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.]

(a): First we prove it using brute force. If $f(x) = \sum a_k x^k$ and $g(x) = \sum b_\ell x^\ell$ then we have

$$\begin{aligned}
&x\,[f(x)Dg(x) + Df(x)g(x)]\\
&= f(x)xDg(x) + xDf(x)g(x)\\
&= \left(\sum a_k x^k\right)\left(\sum \ell b_\ell x^\ell\right) + \left(\sum k a_k x^k\right)\left(\sum b_\ell x^\ell\right)\\
&= \sum_m \left(\sum_{k+\ell=m} \ell a_k b_\ell\right) x^m + \sum_m \left(\sum_{k+\ell=m} k a_k b_\ell\right) x^m\\
&= \sum_m \left(\sum_{k+\ell=m} \ell a_k b_\ell + k a_k b_\ell\right) x^m\\
&= \sum_m \left(\sum_{k+\ell=m} (k+\ell) a_k b_\ell\right) x^m\\
&= \sum_m \left(\sum_{k+\ell=m} m a_k b_\ell\right) x^m\\
&= \sum_m m \left(\sum_{k+\ell=m} a_k b_\ell\right) x^m\\
&= xD[f(x)g(x)].
\end{aligned}$$

Then cancel x from both sides to get the result. Here is a fancier proof. Let U, V, W be vector spaces over $\mathbb{F}$. A function $\langle -, - \rangle : U \times V \to W$ is called $\mathbb{F}$-*bilinear* if it is $\mathbb{F}$-linear in each coordinate. Being linear in the first coordinate means that for any fixed vector $\mathbf{v} \in V$, and for any vectors $\mathbf{u}_k \in U$ and scalars $a_k \in \mathbb{F}$ we have

$$\left\langle \sum a_k x^k, \mathbf{v} \right\rangle = \sum a_k \langle \mathbf{u}_k, \mathbf{v} \rangle.$$

Then for any vectors $\mathbf{v}_\ell \in V$ and scalars $b_\ell \in \mathbb{F}$ using linearity in the second coordinate gives

$$\left\langle \sum a_k \mathbf{u}_k, \sum b_\ell \mathbf{v}_\ell \right\rangle = \sum_{k,\ell} a_k b_\ell \langle \mathbf{u}_k, \mathbf{v}_\ell \rangle.$$

If $\mathbf{u}_k$ and $\mathbf{v}_\ell$ are bases for U and V, respectively, then we see that the function $\langle -, - \rangle$ is completely determined by the values $\langle \mathbf{u}_k, \mathbf{v}_\ell \rangle$. It is easy to check that the two functions

$\langle f,g\rangle := D[f(x)g(x)]$ and $[f,g] := f(x)Dg(x) + Df(x)g(x)$ from $\mathbb{F}[x]\times\mathbb{F}[x]\to\mathbb{F}[x]$ are $\mathbb{F}$-bilinear. Finally, in order to prove $\langle f,g\rangle = [f,g]$ for all $f(x), g(x)\in\mathbb{F}[x]$ we only need to check that $\langle x^m, x^n\rangle = [x^m, x^n]$ for all $m,n\in\mathbb{N}$ since the powers of x are a basis for $\mathbb{F}[x]$. Indeed:

$$\begin{aligned}\langle x^m, x^n\rangle &= D[x^m x^n]\\ &= D[x^{m+n}]\\ &= (m+n)x^{m+n-1}\end{aligned}$$

and

$$\begin{aligned}[x^m, x^n] &= x^m D[x^n] + D[x^m]x^n\\ &= x^m n x^{n-1} + m x^{m-1}x^n\\ &= n x^{m+n-1} + m x^{m+n-1}\\ &= (m+n)x^{m+n-1}.\end{aligned}$$

I think the fancy proof is easier.

(b): The result is true for $n=1$, so assume $n\geq 2$. Then we have

$$\begin{aligned}D[f(x)^n] &= D[f(x)f(x)^{n-1}]\\ &= f(x)D[f(x)^{n-1}] + Df(x)f(x)^{n-1} && \text{(a)}\\ &= f(x)(n-1)f(x)^{n-2}Df(x) + Df(x)f(x)^{n-1} && \text{induction}\\ &= (n-1)f(x)^{n-1}Df(x) + f(x)^{n-1}Df(x)\\ &= [(n-1)+1]f(x)^{n-1}Df(x)\\ &= nf(x)^{n-1}Df(x).\end{aligned}$$

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 $\mathbb{E}[x]$.]

