Math 562/662 **Spring 2024**
Homework 5 **Drew Armstrong**

---

1. Formal Derivatives. For any field $\mathbb{F}$ we consider the $\mathbb{F}$-linear function $D : \mathbb{F}[x] \to \mathbb{F}[x]$ defined on the basis $1, x, x^2, \ldots$ by $Dx^n := nx^{n-1}$. That is, we define

$$D\left(\sum_{k\geq 0} a_k x^k\right) := \sum_{k\geq 1} k a_k x^{k-1}.$$

(a) For all $f(x), g(x) \in \mathbb{F}[x]$ prove that $D[f(x)g(x)] = f(x)Dg(x) + Df(x)g(x)$.
(b) For all $f(x) \in \mathbb{F}[x]$ and $n \geq 1$ prove that $D[f(x)^n] = nf(x)^{n-1}Df(x)$. [Hint: Use part (a) and induction.]

2. Invariance of GCD. Consider a field extension $\mathbb{E} \supseteq \mathbb{F}$ and two polynomials $f(x), g(x) \in \mathbb{F}[x]$. Let $d(x) \in \mathbb{F}[x]$ be the (monic) GCD of $f(x)$ and $g(x)$ in $\mathbb{F}[x]$ and let $D(x) \in \mathbb{E}[x]$ be the (monic) GCD of $f(x)$ and $g(x)$ in $\mathbb{E}[x]$. Prove that $d(x) = D(x)$. [Hint: The Euclidean Algorithm produces $a(x), b(x) \in \mathbb{F}[x]$ and $A(x), B(x) \in \mathbb{E}[x]$ such that $f(x)a(x) + g(x)b(x) = d(x)$ and $f(x)A(x) + g(x)B(x) = D(x)$. Use this to show that $d(x)|D(x)$ and $D(x)|d(x)$ in $\mathbb{E}[x]$, which implies that $d(x)$ and $D(x)$ are associate in $\mathbb{E}[x]$.]

3. Repeated Factors of Polynomials. If $\mathbb{F}$ is a field then we know that $\mathbb{F}[x]$ is a unique factorization domain. That is, for all $f(x), p(x) \in \mathbb{F}[x]$ with $p(x)$ irreducible, there is a well-defined *multiplicity* $v_p(f) \in \mathbb{N}$, which is the number of times that $p(x)$ occurs in the prime factorization of $f(x)$. We say that $p(x)$ is a *repeated factor* when $v_p(f) \geq 2$.

(a) If $f(x) \in \mathbb{F}[x]$ has a repeated prime factor, show that $\gcd(f, Df) \neq 1$. [Hint: Suppose that $f(x) = p(x)^2 g(x)$. Apply Problem 1 to show that $p(x)$ also divides $Df(x)$.]
(b) If $\gcd(f, Df) \neq 1$, show that $f(x)$ has a repeated prime factor. [Hint: Suppose that $p(x)$ is a common prime divisor of $f(x)$ and $Df(x)$. Say $f(x) = p(x)g(x)$. Apply Problem 1 to show that $p(x)$ divides $Dp(x)g(x)$. Then use Euclid's Lemma and the fact that $\deg(Dp) < \deg(p)$ to show that $p(x)$ divides $g(x)$.]
(c) It follows from (a) and (b) that

$$f(x) \text{ has no repeated prime factor in } \mathbb{F}[x] \quad \Leftrightarrow \quad \gcd(f, Df) = 1 \text{ in } \mathbb{F}[x].$$

We will apply this result to roots. We say that $f(x) \in \mathbb{F}[x]$ is *separable* if it has no repeated root in any field extension. Show that

$$f(x) \text{ is separable} \quad \Leftrightarrow \quad \gcd(f, Df) = 1 \text{ in } \mathbb{F}[x].$$

[Hint: For any field extension $\mathbb{E} \supseteq \mathbb{F}$, Problem 2 says that

$$\gcd(f, Df) = 1 \text{ in } \mathbb{F}[x] \quad \Longleftrightarrow \quad \gcd(f, Df) = 1 \text{ in } \mathbb{E}[x].]$$

4. Counting Reduced Fractions. For any $n \geq 1$ we consider the following subsets of $\mathbb{Q}$:

$$\begin{aligned} F_n &:= \{k/n : 0 \leq k < n\}, \\ F'_n &:= \{k/n : 0 \leq k < n \text{ and } \gcd(k, n) = 1\} \end{aligned}$$

Note that $\#F_n = n$ and $\#F'_n = \phi(n)$. In this problem we will show that

$$F_n = \coprod_{d|n} F'_d,$$

which implies that $n = \sum_{d|n} \phi(d)$.

