Math 111C HW1

Zih-Yu Hsieh

April 5, 2025

1

Question 1 *Show, using Eisenstein's criterion, that $f(X) = X^3 - 3X - 1$ is irreducible over $\mathbb{Q}$. Let α be a root of f in $\mathbb{C}$. Express $\frac{1}{\alpha}$ and $\frac{1}{\alpha+3}$ as linear combinations of 1, α and α^2.*

Pf:

Consider the ring homomorphism $\phi : \mathbb{Z}[X] \to \mathbb{Z}[X]$ by $\phi(f) = f(X+1)$. Which, ϕ is injective, since if $f(X+1)$ is constantly 0, its leading coefficient $a_n = 0$, which helps us inductively prove that $f = 0$.

Then, for $f(X) = X^3 - 3X - 1$ given above:

$$\phi(f) = f(X+1) = (X+1)^3 - 3(X+1) - 1 = (X^3 + 3X^2 + 3X + 1) - (3X + 3) - 1 = X^3 + 3X^2 - 3$$

Then, since leading coefficient is 1, while the rest of the coefficients (namely $3, 0, -3$) are divisible by 3, and -3 is not divisible by 3^2, so by Eisenstein's criterion, $\phi(f) = X^3 + 3X^2 - 3$ is irreducible over $\mathbb{Q}$. Then, since $\phi(f) = f(X+1)$ is irreducible over $\mathbb{Q}$, then f itself must also be irreducible:

Since $f(x) = x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$, then $(f(x)) \subseteq \mathbb{Q}[x]$ is in fact a maximal ideal, hence $K = \mathbb{Q}[x]/(f(x))$ is a field, where $\overline{x} \in K$ is a zero of $f(\theta) \in K[\theta]$.

Now, for the rest of the part, consider the ring homomorphism $\phi : K \to \mathbb{C}$ by $\phi(\overline{x}) = \alpha$. Which, since f is irreducible over $\mathbb{Q}$, $0 \in \mathbb{Q}$ is not a zero of f, hence if $f(\alpha) = 0$ over $\mathbb{C}$, then $\alpha \neq 0$. This implies that ϕ is not a zero map, hence because K is a field, ϕ must be injective.

So, because $\mathbb{C}$ is also a field (an integral domain), then $\phi(1) = 1 \in \mathbb{C}$, showing that for all nonero $k \in K$, $\phi(k^{-1})\phi(k) = \phi(1) = 1$, with $\phi(k) \neq 0$, then $\phi(k^{-1}) = (\phi(k))^{-1}$.

Expression of $\frac{1}{\alpha}$:

Since $\frac{1}{\alpha} = \alpha^{-1}$, and $\phi(\overline{x}) = \alpha$, then $\alpha^{-1} = \phi(\overline{x})^{-1} = \phi(\overline{x}^{-1})$. It suffices to find the inverse of $\overline{x} \in K$.

Given that $\overline{f(x)} = \overline{x^3 - 3x - 1} = 0 \in K$, then $\overline{x^3 - 3x} = \overline{1} \in K$, hence $\overline{x} \cdot \overline{x^2 - 3} = \overline{1}$, showing that $\overline{x^2 - 3} = (\overline{x})^{-1}$. Hence, the following is true:

$$\alpha^{-1} = \phi(\overline{x}^{-1}) = \phi(\overline{x^2 - 3}) = \alpha^2 - 3$$

Expression of $\frac{1}{\alpha+3}$:

Again, since $\frac{1}{\alpha+3} = (\alpha+3)^{-1} = (\phi(\overline{x+3}))^{-1} = \phi((\overline{x+3})^{-1})$, it suffices to find the inverse of $\overline{x+3} \in K$.

Since $K = \mathbb{Q}[x]/(f(x))$ is a degree 2 field extension of $\mathbb{Q}$ with basis $\{\overline{1}, \overline{x}, \overline{x^2}\}$, guess $\overline{x+3}^{-1} = \overline{ax^2 + bx + c}$ for some $a, b, c \in \mathbb{Q}$. Then, the following equation is satisfied:

$$\overline{(x+3)(ax^2 + bx + c)} = \overline{1}, \quad (x+3)(ax^2 + bx + c) \mod (f(x)) = 1 \mod (f(x))$$

$$\exists q(x) \in \mathbb{Q}[x], \quad (x+3)(ax^2+bx+c) = q(x)f(x)+1 = q(x)(x^3-3x-1)+1$$

Since $(x+3)(ax^2+bx+c) = q(x)(x^3-3x-1)+1$, while $ax^2+bx+c \neq 0$ (since over K, it is the inverse of $\overline{x+3}$), then $1 = \deg(x+3) \leq \deg((x+3)(ax^2+bx+c)) \leq 3$.

Hence, in case for $q(x)(x^3-3x-1)+1$ to have degree at least 1, we need $q(x) \neq 0$ (if $q=0$, then the expression is just 1, which violates the degree ≥ 1); also, for its degree to be at most 3 while (x^3-3x-1) has degree 3, the only possibility is $q(x)$ being a constant (since $q(x)(x^3-3x-1)$ is nonconstant, then $\deg(q(x)(x^3-3x-1)+1) = \deg(q(x)(x^3-3x-1)) = \deg(q) + \deg(x^3-3x-1) \geq 3$).

