Math 111C HW4

Zih-Yu Hsieh

May 5, 2025

1

Question 1 *Let F be a field and $f \in F[x]$ be an irreducible polynomial. Prove that all roots of $f(x)$ in $\overline{F}$ have the same multiplicity.*

Pf:

Given $f(x) \in F[x]$ an irreducible polynomial, which WLOG, can assume f is monic (by dividing the nonzero leading coefficient). Then, for any root α of f in some field extension of F, since f is monic and irreducible, it is in fact a minimal polynomial of α.

Hence, the following forms a well-defined field isomorphism that fixes F:

$$\phi_\alpha : F[x]/(f(x)) \to F(\alpha), \quad \forall c_0, c_1, ..., c_n \in F, \quad \phi_\alpha(c_0 + c_1\overline{x} + ... + c_n\overline{x}^n) = c_0 + c_1\alpha + ... + c_n\alpha^n$$

Whih, given α, β two roots of f, the following map is a well-defined field isomorphism that fixes F also:

$$\psi = \phi_\beta \circ \phi_\alpha^{-1} : F(\alpha) \to F(\beta), \quad \forall c_0, c_1, ..., c_n \in F$$

$$\psi(c_0 + c_1\alpha + ... + c_n\alpha^n) = \phi_\beta \circ \phi_\alpha^{-1}(c_0 + c_1\alpha + ... + c_n\alpha^n) = \phi_\beta(c_0 + c_1\overline{x} + ... + c_n\overline{x}^n) = c_0 + c_1\beta + ... + c_n\beta^n$$

Notice that such field isomorphism $psi : F(\alpha) \to F(\beta)$ can be extended to a ring isomorphism $\overline{\psi} : F(\alpha)[x] \to F(\beta)[x]$, given as:

$$\forall a_0, a_1, ..., a_n \in F(\alpha), \quad \overline{\psi}(a_0 + a_1x + ... + a_nx^n) = \psi(a_0) + \psi(a_1)x + ... + \psi(a_n)x^n$$

So, $\overline{\psi} \mid_{F(\alpha)} = \psi$. Which, because $f(x) \in F[x]$, it has all the coefficients being in F, then $\overline{\psi}(f(x)) = f(x) \in F(\beta)[x]$.

Now, given that α has multiplicity k, and β has multiplicity l, this implies that $(x-\alpha)^k \mid f(x)$ over $F(\alpha)$ (with any $n > k$ fails to satisfy this condition), while $(x-\beta)^l \mid f(x)$ over $F(\beta)$ (with any $m > l$ fails to satisfy this condition).

Then, since $f(x) = (x-\alpha)^k p_1(x)$ for some $p_1(x) \in F(\alpha)[x]$, we have the following:

$$f(x) = \overline{\psi}(f(x)) = \overline{\psi}((x-\alpha)^k)\overline{\psi}(p_1(x)) = (x-\beta)^k\overline{\psi}(p_1(x))$$

(Note: since $\overline{\psi}(x-\alpha) = x - \psi(\alpha) = x - \beta$, the above equality holds).

Which, the above equation shows that $(x-\beta)^k \mid f(x)$, hence $k \leq l$; on the other hand, if consider $\overline{\psi}^{-1}$, since $f(x) = (x-\beta)^l p_2(x)$ for some $p_2(x) \in F(\beta)[x]$, we have the following:

$$f(x) = \overline{\psi}^{-1}(f(x)) = \overline{\psi}^{-1}((x-\beta)^l)\overline{\psi}^{-1}(p_2(x)) = (x-\alpha)^l\overline{\psi}^{-1}(p_2(x))$$

Hence, $(x-\alpha)^l \mid f(x)$, showing that $l \leq k$. Which, we can conclude that $l = k$, so α, β have the same multiplicity.

