

Llicenciatura de Matemàtiques FME
Examen final d'Àlgebra Abstracta
15 de gener de 2008

Problema 1. Sigui P un p -grup i C un grup cíclic, i sigui $G = P \times C$ el grup producte cartesià. Demostreu que per a tot enter n que divideixi el nombre d'elements de G existeix un subgrup de G que té ordre n .

SOLUCIÓ: Tot p -grup és resoluble. Sigui

$$\{1\} = P_0 \subset P_1 \subset P_2 \subset \dots \subset P_r = P$$

una sèrie de composició. Aleshores els quocients P_i/P_{i-1} són cíclics d'ordre p (ja que són grups abelians simples d'ordre potència de p) i, per tant, cada grup P_i té ordre p^i , ja que $|P_0| = 1 = p^0$ i, per inducció sobre i ,

$$|P_i| = [P_i : P_{i-1}] \cdot |P_{i-1}| = p \cdot p^{i-1} = p^i.$$

Sigui m l'ordre del grup cíclic C . El producte cartesià G té ordre $|G| = |P| \cdot |C| = p^r m$. Tot divisor n d'aquest ordre és un producte de dos nombres que són divisors de p^r i de m , respectivament; sigui $n = p^i d$ amb $0 \leq i \leq r$ i $d \mid m$. Sigui $C_d \subseteq C$ un (l'únic) subgrup de C d'ordre d . El subgrup $P_i \subseteq P$ té ordre p^i . Aleshores el producte cartesià $P_i \times C_d$ és un subgrup de G d'ordre $p^i d = n$.

Problema 2. L'objectiu d'aquest problema és demostrar que \mathbb{C} és algebraicament tancat fent servir només el teorema de Bolzano sobre \mathbb{R} (tota funció contínua té almenys un zero entre dos punts on prengui valors de signes oposats).

(a) Demostreu que tota extensió finita no trivial de \mathbb{R} té grau parell.

(b) Demostreu que tota extensió finita de \mathbb{R} té grau potència de 2.

INDICACIÓ: Considereu la clausura normal i un 2-Sylow del seu grup de Galois.

(c) Demostreu que \mathbb{C} no té extensions finites de grau 2.

(d) Deduïu que \mathbb{C} és algebraicament tancat.

SOLUCIÓ:

(a) Si E/\mathbb{R} és finita no trivial sigui $\alpha \in E \setminus \mathbb{R}$. El polinomi irreductible $\text{Irr}(\alpha, \mathbb{R}; X)$ té grau parell ja que tot polinomi de $\mathbb{R}[X]$ de grau senar té alguna arrel, per Bolzano. Aleshores $\mathbb{R}(\alpha)$ és una subextensió de grau parell i, per tant, $[E : \mathbb{R}] = [E : \mathbb{R}(\alpha)][\mathbb{R}(\alpha) : \mathbb{R}]$ és parell.

(b) Sigui E/\mathbb{R} finita i sigui N/E la seva clausura normal, que és normal i per tant de Galois sobre \mathbb{R} . Sigui P un 2-subgrup de Sylow de $G = \text{Gal}(N/\mathbb{R})$. Sigui $F = N^P$. Aleshores N/F és una extensió de Galois de grau $|P|$ i N/\mathbb{R} és de Galois de grau $|G|$. Per tant, l'extensió F/\mathbb{R} té grau $|G|/|P|$, que és senar ja que l'ordre de P és la màxima potència de 2 que divideix $|G|$. Per l'apartat anterior, aquesta extensió ha de ser trivial, i es dedueix que $G = P$, de manera que $[N : \mathbb{R}]$ és una potència de 2. Com que E és una subextensió, el seu grau $[E : \mathbb{R}]$ divideix $[N : \mathbb{R}]$ i per tant també és potència de 2.

