Facultat de Matemàtiques i Estadística
Examen extraordinari d'Estructures Algebraiques
30 de juny de 2015

Trieu quatre dels cinc problemes següents. Tots puntuen igual.

Problema 1. Definiu domini euclidià i domini d'ideals principals, i demostreu que tot domini euclidià és un domini d'ideals principals.

Problema 2. Sigui $G = \mathrm{GL}_2(\mathbb{Q}) \subset \mathrm{GL}_2(\mathbb{C})$ el grup de les matrius invertibles 2×2 a coeficients racionals.

1. Demostreu que, en qualsevol grup, dos elements conjugats tenen el mateix ordre.
2. Demostreu que una matriu $\gamma \in \mathrm{GL}_2(\mathbb{C})$ té ordre finit en aquest grup si, i només si, diagonalitza i els seus valors propis són arrels de la unitat. Doneu l'ordre de γ en funció dels ordres dels seus valors propis.
   Indicació: Quan no diagonalitza considereu la seva forma de Jordan.
3. Trobeu tots els polinomis ciclotòmics $\Phi_n(X)$ de graus 1 o 2.
4. Sigui $\gamma \in G$. Demostreu que si $\mathrm{ord}(\gamma) = n$ és finit, aleshores $n = 1, 2, 3, 4$ o 6.
5. Per a aquests valors $n = 1, 2, 3, 4$ i 6 doneu un element de G que tingui ordre n.

Solució:

1. Siguin $a, b \in G$ amb $b = xax^{-1}$ per a un $x \in G$. Per a tot enter $n \geqslant 1$ es té $a^n = 1 \Leftrightarrow b^n = 1$, ja que $b^n = xa^nx^{-1}$. Per tant el mínim n tal que $a^n = 1$ és el mateix que el mínim n tal que $b^n = 1$.

2. Si $\gamma \in \mathrm{GL}_2(\mathbb{C})$ diagonalitza i els seus valors propis són arrels de la unitat γ és conjugada de la matriu $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$, amb λ i μ arrels de la unitat. Si $\lambda^n = 1$ i $\mu^m = 1$ aleshores $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)^{nm} = \boldsymbol{I}_2$. Per tant, $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ té ordre finit i la seva conjugada γ també.

   Recíprocament, suposi's que la matriu té ordre finit n. Si no diagonalitzés la seva forma de Jordan seria $J = \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$ i també tindria ordre n. Però $J^n = \left(\begin{smallmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{smallmatrix}\right) \neq \boldsymbol{I}_2$ per a tot $n \geqslant 1$ ja que si $\lambda^n = 1$ aleshores $\lambda \neq 0$ i també $n\lambda^{n-1} \neq 0$. Per tant, la matriu diagonalitza. Sigui $D = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ la matriu diagonal conjugada corresponent, que també té ordre n. Aleshores $\lambda^n = \mu^n = 1$ i els valors propis λ i μ són arrels de la unitat.

   Si $D = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ és la conjugada diagonal, $\gamma^n = \boldsymbol{I}_2 \Leftrightarrow D^n = \boldsymbol{I}_2 \Leftrightarrow \lambda^n = \mu^n = 1$. Per tant, l'ordre de γ és el mínim comú múltiple dels ordres de les arrels de la unitat λ i μ. En efecte, siguin r, s i t els ordres respectius. Aleshores

   - $D^r = \boldsymbol{I}_2 \Rightarrow \lambda^r = \mu^r = 1 \Rightarrow s \mid r$ i $t \mid r \Rightarrow [s, t] \mid r$;
   - $\lambda^s = \mu^t = 1 \Rightarrow \lambda^{[s,t]} = \mu^{[s,t]} = 1 \Rightarrow D^{[s,t]} = \boldsymbol{I}_2 \Rightarrow r \mid [s, t]$.

