20250402 MATH4302 Assignment 5.

(1)(a) Recall that a complex number α is algebraic over $\mathbb{Q}$ iff the $\mathbb{Q}$-vector space homomorphism $\alpha: \mathbb{C} \to \mathbb{C}, z \mapsto \alpha z$ is annihilated by some monic polynomial $f(x) \in \mathbb{Q}[x]$.

We are going to prove that a complex number α is algebraic over $\mathbb{Q}$ iff the $\mathbb{Q}$-vector space homomorphism $\alpha: \mathbb{C} \to \mathbb{C}, z \mapsto \alpha z$ has a finitely-generated invariant subspace $V \neq \{0\}$.

Proof: We may divide our proof into two parts.

"if" direction: Assume that the $\mathbb{Q}$-vector space homomorphism $\alpha: \mathbb{C} \to \mathbb{C}$, $z \mapsto \alpha z$ has a finitely generated invariant subspace $V \neq \{0\}$.

The restricted $\mathbb{Q}$-vectorspace homomorphism $\alpha|_V : V \to V$ has an eigenpolynomial $f(x)$ because V is finitely-generated, $f(\alpha) v_0 = 0$ for some $v_0 \neq 0$ because $V \neq \{0\}$, $f(\alpha) = 0$ because $\mathbb{C}$ is a field. Hence, α is algebraic over $\mathbb{Q}$.

"only if" direction: Assume that α is algebraic over $\mathbb{Q}$.

The $\mathbb{Q}$-vector space homomorphism $\alpha: \mathbb{C} \to \mathbb{C}, z \mapsto \alpha z$ is annihilated by some monic polynomial $f(x) \in \mathbb{Q}[x]$. Suppose that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

Define $V = \mathbb{Q} + \alpha\mathbb{Q} + \alpha^2\mathbb{Q} + \cdots + \alpha^{n-1}\mathbb{Q}$. As $V \supseteq \mathbb{Q}$, $V \neq \{0\}$.

As $\alpha(\alpha^k \mathbb{Q}) = \alpha^{k+1}\mathbb{Q}$ $(0 \le k < n-1)$, $\alpha(\alpha^{n-1}\mathbb{Q}) = (-a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1})\mathbb{Q}$, V is invariant under α, so $\alpha: \mathbb{C} \to \mathbb{C}, z \mapsto \alpha z$ has a finitely-generated invariant subspace $V = \mathbb{Q} + \alpha\mathbb{Q} + \alpha^2\mathbb{Q} + \cdots + \alpha^{n-1}\mathbb{Q}$.

Date / /

Recall that a complex number α is algebraic over $\mathbb{Z}$ iff the $\mathbb{Z}$-module homomorphism $\alpha: \mathbb{C} \to \mathbb{C}, z \mapsto \alpha z$ is annihilated by some monic polynomial $f(x) \in \mathbb{Z}[x]$.

We are going to prove that a complex number α is algebraic over $\mathbb{Z}$ iff the $\mathbb{Z}$-module homomorphism $\alpha: \mathbb{C} \to \mathbb{C}, z \mapsto \alpha z$ has a finitely-generated invariant submodule $M \neq \{0\}$.

Proof: We may divide our proof into two parts.

"if" direction: Assume that the $\mathbb{Z}$-module homomorphism $\alpha: \mathbb{C} \to \mathbb{C}$, $z \mapsto \alpha z$ has a finitely generated invariant submodule $M \neq \{0\}$.

The restricted $\mathbb{Z}$-module homomorphism $\alpha|_M: M \to M$ has an eigenpolynomial because M is finitely-generated, $f(\alpha) v_0 = 0$ for some $v_0 \neq 0$ because $M \neq \{0\}$, $f(\alpha) = 0$ because $\mathbb{C}$ is a field. Hence, α is algebraic over $\mathbb{Z}$.

"only if" direction: Assume that α is algebraic over $\mathbb{Z}$.

The $\mathbb{Z}$-module homomorphism $\alpha: \mathbb{C} \to \mathbb{C}, z \mapsto \alpha z$ is annihilated by some monic polynomial $f(x) \in \mathbb{Z}[x]$. Suppose that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

Define $M = \mathbb{Z} + \alpha\mathbb{Z} + \alpha^2\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z}$. As $M \supseteq \mathbb{Z}$, $M \neq \{0\}$.

