Math 111C HW2

Zih-Yu Hsieh

April 16, 2025

1

Question 1 *Let $F \subseteq K \subseteq L$ be fields and let $\alpha \in L$ be algebraic over F. Prove that $[K(\alpha) : K] \leq [F(\alpha) : F]$.*

Pf:

Given that $\alpha \in L$ is algebraic over F, there exists minimal polynomial $f_{\alpha,F}(x) \in F[x] \subseteq L[x]$, such that $f_{\alpha,F}(\alpha) = 0$. On the other hand, since $F[x] \subseteq K[x]$, then $f_{\alpha,F}(x)$ as a polynomial over K has α being a root, implies that α is also algebraic over K, hence its minimal polynomial $p_{\alpha,K}(x) \in K[x]$ exists, with $p_{\alpha,K}(\alpha) = 0$.

Now, since $f_{\alpha,F}(x) \in K[x]$ has α being a root, then it implies that $p_{\alpha,K}(x) \mid f_{\alpha,F}(x)$ (since minimal polynomial of α divides all polynomials having α being a root), hence $\deg(p_{\alpha,K}) \leq \deg(f_{\alpha,F})$.

Lastly, since α is algebraic over both F and K, then $F(\alpha) \cong F[x]/(f_{\alpha,F}(x))$ (which the extension has degree being $\deg(f_{\alpha,F})$) and $K(\alpha) \cong K[x]/(p_{\alpha,K}(x))$ (which the extension has degree being $\deg(p_{\alpha,K})$), then:

$$[K(\alpha) : K] = [K[x]/(p_{\alpha,K}(x)) : K] = \deg(p_{\alpha,K}) \leq \deg(f_{\alpha,F}) = [F[x]/(f_{\alpha,K}(x)) : F] = [(\alpha) : F]$$

Hence, $[K(\alpha) : K] \leq [F(\alpha) : F]$.

2

Question 2 *Let K/F be a field extension and $\alpha_1, ..., \alpha_n \in K$ be algebraic over F. Prove that $F(\alpha_1, ..., \alpha_n) = F[\alpha_1, ..., \alpha_n]$.*

Pf:

We'll prove this statement by induction on the number of elements n.

First, for $n = 1$, if $\alpha_1 \in K$ is algebraic over F, if we consider its minimal polynomial $m_{\alpha,F}(x) \in F[x]$, since it is irreducible while $F[x]$ is a PID, then $K' = F[x]/(m_{\alpha,F}(x))$ is a field.

Now, consider the following ring homomorphism $\phi : K' \to F[\alpha_1]$ by $\phi(\bar{x}) = \alpha_1$. Then, since it is a nonzero map, while K' is a field, then ϕ is injective; also, for all $a_k\alpha^k + ... + a_0 \in F[\alpha]$, let $f(x) = a_kx^k + ... + a_0 \in F[x]$, then $\overline{f(x)} = a_k\bar{x}^k + ... + a_0 \in K'$, it satisfies:

$$\phi(\overline{f(x)}) = \phi(a_k\bar{x}^k + ... + a_0) = a_k\phi(\bar{x})^k + ... + a_0 = a_k\alpha_1^k + ... + a_0$$

This shows that ϕ is also surjective.

Then, because ϕ is bijctive, $K' \cong F[\alpha_1]$, hence $F[\alpha_1]$ is a field.

Given that $F(\alpha_1)$ is a field containing all operations of F and α_1¡ we know $F[\alpha_1] \subseteq F(\alpha_1)$; on the other hand, since $F(\alpha_1)$ is defined to be the smallest field containing both α_1 and F, and since $F[\alpha_1]$ also satisfies this property, then $F(\alpha_1) \subseteq F[\alpha_1]$. This shows that $F(\alpha_1) = F[\alpha_1]$.

