Math 111C HW3

Zih-Yu Hsieh

April 24, 2025

1

Question 1 *Let H/F be a field extension and $f(x), g(x) \in F[x]$. Suppose $K_1,\ K_2$ are splitting fields of $f(x)$ and $g(x)$ respectively, contained in H. Prove that $K_1K_2 := K_1(K_2)$ is a splitting field of the polynomial $f(x)g(x)$.*

Pf:

Since K_1 is a splitting field of $f(x)$ and K_2 is a splitting field of $g(x)$, then the following two statements are true:

$$\exists a \in F,\ a_1, ..., a_n \in K_1, \quad f(x) = a(x - a_1)...(x - a_n)$$

$$\exists b \in F,\ b_1, ..., b_m \in K_2, \quad g(x) = b(x - b_1)...(x - b_m)$$

In particular, $K_1 = F(a_1, ..., a_n)$ and $K_2 = F(b_1, ..., b_m)$ based on what we've proven in class.

Then, since $K_1 \subseteq K_1(K_2)$, $a_1, ..., a_n \in K_1(K_2)$; similarly, for all $q \in K_2$, since $1 \cdot q = q \in K_1(K_2)$, then $K_2 \subseteq K_1(K_2)$, hence $b_1, ..., b_m \in K_1(K_2)$.

Because $K_1(K_2)$ contains all roots of $f(x)$ in K_1, and all roots of $g(x)$ in K_2, hence $f(x)g(x)$ also splits completely over $K_1(K_2)$ (since $f(x), g(x)$ both split completely due to the existence of all roots). In particular, the factorization is given as follow, up to unit associates:

$$f(x)g(x) = ab(x - a_1)...(x - a_n) \cdot (x - b_1)...(x - b_m)$$

Now, to consider the splitting field of $f(x)g(x)$, say $E/F \subseteq K_1(K_2)/F$. From the statements proven in class, given the roots of $f(x)g(x)$ above, we know $E = F(a_1, ..., a_n, b_1, ..., b_m) = (F(a_1, ..., a_n))\,(b_1, ..., b_m) = K_1(b_1, ..., b_m)$.

Which, $K_1(b_1, ..., b_m)$ by definition, is the smallest field within $K_1(K_2)$ that's containing both K_1 and the set $\{b_1, ..., b_m\}$; however, since $F \subseteq K_1(b_1, ..., b_m)$, while $K_2 = F(b_1, ..., b_m)$ is defined to be the smallest field containing both F and $\{b_1, ..., b_m\}$, then since $K_1(b_1, ..., b_2)$ contains both, we must have $K_2 = F(b_1, ..., b_m) \subseteq K_1(b_1, ..., b_2)$.

Lastly, since $K_1,\ K_2 \subseteq K_1(b_1, ..., b_2)$, while $K_1(K_2)$ is the smallest field in $K_1(K_2)$ containing both K_1 and K_2, then $K_1(b_1, ..., b_m)$ containing both K_1, K_2 implies $K_1(K_2) \subseteq K_1(b_1, ..., b_m)$, showing that $K_1(K_2) = K_1(b_1, ..., b_m) = E$.

Hence, $K_1(K_2)$ is in fact a splitting field of $f(x)g(x) \in F[x]$.

2

Question 2 *Define the set of algebraic numbers* $\mathbb{A}$ *to be the set of all complex numbers which are algebraic over* $\mathbb{Q}$*. Show that* $\mathbb{A}/\mathbb{Q}$ *is an infinite algebraic extension.*

Pf:

We'll prove this via contradiction. Suppose $\mathbb{A}/\mathbb{Q}$ is a finite extension, say $[\mathbb{A} : \mathbb{Q}] = n < \infty$. Then, for any $\alpha \in \mathbb{A}$, since the list $1, \alpha, \alpha^2, ..., \alpha^n \in \mathbb{A}/\mathbb{Q}$ has length $(n+1)$, while $\mathbb{A}$ as a $\mathbb{Q}$-vector space has dimension n, then the above list is linearly dependent, showing that there exists $a_0, a_1, ..., a_n \in \mathbb{Q}$, such that the following is true:

$$f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Q}[x], \quad f(\alpha) = \sum_{k=0}^{n} a_k \alpha^k = 0$$

Now, take the minimal polynomial of α over $\mathbb{Q}$ (denoted as $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$), since α is a root of $f(x)$ defined above, then $m_{\alpha,\mathbb{Q}}(x) \mid f(x)$, showing that $\deg(m_{\alpha,\mathbb{Q}}) \leq \deg(f) \leq n$. So, all $\alpha \in \mathbb{A}/\mathbb{Q}$ should have minimal polynomial with degree at most n.

However, here is a counterexample: Consider $k > n$, and the polynomial $x^k - 2 \in \mathbb{Q}[x]$: Since over $\mathbb{Z}$, it satisfies the Eisenstein Criterion (the leading coefficient is 1, not divisible by 2; the rest of the coefficients are 0 and 2, which are divisible by 2; and 2 as the constant is not divisible by 2^2), hence $x^k - 2$ is irreducible over $\mathbb{Q}$ (and it is also monic).

Now, consider the element $2^{1/k} \in \mathbb{A}$: Since it satisfies $(2^{1/k})^k - 2 = 2 - 2 = 0$, then it is a root of $x^k - 2$. Then, because $x^k - 2$ is monnic and irreducible over $\mathbb{Q}$, it is in fact the minimal polynomial of $2^{1/k} \in \mathbb{A}$.

Yet, the proposed polynomial has degree $k > n$, while it is a minimal polynomial of some elements in $\mathbb{A}$, which supposedly should have degree at most n, then this forms a contradiction.

Hence, the assumption is false, $\mathbb{A}/\mathbb{Q}$ must be an infinite extension.

3

Question 3 *Let $n \in \mathbb{N}$ and μ_n be the (multiplicative) group of n^{th} roots of unity in $\mathbb{C}$. A generator of μ_n is called a primitive n^{th} root of unity. Let $F_n \subseteq \mathbb{C}$ be the splitting field of $x^n - 1$ over $\mathbb{Q}$.*

(a) If ζ_n is any primitive n^{th} root of unity, prove that $F_n = \mathbb{Q}(\zeta_n)$.

(b) Prove that any complex root of $m_{\zeta_n,\mathbb{Q}}(x)$ is also a primitive n^{th} root of unity.

(c) Prove that $[F_n : \mathbb{Q}] \leq \phi(n)$ where ϕ is the famous Euler's totient function.

Pf:

(a) Given that ζ_n is a primitive n^{th} root of unity, then $\langle \zeta_n \rangle = \mu_n$ (since it generates the whole μ_n). So, for any $\alpha \in \mu_n$, $\alpha = \zeta_n^k$ for some $k \in \mathbb{Z}$, proving that $\alpha \in \mathbb{Q}(\zeta_n)$. Hence, since $\mathbb{Q}(\zeta_n)$ contains all n^{th} roots of unity (all roots of $x^n - 1$ over $\mathbb{C}$), then $x^n - 1$ can be splitted completely over $\mathbb{Q}(\zeta_n)$, which the splitting field of $x^n - 1$, $F_n \subseteq \mathbb{Q}(\zeta_n)$.

On the other hand, since $\mathbb{Q} \subseteq F_n$, while $F_n \subseteq \mathbb{C}$ is the splitting field of $x^n - 1$, in particular, it must contain all roots of $x^n - 1$, which $\zeta_n \in F_n$.

Then, since $\mathbb{Q}(\zeta_n)$ is the smallest field in $\mathbb{C}$, containing both $\mathbb{Q}$ and ζ_n, then because F_n contains both collections, $\mathbb{Q}(\zeta_n) \subseteq F_n$.

