

TEORIA DE GALOIS. CURS 1999/2000. PRÀCTICA 4.
SOLUCIONS.

1. Calcula el cos de descomposició L , el grup de Galois G i els cossos intermedis de la extensió $L/\mathbb{Q}$ per a cadascun dels següents polinomis:

$$f_1(X) = X^3 + 5, \quad f_2(X) = X^3 + X^2 + X + 1, \quad f_3(X) = X^4 + 1, \quad f_4(X) = X^4 - 4.$$

Solució

$f_1(X) = X^3 + 5$

Pas 1:

Trobem primer les arrels de $X^3 + 5$: són

$$\sqrt[3]{-5}, \quad \xi \sqrt[3]{-5}, \quad \xi^2 \sqrt[3]{-5}$$

on ξ és una arrel cúbica de 1 primitiva, per exemple $\xi := \frac{1+\sqrt{-3}}{2}$. Observem que $\sqrt[3]{-5} = -\sqrt[3]{5}$

Pas 2:

Calculem el cos de descomposició i el seu grau sobre $\mathbb{Q}$: Si denotem per E el cos de descomposició, aleshores

$$E = \mathbb{Q}(\sqrt[3]{-5}, \xi \sqrt[3]{-5}, \xi^2 \sqrt[3]{-5}) = \mathbb{Q}(\sqrt[3]{5}, \xi) = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-3})$$

Ara, per a calcular el grau tenim que

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$$

Com que $X^3 - 5$ és irreductible pel criteri d'Eisenstein (amb $p = 5$), tenim que $\text{Irr}(\sqrt[3]{5}, \mathbb{Q}) = X^3 - 5$ i per tant

$$[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = \text{grau}(\text{Irr}(\sqrt[3]{5}, \mathbb{Q})) = 3.$$

Ara, com que $\mathbb{Q}(\sqrt[3]{5})$ està contingut als nombres reals, no conté cap element tal que elevat al quadrat doni -3 , i per tant

$$\text{Irr}(\sqrt{-3}, \mathbb{Q}(\sqrt[3]{5})) = X^2 + 3.$$

Així $[E : \mathbb{Q}(\sqrt[3]{5})] = 2$ i per tant $[E : \mathbb{Q}] = 6$.

Pas 3:

Calculem ara el grup de Galois de $E/\mathbb{Q}$, $G := \text{Gal}(E/\mathbb{Q})$.

Observem primer que el grup de Galois de $E/\mathbb{Q}(\sqrt[3]{5})$ és isomorf a $\mathbb{Z}/2\mathbb{Z}$ i conté un element τ que envia $\sqrt{-3}$ a $-\sqrt{-3}$. Així tenim un element τ a G que actua via

$$\tau(\sqrt{-3}) = -\sqrt{-3} \quad \text{i} \quad \tau(\sqrt[3]{5}) = \sqrt[3]{5}.$$

Prenem ara l'extensió $E/\mathbb{Q}(\sqrt{-3})$; és simple, de grau 3, i tenim un element σ que ens porta $\sigma(\sqrt[3]{5}) = \xi \sqrt[3]{5}$. Així obtenim un element σ a G que actua via

$$\sigma(\sqrt{-3}) = \sqrt{-3} \quad \text{i} \quad \sigma(\sqrt[3]{5}) = \xi \sqrt[3]{5}.$$

És clar que $\tau^2 = id$ i que $\sigma^3 = id$. Podem construir així els elements de G següents: $\{id, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. Són tots ells diferents doncs actuen de manera diferent sobre $\sqrt{-3}$ i sobre $\sqrt[3]{5}$. Com que $\#G = [E : \mathbb{Q}] = 6$ i tenim 6 elements, ja els tenim tots.

Observem que $\sigma\tau = \tau\sigma^2$, per tant G no és abelià, i per tant és S_3 .

També podríem haver dit que G és un subgrup de S_3 doncs és el grup de Galois d'un polinomi de grau 3, i com que té 6 elements ha de ser tot S_3 .