(c) Sigui $[E : \mathbb{C}] = 2$ i sigui $\alpha \in E \setminus \mathbb{C}$. Aleshores $\text{Irr}(\alpha, \mathbb{C}; X)$ és un polinomi de grau 2. Això és una contradicció amb el fet que tot polinomi de grau 2 sobre \mathbb{C} té alguna arrel complexa. En efecte, si $f(X) = X^2 + aX + b$, els nombres complexos $\frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$ en són arrels, i això ho són, de nombres complexos, perquè tot nombre complex té arrel quadrada. Noti's que el fet que tot nombre complex tingui arrel quadrada (i de la mateixa manera es veu que tot nombre

complex té arrel n -èsima per a cada $n \geq 1$) es dedueix novament del teorema de Bolzano. En efecte, escrivint el complex z en forma polar $z = \rho e^{2\pi i\theta}$, les seves arrels quadrades són $\pm\sqrt{z} = \pm\sqrt{\rho} e^{2\pi i(\theta/2)}$, i aquesta expressió requereix l'existència d'arrel quadrada real $\sqrt{\rho}$ del nombre real $\rho > 0$, el que es veu per exemple aplicant Bolzano a la funció contínua $f(x) = x^2 - \rho$.

- (d) Sigui $f(X) \in \mathbb{C}[X]$ un polinomi, i sigui E/\mathbb{C} un cos de descomposició¹. Suposi's que $E \neq \mathbb{C}$. Aleshores E/\mathbb{R} és una extensió finita que, per (b), té grau potència de 2. Com que $[E : \mathbb{R}] = [E : \mathbb{C}][\mathbb{C} : \mathbb{R}] = 2[E : \mathbb{C}]$ es dedueix que E/\mathbb{C} té grau una potència de 2 no trivial² i, per tant, $G = \text{Gal}(E/\mathbb{C})$ és un 2-grup (no trivial ja que s'està suposant $E \neq \mathbb{C}$). Tot 2-grup és resoluble. Sigui $G = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_r = G$ una sèrie de composició, que té quocients cíclics, necessàriament d'ordre 2, ja que aquest ordre és un divisor de $|G|$. El subgrup G_{r-1} té índex 2 a G i per tant l'extensió $E^{G_{r-1}}$ corresponent té grau 2 sobre \mathbb{C} , el que contradiu l'apartat (c). Per tant, ha de ser $E = \mathbb{C}$. Així, el cos de descomposició de tot polinomi és el propi \mathbb{C} i per tant \mathbb{C} és algebraicament tancat.

Problema 3. Siguin α i β els dos nombres reals positius definits per les expressions

$$\alpha = \sqrt{\frac{5 + \sqrt{21}}{2}}, \quad \beta = \sqrt{\frac{5 - \sqrt{21}}{2}}.$$

Fixeu-vos que $\alpha\beta = 1$. Sigui $E = \mathbb{Q}(\alpha)$. Sigui F el cos de descomposició del polinomi $X^4 - 3 \in \mathbb{Q}[X]$. Sigui $L = \mathbb{Q}(e^{2\pi i/84})$.

- (a) Calculeu el polinomi irreductible de α sobre \mathbb{Q} .
 (b) Demostreu que l'extensió E/\mathbb{Q} és un cos de descomposició de $\text{Irr}(\alpha, \mathbb{Q}; X)$.
 (c) Calculeu el grup de Galois de E/\mathbb{Q} i doneu el reticle de subcossos d'aquesta extensió.
 (d) Demostreu que $\sqrt{3}$ i $\sqrt{7}$ són elements de E .
 (e) Diguen quin és el grup de Galois de F i descriu el seu reticle de subcossos (no cal demostrar res: es va fer amb detall a classe).
 (f) Calculeu el grup de Galois de l'extensió EF/\mathbb{Q} composició de E i F .
 (g) Calculeu el grau $[EL : \mathbb{Q}]$ de l'extensió composició de E i L .
 NOTA: podeu fer servir que $\zeta_7 + \zeta_7^2 + \zeta_7^4 = \frac{1}{2}(-1 + \sqrt{-7})$, on $\zeta_7 = e^{2\pi i/7}$ (vist a classe).

SOLUCIÓ:

- (a) Es té

$$\alpha^2 = \frac{5 + \sqrt{21}}{2} \Rightarrow (2\alpha^2 - 5)^2 = 21,$$

i per tant α és arrel del polinomi $(2X^2 - 5)^2 - 21 = 4X^4 - 20X^2 + 4 = 4(X^4 - 5X^2 + 1)$. El polinomi $X^4 - 5X^2 + 1$ és irreductible³. En efecte, per Ruffini els únics candidats a arrels racionals són $X = \pm 1$, que no són arrels⁴, i per tant no té cap descomposició amb un factor

¹NO es pot argumentar amb una clausura algebraica de \mathbb{C} o \mathbb{R} ja que aquestes podrien a priori ser de grau infinit

²D'aquí NO es pot deduir directament que ha de tenir una subextensió de grau 2, ja que, en general, una extensió de grau n no té perquè tenir subextensions de tots els graus dividint n .

