Fall 2023, Math 320: Week 9 Problem Set
Due: Thursday, November 2nd, 2023
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? Hint: consult your notes from Tuesday!

(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) 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?

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

(D3) *Greatest common divisors.* In what follows, assume F is a field. Given polynomials $a(x), b(x) \in F[x]$ not both zero, their *greatest common divisor*, denoted $\gcd(a(x), b(x))$, is the **monic** polynomial of highest degree that divides both $a(x)$ and $b(x)$.

(a) Show $d(x) = x + 2 \in \mathbb{Z}_3[x]$ divides both $a(x) = x^3 + 2x^2 + 2x + 1$ and $b(x) = x^3 + 2$.

(b) Use the following analog of Bézout's identity for $F[x]$ to prove $d(x)$ in part (a) is the greatest common divisor of $a(x)$ and $b(x)$. Hint: $u(x)$ and $v(x)$ will be linear.

Theorem (Bézout's identity)**.** *If $d(x)$ is monic and divides $a(x)$, and $b(x)$, then $d(x) = \gcd(a(x), b(x))$ if and only if there exist $u(x), v(x) \in F[x]$ with $d(x) = a(x)u(x) + b(x)v(x)$.*

(c) Show that $2x + 1$ also divides $a(x)$ and $b(x)$. Why is it not the GCD?

(d) Locate a degree-2 polynomial in $\mathbb{Z}_2[x]$ that is coprime to $x^2 + x$.

(e) 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 $a \mid c$. $\square$

Copy the above proof onto the board **in full**. Then, 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 $a(x) \mid c(x)$.

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) 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 the constant polynomial 4 does not.

(H3) Suppose F is a field. Prove that if $a, b \in F$ with $a \neq b$, then $\gcd(x + a, x + b) = 1$.

(H4) 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 the constant polynomial $f(x) = a$ is also a unit in $R[x]$.

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

(c) For any $a(x), b(x) \in \mathbb{Z}[x]$ with $b(x) \neq 0$, there exist unique $q(x), r(x) \in \mathbb{Z}[x]$ with $\deg r(x) < \deg b(x)$ such that $a(x) = q(x)b(x) + r(x)$.

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.