Given any[1] two polynomials $f(x), g(x)\in\mathbb{F}[x]$ there exists a unique monic polynomial $d(x)\in\mathbb{F}[x]$ with the properties:

- $d(x)|f(x)$ and $d(x)|g(x)$ in $\mathbb{F}[x]$,
- if $e(x)|f(x)$ and $e(x)|g(x)$ in $\mathbb{F}[x]$ then $e(x)|d(x)$ in $\mathbb{F}[x]$.

Furthermore, the Euclidean algorithm gives polynomials $a(x), b(x)\in\mathbb{F}[x]$ such that $f(x)a(x)+g(x)b(x) = d(x)$. Similarly, since $f(x), g(x)\in\mathbb{E}[x]$ there exists a unique monic polynomial $D(x)\in\mathbb{E}[x]$ with the properties

- $D(x)|f(x)$ and $D(x)|g(x)$ in $\mathbb{E}[x]$,
- if $E(x)|f(x)$ and $E(x)|g(x)$ in $\mathbb{E}[x]$ then $E(x)|D(x)$ in $\mathbb{F}[x]$.

[1] not both zero

And the Euclidean algorithm produces $A(x), B(x) \in \mathbb{E}[x]$ satisfying $f(x)A(x) + g(x)B(x) = D(x)$. I claim that $d(x) = D(x)$, which implies that $D(x) \in \mathbb{F}[x]$. Indeed, since $d(x)|f(x)$ and $d(x)|g(x)$ in $\mathbb{F}[x]$, the same holds in $\mathbb{E}[x]$. Hence the equation $f(x)A(x) + g(x)B(x) = D(x)$ implies that $d(x)|D(x)$ in $\mathbb{E}[x]$. Furthermore, since $D(x)|f(x)$ and $D(x)|g(x)$ in $\mathbb{E}[x]$ the equation $f(x)a(x) + g(x)b(x) = d(x)$ implies that $D(x)|d(x)$ in $\mathbb{E}[x]$. Since $\mathbb{E}[x]$ is a domain this implies that $d(x)$ and $D(x)$ are associate, and since $d(x)$ and $D(x)$ are both monic this implies that $d(x) = D(x)$.

Remark: Sometimes people just say that "this is obvious", without giving a proof. It's similar to fact fact that $f(x) = g(x)q(x)$ with $f(x), g(x) \in \mathbb{F}[x]$ and $q(x) \in \mathbb{E}[x]$ implies $q(x) \in \mathbb{F}[x]$ by the existence and uniqueness of quotient and remainder over any field.

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

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

(a): Suppose that $f(x) = p(x)^2 g(x)$ for some non-constant $p(x) \in \mathbb{F}[x]$.[2] From 1 we have

$$Df(x) = 2p(x)g(x) + p(x)Dg(x) = p(x)[2g(x) + p(x)Dg(x)].$$

Then since $p(x)|f(x)$ and $p(x)|Df(x)$ we have $\gcd(f, Df) \neq 1$.

(b): Suppose that $\gcd(f, Df) \neq 1$ and let $p(x)$ be a prime divisor of $\gcd(f, Df)$, so we also have $p(x)|f(x)$ and $p(x)|Df(x)$. Write $f(x) = p(x)g(x)$ and $Df(x) = p(x)h(x)$. Then from Problem 1 we have

$$\begin{aligned} Df(x) &= Dp(x)g(x) + p(x)Dg(x) \\ p(x)h(x) &= Dp(x)g(x) + p(x)Dg(x) \\ p(x)[h(x) - Dg(x)] &= Dp(x)g(x), \end{aligned}$$

hence $p(x)$ divides $Dp(x)g(x)$. Since $p(x)$ is prime, Euclid's Lemma in the ring $\mathbb{F}[x]$ implies that $p(x)$ divides $Dp(x)$ or $g(x)$. But $p(x)$ cannot divide $Dp(x)$ because $\deg(Dp) < \deg(p)$, hence $g(x) = p(x)q(x)$ for some $q(x) \in \mathbb{F}[x]$ and

$$f(x) = p(x)g(x) = p(x)p(x)q(x) = p(x)^2 q(x).$$

[2] For this argument we do not need to assume that $p(x)$ is prime.

Hence $f(x)$ has a repeated prime factor.