³Per veure-ho no es pot esgrimir Eisenstein, ja que el polinomi no és p -Eisenstein per cap primer p , NI tampoc funciona la reducció mòdul un primer ja que totes les reduccions descomponen; en particular $X^4 - 5X^2 + 1 \equiv (X^2 + 1)^2 \pmod{2}$ i $X^4 - 5X^2 + 1 \equiv (X^2 + 2)(X^2 + 3) \pmod{5}$

⁴El fet de no tenir arrels racionals NO és suficient per assegurar la irreductibilitat ja que podria descompondre en producte de dos factors de segon grau.

de grau 1. Si tingués una descomposició en producte amb dos factors de grau 2 seria

$$X^4 - 5X^2 + 1 = (X^2 + a_1X + b_1)(X^2 + a_2X + b_2) \Leftrightarrow \begin{cases} a_1 + a_2 = 0 \\ a_1a_2 + b_1 + b_2 = -5 \\ a_1b_2 + a_2b_1 = 0 \\ b_1b_2 = 1 \end{cases}$$

La primera equació equival a $a_2 = -a_1$ i substituint la tercera es converteix en $a_1(b_2 - b_1) = 0$; a les dues possibilitats de que un dels factors sigui zero corresponen els dos sistemes

$$\left. \begin{cases} b_1 + b_2 = -5 \\ b_1b_2 = 1 \end{cases} \right\} \Leftrightarrow b_i = \frac{5 \pm \sqrt{21}}{2}, \quad i \quad \left. \begin{cases} -a_1^2 + 2b_1 = -5 \\ b_1^2 = 1 \end{cases} \right\} \Leftrightarrow \begin{cases} b_1 = 1, a_1 = \pm\sqrt{3}, \\ b_1 = -1, a_1 = \pm\sqrt{7}. \end{cases}$$

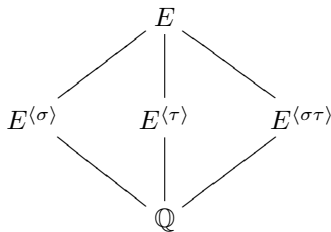
Així, la descomposició anterior no té solucions amb coeficients racionals i el polinomi $X^4 - 5X^2 + 1$ és irreductible sobre \mathbb{Q} .

Una altra manera d'acabar de comprovar que $X^4 - 5X^2 + 1$ és irreductible sobre \mathbb{Q} és utilitzar que les seves quatre arrels α_i són $\pm\alpha$ i $\pm\beta$ i veure que cap dels seus 6 factors $(X - \alpha_i)(X - \alpha_j)$ de grau 2, que es calculen fàcilment, té coeficients racionals.

Com que aquest polinomi és mònic i irreductible, és el polinomi $\text{Irr}(\alpha, \mathbb{Q}; X)$.

- (b) Amb la fórmula per les arrels d'un polinomi de segon grau es calculen les quatre arrels del polinomi biquadràtic $\text{Irr}(\alpha, \mathbb{Q}; X) = X^4 - 5X^2 + 1$, que resulten ser $\pm\alpha, \pm\beta$. Totes quatre són elements de $\mathbb{Q}(\alpha)$, ja que $-\alpha, \beta = \alpha^{-1}$ i $-\beta = -\alpha^{-1}$ pertanyen a aquest cos.
- (c) L'extensió E/\mathbb{Q} és de grau 4 i, gràcies a l'apartat anterior, és de Galois. El seu grup de Galois és un grup de 4 elements, que només pot ser el cíclic C_4 o bé isomorf a un producte $C_2 \times C_2$ de cíclics d'ordre 2. Donades dues arrels del polinomi $X^4 - 5X^2 + 1$ existeix algun \mathbb{Q} -automorfisme de E (que és el mateix que una immersió $E \hookrightarrow \overline{E}$) que envia l'una a l'altra. Per tant els quatre automorfismes queden determinats per l'arrel on envien α . La identitat deixa α fix. Sigui σ un automorfisme que envii α a β . Aleshores $\sigma\beta = \sigma\alpha^{-1} = \sigma\alpha^{-1} = \beta^{-1} = \alpha$. Per tant, σ és la permutació que intercanvia α amb β i $-\alpha$ amb $-\beta$. Sigui τ un automorfisme de E que envii α a $-\alpha$. És clar que τ intercanvia α amb $-\alpha$ i β amb $-\beta$. El producte $\sigma\tau$ intercanvia α amb $-\beta$ i β amb $-\alpha$. És clar que σ^2, τ^2 i $(\sigma\tau)^2$ són la identitat. Així, el grup de Galois $\text{Gal}(E/\mathbb{Q})$ és el grup $\{\text{Id}, \sigma, \tau, \sigma\tau\}$, que és isomorf a $C_2 \times C_2$ ja que tots els seus elements no trivials són d'ordre 2.