2

Question 2

(a) *Let $\zeta_6 \in \mathbb{C}$ be a primitive 6^{th} root of unity. Find $m_{\zeta_6,\mathbb{Q}}(x)$.*

(b) *Let $m, n \in \mathbb{N}$ such that $m \equiv 2 \mod 6$ and $n \equiv 4 \mod 6$. Prove that $f(x) = x^m + x^n + 1$ is not irreducible over $\mathbb{Q}$.*

Pf:

(a) Since ζ_6 satisfies $(\zeta_6)^6 - 1 = 0$, then ζ_6 is a root of the polynomial $x^6 - 1 \in \mathbb{Q}[x]$.

Notice that $x^6 - 1$ has the following factorization in $\mathbb{Q}$:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$$

(Note: the two above quadratic polynomials are irreducible over $\mathbb{Q}$, since the only possible rational roots are ± 1, while none of them are actually the root of the quadratic polynomials).

Which, ζ_6 cannot be the root of $(x - 1)$ or $(x + 1)$ (since $\zeta_6 \notin \mathbb{Q}$), and ζ_6 cannot be a root of $x^2 + x + 1$ either: Suppose the contrary that ζ_6 is a root of $x^2 + x + 1$, then it implies that $0 = (\zeta_6 - 1) \cdot 0 = (\zeta_6 - 1)((\zeta_6)^2 + \zeta_6 + 1) = (\zeta_6)^3 - 1$. So, $\zeta_6 \in \mu_3$ (where μ_3 is the multiplicative group of the 3^{rd} roots of unity). Then, the multiplicative group of the 6^{th} roots of unity, $\mu_6 = \langle \zeta_6 \rangle \subseteq \mu_3$, which is a contradiction (since μ_6 contains more elements than μ_3), hence the assumption is false, ζ_6 cannot be a root of $x^2 + x + 1$.

Then, since ζ_6 is a root of $x^6 - 1$, while not a root for $(x - 1), (x + 1)$, and $(x^2 + x + 1)$, then it must be a root of $x^2 - x + 1$.

Since $(x^2 - x + 1)$ is irreducible (since it has no roots over $\mathbb{Q}$, and has degree 2) while being monic, then it must be the irreduible polynomial of ζ_6. So:

$$m_{\zeta_6,\mathbb{Q}}(x) = x^2 - x + 1$$

(b) Given that $m = 6k + 2$ and $n = 6l + 4$ for some $k, l \in \mathbb{Z}$. Notice that since $(\zeta_6)^6 = ((\zeta_6)^2)^3 = 1$, then $(\zeta_6)^2 \neq 1$ is in fact a 3^{rd} root of unity. Then, plug ζ_6 into the polynomial $x^m + x^n + 1$, we get:

$$(\zeta_6)^m + (\zeta_6)^n + 1 = (\zeta_6)^{6k+2} + (\zeta_6)^{6l+4} + 1 = (\zeta_6)^2 + (\zeta_6)^4 + 1 = ((\zeta_6)^2)^2 + (\zeta_6)^2 + 1$$

Which, from the relation $(\zeta_6)^6 - 1 = 0$, we get:

$$0 = ((\zeta_6)^2)^3 - 1 = ((\zeta_6)^2 - 1)(((\zeta_6)^2)^2 + (\zeta_6)^2 + 1)$$

And, since $(\zeta_6)^2 \neq 1$, the first linear term is not zero. Therefore, for the above expression to be 0, we need:

$$((\zeta_6)^2)^2 + (\zeta_6)^2 + 1 = 0$$

Hence, ζ_6 is a root of $x^m + x^n + 1$, showing that $m_{\zeta_6,\mathbb{Q}}(x) \mid (x^m + x^n + 1)$. Also, because both $m, n \in \mathbb{N}$, then $m \equiv 2 \mod 6$ enforces $m \geq 2$, and $n \equiv 4 \mod 6$ enforces $n \geq 4$, so $\deg(x^m + x^n + 1) \geq 4$, while $\deg(m_{\zeta_6,\mathbb{Q}}) = 2$ (given in **part (a)**), so $m_{\zeta_6,\mathbb{Q}} \neq x^m + x^n + 1$. Hence, $x^m + x^n + 1$ is reducible over $\mathbb{Q}$ (since $m_{\zeta_6,\mathbb{Q}}$ is a proper factor of it).

