Fall 2018, Math 320: Week 9 Problem Set
Due: Tuesday, October 30th, 2018
Polynomial Factorization and Irreducibility

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

(D1) *Factoring polynomials over* $\mathbb{Z}_n$.

(a) Compare your answers to (P1). Over each ring, compare $\deg f(x)$ to the number of roots, and check these against Corollary 4.17.

(b) Factor $x^3 + 3x + 1$ and $x^3 + 3x^2 + 2x + 4$ over $\mathbb{Z}_5$ as products of irreducibles. Hint: we can use the root theorem when the degree is at most 3.

(c) Factor $x^4 + x^3 + 2x^2 + 2x + 1$ over $\mathbb{Z}_3$. Does it suffice to look for roots?

(d) Factor $x^5 + 1$ over $\mathbb{Z}_5$. Do the same over $\mathbb{Z}_3$.

(e) Factor $x^4 + 4$ over $\mathbb{Z}_5$. Does it factor over $\mathbb{Q}$? (The answer may surprise you!)

(f) Let $f(x) = x^3 + 2x + 1$. Find a polynomial $g(x) \neq f(x)$ with $f(a) = g(a)$ for all $a \in \mathbb{Z}_3$. Are $f(x)$ and $g(x)$ the same element of $\mathbb{Z}_3[x]$?

(g) Find all roots of $3x + 3$ over $\mathbb{Z}_6$. Why is this surprising?

(h) Find a linear (i.e. degree 1) polynomial over $\mathbb{Z}_6$ with no solutions.

(D2) *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 $a \mid c$. $\square$

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 $cd = \gcd(ca, cb)$. $\square$

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

(d) Complete the following proof that if $a(x), b(x) \in F[x]$ satisfy $a(x) \mid b(x)$ and $b(x) \mid a(x)$, then $b(x) = Ca(x)$ for some $C \in F$.

Proof. Since $a(x) \mid b(x)$, we have $b(x) = a(x)f(x)$ for some $f(x) \in F[x]$, and since $b(x) \mid a(x)$, we have ______________. This means

$$\deg b(x) = \deg f(x) + \deg a(x) \geq \deg a(x) = \underline{\hspace{3cm}} \geq \deg b(x),$$

so $\deg b(x) = \deg$ _____ and $\deg f(x) = 0$. Choosing $C =$ _____ completes the proof. $\square$

(e) Fill in the details in the proof that if $a, b \in F$ with $a \neq b$, then $\gcd(x + a, x + b) = 1$.

Proof Sketch. Suppose $f(x) \in F[x]$ is monic with $f(x) \mid (x + a)$ and $f(x) \mid (x + b)$. Either $\deg f(x) = 0$ or $\deg f(x) = 1$. If $\deg f(x) = 1$, then $f(x) = x + c$ for some $c \in F$, which is impossible since $a \neq b$. This means $\deg f(x) = 0$. $\square$

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

(R1) Factor $f(x) = x^3 + 6x^2 + 1$ over $\mathbb{Z}_3$, $\mathbb{Z}_5$, and $\mathbb{Z}_7$. Does it factor over $\mathbb{Q}$?

(R2) Factor $f(x) = x^5 + 4x^4 + 8x^3 + 11x$ over $\mathbb{Q}$. Hint: first try to factor $f(x)$ over $\mathbb{Z}_3$ and $\mathbb{Z}_5$.

(R3) Find all monic irreducible polynomials in $\mathbb{Z}_3[x]$ of degree at most 2.

(R4) Factor $x^4 - x$ and $x^8 - x$ over $\mathbb{Z}_2$.

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) Consider the set $R = \{a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Q}[x] : a_0 \in \mathbb{Z}\}$ of polynomials over $\mathbb{Q}$ with integer constant term.

- (a) Prove that R is a subring of $\mathbb{Q}[x]$.
- (b) Show that some elements of R cannot be factored into a finite product of irreducibles. Hint: consider the element $f(x) = x$.

(S2) Consider the set $R = \{a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Q}[x] : a_1 = 0\}$ of polynomials over $\mathbb{Q}$ with no linear term.

- (a) Prove that R is a subring of $\mathbb{Q}[x]$.
- (b) Show that there are elements of R that can be factored as a product of irreducibles in more than one distinct way. Hint: consider the element $f(x) = x^6$.

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) Suppose $p > 0$ is prime, and fix a polynomial $f(x) \in \mathbb{Z}_p[x]$. Prove that there are infinitely many polynomials $g(x)$ such that $f(a) = g(a)$ for all $a \in \mathbb{Z}_p$.