As $\alpha(\alpha^k \mathbb{Z}) = \alpha^{k+1}\mathbb{Z}$ $(0 \le k < n-1)$, $\alpha(\alpha^{n-1}\mathbb{Z}) = (-a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1})\mathbb{Z}$, M is invariant under α, so $\alpha: \mathbb{C} \to \mathbb{C}, z \mapsto \alpha z$ has a finitely-generated invariant submodule $M = \mathbb{Z} + \alpha\mathbb{Z} + \alpha^2\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z}$.

Date / /

(b) Take the minimal polynomial $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ of α over $\mathbb{Q}$.

On one hand, $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ is a basis of $\mathbb{Q}[\alpha]$, and $\alpha\mathbb{Q}[\alpha]\subseteq\mathbb{Q}[\alpha]$.
On the other hand, every finitely-generated invariant subspace $V\neq\{0\}$ contains some $v_0\neq 0$, thus containing a linearly independent list $v_0,\alpha v_0,\alpha^2 v_0,\cdots,\alpha^{n-1}v_0$, which implies the vector space $\mathbb{Q}[\alpha]$ is embedded in V.
Hence, $\mathbb{Q}[\alpha]$ is minimal up to embeddings. The minimal dimension is n.

~~Take the minimal polynomial $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ of α over $\mathbb{Z}$.~~

~~On one hand, $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ is a basis of $\mathbb{Z}[\alpha]$, and $\alpha\mathbb{Z}[\alpha]\subseteq\mathbb{Z}[\alpha]$.~~
~~On the other hand, every finitely-generated invariant submodule $M\neq\{0\}$ contains some $r_0\neq 0$, thus containing a linearly independent list $r_0,\alpha r_0,\alpha^2 r_0,\cdots,\alpha^{n-1}r_0$, which implies the module $\mathbb{Z}[\alpha]$ is embedded in M.~~
~~Hence, $\mathbb{Z}[\alpha]$ is minimal up to embeddings. The minimal rank is n.~~

(2)(a) Proof: $\alpha\in\overline{\mathbb{Z}}\cap\mathbb{Q}\Leftrightarrow\alpha$ has a minimal polynomial over $\mathbb{Z}$ (which is the same in $\mathbb{Q}$) and the minimal polynomial of α over $\mathbb{Q}$ is linear
$\Leftrightarrow$ the minimal polynomial of α over $\mathbb{Z}$ is linear $\Leftrightarrow\alpha\in\mathbb{Z}$

(b) Proof: $\alpha\in\overline{\mathbb{Q}}\Rightarrow\alpha$ has a minimal polynomial over $\mathbb{Q}$, say, $x^n+\frac{p_{n-1}}{q_{n-1}}x^{n-1}+\cdots+\frac{p_0}{q_0}$.
$\Rightarrow(q_{n-1}\cdots q_0)\alpha$ has a minimal polynomial over $\mathbb{Z}$
$\Rightarrow(q_{n-1}\cdots q_0)\alpha\in\overline{\mathbb{Z}}$.

Date / /

(c) Proof: $\alpha \in \overline{\mathbb{Z}} \Leftrightarrow \alpha$ has a minimal polynomial over $\mathbb{Z}$ (which is the same in $\mathbb{Q}$)

$\Leftrightarrow \alpha \in \overline{\mathbb{Q}}$ and the minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$

(d) Proof: 0 has a finitely generated invariant submodule $\mathbb{Z} \neq \{0\} \Rightarrow 0 \in \overline{\mathbb{Z}}$

1 has a finitely generated invariant submodule $\mathbb{Z} \neq \{0\} \Rightarrow 1 \in \overline{\mathbb{Z}}$

$\alpha \in \overline{\mathbb{Z}} \Rightarrow \alpha$ has a finitely generated invariant submodule $M \neq \{0\}$

$\Rightarrow -\alpha$ has a finitely generated invariant submodule $M \neq \{0\}$

$\Rightarrow -\alpha \in \overline{\mathbb{Z}}$

$\alpha, \beta \in \overline{\mathbb{Z}} \Rightarrow \alpha, \beta$ have finitely generated invariant submodules $M, N \neq \{0\}$

$\Rightarrow \alpha + \beta$ has a finitely generated invariant submodule $MN \neq \{0\}$