El grup $C_2 \times C_2$ té cinc subgrups: el trivial, d'ordre 1, tres subgrups d'ordre 2 generats per cadascun dels elements d'ordre 2, i el grup total d'ordre 4, als quals els corresponen les cinc subextensions de E/\mathbb{Q} que són, respectivament, $E^{\{\text{Id}\}} = E$, tres extensions $E^{(\sigma)}, E^{(\tau)}$ i $E^{(\sigma\tau)}$ que són de grau 2 (de Galois) sobre \mathbb{Q} i l'extensió $E^{\text{Gal}(E/\mathbb{Q})} = \mathbb{Q}$. El reticle és, doncs,



La determinació del grup de Galois es pot fer també de la manera explicada a classe per calcular el grup de Galois d'un polinomi de grau 4 amb la informació que proporcionen la resolvent cúbica i el discriminant. En aquest cas, tot i que a l'enunciat no es donen les fórmules perquè fer-ho directament és millor i ajuda a entendre els demés apartats del problema, és fàcil calcular les arrels de la resolvent cúbica $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, etc., que resulten ser els nombres racionals 5, 2 i -2 (tot i que no calen) i també el discriminant $\prod_{i < j} (\alpha_i - \alpha_j)^2 = \text{Res}(f, f')$, que és 84^2 , a partir de les expressions radicals que es tenen de les arrels α_i . Només sabent que el discriminant és un element de \mathbb{Q}^2 ja es dedueix que el grup de Galois, vist com a subgrup de les permutacions de les arrels, està contingut a l'alternat, i per tant és isomorf a $C_2 \times C_2$ i no a C_4 , que és l'únic que calia.

- (d) Per calcular quines són les tres extensions quadràtiques de \mathbb{Q} contingudes a E n'hi ha prou a trobar elements de E fixos pels grups corresponents. Per exemple, $\alpha^2 = \frac{1}{2}(5 + \sqrt{21})$ queda fix per τ , i, per tant, també queda fix $\sqrt{21}$. Així, $E^{(\tau)} = \mathbb{Q}(\sqrt{21})$.

L'element $\gamma = \alpha + \beta$ queda fix per σ ja que σ intercanvia els dos sumands. Elevant al quadrat es té

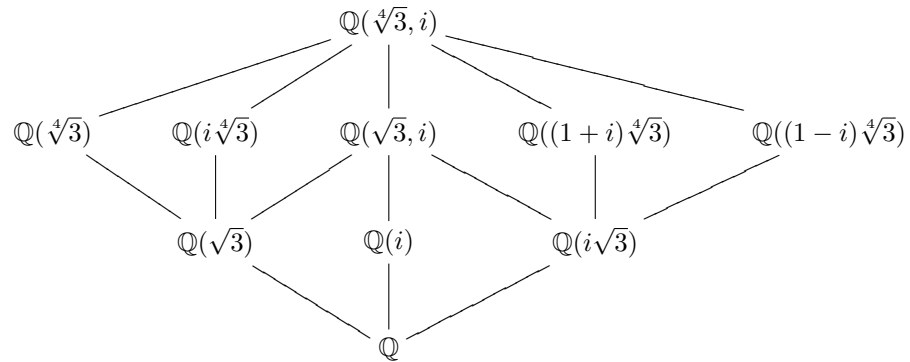
$$\gamma^2 = \frac{5 + \sqrt{21}}{2} + \frac{5 - \sqrt{21}}{2} + 2\alpha\beta = 5 + 2 = 7 \Rightarrow \gamma = \sqrt{7} \notin \mathbb{Q},$$

(arrel positiva ja que $\gamma > 0$) i, per tant, $E^{(\sigma)} = \mathbb{Q}(\sqrt{7})$.

