Math 111C HW5

Zih-Yu Hsieh

May 15, 2025

1

Question 1 *Let F be a finite field. Prove that $|F| = p^n$ for some prime p and $n \in \mathbb{N}$.*

Pf:

Since F is a finite field, then $\text{char}(F) = p$ for some prime p. It suffices to show that $|F| = p^n$ for some $n \in \mathbb{N}$.

Suppose the contrary that the above statement doesn't hold, then there exists some distinct prime number $q \neq p$, such that q divides $|F|$. Recall that F is a finite abelian group under addition, hence **Cauchy's Theorem** applies, there exists $a \in F$, such that its order with respect to addition (denoted as $\text{order}(a)$) is q.

However, since p, q are distinct primes, then by **Bezout's Lemma**, there exists $s, t \in \mathbb{Z}$, with $sp+tq = 1$. Then, let $n \cdot a$ denotes the addition of a total of n times (if n is negative, do the addition of $-a$ total of $|n|$ times instead) and let 1_p denote the identity of F, then we get the following:

$$a = (sp + tq) \cdot a = (s \cdot (p \cdot 1_p)) \cdot a + t(q \cdot a) = (s \cdot 0) \cdot a + t \cdot 0 = 0$$

Which shows that $a = 0$. But, if $a = 0$, then $\text{order}(a) = 1$, which contradicts the statement that $\text{order}(a) = q > 1$.

So, our assumption is false, $|F| = p^n$ for some $n \in \mathbb{N}$.

2

Question 2 *Show that $\mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_2[y]/(y^3 + y^2 + 1)$ and find an explicit isomorphism.*

Pf:

Let $K_1 = \mathbb{F}_2[x]/(x^3 + x + 1)$, and $K_2 = \mathbb{F}_2[y]/(y^3 + y^2 + 1)$. Which, since the extensions are based on two degree 3 polynomial, then $[K_1 : \mathbb{F}_2] = [K_2 : \mathbb{F}_2] = 3$, which implies that $|K_1| = |K_2| = 2^3 = 8$.

Now, consider $\overline{\mathbb{F}}_2$: Since both K_1, K_2 are finite extensions of $\mathbb{F}_2$, they're algebraic extensions of $\mathbb{F}_2$. Hence, there exists embeddings $\phi_1 : K_1 \to \overline{\mathbb{F}}_2$ and $\phi_2 : K_2 \to \overline{\mathbb{F}}_2$.

Now, since $\phi_1(K_1) \cong K_1$ and $\phi_2(K_2) \cong K_2$, then $|\phi_1(K_1)| = |K_1| = 8 = |K_2| = |\phi_2(K_2)|$. So, since $8 = 2^3$, under $\overline{\mathbb{F}}_2$, there exists a unique finite field $\mathbb{F}_{2^3} \subset \overline{\mathbb{F}}_2$ with order $|\mathbb{F}_{2^3}| = 2^3$. Hence, this enforces $\phi_1(K_1) = \phi_2(K_2) = \mathbb{F}_{2^3}$.

So, after restriction, we get the following relationships of isomorphisms:

$$\phi_1 : K_1 \tilde{\to} \mathbb{F}_{2^3}, \quad \phi_2 : K_2 \tilde{\to} \mathbb{F}_{2^3}$$

Hence, $\phi_2^{-1} \circ \phi_1 : K_1 \to K_2$ is an isomorphism, showing that $K_1 \cong K_2$.

Construction of Isomorphism:

Now, consider the element $(y+1) \in \mathbb{F}_2[y]$, it satisfies the following:

$$(y+1)^3 + (y+1) + 1 = (y+1)(y+1)^2 + (y+1) + 1 = (y+1)(y^2+1^2) + (y+1) \cdot 1 + 1$$

$$= (y+1)(y^2+1+1) + 1 = (y+1)y^2 + 1 = y^3 + y^2 + 1$$

So, this implies that $(\overline{y+1})^3 + \overline{y+1} + 1 = \overline{y^3+y^2+1} = 0$ in K_2.

Hence, consider the ring isomorphism by $\phi : \mathbb{F}_2[x] \to \mathbb{F}_2[y]$ by $\phi(x) = (y+1)$, if take the projection $\pi_y : \mathbb{F}_2[y] \to K_2$ by $\pi_y(p(y)) = \overline{p(y)} = p(y) \mod (y^3+y^2+1)$, the composition $\pi_y \circ \phi : \mathbb{F}_2[x] \to K_2$ becomes a ring homomorphism (Note: recall that $K_2 = \mathbb{F}_2[y]/(y^3+y^2+1)$).

