Fall 2018, Math 320: Week 10 Problem Set
Due: Tuesday, November 6th, 2018
Congruence Classes in $F[x]$

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

(D1) *Arithmetic modulo $p(x)$.* Assume F is a field and $p(x) \in F[x]$.

(a) Determine whether $x^3 + 2x + 1 \equiv x^2 + 1 \bmod (x^2 - 1)$ over $\mathbb{Q}$.

(b) Use the fact that $[x^2] = [1]$ in $\mathbb{Q}[x]/\langle x^2-1\rangle$ to determine whether $[x^3+2x+1] = [x^2+1]$.

(c) Demonstrate $[x - 1] \in \mathbb{Q}[x]/\langle x^2 - 2x + 1\rangle$ is a zero-divisor.

(d) Demonstrate $[x - 2] \in \mathbb{Q}[x]/\langle x^2 - 2x + 1\rangle$ is a unit.

(e) 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?

(f) Consider the ring $R = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$.

(i) List every element in 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?

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

(a) 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 (e) of Problem (D1).

(b) 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.

(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.

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 (a) and (c) to familiar theorems for $\mathbb{Z}_n$.

(e) Fix $a \in F$, and let $R = F[x]/\langle x - a\rangle$. Fill in the details in the proof below that $R \cong F$.

Proof sketch. The map $\phi : F \to R$ given by $b \mapsto [b]$ is injective since $\deg(x - a) = 1$, and surjective since for each element $f(x) = b_d x^d + \cdots + b_1 x + b_0 \in F[x]$ we have

$$[f(x)] = [b_d a^d + \cdots + b_1 a + b_0] \in R.$$

Verifying ϕ is a homomorphism completes the proof. □

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

(R1) Determine whether $x^3 + x^2 \equiv x \bmod (x^2 + x + 1)$ over $\mathbb{Z}_2$ Do the same over $\mathbb{Z}_3$.

(R2) Every element of $R = \mathbb{Q}[x]/\langle x^2 + 2x - 1\rangle$ can be written as $[ax + b]$ for some $a, b \in \mathbb{Q}$. If $[ax + b][cx + d] = [rx + t]$ with $a, b, c, d, r, t \in \mathbb{Q}$, find r and t in terms of the others.

(R3) Let $R = \mathbb{Z}_2[x]/\langle x^3+x+1\rangle$. Find an element $r \in R$ with the property that every nonzero element of R is a power of r (that is, every nonzero element of R occurs in the list $r, r^2, r^3, \ldots$).

(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) The element $[x + 1] \in \mathbb{Q}[x]/\langle x^2 + x\rangle$ is a zero-divisor.

(b) The element $[x + 1] \in \mathbb{Q}[x]/\langle x^2 + x\rangle$ is a unit.

(c) If F is a field, $p(x) \in F[x]$, and $R = F[x]/\langle p(x)\rangle$, then R is a field.

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) Let $R = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. In Problem (S1) from Week 4, it was shown that R is a subring of $\mathbb{R}$ (you may assume that fact for this problem). Prove the map $R \to \mathbb{Q}[x]/\langle x^2 - 2\rangle$ given by $a + b\sqrt{2} \mapsto [a + bx]$ is an isomorphism.

(S2) Prove the map $\mathbb{C} \to \mathbb{R}[x]/\langle x^2 + 1\rangle$ given by $a + bi \mapsto [a + bx]$ is an isomorphism.

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) Characterize the units and zero-divisors of $\mathbb{Q}[x]/\langle x^2\rangle$.