This proves that $F_n = \mathbb{Q}(\zeta_n)$.

(b) Suppose $\alpha \in \mathbb{C}$ is also a root of $m_{\zeta_n,\mathbb{Q}}(x)$, then since $m_{\zeta_n,\mathbb{Q}(x)} \mid x^n - 1$ due to the fact that $\zeta_n^n - 1 = 0$ and $m_{\zeta_n,\mathbb{Q}}(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$, then α is also an n^{th} root of unity.

However, if α is not a primitive n^{th} root of unity, there exists $k < n$, such that $\alpha^k - 1 = 0$. Choose the smallest k, then α is in fact a primitive k^{th} root of unity. Because $m_{\zeta_n,\mathbb{Q}}(x) \in \mathbb{Q}[x]$ is both monic and irreducible, then since α is its root, it must also be the minimal polynomial of α. Which, $\alpha^k - 1 = 0$ implies that $m_{\zeta_n,\mathbb{Q}}(x) \mid x^k - 1$ (since α is also a root of $x^k - 1$), which all roots β of $m_{\zeta_n,\mathbb{Q}}(x)$ satisfies $\beta^k - 1 = 0$, including ζ_n.

However, this is a contradiction, since ζ_n as a primitive n^{th} root of unity of μ_n, supposedly has order n (or else it can't generate all the elements), while now $\zeta_n^k - 1 = 0$, showing that order of ζ_n is at most $k < n$. So, our assumption is false, if α is a root of $m_{\zeta_n,\mathbb{Q}}(x)$, it must also be a primitive n^{th} root of unity.

(c) Recall that in group theory, given a finite cyclic group $\langle a \rangle$ with order $|\langle a \rangle| = n$, then any $a^k \in \langle a \rangle$ is a generator of $\langle a \rangle$ iff $\gcd(k, n) = 1$. Then, since $|\mu_n| = |\langle \zeta_n \rangle| = n$, all the primitive n^{th} roots of unity in μ_n (the generators) must be in the form ζ_n^k, where $k \in \mathbb{Z}_n$ satisfies $\gcd(k, n) = 1$.

This implies that the number of primitive roots of unity for μ_n is precisely given by $\phi(n)$ (or, the number of elements in $\mathbb{Z}_n$ that is coprime to n).

Now, from **part (b)**, since we've proven that $m_{\zeta_n,\mathbb{Q}}(x)$ must have all of its roots being primitive n^{th} roots of unity, then it can have at most $\phi(n)$ roots, showing that $\deg(m_{\zeta_n,\mathbb{Q}}) \leq \phi(n)$.

Finally, since $F_n = \mathbb{Q}(\zeta_n)$, while $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(m_{\zeta_n,\mathbb{Q}}(x))$, then since $[\mathbb{Q}[x]/(m_{\zeta_n,\mathbb{Q}}(x)) : \mathbb{Q}] = \deg(m_{\zeta_n,\mathbb{Q}}) \leq \phi(n)$, then $[F_n : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$.

4

Question 4 *Let $f(x) = x^n - 2 \in \mathbb{Q}[x]$ with $n \in \mathbb{N}$. Let $\alpha \in \mathbb{C}$ be any n^{th} root of 2 and $\zeta_n = e^{2\pi i/n}$. Let $E \subseteq \mathbb{C}$ be the splitting field of $f(x)$ over $\mathbb{Q}$.*

(a) Show that $E = \mathbb{Q}(\alpha, \zeta_n)$.

(b) Let $n \geq 3$. Prove that $E \neq \mathbb{Q}(\alpha)$ and $E \neq \mathbb{Q}(\zeta_n)$.