3. El grau del polinomi ciclotòmic $\Phi_n(X)$ és l'indicador d'Euler $\varphi(n)$, que és igual a 1 per a $n = 1, 2$, igual a 2 per a $n = 3, 4, 6$, i és > 2 per a tots els demés valors de n. En efecte, si $n = \prod p_i^{m_i}$ la fórmula per a l'indicador d'Euler és $\varphi(n) = \prod p_i^{m_i - 1}(p_i - 1)$ i

- si un primer $p \geqslant 5$ divideix n aleshores $p-1 \geqslant 4$ divideix $\varphi(n)$;
- si 3 divideix almenys dues vegades n aleshores 3 divideix $\varphi(n)$;
- si 2 divideix almenys tres vegades n aleshores 4 divideix $\varphi(n)$.

Aleshores, si $\varphi(n) \leqslant 2$, n només es pot dividir per 2 un màxim de dues vegades i per 3 un màxim d'una vegada. Els nombres que compleixen això són $1, 2, 3, 4, 6$ i 12 i tots tenen $\varphi(n) \leqslant 2$ excepte $\varphi(12) = 4$. Els polinomis ciclotòmics de grau $\leqslant 2$ són

$$\Phi_1(X) = X - 1, \qquad \Phi_2(X) = X + 1,$$

$$\Phi_3(X) = X^2 + X + 1, \qquad \Phi_4(X) = X^2 + 1, \qquad \Phi_6(X) = X^2 - X + 1.$$

4. Sigui $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ d'ordre finit. Aleshores γ diagonalitza sobre $\mathbb{C}$ i els seus valors propis són arrels de la unitat. Els valors propis són arrels del polinomi característic $P(X) = \det(\gamma - \boldsymbol{I}_2 X) \in \mathbb{Q}[X]$, i per tant els seus polinomis mínims, que són polinomis ciclotòmics, divideixen $P(X)$.

   Hi ha dos casos: si $P(X)$ descompon com a producte de dos polinomis de grau 1, les arrels de la unitat han de tenir polinomi ciclotòmic de grau 1 i només poden ser $\zeta = 1$ i $\zeta = -1$ ja que per l'apartat anterior l'ordre és 1 o 2. En aquest cas la matriu té ordre 1 o 2.

   Si, en canvi, $P(X)$ és irreductible aleshores ha de ser un polinomi ciclotòmic. Per l'apartat anterior ha de ser $n = 3, 4$ o 6 i en tots tres casos els valors propis de γ són les dues arrels n-èsimes primitives de la unitat, que són les arrels diferents de $\Phi_n(X)$. Per tant, l'ordre de γ és $n = 3, 4$ o 6, respectivament.

5. En tot grup l'únic element d'ordre 1 és el neutre; en aquest cas l'element d'ordre 1 de G és la matriu $\boldsymbol{I}_2$. Un element d'ordre 2 té valors propis que són arrels quadrades de la unitat, i per tant són ± 1. Clarament $\gamma_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ té ordre 2. Per a trobar elements d'ordres 3, 4 i 6 es pot observar que $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$ i $\Phi_6(X) = X^2 - X + 1$. Si els valors propis han de ser arrels cúbiques, quartes o sisenes de la unitat el polinomi característic ha de ser un dels donats: el coeficient del mig és menys la traça i el terme independent és el determinant. Per exemple, les matrius següents:

$$\gamma_3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \gamma_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \gamma_6 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},$$

   tenen l'ordre corresponent, tal com es pot comprovar directament. De fet, qualsevol matriu de traça -1 i determinant 1 té ordre 3, qualsevol matriu de traça 0 i determinant 1 té ordre 4 i qualsevol matriu de traça 1 i determinant 1 té ordre 6.

Problema 3.

1. Demostreu el *teorema xinès del residu* en un domini d'ideals principals $\mathbb{A}$: si $a, b \in \mathbb{A}$ són elements relativament primers aleshores es té un isomorfisme d'anells:

$$\mathbb{A}/\langle ab \rangle \simeq \mathbb{A}/\langle a \rangle \times \mathbb{A}/\langle b \rangle.$$

2. Trobeu tres polinomis mònics $f_i(X) = X^2 + aX + b \in \mathbb{R}[X]$ de grau 2 tals que:

   (a) L'anell quocient $\mathbb{A}_1 = \mathbb{R}[X]/\langle f_1(X) \rangle$ és un cos.