$\Rightarrow \alpha + \beta \in \overline{\mathbb{Z}}$

$\alpha\beta \in \overline{\mathbb{Z}} \Rightarrow \alpha, \beta$ have finitely generated invariant submodules $M, N \neq \{0\}$

$\Rightarrow \alpha\beta$ has a finitely generated invariant submodule $MN \neq \{0\}$

$\Rightarrow \alpha\beta \in \overline{\mathbb{Z}}$

(e) Proof: On one hand, $\alpha \in \overline{\mathbb{Q}} \Rightarrow \alpha = \frac{\beta}{n}$, where $\beta \in \overline{\mathbb{Z}}, n \in \mathbb{Z}_{\neq 0}$

$\Rightarrow \alpha = \frac{\beta}{n}$, where $\beta, n \in \overline{\mathbb{Z}}, n \neq 0 \Rightarrow \alpha \in \mathrm{Frac}\,\overline{\mathbb{Z}}$

On the other hand, $\alpha \in \overline{\mathbb{Q}}$ and $\alpha \neq 0$

$\Rightarrow \alpha$ has a finite-dimensional invariant subspace $V \neq \{0\}$.

$\Rightarrow \frac{1}{\alpha}$ has a finite-dimensional invariant subspace $V \neq \{0\}$,

because an invertible matrix A in $\mathbb{Q}$ has rational inverse $\frac{\mathrm{adj}A}{\det A}$

$\Rightarrow \frac{1}{\alpha} \in \overline{\mathbb{Q}}$, by minimality, $\overline{\mathbb{Q}} = \mathrm{Frac}\,\overline{\mathbb{Z}}$.

Date / / 25.

Date / /

(3)(a) Proof: $\alpha = e^{\frac{2\pi i}{n}} \Rightarrow \alpha - e^{\frac{2\pi i}{n}} = 0$

$\Rightarrow \alpha^2 - 2\alpha\cos\frac{2\pi}{n} + 1 = (\alpha - e^{\frac{2\pi i}{n}})(\alpha - e^{-\frac{2\pi i}{n}}) = 0$

(b) Proof: $\frac{2\pi}{n}$ is constructable $\Rightarrow e^{\frac{2\pi i}{n}}$ is constructable

$\Rightarrow$ The field extension $\mathbb{Q}[e^{\frac{2\pi i}{n}}]/\mathbb{Q}$ is obtained by a tower of degree 2 extensions

$\Rightarrow \exists k \geq 0, \varphi(n) = [\mathbb{Q}[e^{\frac{2\pi i}{n}}] : \mathbb{Q}] = 2^k$

(4)(1) Let's prove some general facts on cubic polynomials.

Proposition 1: The splitting field K of an irreducible polynomial $f(x) = x^3 - 3MNx - M^3 - N^3$ over $\mathbb{Q}$ is generated by one root α_1 and the discriminant $\sqrt{\Delta} = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$.

Proof 1: It suffices to express α_2, α_3 in terms of $\alpha_1, \sqrt{\Delta}$, MN and $M^3 + N^3$.

$$x^3 - 3MNx - M^3 - N^3 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \alpha_1\alpha_2\alpha_3 = M^3 + N^3, \quad \alpha_2 + \alpha_3 = -\alpha_1$$

$$\alpha_1\sqrt{\Delta} = \alpha_1(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$$

$$= [\alpha_1\alpha_2\alpha_3 - \alpha_1^2(\alpha_2 + \alpha_3) + \alpha_1^3](\alpha_3 - \alpha_2)$$

$$= (2\alpha_1^3 + M^3 + N^3)(\alpha_3 - \alpha_2)$$

$$\alpha_3 - \alpha_2 = \frac{\alpha_1\sqrt{\Delta}}{2\alpha_1^3 + M^3 + N^3},$$

$$\alpha_2 = \frac{1}{2}\left[-\alpha_1 - \frac{\alpha_1\sqrt{\Delta}}{2\alpha_1^3 + M^3 + N^3}\right] \in \mathbb{Q}[\alpha_1, \sqrt{\Delta}] \subseteq \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = K$$

$$\alpha_3 = \frac{1}{2}\left[-\alpha_1 + \frac{\alpha_1\sqrt{\Delta}}{2\alpha_1^3 + M^3 + N^3}\right] \in \mathbb{Q}[\alpha_1, \sqrt{\Delta}] \subseteq \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = K.$$

Proposition 2: If $\sqrt{\Delta} = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \in \mathbb{Q}$, then $\mathrm{Gal}(K/\mathbb{Q}) = \{e, (\alpha_1, \alpha_2, \alpha_3), (\alpha_3, \alpha_2, \alpha_1)\}$, where $K = \mathbb{Q}[\alpha_1]$ is the splitting field of $f(x) = x^3 - 3MNx - M^3 - N^3$ over $\mathbb{Q}$.

