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 (insert commutative diagram)

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 $|\phi_1(K_1)| = |K_1| = 8 = |K_2| = |\phi_2(K_2)|$. Then, 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:

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

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 $\phi(x) = (y+1)$, the maximal ideal $(x^3+x+1) \subset \mathbb{F}_2[x]$ has its image $\phi((x^3+x+1)) = ((y+1)^3 + (y+1) + 1) = (y^3+y^2+1)$, hence 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 where the kernel is valid.

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:

Insert commutative diagram

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 implis 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 char$(F) = p$, then char$(K) = p$, which 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 (infinite case not done)

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 is a finite extension:

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 $\overline{F}$.

Since L/F is a finite extension, then it is also algebraic, hence there exists embedding $\phi : L \to \overline{F}$ that fixes F, which can be extended to an injective ring homomorphism $\overline{\phi} : L[x] \to \overline{F}[x]$, by the following:

$$\forall a_n, ..., a_0 \in L, \quad \overline{\phi}(a_n x^n + ... + a_0) = \phi(a_n)x^n + ... + \phi(a_0)$$

(Note: it is injective, since if the output is 0, then each coefficient a_i must satisfy $\phi(a_i) = 0$, and since ϕ is a field embedding, it is injective, so each $a_i = 0$, showing the input is 0).

Now, since $\alpha \in L$ is a root of $m_{\alpha,F}(x) \in F[x] \subseteq L[x]$, then let $k \in \mathbb{N}$ be the multiplicity of α as a root of $m_{\alpha,F}(x)$, we get $(x-\alpha)^k \mid m_{\alpha,F}(x)$, or $m_{\alpha,F}(x) = (x-\alpha)^k q(x)$ for some $q(x) \in L[x]$. Then, since $m_{\alpha,F}(x) \in F[x]$, we know $\overline{\phi}(m_{\alpha,F}(x)) = m_{\alpha,F}(x)$ (since ϕ fixes F, $\overline{\phi}$ also fixes F. Apply the extended ring homomorphism, we get:

$$m_{\alpha,F}(x) = \overline{\phi}(m_{\alpha,F}(x)) = \overline{\phi}((x-\alpha)^k q(x)) = (x-\phi(\alpha))^k \overline{\phi}(q(x)) \in \overline{F}[x]$$

This shows that $\phi(\alpha)$ is a root of $m_{\alpha,F}(x)$ in $\overline{F}$ with multiplicity $\geq k$. Then, because $m_{\alpha,F}(x)$ has simple roots in $\overline{F}$, $\phi(\alpha)$ as a root must have multiplicity of 1, hence $k \leq 1$. This implies that $k = 1$, which α as a root of $m_{\alpha,F}(x)$ must have multiplicity 1.

Finally, 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 $[K : F] = \infty$:

5

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:

(a)

(b)

(c)

(d)