(b) L'anell quocient $\mathbb{A}_2 = \mathbb{R}[X]/\langle f_2(X)\rangle$ conté elements nilpotents diferents de zero (un element nilpotent d'un anell és un element α tal que $\alpha^n = 0$ per a algun exponent $n \geqslant 1$).

(c) L'anell quocient $\mathbb{A}_3 = \mathbb{R}[X]/\langle f_3(X)\rangle$ no és isomorf a cap dels dos anteriors.

3. Demostreu que per a tot polinomi $f(X) = X^2 + aX + b \in \mathbb{R}[X]$ l'anell quocient $\mathbb{R}[X]/\langle f(X)\rangle$ és isomorf a un dels tres anells $\mathbb{A}_i$ de l'apartat anterior.

Solució:

1. Com que a i b són relativament primers l'ideal que generen és el total: $\langle a\rangle + \langle b\rangle = \langle a, b\rangle = \mathbb{A}$. Siguin $u \in \langle a\rangle$ i $v \in \langle b\rangle$ elements tals que $u + v = 1$.

   Es considera l'homomorfisme d'anells $\mathbb{A} \to \mathbb{A}/\langle a\rangle \times \mathbb{A}/\langle b\rangle$ que és la projecció canònica en cada component, que envia $\alpha \in \mathbb{A}$ al parell $(\alpha + \langle a\rangle, \alpha + \langle b\rangle)$. Aquest homomorfisme és exhaustiu: donats elements x i y de $\mathbb{A}$ sigui $\alpha = uy + vx$. Aleshores, com que $u \in \langle a\rangle$ també ux i uy són elements de $\langle a\rangle$ i per tant $\alpha + \langle a\rangle = uy + vx + \langle a\rangle = ux + vx + \langle a\rangle = x + \langle a\rangle$; de la mateixa manera $\alpha + \langle b\rangle = y + \langle b\rangle$.

   El nucli de l'homomorfisme és $\langle a\rangle \cap \langle b\rangle$, que com que a i b són relativament primers, és l'ideal $\langle ab\rangle$. Aplicant el teorema d'isomorfisme es dedueix l'isomorfisme de l'enunciat.

2. Siguin $f_1(X) = X^2 + 1$, $f_2(X) = X^2$, $f_3(X) = X^2 - 1$. Aleshores

   (a) Com que $f_1(X)$ és irreductible a $\mathbb{R}$ i té arrels complexes $\pm i$ l'anell $\mathbb{A}_1 = \mathbb{R}[X]/\langle X^2 + 1\rangle$ és un cos, isomorf al cos dels nombres complexos $\mathbb{C} = \mathbb{R}(i)$, que és el cos obtingut adjuntant a $\mathbb{R}$ una arrel d'aquest polinomi.

   (b) A l'anell quocient $\mathbb{A}_2 = \mathbb{R}[X]/\langle X^2\rangle$ el polinomi X no és zero ja que no és múltiple de X^2 i en canvi el seu quadrat X^2 sí que és zero. Per tant, X és un element nilpotent a $\mathbb{A}_2$.

   (c) L'anell $\mathbb{A}_3 = \mathbb{R}[X]/\langle f_3(X)\rangle$ no és íntegre ja que els elements $X - 1$ i $X + 1$ són diferents de zero amb producte zero. Per tant, com que tot cos és íntegre, $\mathbb{A}_3 \not\simeq \mathbb{A}_1$. A més, $\mathbb{A}_3$ no té elements no nuls amb quadrat zero. En efecte, tot element no nul és un polinomi $a + bX$ de grau $\leqslant 1$ amb $a \neq 0$ o $b \neq 0$. El seu quadrat és $a^2 + 2abX + b^2X^2 = a^2 + b^2 + 2abX$ (ja que $X^2 - 1 = 0 \Rightarrow X^2 = 1$), que no és zero ja que $a^2 + b^2 \neq 0$ a $\mathbb{R}$ per ser $a \neq 0$ o $b \neq 0$. Per tant, $\mathbb{A}_3 \not\simeq \mathbb{A}_2$.