Which, since $\phi(x^3+x+1) = (y+1)^3+(y+1)+1 = y^3+y^2+1$, then $\pi_y \circ \phi(x^3+x+1) = \overline{y^3+y^2+1} = 0$, hence $x^3+x+1 \in \ker(\pi \circ \phi)$, or $(x^3+x+1) \subseteq \ker(\pi \circ \phi)$. Then, by **Generalized First Isomorphism Theorem**, there exists unique well-defined ring homomorphism $\overline{\phi} : \mathbb{F}_2[x]/(x^3+x+1) \to K_2$, such that with the projection $\pi_x : \mathbb{F}_2[x] \to K_1$ by $\pi(p(x)) = \overline{p(x)} = p(x) \mod (x^3+x+1)$, the following diagram commutes:

$$\begin{tikzcd}
\mathbb{F}_2[x] \arrow[r, "\phi"] \arrow[d, two heads, "\pi_x"'] & \mathbb{F}_2[y] \arrow[d, two heads, "\pi_y"] \\
K_1 \arrow[r, "\overline{\phi}"] & K_2
\end{tikzcd}$$

Or, $\overline{\phi} \circ \pi_x = \pi_y \circ \phi$.

Then, since $\pi_y \circ \phi$ is surjective (since both π_y and ϕ are surjective), while π_x is surjective, then in case for $\overline{\phi} \circ \pi_x$ to be surjective, $\overline{\phi}$ is surjective. On the other hand, since $\overline{\phi} : K_1 \to K_2$ with K_1 being a field, this map is injective.

So, $\overline{\phi}$ is a well-defined isomorphism between K_1 and K_2, with the following formula:

$$\overline{\phi}(1) = 1, \quad \overline{\phi}(\overline{x}) = \overline{y+1} \in K_2$$

3

Question 3 *Let F be a perfect field with char$(F) = p$. Prove that $F = F^p$.*

Pf:

We'll prove by contradiction. Suppose F is a perfect field, while $F \neq F^p$, then since $F^p \subsetneq F$, there exists $\alpha \in F \setminus F^p$, which implies that for all $\beta \in F$, $\beta^p \neq \alpha$.

So, the polynomial $x^p - \alpha \in F[x]$ has no solution in F, which based on **HW 2 Question 3**, this polynomial is in fact irreducible in $F[x]$.

Now, consider $K = F[x]/(x^p - \alpha)$ a finite extension, and take $\theta = \overline{x} \in K$: since it satisfies $\overline{x}^p - \alpha = \overline{(x^p - \alpha)} = 0$, then $\overline{x}^p = \alpha$, and $\theta = \overline{x}$ is a root of the monic polynomial $x^p - \alpha \in F[x] \subset K[x]$; also, since $x^p - \alpha$ is proven to be irreducible, then $m_{\theta,F}(x) = x^p - \alpha$.

But, because $\text{char}(F) = p$, then $\text{char}(K) = p$, which $\text{char}(K[x]) = p$. So, based on Frobenius Endomorphism, $(x - \theta)^p = x^p - \theta^p$, showing that $(x - \theta)^p$ is a factorization of $x^p - \alpha$ in $K[x]$; then, since $K[x]$ is a UFD, such factorization is unique. Hence, $m_{\theta,F}(x) = (x - \theta)^p$, showing that the minimal polynomial of θ over F has θ as a root with multiplicity $p > 1$, so $\theta \in K$ is not separable over F, or K/F is not a separable extension.

Yet, recall that F is assumed to be a perfect field, while K/F is a finite extension, then K/F should be a separable extension by the definition of perfect field. So, we reach a contradiction, therefore the initial assumption is false, if F is a perfect field, then $F = F^p$.

4

Question 4 *Show that an algebraic extension of a perfect field is perfect.*

Pf:

Suppose F is a perfect field, then all finite extension is a separable extension. Which, for any algebraic extension K/F, there are two cases to consider:

1. When $[K : F] < \infty$**:**

Given any finite extension K/F, and consider any finite extension L/K: Since both extensions are finite (with $F \subseteq K \subseteq L$), then L/F is also a finite extension. Based on the assumption that F is perfect, L/F is a separable extension.

Which, for all $\alpha \in L$, its minimal polynomial $m_{\alpha,F}(x) \in F[x]$ must have simple roots in $\overline{F}$. Hence, α must be a simple root of $m_{\alpha,F}(x)$, or $(x - \alpha)^k \mid m_{\alpha,F}(x)$ is only true for integer $k \leq 1$.