So, $q(x) = f \in \mathbb{Q}$, and $f \neq 0$.

Now, expand the above equation of polynomials, we get:

$$(x+3)(ax^2+bx+c) = q(x)(x^3-3x-1)+1 = f(x^3-3x-1)+1$$

$$ax^3+(3a+b)x^2+(3b+c)x+3c = fx^3-3fx+(-f+1)$$

Which, the coefficient of x^3 provides $a = f$; coefficient of x^2 provides $(3a+b) = 0$, so $b = -3a$; coefficient of x provides $(3b+c) = -3f = -3a$, then $c = -3b-3a = -3(-3a)-3a = 6a$; finally, the constant term provides $3c = (-f+1) = (-a+1)$, hence $18a = (-a+1)$, $19a = 1$, so $a = \frac{1}{19}$.

Plug all the coefficients back, we get:

$$ax^3+bx+c = ax^3-3ax+6a = a(x^2-3x+6) = \frac{1}{19}(x^2-3x+6)$$

Which, multiply by $(x+3)$, we get:

$$\frac{1}{19}(x+3)(x^2-3x+6) = \frac{1}{19}(x^3-3x+18) = \frac{1}{19}((x^3-3x-1)+19) = \frac{1}{19}(x^3-3x-1)+1$$

$$\frac{1}{19}(x+3)(x^2-3x+6) \mod (f(x)) = 1 \mod (f(x))$$

The above is true since $f(x) = x^3-3x-1$. Hence, this shows that $\overline{\frac{1}{19}(x^2-3x+6)}$ is in fact the inverse of $\overline{x+3} \in K$.

Then, return to the original equation, $\frac{1}{\alpha+3}$ can be expressed as:

$$\frac{1}{\alpha+3} = \phi((\overline{x+3})^{-1}) = \phi\left(\overline{\frac{1}{19}(x^2-3x+6)}\right) = \frac{1}{19}(\alpha^2-3\alpha+6)$$

2

Question 2 *Let $K = F(\alpha)$, where α is a root of the irreducible polynomial*

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

Express $\frac{1}{\alpha}$ in terms of α and the coefficients a_i.

Pf:

First, since f is irreducible in $F[x]$, then f has no zeroes in F. Hence, 0 cannot be a zero of f, so $\alpha \neq 0$. This also implies that $a_0 \neq 0$ (or else if $a_0 = 0$, 0 is a zero of f).

Then, consider $K' = F[x]/(f(x))$: Since f is an irreducible polynomial over F, then since $F[x]$ is a PID, the ideal $(f(x))$ is in fact maximal, hence $K' = F[x]/(f(x))$ is a field.

Now, consider $\overline{x} = x \mod (f(x)) \in K'$: since it satisfies the following:

$$f(\overline{x}) = \overline{x}^n + a_{n-1}\overline{x}^{n-1} + ... + a_1\overline{x} + a_0 = \overline{x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0} = 0 \mod (f(x)) \in K'$$

then K' is a field containing a zero of $f(x)$.

Then, consider the ring homomorphism $\phi : K' \to K$, by $\phi(\overline{x}) = \alpha$: Since 0 is not a zero of f, then $\alpha \neq 0 \in F(\alpha)$. Hence, the ring homomorphism ϕ is not the zero map, showing that $\ker(\phi) \neq K'$; then, since K' is a field, while $\ker(\phi) \neq K'$, the map is injective.

Lastly, consider the inverse of $\overline{x} \in K'$: Since $a_0 \neq 0$ in F, then $a_0^{-1}f(x) = a_0^{-1}(x^n + a_{n-1}x^{n-1} + ... + a_1 x) + 1$. Hence, the following is true:

$$0 = a_0^{-1}f(x) \mod (f(x)) = (a_0^{-1}(x^n + a_{n-1}x^{n-1} + ... + a_1 x) + 1) \mod (f(x))$$

$$\implies \overline{1} = \overline{a_0^{-1}(x^n + a_{n-1}x^{n-1} + ... + a_1 x)} \in K' = F[x]/(f(x))$$

So, $\overline{1} = \overline{a_0^{-1}(x^n + a_{n-1}x^{n-1} + ... + a_1 x)} = \overline{x} \cdot \overline{a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)}$, hence the inverse of $\overline{x}$ in K' is $\overline{a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)}$. Then, since ring homomorphism maps an element's inverse to the output's inverse, then $\phi(\overline{x}) = \alpha$ implies the following:

$$\frac{1}{\alpha} = \alpha^{-1} = \phi((\overline{x})^{-1}) = \phi\left(\overline{a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)}\right) = a_0^{-1}(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + ... + a_1)$$

3

Question 3 *Show that* x^4+1 *is irreducible over* $\mathbb{Q}$, *but not over* $\mathbb{Q}(\sqrt{2})$.