(c): First suppose that $\gcd(f, Df) \neq 1$ in $\mathbb{F}[x]$. By part (b) this implies that $f(x) = p(x)^2 g(x)$ for some prime $p(x) \in \mathbb{F}[x]$. Let $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ be a root of $f(x)$ in some field extension $\mathbb{E}[x]$,[3] so that $f(x) = (x - \alpha)^2 h(x)$ for some $h(x) \in \mathbb{E}[x]$. The other direction is harder and uses Problem 2. Let $f(x) \in \mathbb{F}[x]$ have a repeated root $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ in some field extension $\mathbb{E}$, so $f(x)$ has the repeated factor $x - \alpha$ in $\mathbb{E}[x]$. This implies that $\gcd(f, Df) \neq 1$ in $\mathbb{E}[x]$ and hence $\gcd(f, Df) \neq 1$ in $\mathbb{F}[x]$ from Problem 2.

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

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

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 $e|d$.]

(a): Consider any $k/n \in F_n$ and let $d = \gcd(k, n)$ with $k = dk'$ and $n = dn'$. By the Euclidean algorithm there exist $x, y \in \mathbb{Z}$ with $d = kx + ny = dk'x + dn'y$. Then canceling d from both sides gives $1 = k'x + n'y$ which implies that $\gcd(k', n') = 1$. Hence $k/n = k'/n'$ is in $F'_{n/n'}$.

(b): Consider any $d|n$ and $k/d \in F'_d$ (i.e. with $0 \leq k < d$ and $\gcd(k, d) = 1$). If $n = dn'$ then we have $k/d = kn'/dn' = kn'/n$ with $0 \leq kn' < dn' = n$. Hence $k/d \in F_n$.

(c): Suppose that $F'_d \cap F'_e \neq \emptyset$ so that $k/d = \ell/e$ for some $0 \leq k < \ell$ and $0 \leq \ell < e$ with $\gcd(k, d) = \gcd(\ell, e) = 1$. The equation $ek = d\ell$ implies that $d|ek$. But since $\gcd(d, k) = 1$ we must have $d|e$.[4] Similarly, since $e|d\ell$ and $\gcd(e, \ell) = 1$ we have $e|d$. Since $d|e$ and $e|d$ we have $d = \pm e$, which implies that $d = e$ because $d, e \in \mathbb{N}$.

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 $\{\alpha^k : 0 \leq k < d \text{ and } \gcd(k, d) = 1\}$.]

---

[3] For example, let $\mathbb{E} := \mathbb{F}[x]/p(x)\mathbb{F}[x]$ and $\alpha = [x]$.

[4] Proof: Take $dx + ky = 1$ and multiply both sides by e to get $dex + key = e$, hence $dex + d\ell y = e$, hence $d|e$.

(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.]

(a): Let $\#\mathbb{E} = p^n$ and let $(\mathbb{E}^\times, \times, 1)$ be the group of units, so that $\#\mathbb{E}^\times = p^n - 1$. Let $\alpha \in \mathbb{E}^\times$ be an element of order d so that

$$\#\langle\alpha\rangle = \#\{\alpha^k : k \in \mathbb{Z}\} = d.$$

According to Lagrange's Theorem, the size of any subgroup divides the size of the group. Since $\langle\alpha\rangle$ is a subgroup of $\mathbb{E}^\times$ this implies that d divides p^n-1.

(b): Hence any element of the group $\mathbb{E}^\times$ has order dividing p^n-1. For any $d|p^n-1$ that the number of elements of order d is either zero or $\phi(d)$. Indeed, if the number of elements of order d is zero then we are done. Otherwise, let $\alpha \in \mathbb{E}^\times$ be an element of order d and consider the d distinct elements $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$. Each of these is a root of the polynomial $x^d - 1$ because $(\alpha^k)^d = (\alpha^d)^k = 1^k = 1$. Since the polynomial x^d-1 has degree d, this is the complete solution of the equation $x^d - 1 = 0$. If $\beta \in \mathbb{E}^\times$ is any other element of order d it follows that $\beta = \alpha^k$ for some k. But not every k occurs. Recall, if α has order d then α^k has order $d/\gcd(k,d)$, hence α^k has order d if and only if $\gcd(k,d)=1$. It follows that the set of elements of order d is exactly $\{\alpha^k : 1 \leq k \leq d-1, \gcd(k,d)=1\}$, which has size $\phi(d)$.

(c): For any $d|(p^n-1)$ let N_d be the number of elements of order d in $\mathbb{E}^\times$, so that $N_d = 0$ or $N_d = \phi(d)$. Since each of the p^n-1 elements of $\mathbb{E}^\times$ has **some order**, we have

$$p^n - 1 = \sum_{d|(p^n-1)} N_d,$$

and from Problem 4 we have

$$p^n - 1 = \sum_{d|(p^n-1)} \phi(d).$$

If at least one of the N_d is zero then we obtain a contradiction

$$p^n - 1 = \sum_{d|(p^n-1)} N_d < \sum_{d|(p^n-1)} \phi(d) = p^n - 1.$$

Hence we must have $N_d = \phi(d)$ for all $d|(p^n-1)$. In particular, we have

$$N_{p^n-1} = \phi(p^n-1) \geq 1,$$

which shows that $\mathbb{E}^\times$ is a cyclic group.