3. Sigui $f(X) = X^2 + aX + b \in \mathbb{R}[X]$ un polinomi mònic de segon grau. Aleshores, l'anell $\mathbb{A} = \mathbb{R}[X]/\langle f(X)\rangle$ és isomorf a l'anell $\mathbb{A}_1$, $\mathbb{A}_2$ o $\mathbb{A}_3$ segons que $f(X)$ no tingui arrels reals (discriminant $a^2 - 4b$ negatiu) o tingui una arrel real doble (discriminant zero) o tingui dues arrels reals diferents (discriminant positiu). En efecte,

   - Si f és irreductible a $\mathbb{R}[X]$ aleshores $\mathbb{A}$ és isomorf al cos obtingut adjuntant a $\mathbb{R}$ el nombre complex $\alpha = \frac{1}{2}(-a + \sqrt{a^2 - 4b})$, i per tant és isomorf a $\mathbb{C} \simeq \mathbb{A}_1$.
   - Sigui $f(X) = (X - \alpha)^2$, amb $\alpha \in \mathbb{R}$. L'aplicació $\mathbb{R}[X] \to \mathbb{R}[X]$ que envia cada polinomi $P(X)$ al polinomi $P(X - \alpha)$ és un isomorfisme d'anells (amb invers l'aplicació que envia $P(X)$ a $P(X+\alpha)$), i envia l'ideal $\langle X^2\rangle$ a l'ideal $\langle (X-\alpha)^2\rangle$. Per tant, en passar al quocient dóna un isomorfisme entre $\mathbb{A}_2$ i $\mathbb{A}$.
   - Sigui $f(X) = (X - \alpha)(X - \beta)$ amb α i β nombres reals diferents. Aleshores els ideals $X - \alpha$ i $X - \beta$ són elements relativament primers a $\mathbb{R}[X]$ i per tant el teorema xinès del residu dóna un isomorfisme d'anells

$$\mathbb{R}[X]/\langle f(X)\rangle \simeq \mathbb{R}[X]/\langle X - \alpha\rangle \times \mathbb{R}[X]/\langle X - \beta\rangle.$$

Per altra banda l'aplicació $P(X) \mapsto P(\alpha)$ és un homomorfisme d'anells $\mathbb{R}[X] \to \mathbb{R}$ exhaustiu amb nucli generat per $X-\alpha$ i per tant es té un isomorfisme d'anells $\mathbb{R}[X]/\langle X-\alpha\rangle \simeq \mathbb{R}$. De la mateixa manera, $\mathbb{R}[X]/\langle X-\beta\rangle \simeq \mathbb{R}$. Això vol dir que tots els anells $\mathbb{R}[X]/\langle f(X)\rangle$ on $f(X)$ és un polinomi amb dues arrels reals diferents (entre ells, en particular, l'anell $\mathbb{A}_3$) són isomorfs al producte cartesià d'anells $\mathbb{R} \times \mathbb{R}$.

Problema 4. De les afirmacions següents, digueu si són certes o falses; si són certes demostreu-les i si són falses doneu un contraexemple.

1. Sigui E/K una extensió finita de grau n. Per a tot element $\alpha \in E$ el grau del polinomi mínim $\mathrm{Irr}(\alpha, K; X)$ és un divisor de n.
2. Si E/K és una extensió infinita existeix algun element $\alpha \in E$ que és transcendent sobre K.
3. El cos finit $\mathbb{F}_q$ de $q = p^n$ elements conté subcossos d'ordre p^m per a $m = 1, 2, \ldots, n$.
4. Donats nombres complexos $\alpha_1, \cdots, \alpha_n$, si l'extensió $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)/\mathbb{Q}$ és algebraica aleshores és finita.
5. Si els polígons regular de n i de m costats són construïbles i $\gcd(n, m)$ és parell, aleshores el polígon regular de nm costats també és construïble.
6. Si p és un primer senar, $\zeta = e^{2\pi i/p}$ i $H \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ és un subgrup, aleshores $\zeta^H = \sum_{a \in H} \zeta^a$ és un nombre real si, i només si, $-1 \in H$.