Pf:
If consider $x^4+1 \in \mathbb{Z}[x]$, if we do a substitution $x \mapsto (x+1)$, then we get the following:

$$(x^4+1) \mapsto (x+1)^4+1 = (x^4+4x^3+6x^2+4x+1)+1 = x^4+4x^3+6x^2+4x+2$$

Notice that since leading coefficient 1 is not divisible by 2, the other coefficients $4,6,4,2$ are divisible by 2, while the constant term 2 is not divisible by 2^2, then by Eisenstein's criterion, $(x+1)^4+1$ is irreducible over $\mathbb{Q}$. Hence, the original polynomial x^4+1 is also irreducible over $\mathbb{Q}$.

Now, consider x^4+1 over $\mathbb{Q}(\sqrt{2})$: since $\sqrt{2}$ is an element in the given field, then the following is a factorization of x^4+1:

$$((x^2+1)-\sqrt{2}x)((x^2+1)+\sqrt{2}x) = (x^2+1)^2-(\sqrt{2}x)^2 = (x^4+2x^2+1)-(2x^2) = x^4+1$$

Since x^4+1 can be factored into smaller degree nonconstant polynomial, this indicates x^4+1 is reducible over $\mathbb{Q}(\sqrt{2})$.

4

Question 4 *Find the minimal polynomial for* $\alpha = \frac{1}{5}\sqrt{50-10\sqrt{5}}$ *over* $\mathbb{Q}$.

Pf:
FIrst, given α above, we get the following:

$$5\alpha = 5\cdot\frac{1}{5}\sqrt{50-10\sqrt{5}} = \sqrt{50-10\sqrt{5}}, \quad 25\alpha^2 = (5\alpha)^2 = \left(\sqrt{50-10\sqrt{5}}\right)^2 = 50-10\sqrt{5}$$

$$25\alpha^2 = 5(10-2\sqrt{5}), \quad 5\alpha^2 = 10-2\sqrt{5}, \quad 2\sqrt{5} = 10-5\alpha^2$$

$$20 = (2\sqrt{5})^2 = (10-5\alpha^2)^2 = 25\alpha^4-100\alpha^2+100, \quad 25\alpha^4-100\alpha^2+80=0$$

$$5\alpha^4-20\alpha^2+16=0$$

So, α is a zero of $5x^4-20x^2+16 \in \mathbb{Z}[x]$.

Now, we'll prove that $5x^4-20x^2+16 \in \mathbb{Z}[x]$ is irreducible: Suppose the contrary, that $5x^4-20x^2+16$ is reducible, we can be written as $5x^4-20x^2+16 = f(x)g(x)$, where both f,g are nonconstant polynomials. If we do an inclusion into the Laurant Polynomial $\mathbb{Z}[x,x^{-1}]$, since $f(x)g(x) = 5x^4-20x^2+16 = x^4(5-20\frac{1}{x^2}+16\frac{1}{x^4})$, then $\frac{1}{x^4}f(x)g(x) = 5-20\frac{1}{x^2}+16\frac{1}{x^4}$.

Let $\deg(f)=k$, $\deg(g)=l$, then we know $k+l = \deg(f+g) = \deg(5x^4-20x^2+16) = 4$. Hence, $\frac{1}{x^4}f(x)g(x) = \left(\frac{1}{x^k}f(x)\right)\left(\frac{1}{x^l}g(x)\right)$, where both $\frac{1}{x^k}f(x), \frac{1}{x^l}g(x)$ are nonconstant laurent polynomials with only non-positive degrees. Because of so, there exists nonconstant polynomials $\bar{f}(x), \bar{g}(x) \in \mathbb{Z}[x]$, such that doing the substitution x by $\frac{1}{x}$, $\bar{f}(\frac{1}{x}) = \frac{1}{x^k}f(x)$, and $\bar{g}(\frac{1}{x}) = \frac{1}{x^l}g(x)$.

Hence, $\bar{f}(\frac{1}{x})\bar{g}(\frac{1}{x}) = \left(\frac{1}{x^k}f(x)\right)\left(\frac{1}{x^l}g(x)\right) = 5 - 20\frac{1}{x^2} + 16\frac{1}{x^4}$, then take $q(x) = 16x^4 - 20x^2 + 5$, we have $\bar{f}(x)\bar{g}(x) = 5 - 20x^2 + 16x^4 = q(x)$. So, $\bar{f}(x)\bar{g}(x)$ is a nontrivial factorization of $q(x) = 5 - 20x^2 + 16x^4$, showing that $q(x)$ is reducible.

Yet, with prime $p = 5$, since leading coefficient 16 is not divisible by 5, both $-20, 5$ are divisible by 5, and the constant term 5 is not divisible by 5^2, hence $q(x) = 5 - 20x^2 + 16x^4$ satisfies Eisenstein Criterion, which is irreudicble. This contradicts the fact that $q(x)$ is reducible from above. Therefore, our assumption must be false, $5x^4 - 20x^2 + 16$ is in fact irreducible.