Date / /

Proof 2: On one hand, $\mathbb{Q}[t_1] \to \mathbb{Q}[t_2]$, $g(t_1) \mapsto g(t_2)$ is a ring isomorphism fixing $\mathbb{Q}$.

Hence, $\mathbb{Q}[t_1]/\langle t_1^3 - 3MNt_1 - M^3 - N^3 \rangle \to \mathbb{Q}[t_2]/\langle t_2^3 - 3MNt_2 - M^3 - N^3 \rangle$,

$\| \qquad\qquad\qquad\qquad\qquad\qquad \|$

$\mathbb{Q}[\alpha_1] \cong K \cong \mathbb{Q}[\alpha_2]$

$g(\alpha_1) \mapsto g(\alpha_2)$

is a field isomorphism fixing $\mathbb{Q}$.

This means $(\alpha_1, \alpha_2, \alpha_3) \in Gal(K/\mathbb{Q})$, so $\{e, (\alpha_1,\alpha_2,\alpha_3), (\alpha_3,\alpha_2,\alpha_1)\} \subseteq Gal(K/\mathbb{Q})$

On the other hand every $\sigma \in Gal(K/\mathbb{Q})$ restricts to a permutation of $\{\alpha_1, \alpha_2, \alpha_3\}$. As transpositions (α_2, α_1), (α_1, α_3), (α_2, α_3) fails to fix the rational number $\sqrt{\Delta} = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$, they don't belong to $Gal(K/\mathbb{Q})$, so $Gal(K/\mathbb{Q}) = \{e, (\alpha_1,\alpha_2,\alpha_3), (\alpha_3,\alpha_2,\alpha_1)\}$.

Proposition 3: If $\sqrt{\Delta} = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \notin \mathbb{Q}$, then $Gal(K/\mathbb{Q}) = \{e, (\alpha_1,\alpha_2,\alpha_3), (\alpha_3,\alpha_2,\alpha_1), (\alpha_1,\alpha_2), (\alpha_2,\alpha_3), (\alpha_1,\alpha_3)\}$, where $K = \mathbb{Q}[\alpha_1, \sqrt{\Delta}]$ is the splitting field of $f(x) = x^3 - 3MNx - M^3 - N^3$ over $\mathbb{Q}$.

Proof 3: On one hand, $(\mathbb{Q}[\sqrt{\Delta}])[t_1] \to (\mathbb{Q}[\sqrt{\Delta}])[t_2]$, $g(t_1) \mapsto g(t_2)$ is a ring isomorphism fixing $\mathbb{Q}[\sqrt{\Delta}]$, thus fixing $\mathbb{Q}$.

Hence, $(\mathbb{Q}[\sqrt{\Delta}])[t_1]/\langle t_1^3 - 3MNt_1 - M^3 - N^3 \rangle \to (\mathbb{Q}[\sqrt{\Delta}])[t_2]/\langle t_2^3 - 3MNt_2 - M^3 - N^3 \rangle$

$\| \qquad\qquad\qquad\qquad\qquad\qquad \|$

$\mathbb{Q}[\alpha_1, \sqrt{\Delta}] \cong K \cong \mathbb{Q}[\alpha_2, \sqrt{\Delta}]$

$g(\alpha_1) \mapsto g(\alpha_2)$

is a field isomorphism fixing $\mathbb{Q}$.

This means $(\alpha_1, \alpha_2, \alpha_3) \in Gal(K/\mathbb{Q})$, so $\{e, (\alpha_1,\alpha_2,\alpha_3), (\alpha_3,\alpha_2,\alpha_1)\} \subseteq Gal(K/\mathbb{Q})$.