Finalment, l'element $\delta = \alpha + (-\beta) = \alpha - \beta$ queda fix per $\sigma\tau$ i de la mateixa manera es veu que $\delta^2 = 3$. Per tant $E^{(\sigma\tau)} = \mathbb{Q}(\sqrt{3})$.

En particular, $\sqrt{7} = \alpha + \alpha^{-1}$ i $\sqrt{3} = \alpha - \alpha^{-1}$ són elements del cos E .

- (e) El grup de Galois del polinomi $X^4 - 3$ és el grup diedral D_8 de 8 elements, i a partir del seu reticle de subgrups es calcula el reticle de subextensions de F , que resulta ser



És a dir, F té, apart de la trivial i la total, tres subextensions quadràtiques, que s'obtenen adjuntant les arrels quadrades dels nombres 3, -1 i -3 , i cinc subextensions de grau 4. D'aquestes cinc, quatre no són normals i, en canvi, una, que és la composició de les tres quadràtiques, sí que ho és.

- (f) Com que $E = \mathbb{Q}(\sqrt{3}, \sqrt{7})$ es té $EF = F(\sqrt{3}, \sqrt{7})$, i com que $\sqrt{3} \in F$, això és el mateix que $F(\sqrt{7})$. Com que $\sqrt{7} \notin F$, ja que el cos F no conté $\mathbb{Q}(\sqrt{7})$ com a subcos (les tres subextensions quadràtiques de F s'han donat a l'apartat anterior i cap d'elles és aquesta), l'extensió $EF = F(\sqrt{7})$ és de grau 2 sobre F i, per tant, té grau 16 sobre \mathbb{Q} .

El cos EF es pot donar també com la composició de $\mathbb{Q}(\sqrt{7})$ amb F . El grup de Galois de la composició de dues extensions de Galois U i V d'un cos K és isomorf a un subgrup del producte cartesià dels grups de totes dues extensions, ja que l'aplicació $\sigma \mapsto (\sigma|_U, \sigma|_V)$ és un morfisme de grups injectiu $\text{Gal}(UV/K) \rightarrow \text{Gal}(U/K) \times \text{Gal}(V/K)$. Aplicat al el cas que ens ocupa, això implica que $\text{Gal}(EF/\mathbb{Q})$ és un grup d'ordre 16 isomorf a un subgrup del producte cartesià $\text{Gal}(\mathbb{Q}(\sqrt{7})/\mathbb{Q}) \times \text{Gal}(F/\mathbb{Q}) \simeq C_2 \times D_8$, i, com que aquest grup té ordre 16, ha de ser el total. Per tant, $\text{Gal}(EF/\mathbb{Q}) \simeq C_2 \times D_8$.

- (g) L'extensió ciclotòmica L està generada per una arrel primitiva de la unitat $\zeta_{84} = e^{2\pi i/84}$ d'ordre $84 = 4 \times 3 \times 7$. Per tant, conté arrels primitives quartes $\zeta_4 = \zeta_{84}^{21}$, cúbiques $\zeta_3 = \zeta_{84}^{28}$ i setenes $\zeta_7 = \zeta_{84}^{12}$. Com que $\zeta_4 = i = \sqrt{-1}$ i $\zeta_3 = \frac{1}{2}(-1 + \sqrt{-3})$, i fent servir la indicació, es té que $\sqrt{-1}, \sqrt{-3}, \sqrt{-7} \in L$. Multiplicant es dedueix que $\sqrt{3}, \sqrt{7} \in L$. Per tant, $E \subseteq L$, de manera que $EL = L$ i el que es demana és simplement el grau de l'extensió L sobre \mathbb{Q} . El grup de Galois de l'extensió ciclotòmica n -èsima $\mathbb{Q}(e^{2\pi i/n})$ és isomorf al grup multiplicatiu $(\mathbb{Z}/n\mathbb{Z})^*$, d'ordre l'indicador d'Euler $\varphi(n)$. Per tant,

$$[L : \mathbb{Q}] = \varphi(84) = \varphi(2^2 \cdot 3 \cdot 7) = 2 \cdot 2 \cdot 6 = 24.$$