Then, since α is a root of $5x^4 - 20x^2 + 16$, while the polynomial is irreducible, there doesn't exist a smaller degree nonzero polynomial, with α being its root: Suppose the contrary again, if α has minimal polynomial $p(x)$, where $\deg(p) < 4 = \deg(5x^4 - 20x^2 + 16)$, then since in $\mathbb{Q}[x]$, polynomial division exists, then there exists unique $q(x), r(x) \in \mathbb{Q}[x]$, such that $(5x^4 - 20x^2 + 16) = q(x)p(x) + r(x)$, with $r(x) = 0$ or $\deg(r) < \deg(p)$.

However, plug in α to the equation above, we get $0 = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha)$ (since $p(\alpha) = 0$ by the assumption of it being the minimal polynomial). If $r(x) \neq 0$, then it is a polynomial with degree less than $\deg(p)$, while $r(\alpha) = 0$, this contradicts the assumption that $p(x)$ is the minimal polynomial of α (the smallest degree monic polynomial with α being a root), hence $r(x) = 0$.

Yet, this implies that $q(x)p(x) = 5x^4 - 20x^2 + 16$. Because this polynomial is irreducible, this implies that $q(x)$ or $p(x)$ is invertible; but since $p(\alpha) = 0$, $p(x)$ is not invertible (since it cannot be constant, while the only invertible elements in $\mathbb{Q}[x]$ are nonzero constants). Therefore, $q(x)$ must be invertible, which is a constant. So, $q(x) = q \in \mathbb{Q}$, and $q \cdot p(x) = 5x^4 - 20x^2 + 16$, showing that $\deg(p) = 4$. But, this again contradicts the assumption that $\deg(p) < 4$, so our initial assumption must again be false, showing that there doesn't exists a nonzero polynomial with degree smaller than 4, while α is a root.

Lastly, because α has minimal polynomial with degree at least 4, while the polynomial $x^4 - 4x^2 + \frac{16}{5} = \frac{1}{5}(5x^4 - 20x^2 + 16)$ has α being a root of it, then $x^4 - 4x^2 + \frac{16}{5}$ must be the minimal polynomial of α.

5

Question 5 *Is* $\mathbb{Q}(\sqrt{2})$ *isomorphic to* $\mathbb{Q}(\sqrt{3})$*?*

Pf:

We'll prove by contradiction that the two fields are not isomorphic.

Suppose the contrary, that the two fields are isomorphic, then there exists bijective ring homomorphism $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$.

First, since $\phi(\mathbb{Q}(\sqrt{2})) = \mathbb{Q}(\sqrt{3})$ by assumption that ϕ is a bijection, then $\phi(1) = 1 \in \mathbb{Q}(\sqrt{3})$. Which, this implies that $\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1 + 1 = 2 \in \mathbb{Q}(\sqrt{3})$. Hence, since $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ satisfies $(\sqrt{2})^2 = 2$, then $2 = \phi(2) = \phi((\sqrt{2})^2) = \phi(\sqrt{2})^2 \in \mathbb{Q}(\sqrt{3})$.

Now, let $\phi(\sqrt{2}) = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, which $a, b \in \mathbb{Q}$. Then, it satisfies the following:

$$2 + 0\sqrt{3} = 2 = \phi(\sqrt{2})^2 = (a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3}$$

Hence, for the coefficients to match up, we need $2ab = 0$, which $a = 0$ or $b = 0$.

Yet, both leads to a contradiction:

- Suppose $a = 0$, then $2 = (a + b\sqrt{3})^2 = (b\sqrt{3})^2 = 3b^2$. Since $b = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$ with $q \neq 0$ (WLOG, assume $\gcd(p, q) = 1$), then $2 = 3b^2 = 3(\frac{p}{q})^2$, hence $3p^2 = 2q^2$.

  Since $3p^2$ is divisible by 2, while 3 is coprime with 2, then 2 divides p^2, hence 2 divides p. So, $p = 2k$ for some $k \in \mathbb{Z}$.

  Which, $2q^2 = 3p^2 = 3(2k)^2 = 4 \cdot 3k^2$, so $q^2 = 2 \cdot 3k^2$. Since q^2 is now divisible by 2, this implies that 2 divides q.

  Yet, since both p, q are divisible by p, $\gcd(p, q) \geq 2$, which violates the assumption that $\gcd(p, q) = 1$, so we reach a contradiction.

- Else, suppose $b = 0$, then $2 = (a + b\sqrt{3})^2 = a^2$, where $a \in \mathbb{Q}$. However, this violates the fact that 2 has no square root in $\mathbb{Q}$, which is again a contradiction.

Since both leads to a contradiction, our initial assumption must be false. Hence, the two fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ can't be isomorphic.