Date / /

On the other hand, $(\mathbb{Q}[x_1])[d] \to (\mathbb{Q}[x])[d]$, $g(d) \mapsto g(-d)$ is a ring isomorphism fixing $\mathbb{Q}[x_1]$, thus fixing $\mathbb{Q}$. Hence, $(\mathbb{Q}[x_1])[d]/\langle d^2-\Delta\rangle \to (\mathbb{Q}[x_1])[d]/\langle d^2-\Delta\rangle$

$\| \qquad\qquad \|$

$\mathbb{Q}[x_1,\sqrt{\Delta}] \cong K \cong \mathbb{Q}[x_1,\sqrt{\Delta}]$

$g(\sqrt{\Delta}) \mapsto g(-\sqrt{\Delta})$

is a field isomorphism fixing $\mathbb{Q}$.

This means $(x_2 x_3) \in Gal(K/\mathbb{Q})$, so $\{(x_1x_2),(x_1x_3),(x_2x_3)\} \subseteq Gal(K/\mathbb{Q})$.

As $Gal(K/\mathbb{Q}) \subseteq \{e,(x_1x_2x_3),(x_3x_2x_1),(x_1x_2),(x_1x_3),(x_2x_3)\}$

and $Gal(K/\mathbb{Q}) \supseteq \{e,(x_1x_2x_3),(x_3x_2x_1),(x_1x_2),(x_1x_3),(x_2x_3)\}$,

it follows that $Gal(K/\mathbb{Q}) = \{e,(x_1x_2x_3),(x_3x_2x_1),(x_1x_2),(x_1x_3),(x_2x_3)\}$.

no blank no blank

https://planetmath.org/galois group of a cubic polynomial

For the purpose of evaluating $[K_f:\mathbb{Q}]$, where $f(x)=x^3-2$,

~~First, take a prime $p=2$, $p\nmid 1$, $p\mid 2$, $p^2\mid 2$, so $f(x)$ is irreducible over $\mathbb{Z}$ and $\mathbb{Q}$.~~

Second, $x_1=\sqrt[3]{2}$, $x_2=\omega\sqrt[3]{2}$, $x_3=\omega^2\sqrt[3]{2}$, $\sqrt{\Delta}=(x_2-x_1)(x_3-x_1)(x_3-x_2)=-\omega\sqrt{3}i\notin\mathbb{Q}$

Hence, $[K_f:\mathbb{Q}]=6$, $Gal(K_f/\mathbb{Q})=\{e,(\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}),(\omega^2\sqrt[3]{2},\omega\sqrt[3]{2},\sqrt[3]{2}),(\sqrt[3]{2},\omega^2\sqrt[3]{2}),(\sqrt[3]{2},\omega\sqrt[3]{2}),(\omega\sqrt[3]{2},\omega^2\sqrt[3]{2})\}$

(2) $f(x)=x^4-1=(x+1)(x-1)(x^2+1)$.

The splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}[\sqrt{-1}]$, where:

$[\mathbb{Q}[\sqrt{-1}]:\mathbb{Q}]=2$, $Gal(\mathbb{Q}[\sqrt{-1}]/\mathbb{Q})=\{e,(\sqrt{-1},-\sqrt{-1})\}$.

Date / /

(3) $f(x)=(x^2-2)(x^3-2)$

The splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}[\sqrt[6]{2}, \omega]$.

$[\mathbb{Q}[\sqrt[6]{2}, \omega]:\mathbb{Q}] = [\mathbb{Q}[\sqrt[6]{2}, \omega]:\mathbb{Q}[\sqrt[6]{2}]][\mathbb{Q}[\sqrt[6]{2}]:\mathbb{Q}] = 2 \cdot 6 = 12.$

(5) Solution: The splitting field L of $f(x)=x^7-1$ over $\mathbb{Q}$ is $\mathbb{Q}[\zeta]$, where $\zeta = e^{\frac{2\pi i}{7}}$.

$\zeta, \zeta^2, \zeta^3, \cdots, \zeta^6$ is a basis of L over $\mathbb{Q}$, $[L:\mathbb{Q}]=6$.

(6) Solution: Note that $f(x)=(x-1)^7$ already splits over $\mathbb{F}_7$,

so $M=\mathbb{F}_7$, $[M:\mathbb{F}_7]=1$.