Spring 2019, Math 320: Week 10 Problem Set
Due: Tuesday, April 16th, 2019
Polynomial Factorization and Irreducibility

Discussion problems. The problems below should be worked on 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) Find all roots of $3x + 3$ over $\mathbb{Z}_6$. Why is this surprising?

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

(d) Consider $f(x) = x^2 - x = (x)(x - 1)$ over $\mathbb{Z}_6$. Find all roots of $f(x)$ and the roots of its factors x and $x - 1$. What do you notice? Relate this to the root theorem.

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

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

(g) Show that $a(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$. Why is it **not** enough to verify $a(x)$ has no roots? Hint: write $a(x) = (x^2 + Ax + B)(x^2 + Cx + D)$ and prove no choice of A, B, C, and D works.

(h) Factor $x^5 + 1$ over $\mathbb{Z}_5$. Do the same over $\mathbb{Z}_2$.

(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 $a \mid c$. □

Copy the above proof onto the board. Then, prove that 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 $F[x]$.

(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

$$\deg b(x) = \deg f(x) + \deg a(x) \geq \deg a(x) = \text{______________} \geq \deg b(x),$$

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

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

(H1) Factor $f(x) = x^3 + 6x^2 + 1$ over $\mathbb{Z}_3$, $\mathbb{Z}_5$, and $\mathbb{Z}_7$. Based on this, does $f(x)$ factor over $\mathbb{Q}$?

(H2) Factor $f(x) = x^5 + 4x^4 + 8x^3 + 11x$ over $\mathbb{Q}$. Be sure to prove your factors are irreducible! Hint: first try to factor $f(x)$ over $\mathbb{Z}_3$ and $\mathbb{Z}_5$.

(H3) Find all monic irreducible polynomials in $\mathbb{Z}_2[x]$ of degree at most 4. Hint: be systematic!

(H4) Factor $x^4 - x$, $x^8 - x$, and $x^{16} - x$ over $\mathbb{Z}_2$. How does your answer relate to Problem (H3)?

(H5) Suppose $p > 0$ is prime, and $f(x) \in \mathbb{Z}_p[x]$. Prove that there are infinitely many polynomials $g(x)$ such that $f(a) = g(a)$ for all $a \in \mathbb{Z}_p$.

Hint: first find a polynomial $g(x)$ with positive degree such that $g(a) = 0$ for all $a \in \mathbb{Z}_p$.

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) Consider the set

$$R = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x] : a_0 \in \mathbb{Z}\}$$

of polynomials over $\mathbb{Q}$ with integer constant term.

(a) Prove that R is a subring of $\mathbb{Q}[x]$.

(b) Show that $f(x) = x \in R$ cannot be factored as a finite product of irreducibles.

(C2) Consider the set

$$R = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x] : a_1 = 0\}$$

of polynomials over $\mathbb{Q}$ with no linear term.

(a) Prove that R is a subring of $\mathbb{Q}[x]$.

(b) Show that $f(x) = x^6 \in R$ can be factored as a product of irreducibles in more than one way (that is, the factors are not simply associates of one another).