Fall 2023, Math 320: Week 11 Problem Set
Due: Thursday, November 16th, 2023
Congruence Classes in $F[x]$

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

(D1) *Arithmetic modulo $p(x)$.* For this problem, all polynomials have coefficients in $\mathbb{Q}$.

(a) Determine whether $x^3 + 2x + 1 \equiv x^2 + 1 \bmod (x^2 - 1)$.
(b) Locate the canonical representative of $x^3 + 2x + 1$ modulo $x^2 - 1$.
(c) Use the fact that $[x^2 - 1] = [0]$ in $\mathbb{Q}[x]/\langle x^2 - 1\rangle$ to demonstrate $[x]^2 = [1]$.
(d) Use part (c) to find the canonical representative of $[x^5 - 2x^4 + 2x + 1]$ **without** division.
(e) Demonstrate $[x - 1] \in \mathbb{Q}[x]/\langle x^2 - 2x + 1\rangle$ is a zero-divisor., and $[x - 2]$ is a unit.

(D2) *Interpreting quotient rings.* Consider the rings

$$R = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R} \qquad \text{and} \qquad T = \mathbb{Q}[x]/\langle x^2 - 2\rangle.$$

(a) Determine whether $\mathbb{Q} \subseteq R$.
(b) Find the sum and product of $2 + 3\sqrt{2}$ and $5 + 7\sqrt{2}$ in R.
(c) Find the canonical representative of $[x]^2$ in T.
(d) Find the sum and product of $[2 + 3x]$ and $[5 + 7x]$ in T. Do they look familiar?
(e) Define $\varphi : R \to T$ by $\varphi(a + b\sqrt{2}) = [a + bx]$. We will show φ is an isomorphism.
  (i) Begin by proving φ is a homomorphism.
  (ii) Fill in the gaps in the following proof that φ is injective.

  Proof. Suppose $\varphi(a + b\sqrt{2}) = \varphi(c + d\sqrt{2})$. This implies $[a + bx] = [c + dx]$, so

$$(a - c) + (b - d)x = (a + bx) - (c + dx) = \underline{\hspace{3cm}}$$

  for some $k(x) \in \mathbb{Q}[x]$. Since $\deg(k(x)\underline{\hspace{3.5cm}}) = 1$, we must have $k(x) = 0$. This yields $a - c = 0$ and $b - d = 0$, and thus $a + b\sqrt{2} = c + d\sqrt{2}$. □

  (iii) Complete the only remaining part of the proof that φ is an isomorphism.

(D3) *Identifying familiar quotient rings.*

(a) Find a field F and a polynomial $p(x)$ so that $\mathbb{Q}[\sqrt{5}] \cong F[x]/\langle p(x)\rangle$. No proof is required, but specify the isomorphism you would use.
(b) Consider the **set**

$$R = \{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}.$$

Is R a ring? If not, what must be added to ensure R is closed under both operations?
(c) Based on part (b), how should $\mathbb{Q}[\sqrt[3]{2}]$ be defined so that it is a subring of $\mathbb{R}$?
(d) Find a field F and a polynomial $p(x)$ so that $\mathbb{Q}[\sqrt[3]{2}] \cong F[x]/\langle p(x)\rangle$. No proof is required, but specify the isomorphism you would use.
(e) Fix a field F, $a \in F$, and $f(x) \in F[x]$, and let $R = F[x]/\langle x - a\rangle$. Locate and correct the (subtle!) error in the proof that the canonical representative of $[f(x)]$ is $[f(a)]$.

Proof. Write $f(x) = b_d x^d + \cdots + b_1 x + b_0$, where $d \in \mathbb{Z}_{\geq 0}$ and $b_0, \ldots, b_d \in F$. Since $[x - a] = [0]$, we have $[x] = [a]$, so

$$\begin{aligned}[f(x)] &= [b_d x^d + \cdots + b_1 x + b_0] = [b_d][x]^d + \cdots + [b_1][x] + [b_0] \\ &= [b_d][a]^d + \cdots + [b_1][a] + [b_0] = [b_d a^d + \cdots + b_1 a + b_0] = [f(a)]\end{aligned}$$

Since $f(a)$ is a constant, $\deg f(a) = 0$, so $\deg f(a) < \deg(x - a)$, as desired. □

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

(H1) Determine whether $x^3 + x^2 \equiv x \bmod (x^2 + x + 1)$ over $\mathbb{Z}_2$ Do the same over $\mathbb{Z}_3$.

(H2) Every element of $R = \mathbb{Q}[x]/\langle x^2+2x-1\rangle$ can be written in the form $[ax+b]$ for some $a, b \in \mathbb{Q}$ (this is the canonical representative). If $[ax + b][cx + d] = [rx + t]$ with $a, b, c, d, r, t \in \mathbb{Q}$, find formulas for r and t in terms of a, b, c, and d (this is the *multiplication rule* for R).

(H3) Prove the map $\varphi : \mathbb{C} \to \mathbb{R}[x]/\langle x^2 + 1\rangle$ given by $a + bi \mapsto [a + bx]$ is an isomorphism.

(H4) Consider the ring $R = \mathbb{Q}[x]/\langle x^2\rangle$. It turns out every nonzero element of R is either a unit or a zero-divisor (you do **not** need to prove this). Determine which elements are units and which are zero-divisors.

(H5) 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 $[x - 2] \in \mathbb{Q}[x]/\langle x^2 - 2x\rangle$ is a zero-divisor.

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

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 $R = \mathbb{Z}_3[z]/\langle z^2 + z + 2\rangle$.

(a) Prove that R is a field by locating the multiplicative inverse of each nonzero element.

(b) Factor $x^9 - x \in \mathbb{Z}_3[x]$ and $x^9 - x \in R[x]$. Remember: z is a **coefficient** in $R[x]$.