(a) Show that F_n is a subset of $\cup_{d|n} F'_d$. [Hint: Every fraction can be reduced.]
(b) Show that $\cup_d F'_d$ is a subset of F_n.
(c) Show that $d \neq e$ implies $F'_d \cap F'_e = \emptyset$. [Hint: Suppose for contradiction that α is in F'_d and F'_e, so we can write $\alpha = k/d = \ell/e$ with $0 \leq k < d$, $0 \leq \ell < e$ and $\gcd(k,d) = \gcd(\ell, e) = 1$. Use this to show that $d|e$ and $e|d$.]

5. The Primitive Root Theorem. If $\mathbb{E}$ is a finite field then we will prove that $(\mathbb{E}^\times, \cdot, 1)$ is a cyclic group. Suppose that $\#\mathbb{E} = p^n$, and hence $\#\mathbb{E}' = p^n - 1$.

(a) If $\alpha \in \mathbb{E}^\times$ has order d, use Lagrange's Theorem to show that $d|(p^n - 1)$.
(b) Let $d|(p^n-1)$. Show that $\mathbb{E}^\times$ contains either 0 or $\phi(d)$ elements of order d. [Hint: If $\alpha \in \mathbb{E}^\times$ is an element of order d then $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is the full solution of $x^d = 1$. But recall that α^k has order $d/\gcd(d,k)$. Use this to show that the full set of elements of order d is $\{\alpha^k : 0 \leq k < d \text{ and } \gcd(k,d) = 1\}$.]
(c) Combine (b) with Problem 4 to show that that $\mathbb{E}^\times$ contains exactly $\phi(d)$ elements of order d for each $d|(p^n - 1)$. In particular, $\mathbb{E}^\times$ contains **at least one element** α **of order** $p^n - 1$, hence $\mathbb{E}^\times = \langle \alpha \rangle$ is a cyclic group. [Hint: Let N_d be the number of elements of order d in $\mathbb{E}^\times$ and observe that $p^n - 1 = \sum_{d|(p^n-1)} N_d$. We know that $N_d \leq \phi(d)$ for all d. But if $N_d < \phi(d)$ for some d then we have
$$p^n - 1 = \sum_{d|(p^n-1)} N_d < \sum_{d|(p^n-1)} \phi(d) = p^n - 1.]$$
(d) **Corollary.** Prove that there exist irreducible polynomials in $\mathbb{F}_p[x]$ of all degrees. [Hint: For any prime power p^n we already know that a field of size p^n exists. Let $\mathbb{E} \supseteq \mathbb{F}_p$ have size p^n and let $\alpha \in \mathbb{E}^\times$ be a primitive root, which exists by part (c). Show that the minimal polynomial of α over $\mathbb{F}_p$ has degree n.]

6. The Frobenius Automorphism. Let $p \geq 2$ be prime and let $\mathbb{E} \supseteq \mathbb{F}_p$ be a field of size p^n for some $n \geq 1$. Let $\varphi : \mathbb{E} \to \mathbb{E}$ denote the function $\varphi(\alpha) := \alpha^p$.

(a) Prove that φ is a ring homomorphism.
(b) Prove that φ is injective. Since $\mathbb{E}$ is finite this implies that φ is also surjective. In other words, *every element of* $\mathbb{E}$ *has a unique* p*-th root.* [Hint: A ring homomorphism φ is injective if and only if $\ker \varphi = \{0\}$.]
(c) Show that $\varphi^n : \mathbb{E} \to \mathbb{E}$ is the identity function. If $0 < k < n$, show that φ^k is **not** the identity function. [Hint: If $k < n$ and $\alpha^{p^k} = \alpha$ for all $\alpha \in \mathbb{E}$ then the polynomial $x^{p^k} - x$ has too many roots in $\mathbb{E}$.]
(d) For all $\alpha \in \mathbb{E}$, show that $\alpha \in \mathbb{F}_p$ if and only if $\varphi(\alpha) = \alpha$.
(e) **Harder.** Show that *every* invertible ring homomorphism $\sigma : \mathbb{E} \to \mathbb{E}$ has the form $\sigma = \varphi^k$ for some k. [Hint: From the Primitive Root Theorem we know that $\mathbb{E}^\times = \langle \alpha \rangle$ for some α. Let $S = \{\alpha, \varphi(\alpha), \varphi^2(\alpha), \ldots, \varphi^{n-1}(\alpha)\}$ and let
$$f(x) = \prod_{\beta \in S} (x - \beta) \in \mathbb{E}[x].$$
Note that φ permutes the roots of $f(x)$, hence it fixes the coefficients of $f(x)$. By (d) this implies that $f(x) \in \mathbb{F}_p[x]$. Use this to show that $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, and hence $\sigma(\alpha) \in S$. Let's say $\sigma(\alpha) = \varphi^k(\alpha)$. In this case show that $\sigma = \varphi^k$.][1]

[1] Thanks to Qiaochu Yuan for this proof.