Pas 4:

Calculem tots els subgrups de S_3 ; només hi ha el total i els generats per un sol element, doncs si tenim un subgrup de S_3 ha de tenir ordre divisor de 6, i per tant sols pot ser d'ordre 1, 2, 3 o 6. Si és d'ordre 1, 2 o 3, aleshores és cíclic (com a grup), i per tant generat per un sol element. Si és d'ordre 6, és el total.

Amb la notació introduïda al pas 3, tenim per tant els subgrups

$$\{id\}, \langle \sigma \rangle, \langle \tau \rangle, \langle \tau\sigma \rangle, \langle \tau\sigma^2 \rangle, G.$$

Pas 5:

Calculeu ara els cossos fixes per els diferents subgrup per a tenir tots els cossos intermedis. Trivialment

$$E^{\{id\}} = E, \quad E^G = \mathbb{Q}.$$

Ara, el cos fix per τ : tenim que τ deixa fixe $\sqrt[3]{5}$, per tant $\sqrt[3]{5} \in E^{\langle \tau \rangle}$. Però $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ i $[E^{\langle \tau \rangle} : \mathbb{Q}] = \#G/\#\langle \tau \rangle = 6/2 = 3$. Per tant $E^{\langle \tau \rangle} = \mathbb{Q}(\sqrt[3]{5})$.

De la mateixa manera veiem el reste de cossos:

$$E^{\langle \tau \rangle} = \mathbb{Q}(\sqrt[3]{5}) \quad E^{\langle \tau\sigma \rangle} = \mathbb{Q}(\xi \sqrt[3]{5}) \quad E^{\langle \tau\sigma^2 \rangle} = \mathbb{Q}(\xi^2 \sqrt[3]{5}) \quad E^{\langle \sigma \rangle} = \mathbb{Q}(\sqrt{-3})$$

observant que, com que $\tau(\xi) = \xi^2$ i que $\sigma(\xi) = \xi$,

$$\tau\sigma(\xi \sqrt[3]{5}) = \tau\sigma(\xi)\tau\sigma(\sqrt[3]{5}) = \tau(\xi)\tau(\xi \sqrt[3]{5}) = \tau(\xi)^2 \sqrt[3]{5} = \xi^4 \sqrt[3]{5} = \xi \sqrt[3]{5}.$$

$$\boxed{f_2(X) = X^3 + X^2 + X + 1}$$

Observem que $X^3 + X^2 + X + 1$ té com a arrel -1. Dividint $f_2(X)$ per $X + 1$ obtenim el polinomi $X^2 + 1$. Les seves arrels són i i $-i$. El cos de descomposició és $\mathbb{Q}(i)$; té grau 2 sobre $\mathbb{Q}$. El grup de Galois té ordre 2 i per tant és isomorf a $\mathbb{Z}/2\mathbb{Z}$. Els únics cossos intermedis són $\mathbb{Q}(i)$ i $\mathbb{Q}$.

$$\boxed{f_3(X) = X^4 + 1}$$

Pas 1:

Troben primer les arrels de $X^4 + 1$: Observem que $X^8 - 1 = (X^4 - 1)(X^4 + 1)$; així les arrels de $f_3(X)$ són arrels vuitenes de la unitat, i, si denotem per $\xi := e^{2\pi i/8} = e^{\pi i/4}$, tenim les arrels

$$\xi := \frac{\sqrt{2} + \sqrt{2}i}{2}, \xi^3, \xi^5, \xi^7.$$

Pas 2:

Calculem el cos de descomposició i el seu grau sobre $\mathbb{Q}$: Si denotem per E el cos de descomposició, aleshores $E = \mathbb{Q}(\xi)$. Ara, per a calcular el grau observem que

$$\text{Irr}(\xi, \mathbb{Q}) = X^4 + 1$$

per ser $X^4 + 1$ irreductible: no té arrels a $\mathbb{Q}$ i si fos producte de dos polinomis de grau 2 sobre $\mathbb{Q}$, aleshores un dels polinomis hauria de ser igual a

$$(X - \xi)(X - \xi^j) = X^2 - (\xi + \xi^j)X + \xi\xi^j$$

per a $j = 3, 5$ o 7 . Però

$$\xi + \xi^3 = \frac{\sqrt{2} + \sqrt{2}i}{2} + \frac{-\sqrt{2} + \sqrt{2}i}{2} = \sqrt{2}i$$

i

$$\xi + \xi^7 = \sqrt{2},$$

que no són de $\mathbb{Q}$, així que sols podria ser $i = 5$, i $\xi\xi^5 = \xi^6 = -i$ que tampoc és de $\mathbb{Q}$.

