Fall 2018, Math 320: Week 8 Problem Set
Due: Tuesday, October 23rd, 2018
Polynomial Rings and Divisibility

Discussion problems. The problems below should be completed in class.

(D1) *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. For which n is this possible in $\mathbb{Z}_n[x]$?

(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 the common divisor of $2x$ and $4x$ over $\mathbb{Z}_6$ of highest degree (note the Euclidean algorithm can't be used here).

(D2) *Similarities between* $F[x]$ *and* $\mathbb{Z}$. In what follows, assume F is a field.

(a) Below is the proof that for any $a, b, c \in \mathbb{Z}$, if $a \mid bc$ 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 that for any $a(x), b(x), c(x) \in F[x]$, if $a(x) \mid b(x)c(x)$ 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 $F[x]$.

(d) Prove that if $a(x), b(x) \in F[x]$ satisfy $a(x) \mid b(x)$ and $b(x) \mid a(x)$, then $a(x) = Cb(x)$ for some $C \in F$. Hint: consider $\deg a(x)$ and $\deg b(x)$.

(e) Prove that in part (d), if $a(x)$ and $b(x)$ are both monic, then $a(x) = b(x)$.

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

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) 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 tell you whether $g(x)$ divides $f(x)$ over $\mathbb{Q}$?

(R2) 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.

(R3) 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.

(R4) 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 field, then $R[x]$ is a field.

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

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) Suppose R is a nonzero ring, and let $\phi : R[x] \to R$ denote the map given by

$$\phi(a_d x^d + \cdots + a_1 x + a_0) = a_0.$$

for any $a_0, a_1, \ldots, a_d \in R$. Prove ϕ is a surjective homomorphism, but not an isomorphism.

(S2) Fix a ring R, and let $D : \mathbb{R}[x] \to \mathbb{R}[x]$ denote the *derivative* map from calculus, that is,

$$D(a_d x^d + \cdots + a_2 x^2 + a_1 x + a_0) = d a_d x^{d-1} + \cdots + 3a_3 x^2 + 2a_2 x + a_1$$

for all $a_0, a_1, \ldots, a_d \in \mathbb{R}$. Determine which of the isomorphism requirements D satisfies.

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) Let R be a commutative ring, and fix $a(x) \in R[x]$. Prove that there exists a *unique* homomorphism $\phi : R[x] \to R[x]$ satisfying $\phi(r) = r$ for every $r \in R$ and $\phi(x) = a(x)$.