Pf:

(a) First, if we consider $x^n - 2 \in \mathbb{C}[x]$, it has at most n roots counting multiplicity; now, for all integer $1 \leq k \leq n$, since $\sqrt[n]{2}e^{2\pi i \cdot k/n}$ satisfies $(\sqrt[n]{2}e^{2\pi i \cdot k/n})^n - 2 = 2 - 2 = 0$, while each k corresponds to a distinct element in $\mathbb{C}$, then there are in fact n distinct roots for $x^n - 2$ in $\mathbb{C}$, given as the above form. And, $E = \mathbb{Q}(\alpha_1, ..., \alpha_n)$, where each $\alpha_k = \sqrt[n]{2}e^{2\pi i \cdot k/n}$.

First, for all root $\alpha_k = \sqrt[n]{2}e^{2\pi i \cdot k/n}$, since $\alpha = \sqrt[n]{2}e^{2\pi i \cdot m/n}$ for some integer $0 \leq m < n$, then $\alpha_k = \sqrt[n]{2}e^{2\pi i \cdot m/n} \cdot e^{2\pi i \cdot (k-m)/n} = \alpha \cdot (\zeta_n)^{(k-m)}$, hence $\alpha_k \in \mathbb{Q}(\alpha, \zeta_n)$. Since all generators of E are contained in $\mathbb{Q}(\alpha, \zeta_n)$, then $E \subseteq \mathbb{Q}(\alpha, \zeta_n)$.

Then, since $\sqrt[n]{2}$, $\sqrt[n]{2}e^{2\pi i/n} \in \mathbb{C}$ are two roots of $x^n - 2$, then they're also contained in E; hence, $\zeta_n = e^{2\pi i/n} = (\sqrt[n]{2}e^{2\pi i/n})/(\sqrt[n]{2}) \in E$. Also, because $\alpha \in \mathbb{C}$ is a root of $x^n - 2$, $\alpha \in E$. Hence, this implies $\mathbb{Q}(\alpha, \zeta_n) \subseteq E$.

So, $E = \mathbb{Q}(\alpha, \zeta_n)$.

(b) We'll prove the two cases separately, given that $n \geq 3$.

- First, to prove that $E \neq \mathbb{Q}(\zeta_n)$, we'll consider its dimension:

  Since $\mathbb{Q}(\alpha) \subseteq E$ (since $\alpha \in E$), and $\alpha^n - 2 = 0$, this shows that α has its minimal polynomial over $\mathbb{Q}$ divides $x^n - 2 \in \mathbb{Q}[x]$; on the other hand, since $x^n - 2$ is monic, and it satisfies Eisenstein Criterion with prime $p = 2$, it is in fact irreducible, so $x^n - 2$ is the minimal polynomial of α, hence $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(x^n - 2)$, which has dimension n when $\mathbb{Q}$ is a base field. Hence, E as a $\mathbb{Q}$-vector space has dimension at least n (since $\mathbb{Q}(\alpha)$ is a $\mathbb{Q}$-linear subspace with dimension n), so $n \leq [E : \mathbb{Q}]$.

  On the other hand, since ζ_n satisfies $\zeta_n^n - 1 = 0$, or $(\zeta_n - 1)(\sum_{k=0}^{n-1}(\zeta_n)^k) = 0$. Since $\zeta_n \neq 1$ for $n \geq 3$, then $(\zeta_n - 1) \neq 0$. for the equality to hold, we need $\sum_{k=0}^{n-1}(\zeta_n)^k = 0$. Hence, ζ_n is a root of the polynomial $\sum_{k=0}^{n-1} x^k \in \mathbb{Q}[x]$, showing that its minimal polynomial $m_{\zeta_n,\mathbb{Q}}(x) \in \mathbb{Q}[x]$ has degree at most $n - 1$ (since $m_{\zeta_n,\mathbb{Q}}(x) \mid (\sum_{k=0}^{n-1} x^k)$). Therefore, $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(m_{\zeta_n,\mathbb{Q}}(x))$ has dimension at most $n - 1$, or $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq (n - 1)$.