Tenim per tant que $[E : \mathbb{Q}] = \text{grau}(X^4 + 1) = 4$.

Pas 3:

Calculem ara el grup de Galois de $E/\mathbb{Q}$, $G := \text{Gal}(E/\mathbb{Q})$. Com que $[E : \mathbb{Q}] = 4$ i és simple generada per ξ , tenim 4 automorfismes, concretament donats per $\sigma_i(\xi) = \xi^{2i-1}$, de manera que $\sigma_1 = \text{id}$.

Calculem l'ordre de σ_2 :

$$\sigma_2^2(\xi) = \sigma_2(\xi^3) = \sigma_2(\xi)^3 = (\xi^3)^3 = \xi^9 = \xi.$$

El de σ_3 :

$$\sigma_3^2(\xi) = \sigma_3(\xi^5) = \sigma_3(\xi)^5 = (\xi^5)^5 = \xi^{25} = \xi.$$

i el de σ_4 :

$$\sigma_4^2(\xi) = \sigma_4(\xi^7) = \sigma_4(\xi)^7 = (\xi^7)^7 = \xi^{49} = \xi.$$

Tots tenen ordre 2 i per tant $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Pas 4:

Calculem tots els subgrups de G ; només hi ha el total i els generats per un sol element, i tenim així com a subgrups

$$\{\text{id}\}, \langle \sigma_2 \rangle, \langle \sigma_3 \rangle, \langle \sigma_4 \rangle, G.$$

Pas 5:

Calculeu ara els cossos fixes per els diferents subgrup per a tenir tots els cossos intermedis. Trivialment

$$E^{\{\text{id}\}} = E, \quad E^G = \mathbb{Q}.$$

Per a calcular el cos fix per σ_2 , observem que

$$\sigma_2(\xi) = \xi^3, \quad \sigma_2(\xi^3) = \xi, \quad \sigma_2(\xi^5) = \xi^7, \quad \sigma_2(\xi^7) = \xi^5$$

Per tant σ_2 deixa fix $\xi + \xi^3$ i $\xi^5 + \xi^7$. Abans em calculat que $\xi + \xi^3 = \sqrt{2}i$, d'on $\sqrt{2}i \in E^{(\sigma_2)}$. Però $[\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}] = 2$ i $[E^{(\sigma_2)} : \mathbb{Q}] = \#G/\#\langle\sigma_2\rangle = 4/2 = 2$. Per tant $E^{(\sigma_2)} = \mathbb{Q}(\sqrt{2}i)$.

De la mateixa manera, σ_4 deixa fix $\xi + \xi^7 = \sqrt{2}$, i per tant $E^{(\sigma_4)} = \mathbb{Q}(\sqrt{2})$.

Finalment, σ_3 deixa fix $\xi\xi^5 = \xi^6 = -i$, i per tant $E^{(\sigma_3)} = \mathbb{Q}(i)$.

$$\boxed{f_1(X) = X^4 - 4}$$

Pas 1:

Calculem les arrels de $X^4 - 4$: Són

$$\sqrt[4]{4}, i\sqrt[4]{4}, -\sqrt[4]{4}, -i\sqrt[4]{4}$$

(doncs i és una arrel quarta de 1, primitiva). Però $\sqrt[4]{4} = \sqrt{2}$, i per tant les arrels de $X^4 + 4$ són:

$$\sqrt{2}, -\sqrt{2}, i\sqrt{2}, -i\sqrt{2}.$$

Pas 2:

Calculem el cos de descomposició i el seu grau sobre $\mathbb{Q}$: Si denotem per E el cos de descomposició, aleshores $E = \mathbb{Q}(\sqrt{2}, i)$. Per tant tenim que

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

ja que $i \notin \mathbb{Q}(\sqrt{2})$, d'on $\text{Irr}(i, \mathbb{Q}(\sqrt{2})) = X^2 + 1$.

