + 2x^2 + x + 1$ by $b(x) = 2x^2 + x + 1$ over $\mathbb{Q}$. Next, divide $a(x)$ by $b(x)$ over $\mathbb{Z}_7$. How are your answers related?

(b) Divide $a(x) = x^4 + x^3 + 2x^2 + x + 1$ by $b(x) = x^2 + 1$ over $\mathbb{Q}$. Without doing another division, decide whether you would get a remainder if you divided over $\mathbb{Z}_5$.

(c) Determine whether $b(x) = x + 2$ divides $a(x) = x^3 + 3x^2 - 4$ over $\mathbb{Q}$ **without** dividing over $\mathbb{Q}$ (you **may** divide over $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\ldots$).

(D2) *The polynomial ring* $\mathbb{Z}_n[x]$. The goal of this problem is to identify some "nice" properties that $R[x]$ can fail to have when $R$ is not a field.

(a) Which elements of $\mathbb{Z}_3[x]$ are units?

(b) Find a unit in $\mathbb{Z}_4[x]$ with positive degree.

(c) What is the highest degree a zero-divisor can have in $\mathbb{Z}_6[x]$?

(d) Find an element of $\mathbb{Z}_6[x]$ that is **not** a zero-divisor, but whose leading coefficient **is** a zero-divisor of $\mathbb{Z}_6$.

(e) Characterize the zero-divisors of $\mathbb{Z}_4[x]$. State your claim formally, and prove it!

(f) Find $\gcd(84, 32)$ using the Euclidean algorithm. Note: this is a week 1 question!

(g) Use the Euclidean algorithm to find the greatest common divisor of

$$f(x) = x^3 + 3x^2 + 2x - 1 \qquad \text{and} \qquad g(x) = x^3 - 2x + 1$$

in $\mathbb{Q}[x]$. Do the same in $\mathbb{Z}_5[x]$.

(h) Find a non-constant polynomial $f(x) \in \mathbb{Z}_6[x]$ such that $f(x) \mid 2x$ and $f(x) \mid 4x$. What is the highest degree $f(x)$ can have? (Note that the Euclidean algorithm can't be used here.)

(D3) *Similarities between* $F[x]$ *and* $\mathbb{Z}$. In what follows, assume $F$ is a field.

(a) Below is a (correct!) proof that if $a, b, c \in \mathbb{Z}$ with $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

*Proof.* Since $a \mid bc$ and $\gcd(a, b) = 1$, there exist $m \in \mathbb{Z}$ and $x, y \in \mathbb{Z}$ satsifying $am = bc$ and $ax + by = 1$. As such, $c = acx + bcy = acx + amy = a(cx + my)$, so $a \mid c$. □

Prove if $a(x), b(x), c(x) \in F[x]$ with $a(x) \mid b(x)c(x)$ and $\gcd(a(x), b(x)) = 1$, then $a(x) \mid c(x)$.

(b) Fill in the gaps in the proof that if $a, b, c \in \mathbb{Z}$ with $c > 0$, then $\gcd(ca, cb) = c \gcd(a, b)$. Identify where the hypothesis $c > 0$ is used.

*Proof.* Let $d = \gcd(a, b)$, so $a = md$ and $b = nd$ for some $m, n \in \mathbb{Z}$. This means _______ and _______, so $cd \mid ca$ and $cd \mid cb$. Moreover, $ax + by = d$ for some $x, y \in \mathbb{Z}$, so _______, meaning $cd = \gcd(ca, cb)$. □

(c) State and prove an analogous result to part (b) for elements of $F[x]$.

**Homework problems.** You must submit *all* homework problems in order to receive full credit.

(H1) Consider the polynomials $f(x) = x^5 + 3x^4 - 7x^3 + 5x + 4$ and $g(x) = 2x^2 + x + 5$. Use the division algorithm to divide $f(x)$ by $g(x)$ over $\mathbb{Z}_3$. Do the same over $\mathbb{Z}_{11}$. Do your answers allow you to conclude whether $g(x)$ divides $f(x)$ over $\mathbb{Q}$?

(H2) Find the greatest common divisor of $f(x) = x^6 + x^4 + x^2$ and $g(x) = x^4 + x^3 + x$ over $\mathbb{Z}_3$ using the Euclidean algorithm.

(H3) Determine which elements of $\mathbb{Z}_6[x]$ with degree 1 are units, and which are zero-divisors. Reminder: $2x + 3$ and $5x$ both have degree 1, but 4 does not.

(H4) Locate specific $a(x), b(x) \in \mathbb{Z}[x]$ with $b(x) \neq 0$ such that it is impossible to write

$$a(x) = q(x)b(x) + r(x)$$

with $q(x), r(x) \in \mathbb{Z}[x]$ and $\deg r(x) < \deg b(x)$. Why does this not contradict Theorem 4.6?

(H5) Suppose $F$ is a field. Prove that if $a, b \in F$ with $a \neq b$, then $\gcd(x + a, x + b) = 1$.

(H6) Determine whether each of the following statements is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) If $R$ is a ring and $a \in R$ is a unit, then $a$ is also a unit in $R[x]$.

(b) If $R$ is a ring and $a \in R$ is a zero-divisor, then $a$ is also a zero-divisor in $R[x]$.

(c) If $R$ is a ring and $f(x), g(x) \in R[x]$, then $\deg(f(x)g(x)) = (\deg f(x))(\deg g(x))$.

**Challenge problems.** Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Fix an integral domain $R$. Suppose that the division algorithm always holds for $R[x]$ (that is, for every $a(x)$, $b(x) \in R[x]$ with $b(x) \neq 0$, there exist unique $q(x)$, $r(x) \in R[x]$ with $\deg r(x) < \deg b(x)$ such that $a(x) = q(x)b(x) + r(x)$ holds). Prove that $R$ is a field.