Math 461 **Spring 2020**
Homework 5 **Drew Armstrong**

Problem 1. Use the Rational Root Test to split the following polynomial:

$$f(x) = 8x^3 + 4x^2 - 2x - 1 \in \mathbb{Q}[x].$$

Problem 2. Symmetric Polynomials. Suppose that the polynomial $x^3 + x^2 + 2x + 3$ has the roots r, s, t in some field. Find some integer coefficients $a, b, c \in \mathbb{Z}$ such that the polynomial $x^3 + ax^2 + bx + c$ has the roots rs, rt, st.

Problem 3. Some Specific Cyclotomic Polynomials. Recall the definition of the nth cyclotomic polynomial:

$$\Phi_n(x) = \prod_{\substack{1\leq k\leq n \\ \gcd(k,n)=1}} (x - e^{2\pi ik/n}).$$

(a) If p is prime, show that $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$. [Hint: In this case we have $\gcd(k, p) = 1$ for all $1 \leq k < p$ and hence $\Phi_p(x) = (x - \omega)(x - \omega^2)\cdots(x - \omega^{p-1})$ for $\omega = e^{2\pi i/p}$. On the other hand, we know that $x^p - 1 = (x - 1)(x - \omega)\cdots(x - \omega^{p-1})$.]

(b) If $n = 2^m$ for some $m \geq 1$, show that $\Phi_n(x) = 1 + x^{n/2}$. [Hint: Show that the roots of $\Phi_n(x)$ are precisely the $(n/2)$th roots of -1. First, observe that $\gcd(k, n) = 1$ if and only if k is odd, hence the roots of $\Phi_n(x)$ are $(e^{2\pi i/n})^{\text{odd}}$. Second, observe that $\alpha^{n/2} = -1 = e^{i(\pi+2\pi k)}$ implies $\alpha = e^{i(\pi+2\pi k)/(n/2)} = (e^{2\pi i/n})^{1+2k}$ for all $k \in \mathbb{Z}$.]

Problem 4. Uniqueness of Quotient and Remainder. Let $\mathbb{F}$ be a field and consider polynomials $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0(x)$.

(a) Suppose that we have $q_1(x), r_1(x), q_2(x), r_2(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = q_1(x)g(x) + r_1(x), \\ \deg(r_1) < \deg(g), \end{cases} \qquad \begin{cases} f(x) = q_2(x)g(x) + r_2(x), \\ \deg(r_2) < \deg(g). \end{cases}$$

In this case, prove that $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. [Hint: First note that $(q_1 - q_2)g = (r_2 - r_1)$. If $q_1 \neq q_2$ then this implies that $\deg(r_2 - r_1) \geq \deg(g)$. On the other hand, we have $\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\}$.]

(b) Now let $R \subseteq \mathbb{F}$ be a subring. Suppose that we have $f(x), g(x) \in R[x]$ where $g(x)$ has leading coefficient 1, and suppose that $f(x) = g(x)q(x)$ for some $q(x) \in \mathbb{F}[x]$. In this case, use part (a) to show that we must actually have $q(x) \in R[x]$. [Hint: Since $g(x) \in R[x]$ has leading coefficient 1, we may apply long division to obtain $f(x) = g(x)q'(x) + r'(x)$ for some $q'(x), r'(x) \in R[x]$ with $\deg(r') < \deg(g')$. On the other hand, we have assumed that $f(x) = g(x)q(x) + 0$ for some $q(x) \in \mathbb{F}[x]$. Apply (a) to show that $q(x) = q'(x)$, and hence $q(x) \in R[x]$.]

Problem 5. Cyclotomic Polynomials Have Integer Coefficients. We will prove in class that cyclotomic polynomials satisfy the following identity:

$$x^n - 1 = \prod_{\substack{1\leq d\leq n \\ d|n}} \Phi_d(x).$$

Use this identity and Problem 4(b) to prove by induction that $\Phi_n(x) \in \mathbb{Z}[x]$ for all $n \geq 1$. [Hint: Suppose that we have $x^n - 1 = \Phi_n(x)q(x)$ for some polynomial $q(x) \in \mathbb{Z}[x]$. Then since $\Phi_n(x) \in \mathbb{C}[x]$ has leading coefficient 1, we can apply Problem 4(b) with $R = \mathbb{Z}$ and $\mathbb{F} = \mathbb{C}$.]

Problem 6. A Property of Quadratic Field Extensions. The construction of $\mathbb{C}$ from $\mathbb{R}$ can be generalized as follows. Let $\mathbb{E} \supseteq \mathbb{F}$ be fields and let $\iota \in \mathbb{E}$ be some element satisfying $\iota \notin \mathbb{F}$ and $\iota^2 \in \mathbb{F}$. Then I claim that the following set is a **subfield** of $\mathbb{E}$:

$$\mathbb{F}(\iota) := \{a + b\iota : a, b \in \mathbb{F}\}.$$

Furthermore, the conjugation operator $(a + b\iota)^* = (a - b\iota)$ behaves exactly like complex conjugation. Jargon: We say that $\mathbb{F}(\iota) \supseteq \mathbb{F}$ is a *quadratic field extension.* The following Lemma will be useful in our discussion of impossible constructions:

> *Consider a polynomial $f(x) \in \mathbb{F}[x]$ of degree 3. If $f(x)$ has some root $\alpha \in \mathbb{F}(\iota)$ in a quadratic field extension then I claim that $f(x)$ also has a root in $\mathbb{F}$.*

Prove the Lemma. [Hint: Let $\alpha \in \mathbb{F}(\iota)$ be a root of $f(x)$. If $\alpha \in \mathbb{F}$ then we are done. Otherwise, the conjugate $\alpha^* \in \mathbb{F}(\iota)$ is another root of $f(x)$, hence by Descartes' Factor Theorem we have

$$f(x) = (x - \alpha)(x - \alpha^*)g(x) \quad \text{for some } g(x) \in \mathbb{F}(\iota)[x] \text{ of degree } 1.$$

Use Problem 4(b) to show that $g(x) \in \mathbb{F}[x]$, hence $g(x)$ has a root in $\mathbb{F}$.]