6

Question 6 *Prove that* $\mathbb{R}$ *is not a simple extension of* $\mathbb{Q}$*.*

Pf:
Recall that $\mathbb{R}$ is an uncountable set. So, it suffices to show that all simple extension of $\mathbb{Q}$ is countable. Every simple extension of $\mathbb{Q}$ is in the form $K = \mathbb{Q}(\theta) = \{p(\theta)/q(\theta) \mid p, q \in \mathbb{Q}[\theta],\ q \neq 0\}$.
Which, there are several cases to consider:

1. Suppose $\theta \in \mathbb{Q}$, then $K = \mathbb{Q}(\theta) = \mathbb{Q}$, which is countable.

2. Suppose $\theta \notin \mathbb{Q}$, but it is algebraic over $\mathbb{Q}$, then there exists a minimal polynomial $p(x) \in \mathbb{Q}[x]$ that is irreduible, such that $p(\theta) = 0 \in K$. In this case, since $(p(x)) \subset \mathbb{Q}[x]$ is maximal, then $\mathbb{Q}[x]/(p(x))$ is a field extension of $\mathbb{Q}$ containing a zero of $p(x)$, and it is isomorphic to $K = \mathbb{Q}(\theta)$.

   Then, because $K' = \mathbb{Q}[x]/(p(x))$ is a field extension of $\mathbb{Q}$ with degree $[K' : \mathbb{Q}] = \deg(p) = n$, where n is finite, it is also a $\mathbb{Q}$-vector space with dimension n, hence isomorphic to $\mathbb{Q}^n$.

   However, since $\mathbb{Q}$ is countable, for finite $n \in \mathbb{N}$, $\mathbb{Q}^n$ is also countable. Hence, $K \cong K' \cong \mathbb{Q}^n$ is also countable.

3. Suppose $\theta \notin \mathbb{Q}$, and is transcendental over $\mathbb{Q}$, then for all nonzero $p(x) \in \mathbb{Q}[x]$, $p(\theta) \neq 0 \in K$, hence the map $\mathbb{Q}[x] \to \mathbb{Q}(\theta)$ by $x \mapsto \theta$ is injective (since for all nonzero $p(x) \in \mathbb{Q}[x]$, $p(x) \mapsto p(\theta) \neq 0$), hence $\mathbb{Q}(\theta)$ contains $\mathbb{Q}[x]$; furthermore, since every element can be expressed as $\frac{p(\theta)}{q(\theta)}$ for $p, q \in \mathbb{Q}[x]$, and $q \neq 0$, then $\mathbb{Q}(\theta)$ is in fact isomorphic to $F(\mathbb{Q}[x])$, the field of fraction of $\mathbb{Q}[x]$ (since the ring homomorphism $F(\mathbb{Q}[x]) \to \mathbb{Q}(\theta)$ by $x \mapsto \theta$ has $\frac{p(x)}{q(x)} \mapsto \frac{p(\theta)}{q(\theta)}$, showing the map is surjective; also, since $F(\mathbb{Q}[x])$ is a field, the nonzero map is guaranteed to be injective).

   So, for this case it suffices to prove that $F(\mathbb{Q}[x])$ is countable.

   First, $\mathbb{Q}[x]$ is countable: For all $n \in \mathbb{N}$, let $P_n \subset \mathbb{Q}[x]$ be a collection of all polynomials with degree at most n. Which, as a $\mathbb{Q}$-vector space, P_n is isomorphic to $\mathbb{Q}^n$, so it is countable.

   Now, consider $\bigcup_{n\in\mathbb{N}} P_n \subseteq \mathbb{Q}[x]$: For app $p(x) \in \mathbb{Q}[x]$, since its degree $\deg(p) = n$ is finite, then $p(x) \in P_n \subset \bigcup_{n\in\mathbb{N}} P_n$, hence $\mathbb{Q}[x] = \bigcup_{n\in\mathbb{N}} P_n$. Now, since $\bigcup_{n\in\mathbb{N}} P_n$ is a countable union of all P_n, $n \in \mathbb{N}$, while each P_n is countable, then the union is also countable. Hence, $\mathbb{Q}[x]$ is countable.

   Now, consider $F(\mathbb{Q}[x]) = \{\frac{p(x)}{q(x)} \mid p, q \in \mathbb{Q}[x],\ q \neq 0\}$: Since $\mathbb{Q}[x]$ is also a UFD, then gcd for any finite collection of elements exist. For $\frac{p(x)}{q(x)}$ with $p, q \neq 0$, we'll assume $\gcd(p(x), q(x)) = 1$ (so the fraction is irreducible), and for $0 \in F(\mathbb{Q}[x])$, assume it's in the form $\frac{0}{1}$.
   Then, if we do the map $F(\mathbb{Q}[x]) \to (\mathbb{Q}[x] \times \mathbb{Q}[x])$ by $\frac{p(x)}{q(x)} \mapsto (p(x), q(x))$, the map is injective, since if $\frac{p(x)}{q(x)}, \frac{f(x)}{g(x)} \in F(\mathbb{Q}[x])$ (both in irreducible forms) get mapped to the same element, we neec $(p(x), q(x)) = (f(x), g(x))$, showing that the two fractions are the same. Hence, $F(\mathbb{Q}[x])$ is set isomorphic to a subset of $\mathbb{Q}[x] \times \mathbb{Q}[x]$, a set that is countable since $\mathbb{Q}[x]$ is countable. Hence, $F(\mathbb{Q}[x])$ is also countable.