Solució:

1. Cert. L'aplicació $K[X] \to K(\alpha)$ que envia un polinomi $P(X)$ a $P(\alpha)$ és exhaustiva (ja que α és algebraic sobre K per ser E/K finita) amb nucli l'ideal generat pel polinomi mínim $\mathrm{Irr}(\alpha, H; X)$. Per tant es té un isomorfisme $K[X]/\langle \mathrm{Irr}(\alpha, H; X)\rangle \simeq K(\alpha)$ i l'extensió $K(\alpha)/K$ té grau el grau del polinomi irreductible de α. Per multiplicativitat dels graus,

$$[E : K] = [E : K(\alpha)] \cdot [K(\alpha) : K]$$

   i per tant el grau de $\mathrm{Irr}(\alpha, K; X)$ divideix $n = [E : K]$.

2. Fals. Sigui $\overline{\mathbb{Q}} \subset \mathbb{C}$ el subcos format per tots els nombres complexos que són algebraics sobre $\mathbb{Q}$. Aleshores l'extensió $\overline{\mathbb{Q}}/\mathbb{Q}$ és algebraica ja que els elements de $\overline{\mathbb{Q}}$ són tots algebraics sobre $\mathbb{Q}$. En canvi, és una extensió infinita ja que per a cada $n \geqslant 1$ l'extensió $\mathbb{Q}(\sqrt[n]{2})$ està continguda a $\overline{\mathbb{Q}}$ i $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, de manera que $[\overline{\mathbb{Q}} : \mathbb{Q}] \geqslant n$.

   Un altre exemple: sigui $\alpha_n = \sqrt[2^n]{2} \in \mathbb{R}$ i sigui $K_n = \mathbb{Q}(\alpha_n) \subset \mathbb{R}$. Com que $\alpha_{n+1}^2 = \alpha_n$ es tenen inclusions $K_n \subseteq K_{n+1}$, de manera que

$$\mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$$

   Sigui $K = \bigcup_{n \geqslant 1} K_n \subset \mathbb{R}$ la reunió de tots aquests cossos. K és un cos ja que donats dos elements qualsevol estan en algun K_n per n prou gran i aquest $K_n \subset K$ conté la seva suma, resta, producte i quocient (si el segon és no nul). A més $K/\mathbb{Q}$ és una extensió algebraica ja que cada element de K pertany a algun K_n, que és una extensió finita i, per tant, algebraica, de $\mathbb{Q}$. En canvi $K/\mathbb{Q}$ no és finita ja que conté subcossos K_n de grau 2^n arbitràriament gran sobre $\mathbb{Q}$.

3. Fals. El cos $\mathbb{F}_{p^n}$ conté subcossos de cardinal p^m només per als exponents m que són divisors de n. En efecte, si $\mathbb{F}$ és un subcos de $\mathbb{F}_{p^n}$ de p^m elements aleshores $\mathbb{F}_{p^n}$ és un $\mathbb{F}$-espai vectorial. Si k és la dimensió corresponent aleshores el nombre d'elements p^n de $\mathbb{F}_{p^n}$ és $(p^m)^k$, i d'aquí es dedueix que $n = mk$ i per tant m és un divisor de n. Això demostra que la condició $m \mid n$ és necessària de manera que l'enunciat és fals. Es pot veure que la condició $m \mid n$ és suficient veient que, en aquest cas, el polinomi $X^{p^m} - X$ divideix el polinomi $X^{p^n} - X$, però això no cal per fer el problema.