Pas 3:

Calculem ara el grup de Galois de $E/\mathbb{Q}$, $G := \text{Gal}(E/\mathbb{Q})$.

Observem primer que el grup de Galois de $E/\mathbb{Q}(\sqrt{2})$ és isomorf a $\mathbb{Z}/2\mathbb{Z}$ i conté un element τ que envia i a $-i$. Així tenim un element τ a G que actua via

$$\tau(i) = -i \quad \text{i} \quad \tau(\sqrt{2}) = \sqrt{2}.$$

Prenem ara l'extensió $E/\mathbb{Q}(i)$; és simple, de grau 2, i tenim un element σ que ens porta $\sigma(\sqrt{2}) = -\sqrt{2}$. Així obtenim un element σ a G que actua via

$$\sigma(i) = i \quad \text{i} \quad \sigma(\sqrt{2}) = -\sqrt{2}.$$

És clar que $\tau^2 = \text{id}$ i que $\sigma^2 = \text{id}$. Tenim per tant dos elements d'ordre 2, i el grup G té 4 elements, d'on $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Pas 4:

Calculem tots els subgrups de G ; només hi ha el total i els generats per un sol element, i tenim així com a subgrups

$$\{id\}, \langle\sigma\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle, G.$$

Pas 5:

Calculeu ara els cossos fixes per els diferents subgrup per a tenir tots els cossos intermedis. Trivialment

$$E^{\{id\}} = E, \quad E^G = \mathbb{Q}.$$

Els altres cossos estan també clars: com que τ deixa invariant $\sqrt{2}$, utilitzant l'argument dels graus anterior tenim que $E^{\langle \tau \rangle} = \mathbb{Q}(\sqrt{2})$. De la mateixa manera es prova que

$$E^{\langle \tau \rangle} = \mathbb{Q}(\sqrt{2}), \quad E^{\langle \sigma \tau \rangle} = \mathbb{Q}(i\sqrt{2}), \quad E^{\langle \sigma \rangle} = \mathbb{Q}(i).$$

2. Sigui p i q dos nombres primers diferents, $p(X) = (X^2 - p)(X^2 - q)$ i E el cos de descomposició de $p(X)$ sobre $\mathbb{Q}$. Calculeu el grup de Galois de $E/\mathbb{Q}$ i tots els cossos intermedis.

Solució

És clar que el cos de descomposició és $E = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. El seu grau sobre $\mathbb{Q}$ és 4 doncs $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. En efecte, si $(a + b\sqrt{p})^2 = q$ per a certs a, b de $\mathbb{Q}$, aleshores $q = (a + b\sqrt{p})^2 = a^2 + pb^2 + 2ab\sqrt{p}$, d'on tenim que, com que 1, $\sqrt{p}$ són linealment independents sobre $\mathbb{Q}$,

$$a^2 + pb^2 = q \quad \text{i} \quad 2ab = 0.$$

Si $a = 0$, aleshores $pb^2 = q$, i com que p i q són primers, tindríem que $p = q$, contradicció. Si $b = 0$, aleshores $a^2 = q$, i això no pot ser ja que $X^2 - q$ és irreductible sobre $\mathbb{Q}$ (criteri d'Eisenstein).