Then, since α is also algebraic over K (since L/K are finite extensions), then $m_{\alpha,K}(x) \in K[x]$ exists; and since $m_{\alpha,F}(x) \in F[x] \subseteq K[x]$, then $m_{\alpha,K}(x) \mid m_{\alpha,F}(x)$ in $K[x]$.

Because α is a root of $m_{\alpha,K}(x)$, let $l \in \mathbb{N}$ be its multiplicity, we get $(x-\alpha)^l \mid m_{\alpha,K}(x)$ in $L[x]$; also, since $m_{\alpha,K}(x) \mid m_{\alpha,F}(x)$ in $K[x] \subseteq L[x]$, this implies $(x - \alpha)^l \mid m_{\alpha,F}(x)$ in $L[x]$. Hence, since α is proven to be a root of $m_{\alpha,F}(x)$ with multiplicity 1, this implies that $l \leq 1$, or $l = 1$.

So, α as a root of $m_{\alpha,K}(x)$ has multiplicity 1, and since $m_{\alpha,K}(x)$ is irreducible in $K[x]$, all its root in $\overline{K}$ must have the same multiplicity. Which, they must all have multiplicity 1 (or being a simple root), showing that α is actually separable over K.

This shows that L/K is in fact a separable extension, which proves that K is also perfect. So, all finite extension K/F is also perfect.

2. When $[K : F] = \infty$**:**

Suppose K/F is an infinite algebraic extension, then for all finite extension L/K (which is also algebraic), we have L/F also being an algebraic extension. Then for all $\alpha \in L$, there exists $m_{\alpha,K}(x) \in K[x]$, say $m_{\alpha,K}(x) = a_n x^n + ... + a_0$ for some $a_0, ..., a_n \in K$. Then, since K/F is an algebraic extension, all elements in K is algebraic over F, showing that $K' = F(a_0, ..., a_n)$ is a finite extension over F. By the proof in finite case, F is a perfect field implies K'/F is also a perfect field. Then since $K'(\alpha)/K'$ is again a finite extension (since α is algebraic over F, it is algebraic over K'/F), it is a separable extension. Hence, α is separable over K', which $m_{\alpha,K'}(x) \in K'[x]$ must have simple roots in $\overline{K'}$.

However, since $K' \subseteq K$, then $m_{\alpha,K}(x) \mid m_{\alpha,K'}(x)$ in $K[x]$; on the other hand, since $m_{\alpha,K}(x) \in K'[x]$ (since all the coefficients are contained in K'), then this enforces $m_{\alpha,K}(x) = m_{\alpha,K'}(x)$. So, $m_{\alpha,K}(x)$ has simple roots in $\overline{K'}$, while K/K' is an algebraic extension (since K/F is, $K' \subseteq K$, and K'/F is also algebraic), then $\overline{K} \cong \overline{K'}$ via some field homomorphism fixing K', so $m_{\alpha,K}(x)$ is also having simple roots in $\overline{K}$.

This proves that α is separable over K, hence L/K is in fact a separable extension, hence this proves that K is perfect.

So, regardless of the case, if F is perfect, its algebraic extension K/F is perfect.

5 (part b has some problem)

Question 5 *Let $K = \mathbb{F}_p(t, w)$ be the rational function field with two indeterminates t, w over $\mathbb{F}_p$. Let L be the splitting field over K of the polynomial $h(x) = f(x)g(x)$ where $f(x) = x^p - t$ and $g(x) = x^p - w$. Prove the following:*

(a) f and g are irreducible over K.

(b) $[L : K] = p^2$.

(c) L/K is not seperable.

(d) $a^p \in K$ for all $a \in L$.

Pf:

Before starting, let $\mathbb{F}_p(w) = F_1$, and $F_2 = \mathbb{F}_p(t)$, then $K = \mathbb{F}_p(t)(w) = F_2(w)$, and $K = \mathbb{F}_p(w)(t) = F_1(t)$.

(a) Based on what we've proven in **HW 2 Question 3**, since $\text{char}(K) = p$, for any $\alpha \in K$, if $x^p - \alpha$ has no solution in K, then it is irreducible in $K[x]$. Hence, to prove f, g are irreducible in $K[x]$, it suffices to show there's no solution in K.