4. Cert. Suposi's que l'extensió és algebraica. Aleshores cada element α_i és algebraic sobre $\mathbb{Q}$ i, per tant, també és algebraic sobre $\mathbb{Q}(\alpha_1,\ldots,\alpha_{i-1})$. Com que una extensió $K(\alpha)/K$ amb α algebraic sobre K és finita de grau el polinomi mínim de α sobre K, cada extensió $\mathbb{Q}(\alpha_1,\ldots,\alpha_i)=\big(\mathbb{Q}(\alpha_1,\ldots,\alpha_{i-1})\big)(\alpha_i)/\mathbb{Q}(\alpha_1,\ldots,\alpha_{i-1})$ és finita, de grau el del polinomi irreductible de α_i sobre $\mathbb{Q}(\alpha_1,\ldots,\alpha_{i-1})$. Per multiplicativitat dels graus en una torre d'extensions

$$[\mathbb{Q}(\alpha_1,\ldots,\alpha_n):\mathbb{Q}]=[\mathbb{Q}(\alpha_1,\ldots,\alpha_n):\mathbb{Q}(\alpha_1,\ldots,\alpha_{n-1})]\quad\cdots\quad[\mathbb{Q}(\alpha_1):\mathbb{Q}]$$

l'extensió total també és finita.

5. Fals. Contraexemple: $n=m=6$ tenen màxim comú divisor 6 i en canvi el polígon de $36=4\cdot 9$ no és construïble ja que el de 9 costats no ho és.

6. Cert. Un nombre complex és real si, i només si, és igual al seu conjugat. El conjugat d'una arrel de la unitat ζ és la seva inversa ζ^{-1} ja que $\zeta\overline{\zeta}=|\zeta|=1=\zeta\zeta^{-1}$. Si $-1\in H$ aleshores la classe lateral $(-1)H$ coincideix amb H i, per tant,

$$\overline{\zeta^H}=\overline{\sum_{a\in H}\zeta^a}=\sum_{a\in h}\overline{\zeta}^a=\sum_{a\in H}\zeta^{-a}=\sum_{b\in(-1)H}\zeta^b=\sum_{a\in H}\zeta^a=\zeta^H$$

Si, en canvi, $-1\notin H$ aleshores H i $(-1)H$ són classes laterals disjuntes. Suposi's que $\zeta^H=\overline{\zeta^H}$, o sigui, que $\zeta^H=\zeta^{(-1)H}$. Aleshores es tindria una expressió

$$\sum_{a\in H}\zeta^a-\sum_{b\in(-1)H}\zeta^b=0$$

on els exponents a i b són enters diferents entre 1 i $p-1$. Dividint per ζ es dedueix una expressió

$$\sum_{a\in H}\zeta^{a-1}-\sum_{b\in(-1)H}\zeta^{b-1}=0$$

on els exponents $a-1$ i $b-1$ són enters diferents entre 0 i $p-2$. Aquesta expressió assegura que ζ és arrel d'un polinomi no nul a coeficients racionals (tots són 1 o -1) de grau $\leqslant p-2$, però el polinomi irreductible de ζ té grau $\varphi(p)=p-1$. Això és una contradicció.

Problema 5. Donat un primer p, considereu els nombres reals següents:

$$\alpha=\sqrt{p-\sqrt[3]{p}}\,,\qquad \beta=\sqrt[3]{p-\sqrt{p}}\,.$$

1. Calculeu els polinomis mínims de α i de β sobre $\mathbb{Q}$.
2. Proveu que $g(\beta^2)=\beta$ per a algun polinomi $g[X]\in\mathbb{Q}[X]$ i que, en canvi, aquesta igualtat no se satisfà mai per a α en lloc de β.
3. Proveu que, si $\mathbb{Q}(\gamma)/\mathbb{Q}$ és una extensió de grau senar, aleshores $g(\gamma^2)=\gamma$ per a algun polinomi $g[X]\in\mathbb{Q}[X]$.

Solució:

1. $\alpha^2=p-\sqrt[3]{p}\Rightarrow p=(p-\alpha^2)^3=p^3-3p^2\alpha^2+3p\alpha^4-\alpha^6$. Per tant α és arrel del polinomi $X^6-3pX^4+3p^2X^2-p(p^2-1)$, que és irreductible per ser p-Eisenstein.

   $\beta^3=p-\sqrt{p}\Rightarrow p=(p-\beta^3)^2=p^2-2p\beta^3+\beta^6$. Per tant β és arrel del polinomi $X^6-2pX^3+p(p-1)$, que és irreductible per ser p-Eisenstein.