   Finally, since $F(\mathbb{Q}[x])$ is countable, $\mathbb{Q}(\theta)$ that is isomorphic to $F(\mathbb{Q}[x])$, then it is also countable.

Since regardless of the case, the simple extension $\mathbb{Q}(\theta)$ is a countable set, because $\mathbb{R}$ is not countable, it cannot be a simple extension of $\mathbb{Q}$.

7

Question 7 *Let E/F be a field extension, and let $\alpha \in E$. Show that multiplication by α is a linear transformation of E considered as a vector space over F. When is this linear transformation non-singular?*

Pf:

To verify the multiplication by α being a linear transformation of E as a vector space over F, consider all $f, g \in E$, and scalar $\lambda \in F$:

By distributive property of multiplication, we know $\alpha(f+g) = \alpha f + \alpha g$; similarly, since E is a field, the multiplication is commutative, hence $\alpha(\lambda f) = \lambda(\alpha f)$, showing that the multiplication is in fact a linear transformation of E as a vector space over F.

Now, suppose α as a linear transformation is non-singular (i.e. invertible), which we'll verify that such transformation is non-singular iff $\alpha \neq 0$:

$\Longrightarrow$: Suppose $\alpha \neq 0$, then $\alpha^{-1} \in E$ exists since E is a field. Based on the fact that multiplication of any element in E is a linear transformation of E, any $f \in E$ satisfies $\alpha^{-1}(\alpha f) = \alpha(\alpha^{-1} f) = f$, which α^{-1} as a linear transformation over E composes with α to be identity on both sides, this shows that α^{-1} is the inverse transformation of α, hence α is non-singular.

$\Longleftarrow$: We'll prove the contrapositive. Suppose $\alpha = 0$, then since all nonzero $f \in E$ satisfies $\alpha f = 0$, then the transformation α is not injective, hence non-invertible. This shows that α is a singular linear transformation. Then, the contrapositive states that if α is non-singular, the $\alpha \neq 0$.

The above two implication states that α as a linear transformation is non-singular, iff $\alpha \neq 0$.

8

Question 8 *Let E/F be a field extension, and let $p(x)$ be an irreducible polynomial over F. Show that if the degree of $p(x)$ and $[E : F]$ are coprime, then $p(x)$ has no zeros in E.*

Pf:

We'll prove the contrapositive. Suppose $p(x)$ has a zero in E, say $\alpha \in E$, and $m = [E : F]$ is finite.

Given that $p(x)$ is irreducible over F, then it has no zero in F. Hence, $p(0) \neq 0$. Then, since $p(\alpha) = 0$, $\alpha \neq 0$.

First, we'll consider the ring $K' = F[x]/(p(x))$: Since $p(x) \in F[x]$ is irreducible, and $F[x]$ is a PID, the ideal $(p(x)) \subset F[x]$ is in fact maximal. Hence, $K' = F[x]/(p(x))$ is a field.

Now, given that $p(x) = a_n x^n + ... + a_1 x + a_0$, since $\overline{x} = x \mod (p(x)) \in K'$ satisfies the following:

$$p(\overline{x}) = a_n \overline{x}^n + ... + a_1 \overline{x} + a_0 = (a_n x^n + ... + a_1 x + a_0) \mod (p(x)) = p(x) \mod (p(x)) = 0 \in K'$$

Hence, $p(x)$ has a zero over the field K'.

Then, consider the ring homomorphism $\phi : K' \to E$ given by $\phi(\overline{x}) = \alpha$: since $\alpha \neq 0$ in E and $\overline{x} \neq 0$ in K', then such ring homomorphism is nonzero, hence $\ker(\phi) \neq K'$. Now, because K' is a field, then it enforces ϕ to be injective. Then, since $K' \cong \phi(K') \subseteq E$, this shows that K' is isomorphic to a subfield of E. Hence, E/K' is also a field extension.

Relationships of E, K', and F:

Now, given that $\deg(p) = n$, then K' as a vector space of F, has dimension n (i.e. $[K' : F] = n$); on the other hand, given that $m = [E : F]$ is finite, then E as a vector space of F has dimension m.

The above implies that $q = [E : K']$ is in fact finite, since K' is a finite-dimensional subspace of vector space E over field F. **(Need to verify)**

Lastly, given E/K' as a field extension, since $q = [E : K']$ by assumption, then there exists distinct nonzero $e_1, ..., e_q \in E$ that represents a basis of E as a vector space over K'.

Also, since $n = [K' : F]$, then there exists distinct nonzero $k_1, ..., k_n \in K'$ that represents a basis of K' as a vector space over F.

