Spring 2019, Math 320: Week 12 Problem Set
Due: Tuesday, April 30th, 2019
Congruence Classes in $F[x]$ (Week 2)

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

(D1) *Polynomial quotients over $\mathbb{Z}_n$.*

- (a) Consider the ring $R = \mathbb{Z}_2[x]/\langle x^2 + 1\rangle$.
  - (i) List every element of R. Identify 0_R and 1_R.
  - (ii) Write down the operation tables for R.
  - (iii) Is R an integral domain? Is R a field?
- (b) Answer the same questions for the ring $T = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$. Is it possible $R \cong T$?
- (c) Demonstrate $[x - 1] \in \mathbb{Z}_7[x]/\langle x^2 - 3x + 2\rangle$ is a zero-divisor.
- (d) Demonstrate $[x^2 - 1] \in \mathbb{Z}_7[x]/\langle x^2 - 3x + 2\rangle$ is a zero-divisor.
- (e) Demonstrate $[x + 1] \in \mathbb{Z}_3[x]/\langle x^2 - 2x + 1\rangle$ is a unit.
- (f) Determine whether $[x^2 + 1] \in \mathbb{Z}_5[x]/\langle x^3 - 2x^2 + x\rangle$ is a zero-divisor, a unit, or neither.
- (g) Determine whether $[x^2 + 4] \in \mathbb{Z}_5[x]/\langle x^3 - 2x^2 + x\rangle$ is a zero-divisor, a unit, or neither.
- (h) Locate a field F with exactly 4 elements (hint: look at parts (a) and (b)). Additionally, locate a field with 8 elements, a field with 9 elements, and a field with 27 elements.

(D2) *Reducibility and quotient rings.* Unless otherwise stated, assume F is an arbitrary field.

- (a) Prove or disprove: in $F[x]/\langle p(x)\rangle$, if $[a(x)][b(x)] = [a(x)][c(x)]$, then $[b(x)] = [c(x)]$. Hint: consider the analogous question in $\mathbb{Z}_n$ first.
- (b) Suppose $p(x) \in F[x]$ is reducible. Prove that $F[x]/\langle p(x)\rangle$ is not an integral domain. Hint: look at parts (c) and (d) of Problem (D1).
- (c) Locate and correct the error in the following proof that if $p(x) \in F[x]$ is irreducible, then $R = F[x]/\langle p(x)\rangle$ is a field.

  Hint: there is a single adjective that can be added to fix the proof.

  Proof. We must show each $[f(x)] \in R$ with $[f(x)] \neq [0]$ has a multiplicative inverse. Since $p(x)$ is irreducible, its only divisors are 1 and $p(x)$, and since $[f(x)] \neq [0]$, we have $p(x) \nmid f(x)$. This means $\gcd(f(x), p(x)) = 1$, so $1 = f(x)u(x) + p(x)v(x)$ for some $u(x), v(x) \in F[x]$. As such,

  $$[f(x)][u(x)] = [f(x)][u(x)] + [p(x)][v(x)] = [f(x)u(x) + p(x)v(x)] = [1],$$

  which completes the proof. □
- (d) Relate parts (b) and (c) to familiar theorems for $\mathbb{Z}_n$.
- (e) Find a polynomial $p(x)$ that is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$. What does this mean about the rings $\mathbb{Q}[x]/\langle p(x)\rangle$ and $\mathbb{R}[x]/\langle p(x)\rangle$?

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

(H1) Let $R = \mathbb{Z}_2[x]/\langle x^3+x+1\rangle$. Find a **specific** element $r \in R$ such that $R\backslash\{0\} = \{r, r^2, r^3, \ldots\}$ (that is, so that every nonzero element of R is a power of r).

Hint: start by listing all of the elements of R.

(H2) Let $R_1 = \mathbb{Z}_2[x]/\langle x^2\rangle$ and $R_2 = \mathbb{Z}_2[z]/\langle z^2+1\rangle$. Prove $R_1 \cong R_2$.

Hint: write out the addition and multiplication tables for each ring, as they can be used to find an isomorphism $\phi : R_1 \to R_2$ and to verify it is indeed an isomorphism.

(H3) Determine whether each of the following statements is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) The ring $R = \mathbb{Z}_4[x]/\langle x^2+1\rangle$ contains no zero-divisors.

(b) The ring $R = \mathbb{Z}_5[x]/\langle x^2+1\rangle$ contains no zero-divisors.

(c) The ring $R = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is isomorphic to $\mathbb{Z}_4$.

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

$$F = \mathbb{Z}_2[x]/\langle x^3+x+1\rangle \qquad \text{and} \qquad F' = \mathbb{Z}_2[z]/\langle z^3+z^2+1\rangle.$$

Find an isomorphism $\varphi : F \to F'$.