2. Per l'apartat anterior se saben els graus $[\mathbb{Q}(\alpha):\mathbb{Q}]=6$ i $[\mathbb{Q}(\beta):\mathbb{Q}]=6$. Es té $\mathbb{Q}\subseteq\mathbb{Q}(\beta^2)\subseteq\mathbb{Q}(\beta)$. Operant amb la identitat $\beta^6-2p\beta^3+p(p-1)=0$ (aïllant una β del terme del mig) s'obté la identitat

$$\beta=\frac{\beta^6+p(p-1)}{2p\beta^2}\in\mathbb{Q}(\beta^2).$$

Per tant, $\mathbb{Q}(\beta)=\mathbb{Q}(\beta^2)$ i tot element de $\mathbb{Q}(\beta)$, en particular el mateix β, pertany a l'extensió simple $\mathbb{Q}(\beta^2)$, els elements de la qual s'escriuen com a polinomis (de grau <6) a coeficients en $\mathbb{Q}$ avaluats en β^2; o sigui $\beta=g(\beta^2)$ per a un $g(X)\in\mathbb{Q}[X]$ (de grau <6).

En canvi α^2 és arrel del polinomi $X^3-3pX^2+3p^2X-p(p^2-1)$ irreductible de grau 3. Per tant $[\mathbb{Q}(\alpha^2):\mathbb{Q}]=3$ i per la multiplicativitat dels graus ha de ser $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^2)]=2$. En particular, $\mathbb{Q}(\alpha)\neq\mathbb{Q}(\alpha^2)$ i $\alpha\notin\mathbb{Q}(\alpha^2)$, de manera que α no pot ser de la forma $g(\alpha^2)$ amb $g(X)\in\mathbb{Q}[X]$.

3. Com que $\gamma^2\in\mathbb{Q}(\gamma)$ es tenen inclusions $\mathbb{Q}\subseteq\mathbb{Q}(\gamma^2)\subseteq\mathbb{Q}(\gamma)$. Per multiplicativitat dels graus, $[\mathbb{Q}(\gamma):\mathbb{Q}(\gamma^2)]$ divideix $[\mathbb{Q}(\gamma):\mathbb{Q}]$, que és un nombre senar, i per tant també és senar. Com que γ és arrel del polinomi $X^2-\gamma^2\in\mathbb{Q}(\gamma^2)[X]$ el seu polinomi irreductible ha de ser un divisor d'aquest polinomi, i té grau senar. Per tant, el grau de $\mathrm{Irr}(\gamma,\mathbb{Q}(\gamma^2);X)$ és igual a 1 i això vol dir que $\gamma\in\mathbb{Q}(\gamma^2)$. Això implica que γ s'escriu de la forma $g(\gamma^2)$ amb g un polinomi a coeficients racionals (de grau menor que el grau de l'extensió $\mathbb{Q}(\gamma^2)/\mathbb{Q}$, que és el mateix que el grau de l'extensió $\mathbb{Q}(\gamma)/\mathbb{Q}$). Una altra manera de veure que $\gamma=\mathbb{Q}(\gamma^2)$ és fer servir el polinomi irreductible $\mathrm{Irr}(\gamma,\mathbb{Q};X)=X^{2n+1}+a_{2n}X^{2n}+\cdots+a_3X^3+a_2X^2+a_1X+a_0$ i a partir de la identitat

$$\begin{aligned}\beta^{2n+1}+a_{2n}\beta^{2n}+\cdots+a_3\beta^3+a_2\beta^2+a_1\beta+a_0&\\ =\beta(\beta^{2n}+\cdots+a_3\beta^2+a_1)+(a_{2n}\beta^{2n}+\cdots+a_2\beta^2+a_0)=0&\end{aligned}$$

aïllar β i obtenir-lo com un element de $\mathbb{Q}(\beta^2)$. Observi's que el denominador no pot ser zero ja que és el valor de β en un polinomi de grau $2n$, que no pot ser zero ja que el polinomi irreductible de β té grau $2n+1$.