Our goal is to prove that the collection $\{k_j e_i \mid 1 \leq j \leq n,\ 1 \leq i \leq q\}$, actually represents a basis of E as a vector space over F: Based on the given bases of E/K' and K'/F above, for all $f \in E$, there exists unique $f_1, ..., f_q \in K'$, with $f = \sum_{i=1}^{q} f_i e_i$. And, for each $f_i \in K'$, there exists unique $l_1^{(i)}, ..., l_n^{(i)} \in F$, with $f_i = \sum_{j=1}^{n} l_j^{(i)} k_j$. Hence, the following is true:

$$f = \sum_{i=1}^{q} f_i e_i = \sum_{i=1}^{q} \left(\sum_{j=1}^{n} l_j^{(i)} k_j \right) e_i = \sum_{i=1}^{q} \sum_{j=1}^{n} l_j^{(i)} k_j e_i$$

Hence, the collection $\{k_j e_i \mid 1 \leq j \leq n,\ 1 \leq i \leq q\}$ actually is a basis of E/F.

On the other hand, suppose the collection of scalars $\{l_j^{(i)} \mid 1 \leq j \leq n,\ 1 \leq i \leq q\}$ satisfies $0 = \sum_{i=1}^{q} \sum_{j=1}^{n} l_j^{(i)} k_j e_i$, then after regrouping, we get the following:

$$0 = \sum_{i=1}^{q} \sum_{j=1}^{n} l_j^{(i)} k_j e_i = \sum_{i=1}^{q} \left(\sum_{j=1}^{n} l_j^{(i)} k_j \right) e_i$$

Since $e_1, ..., e_q \in E/K'$ is a basis of E over field K', the above equation implies that for each $1 \leq i \leq q$, the coefficient $\sum_{j=1}^{n} l_j^{(i)} k_j = 0 \in K'$; similarly, since $k_1, ..., k_n \in K'/F$ is a basis of K' over field f, the above equation implies that $l_1^{(i)}, ..., l_n^{(i)} = 0 \in F$, for all i given.

Hence, this proves the linear independence of the collection $\{k_j e_i \mid 1 \leq j \leq n,\ 1 \leq i \leq q\} \subset E/F$.

Since the collection is linearly independent while spanning E/F, then it is in fact a basis of E/F. Hence, as a vector space over F, E has dimension $n \cdot q = m$.

Since $n = \deg(p)$, while $nq = m = [E : F]$, this proves that n, m are not coprime. Hence, the contrapositive states the following: Given $p(x)$ an irreducible polynomial over F, and $[E : F]$ is finite, then degree of $p(x)$ and $[E : F]$ are coprime implies $p(x)$ has no zeros in E.

(However, if $\deg(p) = 1$, then the above breaks, since $p(x)$ is guaranteed to have a root in $\mathbb{F}$, while $\deg(p)$ is coprime to $[E : F]$).

9

Question 9 *Express* $\sqrt[3]{28}-3$ *as a square in* $\mathbb{Q}(\sqrt[3]{28})$.

Pf:

Since $\alpha = \sqrt[3]{28}$ satisfies $\alpha^3 = 28$, so it is a zero of $\alpha^3 - 28$. Notice that given $x^3 - 28 \in \mathbb{Z}[x]$, since with prime $p = 7$, it satisfies the Eisenstein Criterion (leading coefficient 1 is not divisible by 7; the other coefficients $0, 0, 28$ are divisible by 7, while 28 is not divisible by 7^2). Hence, $x^3 - 28$ is irreducible over $\mathbb{Q}$. Then, $(x^3 - 28) \subset \mathbb{Q}[x]$ is a maximal ideal, which $K = \mathbb{Q}[x]/(x^3 - 28)$ is a field containing a zero of $x^3 - 28$.

Now, consider the ring homomorphism $\phi : K \to \mathbb{Q}(\sqrt[3]{28})$ by $\phi(\overline{x}) = \sqrt[3]{28}$. Which, since all $k \in K$ has $\phi(k^2) = \phi(k)^2$, and $\phi(\overline{x-3}) = \sqrt[3]{28} - 3$, it suffices to find the element $k \in K$, with $k^2 = \overline{x-3}$.

Consider the element $k = \overline{\frac{1}{6}(x^2 - 2x - 2)} \in K$: If we take the square of the element, we get the following:

$$\left(\frac{1}{6}(x^2 - 2x - 2)\right)^2 = \frac{1}{36}((x^4 - 2x^3 - 2x^2) + (-2x^3 + 4x^2 + 4x) + (-2x^2 + 4x + 4))$$

$$= \frac{1}{36}(x^4 - 4x^3 + 8x + 4) = \frac{1}{36}((x^4 - 28x) + (-4x^3 + 112) + (36x - 108))$$

$$= \frac{1}{36}((x-4)(x^3 - 28) + 36(x-3)) = \frac{1}{36}(x-4)(x^3 - 28) + (x-3)$$

$$\overline{\left(\frac{1}{6}(x^2 - 2x - 2)\right)^2} = \left(\frac{1}{36}(x-4)(x^3 - 28) + (x-3)\right) \mod (x^3 - 28) = \overline{x-3}$$

Hence, since the above element satisfies $k^2 = \overline{x-3}$, then $\phi(k^2) = \phi(k)^2 = \phi(\overline{x-3}) = \sqrt[3]{28} - 3$.