First, suppose the contrary that there exists $\alpha \in K$, such that $\alpha^p - w = 0$, then since $K = F_2(w)$, there exists $f(w), g(w) \in F_2[w]$, such that $\alpha = \frac{f(w)}{g(w)}$. Then, it implies the following:

$$\alpha^p - w = \left(\frac{f(w)}{g(w)}\right)^p - w = 0, \quad (f(w))^p = w(g(w))^p$$

Let $k = \deg_w(f)$, and $l = \deg_w(g)$, then $\deg_w(f^p) = kp$, while $\deg_w(wq^p) = \deg_w(w) + \deg_w(q^p) = 1 + lp$. Since $(f(w))^p = w(g(w))^p$, then $kp = 1 + lp$; however, the left side is divisible by p, while the right side is not divisible by p, so we reach a contradiction. Hence, the assumption is false, there doesn't exist $\alpha \in K$, satisfying $\alpha^p - w = 0$. So, $x^p - w \in K[x]$ has no solution in K, showing that it is irreducible.

Now, using the same proof on $x^p - t$ by viewing $K = F_1(t)$, we can also prove that $x^p - t$ has no solution in K, which $x^p - t$ is also irreducible over K.

(b) Since L/K is a splitting field of $h(x) = f(x)g(x)$ (where $f(x) = x^p - t$, and $g(x) = x^p - w$), then both $f(x), g(x)$ splits completely over L. Hence, there exists $\alpha \in L$, such that $f(\alpha) = 0$. Then, since $x^p - t$ is monic, while proven to be irreducible in $K[x]$ by **part (a)**, then $m_{\alpha,K}(x) = x^p - t$.

Now, because $\alpha^p - t = 0$, $\alpha^p = t$. However, since K has characteristic p, then $\text{char}(L) = p$, so $\text{char}(L[x]) = p$. Then, within $L[x]$, since $(x - \alpha)^p = x^p - \alpha^p = x^p - t$, then $(x - \alpha)^p$ is a factorization of $x^p - t$; on the other hand, since $L[x]$ is a UFD, such factorization must be unique. Hence, $(x - \alpha)^p$ is the factorization of $x^p - t$, α is the only root of $x^p - t$.

Let $\beta \in L$ be a root of $g(x) = x^p - w$, then using similar logic we can deduce that $x^p - w = (x - \beta)^p$, so β is the only root of $x^p - w$.

Which, since $h(x) = f(x)g(x) = (x^p - t)(x^p - w)$, then $h(x)$ only has roots α, β in L. Hence, since L/K is a spliting field of $h(x) \in K[x]$, then $L = K(\alpha, \beta)$. So, we'll consider the extensions $K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$.

Since α has its minimal polynomial over K being $x^p - t \in K[x]$, then $K(\alpha) \cong K[x]/(x^p - t)$, hence $[K(\alpha) : K] = p$. So, given that $[L : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K]$, to prove that $[L : K] = p^2 = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot p$, it suffices to show $[K(\alpha, \beta) : K(\alpha)] = p$.

And, if showing that $x^p - w \in K(\alpha)[x]$ is irreducible, since it is monic and β is assumed to be a root of it, then β must have its minimal polynomial over $K(\alpha)$ being $x^p - w$, hence $K(\alpha, \beta) = K(\alpha)(\beta) \cong K(\alpha)[x](x^p - w)$, showing that $[K(\alpha, \beta) : K(\alpha)] = p$. So, the last goal is to prove $x^p - w$ is irreducible over $K(\alpha)$, and the final statement we want to prove directly follows (Note: since $K(\alpha)$ is again having characteristic p, it suffices to show that $x^p - w$ has no roots in $K(\alpha)$).

Suppose the contrary that there exists $\gamma \in K(\alpha)$ which satisfies $\gamma^p - w = 0$, then since $K(\alpha) \cong K[x]/(x^p - t)$, there exists $a_0, ..., a_{p-1} \in K = F_2(w)$, such that the following is true:

$$\gamma = a_{p-1}\alpha^{p-1} + ... + a_0$$

Which, each a_i can be expressed as $\frac{f_i(w)}{g_i(w)}$ for some $f_i(w), g_i(w) \in F_2[w]$. Then, using Frobenius Endomorphism, we get the following:

$$\gamma^p = (a_{p-1}\alpha^{p-1} + ... + a_0)^p = a_{p-1}^p(\alpha^p)^{p-1} + ... + a_0^p$$
$$= \frac{f_{p-1}(w)^p}{g_{p-1}(w)^p}t^{p-1} + ... + \frac{f_0(w)^p}{g_0(w)^p}$$

Also, since $\gamma^p - w = 0$, then $\gamma^p = w$. So, if we take $q(w) = \prod_{i=0}^{p-1} g_i(w)^p \in F_2[w]$, we know that $\deg_w(q) = kp$ for some $k \in \mathbb{N}$ (since its product of polynomials, each to the power of p), and $q(w) \cdot \gamma^p \in F_2[w]$, since $t \in F_2 = \mathbb{F}_p(t)$, and all the denominators $g_i(w)^p$ in γ^p were cancelled out by $q(w)$.