3

Question 3 *Prove that if F is an infinite field, then its multiplicative group $F^\times$ is never cyclic.*

Pf:

Suppose the contrary, that F is infinite while $F^\times$ is cyclic, then there exists $a \in F^\times$, such that $F^\times = \langle a \rangle$ (under multiplication). There are two cases to consider:

Characteristic 0 Field:

Given that $\text{char}(F) = 0$, then $-1 \neq 1$ (since if $-1 = 1$ in F, then $1 + 1 = 0$, showing that 1 has order 2 under addition, or $\text{char}(F) = 2$). So, since $-1 \in F^\times$, then there exists $l \in \mathbb{Z}$, such that $a^l = -1$.

Yet, this implies that $a^{2l} = (-1)^2 = 1$, so $|a| \leq 2l$, which further implies that $|\langle a \rangle| \leq 2l$, so $F^\times = \langle a \rangle$ is in fact finite. And, this is a contradiction.

Characteristic $p > 0$ field:

For all such field F, the prime subfield is $\mathbb{F}_p$. Hence, can view F as a field extension of $\mathbb{F}_p$.

First, notice that $a \neq 0$ (since $a \in F^\times$) and $a \neq 1$ (since $\langle 1 \rangle = \{1\}$, if $a = 1$, then $F^\times$ is finite, contradicting the assumption that $F = F^\times \cup \{0\}$ is infinite).

Also, since $F^\times$ must be infinite based on similar reason, then $a \neq -1$ (since $(-1)^2 = 1$, if $a = -1$, then $|\langle a \rangle| = |a| = 2$ as the order of a, showing that $F^\times$ is again finite, which is a contradiction). So, it implies that $a + 1 \neq 0$, hence $a + 1 \in F^\times$.

Then, there exists $l \in \mathbb{Z}$, such that $a^l = a + 1$, or $a^l - a - 1 = 0$. Which, there are several situations:

- Suppose $l = 0$, then $a^0 = 1$, so $a + 1 = 1$, or $a = 0$, which contradicts the fact that $a \neq 0$, so we don't need to consider this case.
- Suppose $l > 0$, then a is a root of the polynomial $x^l - x - 1 \in \mathbb{F}_p[x]$.
- Else if $l < 0$, then $(-l) > 0$. So, $a^{(-l)}(a^l - a - 1) = 1 - a^{1-l} - a^{-l} = 0$, showing that a is a root of the polynomial $1 - x^{1-l} - x^{-l} \in \mathbb{F}_p[x]$.

So, in either cases, there exists a polynomial $p(x) \in \mathbb{F}_p[x]$, such that $p(a) = 0$, hence $a \in F/\mathbb{F}_p$ is algebraic, its minimal polynomial $m_{a,\mathbb{F}_p}(x) \in \mathbb{F}_p[x]$ exists.

Then, $\mathbb{F}_p(a) \cong \mathbb{F}_p[x]/(m_{a,\mathbb{F}_p}(x))$ is a finite extension, which further implies that $\mathbb{F}_p(a)$ is finite (finite extension of a finite field is finite).

However, for all $b \in F$, if $b = 0$, $b \in \mathbb{F}_p(a)$; on the other hand, if $b \neq 0$, since $b \in F^\times = \langle a \rangle$, then $b = a^l \in \mathbb{F}_p(a)$ for some $l \in \mathbb{Z}$. Hence, $F \subseteq \mathbb{F}_p(a)$, while $\mathbb{F}_p(a) \subseteq F$, showing that $F = \mathbb{F}_p(a)$. This implies that F is finite, which again contradicts the assumption that F is an infinite field.

