Math 562/662 **Spring 2022**
Homework 6 **Drew Armstrong**

---

1. Irreducible Polynomials of Small Degree. Let $\mathbb{F}$ be a field and consider a polynomial $f(x) \in \mathbb{F}[x]$ of degree 2 or 3. Prove that $f(x)$ is irreducible over $\mathbb{F}$ if and only if $f(x)$ has no root in $\mathbb{F}$. [Hint: Equivalently, prove that $f(x)$ if reducible if and only if has a root.]

2. Rational Roots. Consider a polynomial of degree $n \geq 1$ with integer coefficients:

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}[x].$$

If $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, prove that we must have $a|c_0$ and $b|c_n$. Use this result and Problem 1 to prove that the polynomial $4x^3 + 29x - 3$ is irreducible over $\mathbb{Q}$.

3. Repeated Roots. For any field $\mathbb{F}$ we define the function $D : \mathbb{F}[x] \to \mathbb{F}[x]$ by[1]

$$D\left(\sum a_k x^k\right) = \sum k \cdot a_k x^{k-1}.$$

This *formal derivative* satisfies all the usual properties, such as the product rule. Now consider a polynomial $f(x) \in \mathbb{F}[x]$ and an element of a field extension $\alpha \in \mathbb{E} \supseteq \mathbb{F}$.

(a) If $f(x) = (x - \alpha)^2 g(x)$ for some $g(x) \in \mathbb{E}[x]$, prove that $f(\alpha) = 0$ and $Df(\alpha) = 0$.
(b) Conversely, suppose that $f(\alpha) = 0$ and $Df(\alpha) = 0$. In this case, prove that there exists a polynomial $g(x) \in \mathbb{E}[x]$ such that $f(x) = (x - \alpha)^2 g(x)$. [Hint: Use Descartes' Factor Theorem twice.]

4. Characteristic of a Field. For any field $\mathbb{F}$, we have seen that there exists a unique group homomorphism $\varphi : (\mathbb{Z}, +, 0) \to (\mathbb{F}, +, 0)$ sending 1 to 1. Namely,[2]

$$\varphi(k) = k \cdot 1 := \begin{cases} \overbrace{1 + 1 + \cdots + 1}^{k \text{ times}} & \text{if } k \geq 1, \\ 0 & \text{if } k = 0, \\ \underbrace{-1 - 1 - \cdots - 1}_{-k \text{ times}} & \text{if } k \leq -1. \end{cases}$$

One can check that this function $\varphi : \mathbb{Z} \to \mathbb{F}$ is also a ring homomorphism. If $\ker \varphi = n\mathbb{Z}$ then we say that $\mathrm{char}(\mathbb{F}) := n$ is the *characteristic of the field* $\mathbb{F}$.

(a) If $\mathbb{F}$ is finite, show that $\mathrm{char}(\mathbb{F}) \neq 0$. [Hint: The First Isomorphism Theorem says that $\mathbb{Z}/\ker\varphi \cong \mathrm{im}\,\varphi$, where $\mathrm{im}\,\varphi$ is a subring of $\mathbb{F}$. But $\mathbb{Z}/0\mathbb{Z}$ is infinite.]
(b) If $n \geq 1$ is not prime, show that $\mathbb{Z}/n\mathbb{Z}$ is not a domain.
(c) If $\mathbb{F}$ is finite, combine (a) and (b) to show that the characteristic $\mathrm{char}(\mathbb{F})$ is prime. [Hint: A subring of a field is necessarily a domain.]

---

[1] Given $k \in \mathbb{Z}$ and $a_k \in \mathbb{F}$, the element $k \cdot a_k \in \mathbb{F}$ is defined repeated addition or subtraction. See Problem 4.

[2] Previously we used the multiplicative notation $\varphi(a) = a^k$ but the concept is the same.