Now, suppose for given $n \in \mathbb{N}$, any $\alpha_1, ..., \alpha_n \in K$ that are algebraic over F satisfy $F(\alpha_1, ..., \alpha_n) = F[\alpha_1, ..., \alpha_n]$. Then, for the case $(n + 1)$, given arbitrary $\alpha_1, ..., \alpha_n, \alpha_{n+1} \in K$ that are algebraic over F, we know $F(\alpha_1, ..., \alpha_n, \alpha_{n+1}) = F(\alpha_1, ..., \alpha_n)(\alpha_{n+1})$, which by induction hypothesis, $F(\alpha_1, ..., \alpha_n) = F[\alpha_1, ..., \alpha_n] = K''$. Then, since $F \subseteq K''$, while α_{n+1} is algebraic over F, then α_{n+1} is also algebraic over K'', so its minimal polynomial $m(x) \in K''[x]$ exists (with respect to field K'').

Then, using the same logic for the case $n = 1$, we know $K''[x]/(m(x)) \cong K''[\alpha_{n+1}] = K''(\alpha_{n+1})$.

Hence, we have the following:

$$F(\alpha_1, ..., \alpha_n, \alpha_{n+1}) = F(\alpha_1, ..., \alpha_n)(\alpha_{n+1}) = K''(\alpha_{n+1}) = K''[\alpha_{n+1}] = F(\alpha_1, ..., \alpha_n)[\alpha_{n+1}]$$

$$= F[\alpha_1, ..., \alpha_n][\alpha_{n+1}] = F[\alpha_1, ..., \alpha_n, \alpha_{n+1}]$$

This proves that $F(\alpha_1, ..., \alpha_n, \alpha_{n+1}) = F[\alpha_1, ..., \alpha_n, \alpha_{n+1}]$ for the case $(n + 1)$.

Finally, by the principle of mathematical induction, given any $\alpha_1, ..., \alpha_n \in K$ that are algebraic over F, we have $F(\alpha_1, ..., \alpha_n) = F[\alpha_1, ..., \alpha_n]$.

3

Question 3 *Let F be a field of caracteristic p, where p is a prime number. Suppose that $x^p - a$ where $a \in F$, does not have a root in F. Show that $x^p - a$ is irreducible in $F[x]$.*

Pf:

We'll prove by contradiction, that if $x^p - a$ has no roots in F, then $x^p - a \in F[x]$ is irreducible. Suppose it is reducible, then there exists nonconstant polynomials $q(x), r(x) \in F[x]$, with $x^p - a = q(x)r(x)$. (Note: it also implies $p = \deg(x^p - a) > \deg(q), \deg(r)$).

First, given $x^p - a \in F[x]$, we know there exists a field extension K/F, such that K is a splitting field of the polynomial $x^p - a$. Then, since $char(F) = p$ (which is the order of unity element 1 under addition), and F is a subfield of K (which is an integral domain), then in fact F and K both have the same unity element, hence $char(K) = p$.

Now, since $x^p - a$ splits completely over K, in particular, there exists $b \in K \setminus F$, such that $(x - b)$ is a linear factor of K. Hence, $b^p - a = 0$, or $b^p = a$ (since $(x - b)$ is a linear factor iff b is a root). Then, because $char(K) = p$ (which $char(K[x]) = p$ also, since they have the same identity), apply fresher's dream, we get $(x - b)^p = x^p - b^p = x^p - a$, hence $(x - b)^p$ is a factorization of $x^p - a$. Also, because $K[x]$ is a UFD, then such factorization is unique, showing that $x^p - a = q(x)r(x) = (x - b)^p \in K[x]$.

By the property of UFD, because $q(x)r(x) = (x - b)^p$, then $q(x)$ specifically must be factored into some form of $q(x) = (x - b)^k$, where $k = \deg(q) < p$.

4

Question 4

(a) Find all ring homomorphisms $\Psi : \mathbb{Q}[x] \to \mathbb{C}$.

(b) Find all ring homomorphisms $\Psi_1 : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{C}$ and $\Psi_2 : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{R}$.

Pf:

(a) First, the zero map $\Psi = 0$ is an ansewr.

Now, suppose $\Psi \neq 0$, then because $\Psi(\mathbb{Q}[x]) \subset \mathbb{C}$ is a nontrivial subring, while $\mathbb{C}$ is an integral domain, then all its nontrivial subring must have the same identity. Hence, $\Psi(1) = 1 \in \mathbb{C}$.