Hence, we get:

$$q(w) \cdot \gamma^p = w \cdot q(w), \quad \deg_w(q \cdot \gamma^p) = \deg_w(w \cdot q(w)) = \deg_w(w) + \deg(q) = 1 + kp$$

On the other hand, each term $\frac{f_i(w)^p}{g_i(w)^p}t^i$ in γ^p after multiplied by $q(w)$ would become:

$$q(w) \cdot \frac{f_i(w)^p}{g_i(w)^p}t^i = t^i \cdot f_i(w)^p \cdot \prod_{\substack{j=1 \\ j \neq i}}^{p-1} g_j(w)^p \in F_2[w]$$

(Note: the $g_i(w)^p$ in $q(w)$ got cancelled out by the denominator).

Hence, $q(w) \cdot \frac{f_i(w)^p}{g_i(w)^p}t^i$ as a polynomial of w, is in fact having degree $l_i p$ for some $l_i \in \mathbb{N}$ (since it is also product of polynomials, each raised to the power of p).

Then, $q(w) \cdot \gamma^p$ as the summation of all $q(w) \cdot \frac{f_i(w)^p}{g_i(w)^p}t^i$ (with index $i \in \{0, ..., n\}$, since $q(w) \cdot \gamma^p = q(w) \left(\frac{f_{p-1}(w)^p}{g_{p-1}(w)^p}t^{p-1} + ... + \frac{f_0(w)^p}{g_0(w)^p} \right)$), then since it's a sum of polynomials of w with degree being multiples of p, then the sum $q(w) \cdot \gamma^p$ must have its degree $\deg_w(q(w) \cdot \gamma^p) = lp$ for some $l \in \mathbb{N}$.

Hence, we must have $lp = 1 + kp$ (since they're the degree of the same polynomial). But again, since the left side is divisible by p, while the right side is not divisible by p, we reach a contradiction. Hence, our assumption must be false, $K(\alpha)$ can't contain a root of $x^p - w$. Hence, followed from the prove before this section, $[K(\alpha, \beta) : K(\alpha)] = p$, showing that $[L : K] = p^2$.

(c) Using the results from **part (b)**, we know that $(x-\alpha)^p = x^p - t$ is the unique factorization in L. Hence, α as a root of $x^p - t$ with multiplicity $p > 1$, while $x^p - t = m_{\alpha,K}(x) \in K[x]$ is also proven, then $m_{\alpha,K}(x)$ has roots with multiplicity > 1, showing that α is not separable over K, hence L/K is not a separable extension.

(d) In **part (b)**, we've proven that $K(\alpha,\beta) = K(\alpha)(\beta) \cong K(\alpha)[x]/(x^p - w)$, hence for all $a \in K(\alpha,\beta)$, there exists $a_0, ..., a_{p-1} \in K(\alpha)$, such that the following holds:

$$a = a_{p-1}\alpha^{p-1} + ... + a_0$$

Which, applying Frobenius Endomorphism, we get:

$$a^p = (a_{p-1}\alpha^{p-1} + ... + a_0)^p = a_{p-1}^p(\alpha^p)^{p-1} + ... + a_0^p$$

$$= a_{p-1}^p(t)^{p-1} + ... + a_0^p$$

Since $t \in K \subset K(\alpha)$, while each $a_i \in K(\alpha)$, then $a^p \in K(\alpha)$.

Now, for all $\delta \in K(\alpha)$, since $K(\alpha) \cong K[x]/(x^p - t)$, there exists $b_0, ..., b_{p-1} \in K$, such that the following holds:

$$\delta = b_{p-1}\alpha^{p-1} + ... + b_0$$

Then again, applying Frobenius Endomorphism, we get:

$$\delta^p = (b_{p-1}\alpha^{p-1} + ... + b_0)^p = b_{p-1}^p(\alpha^p)^{p-1} + ... + b_0^p$$

$$= b_{p-1}^p t^{p-1} + ... + b_0^p$$

Since each $b_i^p \in K$, while $t \in K$, this shows that $\delta^p \in K$.

Hence, going back to $a^p = a_{p-1}^p(t)^{p-1} + ... + a_0^p$, since each $a_i \in K(\alpha)$, then $a_i^p \in K$, showing that a^p as a finite sum and product of elements in K, is in K.

So, $a^p \in K$, showing that all element $a \in K(\alpha,\beta) = L$ satisfies $a^p \in K$.