Since $\phi(k) = \phi(\overline{\frac{1}{6}(x^2 - 2x - 2)}) = \frac{1}{6}((\sqrt[3]{28})^2 - 2\sqrt[3]{28} - 2)$, then we can conclude the following:

$$\left(\frac{1}{6}((\sqrt[3]{28})^2 - 2\sqrt[3]{28} - 2)\right)^2 = \sqrt[3]{28} - 3$$

10

Question 10 *Let $\beta = \omega\sqrt[3]{2}$, where $\omega = e^{2\pi i/3}$, and let $K = \mathbb{Q}(\beta)$. Prove that -1 cannot be written as a sum of squares in K.*

Pf:

Notice that since $\beta^3 = \omega^3(\sqrt[3]{2})^3 = 2$, then it satisfies $\beta^3 - 2 = 0$, which is a zero of $x^3 - 2 \in \mathbb{Q}[x]$.

Becuase $x^3 - 2 \in \mathbb{Z}[x]$ satisfies eisentstein criterion with $p = 2$, then it is irreducible over $\mathbb{Q}$. Hence, $(x^3 - 2) \subset \mathbb{Q}[x]$ is a maximal ideal, showing that $K' = \mathbb{Q}[x]/(x^3 - 2)$ is a field.

Now, if consider a ring homomorphism $\phi : K' \to \mathbb{Q}(\beta)$ by $\phi(\overline{x}) = \beta$, then because the map is nonzero while K' is a field, ϕ is injective; also, for all $k \in \mathbb{Q}(\beta)$, $k = \frac{p(\beta)}{q(\beta)}$ for $p, q \in \mathbb{Q}[x]$, and $q(\beta) \neq 0$, then since $\phi(\overline{q(x)}) = q(\beta) \neq 0$, we know $\overline{q(x)} \neq 0 \in K$, hence its inverse exists.

Which, we know $\phi(\overline{p(x)} \cdot \overline{q(x)}^{-1}) = \phi(\overline{p(x)}) \cdot \phi(\overline{q(x)})^{-1} = p(\beta) \cdot q(\beta)^{-1} = \frac{p(\beta)}{q(\beta)}$, this shows that ϕ is also surjective.

Because ϕ is bijective, then $K \cong \mathbb{Q}(\beta)$.

Now, notice that because $(\sqrt[3]{2})^3 = 2$, it is also a zero of $x^3 - 2 \in \mathbb{Q}[x]$. Then, given $\mathbb{Q}(\sqrt[3]{2})$, using similar method (by the ring homomorphism $\varphi : K' \to \mathbb{Q}(\sqrt[3]{2})$ with $\varphi(\overline{x}) = \sqrt[3]{2})$, we know $K \cong \mathbb{Q}(\sqrt[3]{2})$.

Then, if compose $\varphi \circ \phi^{-1}$, it becomes a natural ring isomorphism from $\mathbb{Q}(\beta)$ to $\mathbb{Q}(\sqrt[3]{2})$, with $\varphi \circ \phi^{-1}(\beta) = \varphi(\overline{x}) = \sqrt[3]{2}$.

Notice that the map satisfies the property: For all $a + b\beta + c\beta^2 \in \mathbb{Q}(\beta)$ (since it is isomorphic to $K = \mathbb{Q}[x]/(x^3 - 2)$, where every element is in the form $\overline{a + bx + cx^2}$ for $a, b, c \in \mathbb{Q}$, hence every element in $\mathbb{Q}(\beta)$ can be expressed as $\phi(\overline{a + bx + cx^2}) = a + b\beta + c\beta^2$), we get:

$$\varphi \circ \phi^{-1}(a + b\beta + c\beta^2) = \varphi(\overline{a + bx + cx^2}) = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$$

Hence, $-1 \in \mathbb{Q}(\beta)$ has $\varphi \circ \phi^{-1}(-1) = -1$ (since $-1 = -1 + 0\beta + 0\beta^2 \in \mathbb{Q}(\beta)$).

Finally, we can prove that $-1 \in \mathbb{Q}(\beta)$ can't be written as a sum of squares: Suppose not, then there exists $k_1, ..., k_n \in \mathbb{Q}(\beta)$, with $-1 = \sum_{i=1}^n k_i^2 \in \mathbb{Q}(\beta)$. Then, based on the ring isomorphism, we have the following (for simplicity, let $\varphi \circ \phi^{-1} = f$):

$$\varphi \circ \phi^{-1}(-1) = f(-1) = -1, \quad f(-1) = f\left(\sum_{i=1}^n k_i^2\right) = \sum_{i=1}^n f(k_i)^2$$

Now, since each $f(k_i) \in \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, then $f(k_i)^2 \geq 0$; hence, the sum $\sum_{i=1}^n f(k_i)^2 \geq 0$, showing that $-1 \geq 0$.

However, this is a contradiction in $\mathbb{R}$, hence our assumption must be wrong. $-1 \in \mathbb{Q}(\beta)$ cannot be written as sum of squares.