Notice that this also implies that for all $q \in \mathbb{Q}$, $\Psi(q) = q$: Since $\Psi(1) = 1$, then for all $a \in \mathbb{Z}$, $\Psi(a) = a$; now, if represent $q = \frac{a}{b}$ for $a, b \in \mathbb{Z},\ b \neq 0$, then we get:

$$\Psi(q) = \Psi(a \cdot b^{-1}) = \Psi(a) \cdot \Psi(b)^{-1} = a \cdot b^{-1} = q$$

Hence, all the rationals are fixed by the homomorphism.

Now, we can simply define $\Psi(x) = a$ for arbitrary $a \in \mathbb{C}$. Then, for all $f(x) = \sum_{k=0}^{n} f_k x^k \in \mathbb{Q}[x]$, we get:

$$\Psi(f(x)) = \Psi\left(\sum_{k=0}^{n} f_k x^k\right) = \sum_{k=0}^{n} \Psi(f_k) \cdot \Psi(x)^k = \sum_{k=0}^{n} f_k a^k$$

So, all the nonzero possibilities are characterized by $\Psi(1) = 1$, and $\Psi(x) = a$ for arbitrary $a \in \mathbb{C}$.

(b) Notice that since $x^3 - 2$ has no roots over $\mathbb{Q}$, then it must be irreducible. Hence, $\mathbb{Q}[x]/(x^3 - 2)$ is in fact a field (since the ideal $(x^3 - 2) \subset \mathbb{Q}[x]$ is maximal).

Possibility of Ψ_1:

First, the zero map $\Psi_1 = 0$ is always an answer.

For other possibilities, suppose $\Psi_1 \neq 0$, because $\mathbb{Q}[x]/(x^3 - 2)$ is a field, then Ψ_1 must be injective, hence $\mathbb{Q}[x]/(x^3 - 2) \cong \Psi_1(\mathbb{Q}[x]/(x^3 - 2)) \subseteq \mathbb{C}$. In this case, since the image is nontrivial, while $\mathbb{C}$ in particular is an integral domain, then all its subring (including the image of Ψ_1) must have the same identity as $\mathbb{C}$, so $\Psi_1(1) = 1 \in \mathbb{C}$.

Then, since $\bar{x} \in \mathbb{Q}[x]/(x^3 - 2)$ satisfies $\bar{x}^3 - 2 = \overline{x^3 - 2} = 0$, hence $\Psi_1(\bar{x}) \in \mathbb{C}$ must also satisfy this relationship, namely:

$$0 = \Psi_1(\bar{x}^3 - 2) = \Psi_1(\bar{x})^3 - \Psi_1(2) = \Psi_1(\bar{x})^3 - 2$$

(Note: since $\Psi_1(1) = 1$, then $\Psi_1(2) = \Psi_1(1 + 1) = \Psi_1(1) + \Psi_1(1) = 2$).

So, $\alpha = \Psi_1(\bar{x}) \in \mathbb{C}$ must satisfy $\alpha^3 - 2 = 0$, which is a root of $x^3 - 2 \in \mathbb{C}[x]$. Then, the only possibilities of $\alpha \in \mathbb{C}$ is $\alpha = \sqrt[3]{2},\ \sqrt[3]{2}e^{i \cdot 2\pi/3},\ \sqrt[3]{2}e^{i \cdot 4\pi/3}$.

Therefore, if $\Psi_1 \neq 0$, then it must satisfy $\Psi_1(1) = 1$, and $\Psi_1(\bar{x}) = \sqrt[3]{2},\ \sqrt[3]{2}e^{i \cdot 2\pi/3}$, or $\sqrt[3]{2}e^{i \cdot 4\pi/3}$.

Possibility of Ψ_2:

Again, the zero map $\Psi_2 = 0$ is an answer.

Now, suppose $\Psi_2 \neq 0$, again because $\mathbb{Q}[x]/(x^3-2)$ is a field, Ψ_2 must be injective, and $\Psi_2(1) = 1 \in \mathbb{R}$ (based on the same reason as described in Ψ_1).