Remark: This is an indirect proof. For example, it tells us that the field of size 17^3 has exactly $\phi(17^3-1) = 2448$ primitive roots, but it does not tell us how to find one. I don't know a better algorithm than "guess and check".

(d): Let $\mathbb{E}$ be a field of size p^n.[5] Note that $\mathbb{E}$ must be an n-dimensional vector space over $\mathbb{F}_p$, so $[\mathbb{E}/\mathbb{F}_p] = n$. In (c) we showed that there exists $\alpha \in \mathbb{E}^\times$ such that $\mathbb{E}^\times = \langle \alpha \rangle$, and hence

$$\mathbb{E} = \{0\} \cap \mathbb{E}^\times = \{0, 1, \alpha, \ldots, \alpha^{p^n-2}\} = \mathbb{F}_p(\alpha).$$

Let $m(x) \in \mathbb{F}_p(x)$ be the minimal polynomial of $\alpha/\mathbb{F}_p$, which is irreducible over $\mathbb{F}_p$. Then from the Minimal Polynomial Theorem we have $\deg(m) = [\mathbb{F}_p(\alpha)/\mathbb{F}_p] = [\mathbb{E}/\mathbb{F}_p] = n$.

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 $\sigma = \varphi^k$.][6]

(a): Let $\mathbb{E} \supseteq \mathbb{F}_p$ be a field of size p^n for some prime p. Let $\varphi : \mathbb{E} \to \mathbb{E}$ denote the Frobenius map $\varphi(\alpha) := \alpha^p$. To see that this is a ring homomorphism we first note that $\varphi(1) = 1^p = 1$ and $\varphi(0) = 0^p = 0$. Then for any $\alpha, \beta \in \mathbb{E}$ we note that

$$\varphi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \varphi(\alpha)\varphi(\beta)$$

and

$$\varphi(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \varphi(\alpha) + \varphi(\beta).$$

This last identity follows from the Freshman's Binomial Theorem, which you proved on the previous homework.

(b): Recall that a ring homomorphism is injective if and only if its kernel is zero.[7] In our case, if $\alpha^p = \varphi(\alpha) = 0$ then we must have $\alpha = 0$ because $\mathbb{E}$ is a domain. Hence $\alpha \in \ker \varphi$ implies $\alpha = 0$. Hence φ is injective. It follows from injectivity and the finiteness of $\mathbb{E}$ that φ is also surjective.

(c): For any $\alpha \in \mathbb{E}^\times$ note that $\alpha^{p^n-1} = 1$ because $\#\mathbb{E}^\times = p^n - 1$ (see 5a). Multiplying both sides by α gives $\alpha^{p^n} = \alpha$, which also holds when $\alpha = 0$. Thus for any $\alpha \in \mathbb{E}$ we have

$$\varphi^n(\alpha) = \alpha^{p^n} = \alpha,$$

[5] For example, let $\mathbb{E}$ be a splitting field for $x^{p^n} - x$ over $\mathbb{F}_p$.

[6] Thanks to Qiaochu Yuan for this proof.

[7] Indeed, if $\varphi : R \to S$ is injective then for any $\alpha \in \ker \varphi$ we have $\varphi(\alpha) = 0 = \varphi(0)$ and hence $\alpha = 0$. Conversely, if $\ker \varphi = \{0\}$ then for any $\varphi(\alpha) = \varphi(\beta)$ we have $0 = \varphi(\alpha) - \varphi(\beta) = \varphi(\alpha - \beta)$, which implies that $\alpha - \beta = 0$ and hence $\alpha = \beta$.

which shows that $\varphi^n = \mathrm{id}$. But if $0 < k < n$ then I claim that $\varphi^k \neq \mathrm{id}$. To see this, assume for contradiction that $\alpha^{p^k} = \varphi^k(\alpha) = \alpha$ for all $\alpha \in \mathbb{E}$. But then the nonzero polynomial $x^{p^k} - x$ has p^n distinct roots in $\mathbb{E}$, which is more than its degree p^k.

(d): Note that $\varphi(\alpha) = \alpha$ if and only if $\alpha^p = \alpha$, i.e., if and only if α is a root of the polynomial $x^p - x$. This polynomial can have at most p roots in $\mathbb{E}$, and every element $\alpha \in \mathbb{F}_p$ is a root.[8] Since $\mathbb{F}_p$ has p elements we conclude that $\varphi(\alpha) = \alpha$ if and only if $\alpha \in \mathbb{F}_p$.