Per tant el grup de Galois G de E sobre $\mathbb{Q}$ té ordre 4, d'on és isomorf a $\mathbb{Z}/4\mathbb{Z}$ o bé a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Ara, E conté com a mínim dos cossos diferents de $\mathbb{Q}$: $\mathbb{Q}(\sqrt{p})$ i $\mathbb{Q}(\sqrt{q})$ (són diferents ja que $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$). Per tant el grup de Galois G de E sobre $\mathbb{Q}$ ha de contenir com a mínim 2 subgrups que no siguin ni el total ni el trivial. Per tant G no pot ser $\mathbb{Z}/4\mathbb{Z}$, i per tant és $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Així tenim 3 cossos intermedis no trivials; els dos que em dit abans i $\mathbb{Q}(\sqrt{pq})$.

3. Considereu el polinomi $f(X) = X^4 + 3X^2 + 9$.
- Proveu que $f(X)$ és irreductible sobre $\mathbb{Q}$ i calculeu el grau del seu cos de descomposició E sobre $\mathbb{Q}$.
 - Calculeu el grup de Galois de $E/\mathbb{Q}$.
 - Calculeu tots els cossos intermedis de $E/\mathbb{Q}$.
 - Calculeu el grup de Galois de $f(X)$ sobre $\mathbb{Q}(i)$.

Solució

- a) *Proveu que $f(X)$ és irreductible sobre $\mathbb{Q}$ i calculeu el grau del seu cos de descomposició E sobre $\mathbb{Q}$.*

Les arrels de $f(X)$ són les arrels quadrades de les solucions de $Y^2 + 3Y + 9$, o sigui

$$\pm \sqrt{\frac{-3 \pm 3\sqrt{-3}}{2}} = \pm \frac{\sqrt{3} \pm 3i}{2}.$$

Anomenarem $\beta = \frac{-3+3\sqrt{-3}}{2}$ i $\alpha = \sqrt{\frac{-3+3\sqrt{-3}}{2}}$ una arrel quadrada de β qualsevol (per exemple $\frac{\sqrt{3}+3i}{2}$).

Observem que, si $\bar{\beta} = \frac{-3-3\sqrt{-3}}{2}$ és el conjugat de β , aleshores $\sqrt{\beta}\sqrt{\bar{\beta}} = \pm\sqrt{9} = \pm 3$, per a qualsevol elecció de les arrels quadrades.

Ordenem ara les arrels de la manera següent:

$$\alpha_1 := \alpha, \alpha_2 := -\alpha, \alpha_3 := \bar{\alpha}, \alpha_4 := -\alpha_3$$

i tenim que $\alpha_1\alpha_3 = 3$.

Anem a veure que $f(X)$ és irreductible. És clar que $f(X)$ no té arrels a $\mathbb{Q}$, doncs de fet no té arrels a $\mathbb{R}$. Ara, si $f(X)$ factoritzes a $\mathbb{Q}$ com a producte de dos polinomis de grau 2, aleshores la factorització a $\mathbb{Q}$ hauria de ser la factorització a $\mathbb{R}$, o sigui

$$f(X) = p(X)q(X) \text{ on } p(X) = (X-\alpha_1)(X-\alpha_3) \text{ i } q(X) := (X-\alpha_2)(X-\alpha_4)$$

Ara,

$$(\alpha_1 + \alpha_3)^2 = \alpha_1^2 + \alpha_3^2 + 2\alpha_1\alpha_3 = \beta + \bar{\beta} + 6 = \frac{-3}{2} + \frac{-3}{2} + 6 = 3,$$

d'on $\alpha_1 + \alpha_3 = \pm\sqrt{3}$ i per tant $p(X)$ no té coeficients a $\mathbb{Q}$.

Tenim que el cos de descomposició de $f(X)$ sobre $\mathbb{Q}$ és $E = \mathbb{Q}(\alpha_1, \alpha_3)$, i aquest cos és de fet $\mathbb{Q}(\alpha_1)$ ja que $\alpha_3 = 3/\alpha_1$. Per tant

$$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \text{grau}(\text{lrr}(\alpha_1, \mathbb{Q})) = \text{grau}(f(X)) = 4$$

ja que $f(X)$ és irreductible sobre $\mathbb{Q}$.