  Because $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq (n - 1) < n \leq [E : \mathbb{Q}]$ from above, this implies that $\mathbb{Q}(\zeta_n) \neq E$.

- Then, to prove that $E \neq \mathbb{Q}(\alpha)$, we'll consider the following:

  Since all roots of $x^n - 2$ have minimal polynomial being $x^n - 2$ (proven in the first part of (b), that $x^n - 2$ is both monic and irreducible over $\mathbb{Q}$), then $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(x^n - 2) \cong \mathbb{Q}(\sqrt[n]{2})$. And, an explicit field isomorphism is given by $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\sqrt[n]{2})$, $\phi(1) = 1$, and $\phi(\alpha) = \sqrt[n]{2}$. (Note: The above is based on the fact that the maps $\bar{x} \mapsto \alpha$ and $\bar{x} \mapsto \sqrt[n]{2}$ are two field isomorphisms from the intermediate field to the field of $\mathbb{Q}$ adjoint with α or $\sqrt[n]{2}$ respectively, then taking an inverse in the first one and compose with the second one yields the desired isomorphism).

Now, notice that such field isomorphism can be generalized to a ring isomorphism $\bar{\phi} : \mathbb{Q}(\alpha)[x] \to \mathbb{Q}(\sqrt[n]{2})[x]$, such that $\bar{\phi}(a_0 + a_1x + ... + a_nx^n) = \phi(a_0) + \phi(a_1)x + ... + \phi(a_n)x^n$.

If we suppose the contrary that $E = \mathbb{Q}(\alpha)$, then $x^n - 2 = (x - a_1)...(x - a_n) \in \mathbb{Q}(\alpha)[x]$ for some $a_1, ..., a_n \in \mathbb{Q}(\alpha)$, which:

$$x^n-2 = \bar{\phi}(x^n-2) = \bar{\phi}((x-a_1)...(x-a_n)) = \bar{\phi}(x-a_1)...\bar{\phi}(x-a_n) = (x-\phi(a_1))...(x-\phi(a_n)) \in \mathbb{Q}(\sqrt[n]{2})[x]$$

This shows that $x^n - 2$ in fact splits completely over the field $\mathbb{Q}(\sqrt[n]{2})$.

However, since $\mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{C}$ is a field that $x^n - 2$ splits completely, by definition, $E \subseteq \mathbb{Q}(\sqrt[n]{2})$, showing that $\zeta_n \in E \subseteq \mathbb{Q}(\sqrt[n]{2})$. Yet, if $n \geq 3$, since $\zeta_n \notin \mathbb{R}$, then $\zeta_n \in \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{R}$ is a contradiction. Hence, our assumption is false, $E \neq \mathbb{Q}(\alpha)$.

5

Question 5

(a) Find $[\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})]$.

(b) Prove that $x^5 - 2$ *is irreducible over* $\mathbb{Q}(\sqrt{2})[x]$.

Pf:

(a) First, consider the extension $\mathbb{Q}(\sqrt[10]{2})/\mathbb{Q}$: Given $x^{10} - 2 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, since with prime $p = 2$, $x^{10} - 2$ satisfies the Eisenstein Criterion, then it is in fact irreducible over $\mathbb{Q}[x]$.

Now, since $\sqrt[10]{2}$ satisfies $(\sqrt[10]{2})^{10} - 2 = 2 - 2 = 0$, it is a root of $x^{10} - 2$. Then, because $x^{10} - 2$ is monic and irreudicible, it must be the minimal polynomial of $\sqrt[10]{2}$ over $\mathbb{Q}$. So, this implies that $\mathbb{Q}(\sqrt[10]{2}) \cong \mathbb{Q}[x]/(x^{10} - 2)$, which $[\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}] = [\mathbb{Q}[x]/(x^{10} - 2) : \mathbb{Q}] = 10$ (the degree of $x^{10} - 2$).