Since in all cases, $F^\times$ being cyclic would lead to a contradiction, then if F is infinite, $F^\times$ cannot be cyclic.

(Note: The proof fo $\text{char}(F) = p$ is designed for $p = 2$ specifically, since in that case $-1 = 1$, the proof used for $\text{char}(F) = 0$ cannot work. If $p > 2$, the proof for $\text{char}(F) = 0$ works perfectly fine).

4

Question 4 *Let K/F be a field extension and $m, n \in \mathbb{N}$. Let $\alpha, \beta \in K$ with $[F(\alpha) : F] = m$ and $[F(\beta) : F] = n$.*

(a) Show that $[F(\alpha, \beta) : F] \leq mn$.

(b) If $\gcd(m, n) = 1$, show that $[F(\alpha, \beta) : F] = mn$.

Pf:

Given the condition, since $F(\alpha), F(\beta)$ are both finite extensions of F, then α, β are algebraic over F. Also, with the degree given, we know $m = \deg(m_{\alpha,F})$, while $n = \deg(m_{\beta,F})$.

(a) Given $F \subseteq F(\alpha) \subseteq F(\alpha, \beta)$, we have the following relation:

$$[F(\alpha, \beta) : F(\alpha)] \cdot [F(\alpha) : F] = [F(\alpha, \beta) : F]$$

Which, since $m_{\beta,F}(x) \in F[x] \subseteq F(\alpha)[x]$, then β is also algebraic over $F(\alpha)$. Hence, $m_{\beta,F(\alpha)}(x) \in F(\alpha)[x]$ exists, while $m_{\beta,F(\alpha)}(x) \mid m_{\beta,F}(x)$ (since $m_{\beta,F}(\beta) = 0$ by definition). This implies that $\deg(m_{\beta,F(\alpha)}) \leq \deg(m_{\beta,F}) = n$.

Which, since $F(\alpha, \beta) = F(\alpha)(\beta)$, then $[F(\alpha, \beta) : F(\alpha)] = \deg(m_{\beta,F(\alpha)}) \leq n$, hence we get the following inequality:

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot [F(\alpha) : F] \leq mn$$

(b) Now suppose $\gcd(m, n) = 1$, then $\operatorname{lcm}(m, n) = mn$. Which, notice that both $F(\alpha), F(\beta)$ are subfields of $F(\alpha, \beta)$, hence the following two equality holds:

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot [F(\alpha) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot m$$

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)] \cdot [F(\beta) : F] = [F(\alpha, \beta) : F(\beta)] \cdot n$$

Hence, since $m \mid [F(\alpha, \beta) : F]$ and $n \mid [F(\alpha, \beta) : F]$, then $\operatorname{lcm}(m, n) = mn$ divides $[F(\alpha, \beta) : F]$; on the other hand, since in **part (a)** we've shown that $[F(\alpha, \beta) : F] \leq mn$, then $[F(\alpha, \beta) : F] = mn$.

5

Question 5 *Let K be a finite field. Show that K is not algebraically closed.*

Pf:

Suppose the contrary that some finite field K is algebraically closed, it implies that all polynomial in $K[x]$ has a root in K. Hence, the goal is to find a polynomial with no roots in K.

Consider the following example:

$$f(x) = 1 + \prod_{k \in K} (x - k) \in K[x]$$

Since K is finite, the above polynomial is well-defined. Also, for any $a \in K$, if plug into $f(x)$, we get:

$$f(a) = 1 + (a - a) \prod_{\substack{k \in K \\ k \neq a}} (a - k) = 1 + 0 \cdot \prod_{\substack{k \in K \\ k \neq a}} (a - k) = 1$$

This shows that none of the element $a \in K$ is a root of $f(x) \in K[x]$, which contradicts the assumption that K is algebraically closed.

Hence, the assumption is false, any finite field K is not algebraically closed.