- b) *Calculeu el grup de Galois de $E/\mathbb{Q}$.*

Tenim 4 elements naturals del grup de Galois G de $E/\mathbb{Q}$: els que ens porten α_1 a una arrel de $f(X)$. Anomenarem

$$\sigma_1(\alpha_1) = -\alpha_1, \sigma_2(\alpha_1) = \alpha_3, \sigma_3(\alpha_1) = -\alpha_3$$

Aleshores tenim que:

$$\sigma_1^2(\alpha_1) = \sigma_1(-\alpha_1) = \alpha_1,$$

i per tant $\sigma_1^2 = \text{id}$. També tenim que

$$\sigma_2^2(\alpha_1) = \sigma_2(\alpha_3) = \sigma_2(3/\alpha_1) = 3/\sigma_2(\alpha_1) = 3/\alpha_3 = \alpha_1$$

i per tant $\sigma_2^2 = \text{id}$. Igualment tenim que $\sigma_3^2 = \text{id}$. Així G és un grup amb 4 elements tal que tots els elements fora de l'identitat tenen ordre 2, i per tant és isomorf a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

c) Calculeu tots els cossos intermedis de $E/\mathbb{Q}$.

Els subgrups de G són:

$$\{id\}, G, \langle \sigma_1 \rangle, \langle \sigma_2 \rangle, \langle \sigma_3 \rangle$$

Calculem els cossos fixes per a cada subgrup. Tenim $E^{\{id\}} = E$ i $E^G = \mathbb{Q}$.

Per a calcular el cos fixe per σ_1 observem que $\sigma_1(\alpha_1) = -\alpha_1$, i per tant $\sigma_1(\alpha_1^2) = \alpha_1^2$. Com que $\alpha_1^2 = \beta$ i β és arrel del polinomi $X^2 + 3X + 9$ que és irreductible sobre $\mathbb{Q}$ (doncs no té arrels a $\mathbb{Q}$), tenim que β pertany al cos fixe per σ_1 i $\mathbb{Q}(\beta)$ té grau 2 sobre $\mathbb{Q}$, que és l'índex de $\langle \sigma_1 \rangle$ dins de G . Per tant

$$E^{\langle \sigma_1 \rangle} = \mathbb{Q}(\beta) = \mathbb{Q}(3i).$$

Per a calcular el cos fixe per σ_2 observem que $\sigma_2(\alpha_1) = \alpha_3$, i per tant $\sigma_2(\alpha_1 + \alpha_3) = \alpha_1 + \alpha_3 = \sqrt{3}$. Així $\sqrt{3}$ pertany al cos fixe per σ_2 i $\mathbb{Q}(\sqrt{3})$ té grau 2 sobre $\mathbb{Q}$, que és l'índex de $\langle \sigma_2 \rangle$ dins de G . Per tant

$$E^{\langle \sigma_2 \rangle} = \mathbb{Q}(\sqrt{3}).$$

Finalment tenim que $\sigma_1(\alpha_1) = -\alpha_3$, i per tant $\sigma_3(\alpha_1 - \alpha_3) = \alpha_1 - \alpha_3 = 3i$. Així $3i$ pertany al cos fixe per σ_3 i $\mathbb{Q}(3i)$ té grau 2 sobre $\mathbb{Q}$, que és l'índex de $\langle \sigma_3 \rangle$ dins de G . Per tant

$$E^{\langle \sigma_3 \rangle} = \mathbb{Q}(i).$$

d) Calculeu el grup de Galois de $f(X)$ sobre $\mathbb{Q}(i)$.

Com que $\mathbb{Q}(i)$ és un dels cossos fixes que ens han aparegut a l'apartat anterior tenim que E conté a $\mathbb{Q}(i)$. Per tant el cos de descomposició de $f(X)$ sobre $\mathbb{Q}(i)$ és el propi E ; que té grau 2 sobre $\mathbb{Q}(i)$. Així el grup de Galois buscat té ordre 2 i per tant és isomorf a $\mathbb{Z}/2\mathbb{Z}$.