(e): Consider any automorphism $\sigma : \mathbb{E} \to \mathbb{E}$. Note that we must have $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_p$ because $\mathbb{F}_p$ consists of elements of the form $1 + 1 + \cdots + 1$, so[9]

$$\sigma(1 + 1 + \cdots + 1) = \sigma(1) + \sigma(1) + \cdots + \sigma(1) = 1 + 1 + \cdots + 1.$$

From Problem 5 there exists some "primitive root" $\alpha \in \mathbb{E}^\times$ satisfying $\mathbb{E}^\times = \langle \alpha \rangle$, so that

$$\mathbb{E} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}.$$

Let $\varphi : \mathbb{E} \to \mathbb{E}$ be the Frobenius automorphism and define the polynomial

$$f(x) = (x - \alpha)(x - \varphi(\alpha)) \cdots (x - \varphi^{n-1}(\alpha)) \in \mathbb{E}[x].$$

Since $\varphi^n = \mathrm{id}$ we observe that φ permutes the roots of this polynomial, hence it fixes the coefficients. For example, the coefficient of x^{n-1} in $f(x)$ is (the negative of) the sum $\alpha + \varphi(\alpha) + \cdots + \varphi^{n-1}(\alpha)$, and we have

$$\begin{aligned}
\varphi(\alpha + \varphi(\alpha) + \cdots + \varphi^{n-1}(\alpha)) &= \varphi(\alpha) + \varphi^2(\alpha) + \cdots + \varphi^{n-1}(\alpha) + \varphi^n(\alpha) \\
&= \varphi(\alpha) + \varphi^2(\alpha) + \cdots + \varphi^{n-1}(\alpha) + \alpha \\
&= \alpha + \varphi(\alpha) + \cdots + \varphi^{n-1}(\alpha).
\end{aligned}$$

From part (d) this implies that $f(x)$ has coefficients in $\mathbb{F}_p$. Since σ fixes elements of $\mathbb{F}_p$, it fixes the coefficients of $f(x)$ and hence

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

This implies that $\sigma(\alpha)$ is a root of $f(x)$ and hence $\sigma(\alpha) = \varphi^k(\alpha)$ for some k. But if σ and φ^k are automorphisms of $\mathbb{E}$ that agree on α then they must agree on every element of $\mathbb{E}$. Indeed, the elements of $\mathbb{E}$ are just 0 and powers of α, so that

$$\sigma(\alpha^\ell) = \sigma(\alpha)^\ell = \varphi^k(\alpha)^\ell = \varphi^k(\alpha^\ell).$$

Hence $\sigma = \varphi^k$ as functions $\mathbb{E} \to \mathbb{E}$.

Remark: In summary, we have shown that the Galois group of a finite field $\mathbb{E}$ of size p^n is a cyclic group of size n, generated by the Frobenius automorphism φ. Building on this, the Galois correspondence tells us that the subfields of $\mathbb{E}$ are in one-to-one correspondence with the divisors $d|n$. Namely, for each divisor $d|n$ there is a subgroup $\langle \varphi^d \rangle \subseteq \langle \varphi \rangle$, which leads to a subfield $\mathrm{Fix}(\langle \varphi^d \rangle) \subseteq \mathbb{E}$ defined by

$$\begin{aligned}
\mathrm{Fix}(\langle \varphi^d \rangle) &= \{\alpha \in \mathbb{E} : \sigma(\alpha) = \alpha \text{ for all } \sigma \in \langle \varphi^d \rangle\} \\
&= \{\alpha \in \mathbb{E} : \varphi^d(\alpha) = \alpha\} \\
&= \{\alpha \in \mathbb{E} : \alpha^{p^d} = \alpha\}.
\end{aligned}$$

This subfield is the splitting field for $x^{p^d} - x$ over $\mathbb{F}_p$ and it has size p^d. Furthermore, the poset of subfields of $\mathbb{E}$ is isomorphic to the lattice of divisors of n under divisibility.

---

[8] Given $\alpha \in \mathbb{F}_p$ we have $\alpha^{p-1} = 1$ for $\alpha \neq 0$, which implies $\alpha^p = \alpha$. But we also have $\alpha^p = \alpha$ when $\alpha = 0$.

[9] In general, if $\mathbb{E}' \subseteq \mathbb{E}$ is the prime subfield then any automorphism $\sigma : \mathbb{E} \to \mathbb{E}$ fixes the elements of $\mathbb{E}'$.