Again, since $\bar{x} \in \mathbb{Q}[x]/(x^3-2)$ satisfies $\bar{x}^3 - 2 = 0$, hence $0 = \Psi_2(\bar{x}^3-2) = \Psi_2(\bar{x})^3 - \Psi_2(2) = \Psi(\bar{x})^3 - 2$. So, $\beta = \Psi_2(\bar{x}) \in \mathbb{R}$ satisfies $\beta^3 - 2 = 0$, which is a root of $x^3 - 2 \in \mathbb{R}[x]$. Then, the only possibility of $\beta \in \mathbb{R}$ is $\beta = \sqrt[3]{2}$.

Therefore, if $\Psi_2 \neq 0$, then it must satisfy $\Psi_2(1) = 1$, and $\Psi_2(\bar{x}) = \sqrt[3]{2}$.

5

Question 5 *Let p be prime number and F be a finite field with $q = p^k$ elements. Prove that*

$$x^{q-1} - 1 = \prod_{\alpha \in F^\times} (x - \alpha)$$

in $F(x)$. By comparing coefficients of suitable powers of x, conclude that

(a)

$$\sum_{\alpha \in F^\times} \alpha = 0$$

(b)

$$\prod_{\alpha \in F^\times} \alpha = -1$$

Pf:

Since F is a finite field wit order $|F| = q$, then $F^\times$ is a group under multiplication with $|F^\times| = q - 1$ (without 0). Hence, for all $\alpha \in F^\times$, $\alpha^{q-1} = 1$ (since 1 is the identity of $F^\times$, and all element's order of a finite group divides the order of the group itself).

So, given $x^{q-1} - 1 \in F[x]$, since F is a field, and the polynomial has degree $q - 1$, it has at most $q - 1$ roots counting multiplicity; on the other hand, all $\alpha \in F^\times$ satisfies $\alpha^{q-1} - 1 = 1 - 1 = 0$, hence α is a root of $x^{q-1} - 1$. And, since there are $q - 1$ distinct elements in $F^\times$, then $F^\times$ in fact contains (and only contains) all the roots of $x^{q-1} - 1$.

Now, because each $\alpha \in F^\times$ is a root of $x^{q-1} - 1$, then $(x - \alpha) \mid (x^{q-1} - 1)$, $x^{q-1} - 1 = (x - \alpha)q_1(x)$. Then, for a distinct $\beta \in F^\times$, since $0 = \beta^{q-1} - 1 = (\beta - \alpha)q_1(\beta)$, while $\beta \neq \alpha$, then $q_1(\beta) = 0$, showing that $(x - \beta) \mid q_1(x)$. So, inductively, we can factor out all $(x - \alpha)$ (with $\alpha \in F^\times$) as a linear term of $x^{q-1} - 1$, showing the following:

$$x^{q-1} - 1 = q(x) \prod_{\alpha \in F^\times} (x - a), \quad q(x) \in F[x], \quad q(x) \neq 0$$

On the other hand, the left hand side above has degree $q - 1$, while the right hand side has degree $\deg(q) + \deg(\prod_{\alpha \in F^\times} (x - a)) \geq \deg(\prod_{\alpha \in F^\times} (x - a)) = q - 1$ (Note: since there are $q - 1$ elements in $F^\times$, then $\prod_{\alpha \in F^\times} (x - a)$ is a product of $q - 1$ linear factors, hence has degree $q - 1$). So, this enforces $\deg(q) = 0$, which $q(x) \in F$ must be an invertible element.

Lastly, if we consider the leading coefficient, the left hand side has coefficient 1, while the right side has coefficient $q(x)$, hence $q(x) = 1$, showing the following:

$$x^{q-1} - 1 = \prod_{\alpha \in F^\times} (x - a)$$

(a) Given the above statement, if we consider the coefficient of degree $q - 2$, we get 0 for $x^{q-1} - 1$; on the right side, since x^{q-2} can only be obtained by choosing 1 factor to be constant, while the other factors are x, then the x^{q-2} has the coefficient $\sum_{\alpha \in F^\times} \alpha$. Hence, $\sum_{\alpha \in F^\times} \alpha = 0$.

(b) Again, if we consider the constant term, we get -1 for $x^{q-1} - 1$; on the right side, since constant term can only be obtained by the product of all constant terms, then it has constant term $\prod_{\alpha \in F^\times} \alpha$. Hence, $\prod_{\alpha \in F^\times} \alpha = -1$.