Then, because $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[10]{2})$ (since $(\sqrt[10]{2})^5 = \sqrt{2}$, proving that both $\mathbb{Q}, \{\sqrt{2}\} \subseteq \mathbb{Q}(\sqrt[10]{2})$, then $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[10]{2})$), then by the theorem proven in class, we know:

$$10 = [\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

Now, because of the same arument about Eisenstein Criterion, $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible, and since $\sqrt{2}$ is a root of it, while $x^2 - 2$ is being both irreducible and monic, then it is in fact the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. Then, $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$, showing that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}[x]/(x^2 - 2) : \mathbb{Q}] = 2$.

Hence, we get the following:

$$10 = [\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})] \cdot 2$$
$$\implies [\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})] = 5$$

(b) First, consider the element $\sqrt[5]{2} = (\sqrt[10]{2})^2 \in \mathbb{Q}(\sqrt[10]{2})$: Since it satisfies $(\sqrt[5]{2})^5 - 2 = 2 - 2 = 0$, then it is a root of $x^5 - 2 \in \mathbb{Q}(\sqrt{2})[x]$. Hence, let $m_{\sqrt[5]{2}}(x) \in \mathbb{Q}(\sqrt{2})[x]$ be the minimal polynomial of $\sqrt[5]{2}$ over $\mathbb{Q}$, it satisfies $m_{\sqrt[5]{2}}(x) \mid x^5 - 2$.

Now, to prove the statement, suppose the contrary that $x^5 - 2 \in \mathbb{Q}(\sqrt{2})[x]$ is not the minimal polynomial of $m_{\sqrt[5]{2}}(x)$ over $\mathbb{Q}(\sqrt{2})$, then this enforces $\deg(m_{\sqrt[5]{2}}) < \deg(x^5 - 2) = 5$ (or else since $x^5 - 2 = k(x) \cdots m_{\sqrt[5]{2}}(x)$, if $\deg(m_{\sqrt[5]{2}}) = 5$, then $k(x)$ is a constant $k \in \mathbb{Q}(\sqrt{2})$; but since both $x^5 - 2$ and $m_{\sqrt[5]{2}}(x)$ are monic, $k = 1$, showing that $x^5 - 2 = m_{\sqrt[5]{2}}(x)$). Which, $\mathbb{Q}(\sqrt{2})(\sqrt[5]{2})$ is field isomorphic to $\mathbb{Q}(\sqrt{2})[x]/(m_{\sqrt[5]{2}}(x))$, which has degree given as follow:

$$[\mathbb{Q}(\sqrt{2})(\sqrt[5]{2}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})[x]/(m_{\sqrt[5]{2}}(x)) : \mathbb{Q}(\sqrt{2})] = \deg(m_{\sqrt[5]{2}}(x)) < 5$$

However, since $(\sqrt{2})/(\sqrt[5]{2})^2 = \sqrt[10]{2} \in \mathbb{Q}(\sqrt{2})(\sqrt[5]{2})$, then as a $\mathbb{Q}(\sqrt{2})$-vector space, we have $\mathbb{Q}(\sqrt[10]{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt[5]{2})$; yet, in **part (a)** we've proven that $[\mathbb{Q}(\sqrt[10]{2}) : \mathbb{Q}(\sqrt{2})] = 5$, showing that $\mathbb{Q}(\sqrt[10]{2})$ is a 5-dimensional $\mathbb{Q}(\sqrt{2})$-linear subspace of $\mathbb{Q}(\sqrt{2})(\sqrt[5]{2})$, a $\mathbb{Q}(\sqrt{2})$-vector space with dimension strictly less than 5, which is a contradiction.

So, our assumption is false, $x^5 - 2 \in \mathbb{Q}(\sqrt{2})[x]$ is in fact the minimal polynomial of $\sqrt[5]{2}$ over $\mathbb{Q}(\sqrt{2})$, which must be irreducible.