4. Sigui d un nombre enter diferent de 0 i ± 1 . Considereu el polinomi $f(X) = X^4 + X^2 + d^2$.

- Trobeu la condició que ha de verificar d per tal que $f(X)$ sigui irreductible. Calculeu el grau del cos de descomposició E de $f(X)$ sobre $\mathbb{Q}$.
- Calculeu el grup de Galois de l'extensió $E/\mathbb{Q}$.
- Trobeu tots els cossos intermedis de $E/\mathbb{Q}$.

Solució

a) Trobeu la condició que ha de verificar d per tal que $f(X)$ sigui irreductible. Calculeu el grau del cos de descomposició E de $f(X)$ sobre $\mathbb{Q}$.

Suposarem que d és un nombre positiu.

Calculem primer les arrels de $f(X)$: són les arrels quadrades dels zeros de $Y^2 + Y + d^2$, o sigui $\left\{ \frac{-1 \pm \sqrt{1-4d^2}}{2} \right\}$, que són dos nombres complexos conjugats que anomenarem β i $\bar{\beta}$.

Observem que $\beta\bar{\beta} = d^2$, d'on, si escollim α una arrel quadrada de beta, les arrels de $f(X)$ són: $\{\alpha, -\alpha, d/\alpha, -d/\alpha\}$. Tenim que el conjugat de α és d/α (doncs ha de ser una de les arrels i el seu producte ha de ser un nombre real positiu).

Si $f(X)$ no fos irreductible aleshores hauria de descomposar sobre $\mathbb{Q}$ com a producte de dos polinomis de grau 2, ja que no té arrels reals i per tant tampoc de racionals. Ara, per la mateixa raó la descomposició sobre $\mathbb{Q}$ hauria de ser la mateixa descomposició que la descomposició sobre $\mathbb{R}$. En resum, hauriem de tenir que $(X - \alpha)(X - d/\alpha)$ tingues coeficients racionals. Com que $\alpha d/\alpha = d$, una condició necessària i suficient és que $\alpha + d/\alpha$ sigui racional. Tenim que

$$(\alpha + d/\alpha)^2 = \alpha^2 + d^2/\alpha^2 + 2d = \beta + \bar{\beta} + 2d = 2d - 1,$$

d'on $f(X)$ és irreductible si i només si $2d - 1$ no és un quadrat.

Finalment calculem el grau: ja em vist que $E = \mathbb{Q}(\alpha)$, per tant $[E : \mathbb{Q}] = 4$ si $2d - 1$ no és un quadrat i $[E : \mathbb{Q}] = 2$ si $2d - 1$ és un quadrat.

b) *Calculeu el grup de Galois de l'extensió $E/\mathbb{Q}$.*

Si $2d - 1$ és un quadrat, aleshores $[E : \mathbb{Q}] = 2$ i $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Si $2d - 1$ no és un quadrat, tenim 4 elements al grup de Galois, enviant α a les arrels de $f(X)$. De la mateixa manera que en el problema 3 es té que els 4 morfismes naturals tenen ordre 2. Així el grup de Galois és $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

c) *Trobeu tots els cossos intermedis de $E/\mathbb{Q}$.*

El cas en que $f(X)$ no és irreductible és trivial. En l'altre cas tenim que hi ha tres cossos intermedis a part del total i el trivial, tots ells de grau 2 sobre $\mathbb{Q}$. Com que β és arrel d'un polinomi de grau 2 i β és complexa no real (i per tant no racional), tenim que un dels cossos és $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{1 - 4d^2})$.

Com que $\alpha + d/\alpha$ és igual a $\sqrt{2d - 1}$, i $2d - 1$ no és un quadrat, tenim que un altre dels cossos és $\mathbb{Q}(\sqrt{2d - 1})$. No és igual que el que ja teniem ja que aquest cos és real i l'altre no ho és. Finalment tenim el cos $\mathbb{Q}(\sqrt{-1 - 2d})$, que em obtingut a partir de $\sqrt{-1 - 2d} = \sqrt{1 - 4d^2}/\sqrt{2d - 1}$; d'aquesta expressió es fa veure que aquest cos no pot ser cap dels dos anteriors.