周天元 3036127048

20/20

Problem 1.

$\alpha = \sqrt{2+\sqrt{2}}$, $\alpha^2 = 2+\sqrt{2}$, $\alpha^2 - 2 = \sqrt{2}$,

$(\alpha^2-2)^2 = 2$, $\alpha^4 - 4\alpha^2 + 4 = 2$, $\alpha^4 - 4\alpha^2 + 2 = 0$.

4/4

2 is prime $2 \nmid 1$, $2 \mid 0$, $2 \mid -4$, $2 \mid 0$, $2 \mid 2$, $2 \nmid 2^2$ $2^2 \nmid 2$

It follows that $f(x) = x^4 - 4x^2 + 2$ is irreducible over $\mathbb{Z}$ (with root $\sqrt{2+\sqrt{2}}$), thus over $\mathbb{Q}$.

Hence, $[\mathbb{Q}(\sqrt{2+\sqrt{2}}) : \mathbb{Q}] = 4$.

$\mathbb{Q}(\sqrt{2+\sqrt{2}}) \subseteq \mathbb{R}$, so $g(x) = x^2 + 1$ (with root $\sqrt{-1}$) is irreducible over $\mathbb{Q}(\sqrt{2+\sqrt{2}})$, which implies $[\mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{-1}) : \mathbb{Q}(\sqrt{2+\sqrt{2}})] = 2$

By Tower Theorem, $[\mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{-1}) : \mathbb{Q}] = 4 \cdot 2 = 8$.

Problem 2: Assume to the contrary that $(1, \sqrt[7]{2}) \in \mathbb{R}^2$ is constructable.

2/2

Now $\sqrt[7]{2}$ becomes constructable, but $f(x) = x^7 - 2$ (with root $\sqrt[7]{2}$) is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, so $[\mathbb{Q}(\sqrt[7]{2}) : \mathbb{Q}] = 7$, not a power of 2, contradiction!

Problem 3:

5/5

(1) Let α be a complex number.

If for some nonzero polynomial $f(x) = \sum_{k=0}^{n} a_k x^k$ with rational coefficients $f(\alpha) = 0$, then α is an algebraic number.

i is a root of $x^2 + 1 \in \mathbb{Q}[x]$, so i is algebraic over $\mathbb{Q}$.

(2) Step1: $\sqrt{3}$ is a root of $x^2 - 3 \in \mathbb{Q}[x]$, so $\sqrt{3}$ is algebraic over $\mathbb{Q}$.

$\sqrt[7]{34}$ is a root of $x^7 - 34 \in \mathbb{Q}[x]$, so $\sqrt[7]{34}$ is algebraic over $\mathbb{Q}$.

Step2: Linear combinations of algebraic numbers are algebraic, so: $9 - \sqrt[7]{34}$, $23 - \sqrt{3}$ are algebraic over $\mathbb{Q}$.

Step3: $\sqrt[9]{9 - \sqrt[7]{34}}$, $\sqrt[5]{23 - \sqrt{3}}$ are algebraic over $\mathbb{Q}(9 - \sqrt[7]{34}, 23 - \sqrt{3})$, so it follows from tower theorem that they are algebraic over $\mathbb{Q}$.

扫描全能王 创建

Step 4: Linear combinations and products of algebraic numbers are algebraic,
so $\sqrt[9]{9-\sqrt[7]{34}} \pm i\sqrt[5]{23-\sqrt{3}}$ is an algebraic number.

Step 5: As $\sqrt[9]{9-\sqrt[7]{34}} \neq 0$, $\sqrt[9]{9-\sqrt[7]{34}} + i\sqrt[5]{23-\sqrt{3}} \neq 0$,
so the quotient of algebraic numbers

$$\frac{\sqrt[9]{9-\sqrt[7]{34}} - i\sqrt[5]{23-\sqrt{3}} \leftarrow \text{algebraic}}{\sqrt[9]{9-\sqrt[7]{34}} + i\sqrt[5]{23-\sqrt{3}} \leftarrow \text{algebraic}}$$

is an algebraic number.

Problem 4:

(1) Let $K \subseteq L$ be a field extension, and $f(x) \in K[x]$ be a non constant polynomial. If there exist $a_n \in K^{\times}$, $\alpha_1, \alpha_2, \cdots, \alpha_n \in L$, such that:

(1) $$f(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in L[x]$$

(2) $$L = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

Then L is called a splitting field of $f(x)$ over K.

(2) Let K be a field, and $f(x) \in K[x]$ be a non constant polynomial.

Existence→ There exists a splitting field $K \subseteq L$ of $f(x)$ over K.

Uniqueness→ Let $\phi: K_1 \to K_2$ be a field isomorphism, $\Phi: K_1[x] \to K_2[x]$, $\sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=0}^{n} \phi(a_k) x^k$ be the induced ring isomorphism, and $f_1(x), f_2(x)$ be non constant polynomials in $K_1[x], K_2[x]$ with $\Phi(f_1(x)) = f_2(x)$.

If $K_1 \subseteq L_1$, $K_2 \subseteq L_2$ are splitting fields of $f_1(x), f_2(x)$ over K_1, K_2, then there exists a field isomorphism $\psi: L_1 \to L_2$ with $\psi|_{K_1} = \varphi$

扫描全能王 创建

(3) Proof: Assume that L is a splitting field of $f(x) \in K[x]$ over K.

For all irreducible polynomial $g(x) \in K[x]$ with a root $\alpha \in L$,

define (let) M as (be) the (a) splitting field of $f(x)g(x)$ over K.

Note that M is the smallest field that contains the splitting fields of $f(x)$ and $g(x)$.

Goal: For all root β of $g(x)$ in M, we wish to show that $\beta \in L$.

$$\begin{tikzcd} \text{all roots of } f,\ \text{root } \alpha \text{ of } g & L \arrow[l] \arrow[r, "\text{embedding}"] \arrow[d, phantom, "\cup"] & M \arrow[r] \arrow[d, phantom, "\cup"] & \text{all roots of } f \\ & K & \text{all roots of } g,\ \beta \arrow[ul, dashed] & \end{tikzcd}$$

To do so, consider the subfield $K(\alpha)$ of L and the subfield $K(\beta)$ of M.

By one step extension lemma, there exists a field isomorphism $\phi: K(\alpha) \to K(\beta)$ with $\phi|_K = id_K$. As L is the splitting field of $f(x)$ over K, it is a splitting field of $f(x)$ over $K(\alpha)$.

$$\begin{tikzcd} L \arrow[r, dashed, "\psi"] & M \\ K(\alpha) \arrow[u, phantom, "\cup"] \arrow[r, "\phi"] & K(\beta) \arrow[u, phantom, "\cup"] \end{tikzcd}$$

By extension lemma, there exists a field embedding $\psi: L \to M$ with $\psi|_{K(\alpha)} = \phi$, and the image of this ψ is the same as L. As β is in the image, $\beta \in L$, so $K \subseteq L$ is normal.

$\beta = \phi(\alpha) = \psi(\alpha)$

Problem 5:

3/3

Note that a finite field has a prime characteristic $p \geq 2$, and its order is a power p^n of p, where $n \geq 1$.

As p^n is even, p is even, so p is 2. This implies this finite field is the splitting field of $x^{2^n} - x$ over $\mathbb{F}_2$.

For all $\alpha \in \mathbb{F}_{2^n}$, $\alpha^{2^n} - \alpha = 0$, so $\alpha = \left(\alpha^{2^{n-1}}\right)^2$ is a square.

扫描全能王 创建