Facultat de Matemàtiques i Estadística
Examen final d'Estructures Algebraiques
19 de gener de 2015

Trieu cinc dels sis problemes següents. Tots puntuen igual.

Problema 1. Demostreu un dels dos teoremes següents:

- Tot subgrup finit del grup multiplicatiu d'un cos és cíclic.
- Tot grup finit d'ordre divisible per un primer p conté algun element d'ordre p.

De tots els resultats previs que feu servir en la vostra demostració, escriviu l'enunciat amb tota precisió.

Problema 2. Considereu al grup simètric $\mathfrak{S}_9$ les permutacions

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 9 & 1 & 8 & 6 & 3 & 2 & 4 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 9 & 6 & 1 & 8 & 2 & 4 & 3 \end{pmatrix}$$

i els cicles

$$\gamma_1 = (2\ 4\ 6), \quad \gamma_2 = (2\ 7\ 9), \quad \gamma_3 = (1\ 6\ 3\ 9).$$

1. Calculeu σ_1^{2015} i σ_2^{2016}.
2. Doneu, si existeix, una permutació σ tal que $\sigma\gamma_1\gamma_2\gamma_3\sigma^{-1} = \gamma_3\gamma_2\gamma_1$.
3. Demostreu que entre $\sigma_1, \sigma_2, \gamma_1$ i γ_2 no generen tot el grup $\mathfrak{S}_9$.
4. Doneu dos subgrups de $\mathfrak{S}_9$ d'ordre 14 no isomorfs.
5. Sigui $H = \langle c_5, \tau \rangle$ el subgrup generat pel cicle $c_5 = (1\ 2\ 3\ 4\ 5)$ i la transposició $\tau = (1\ 2)$, i sigui N el seu normalitzador dins de $\mathfrak{S}_9$. Digueu si els grups N i N/H són o no resolubles.

Solució:

1. La descomposició en cicles disjunts de les dues permutacions és:

   $$\sigma_1 = (1\ 7\ 3\ 9\ 4)(2\ 5\ 8), \qquad \sigma_2 = (1\ 7\ 2\ 5)(3\ 9)(4\ 6\ 8)$$

   Com que els cicles disjunts commuten s'obté:

   $$\sigma_1^{2015} = (1\ 7\ 3\ 9\ 4)^{2015}(2\ 5\ 8)^{2015} = (2\ 5\ 8)^2 = (2\ 8\ 5).$$

   Per altra banda, com que 2016 és divisible per 2, 3 i 4 es dedueix que σ_2^{2016} és la identitat.

2. Calculant la seva expressió com a producte de cicles disjunts s'obté:

   $$\gamma_1\gamma_2\gamma_3 = (1\ 2\ 7\ 9)(3\ 4\ 6), \qquad \gamma_3\gamma_2\gamma_1 = (1\ 6\ 7)(2\ 3\ 4\ 9).$$

   Com que l'estructura de totes dues és la mateixa (un producte d'un cicle de longitud 4 per un de longitud 3) són conjugades. Per exemple, una permutació que compleix el que es demana és:

   $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 6 & 5 & 7 & 4 & 8 & 9 \end{pmatrix}.$$

3. Aquestes permutacions no poden generar tot $\mathfrak{S}_9$ perquè són totes parells i, per tant, el subgrup que generen està contingut dins del grup alternat $\mathfrak{A}_9$.

4. De grups d'ordre 14 només n'hi ha dos, llevat d'isomorfisme: el cíclic i el diedral. El primer es pot construir, per exemple, com el subgrup de $\mathfrak{S}_9$ generat per la permutació (1 2 3 4 5 6 7)(8 9), que té ordre 14; el grup diedral és isomorf, per exemple, al grup generat per $r = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ i $s = (2\ 7)(3\ 6)(4\ 5)$, que és el grup de les isometries d'un heptàgon regular amb vèrtexs numerats de l'1 al 7: el cicle r és la rotació d'angle $2\pi/7$ i el producte de tres transposicions disjuntes s és la simetria que deixa fix el primer vèrtex. Es té $r^5 = s^2 = 1, rs = sr^{-1}$.

5. El subgrup H és el subgrup de totes les permutacions dels enters $1, 2, 3, 4, 5$, que és isomorf a $\mathfrak{S}_5$. Les permutacions $\sigma \in \mathfrak{S}_9$ tals que $\sigma H \sigma^{-1} \in H$ són les que envien el subconjunt dels enters $1, 2, 3, 4, 5$ a ell mateix. En efecte, $\sigma(1\ 2\ 3\ 4\ 5)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4)\ \sigma(5))$ ha de ser de H i per tant els $\sigma(i)$ han de ser enters del conjunt $\{1, 2, 3, 4, 5\}$; recíprocament per a qualsevol σ tot element de $\sigma H \sigma^{-1}$ només permuta enters del conjunt $\{1, 2, 3, 4, 5\}$ i per tant és de H. Per tant, N és el subgrup de $\mathfrak{S}_9$ que envia els enters $1, 2, 3, 4, 5$ a ells mateixos; això vol dir que també envia els enters $6, 7, 8, 9$ a ells mateixos: els seus elements són el producte d'una permutació de $1, 2, 3, 4, 5$ per una permutació de $6, 7, 8, 9$. Com que dues permutacions com aquestes commuten, el grup N és isomorf al producte cartesià $\mathfrak{S}_5 \times \mathfrak{S}_4$.

   El grup N no és resoluble ja que conté un subgrup isomorf a $\mathfrak{A}_5$, que no és resoluble per ser simple no abelià. En canvi el grup H/N és isomorf a $\mathfrak{S}_4$ i sí que és resoluble (vist a classe).

Problema 3. Sigui $\mathbb{A} = \{\alpha = a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Es considera l'aplicació $N\colon \mathbb{A} \to \mathbb{N}$ definida per $N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2 = a^2 + 5b^2$. Demostreu que:

1. Si $\alpha \mid \beta$ a $\mathbb{A}$ aleshores $N(\alpha) \mid N(\beta)$ a $\mathbb{Z}$.
2. $\alpha \in \mathbb{A}^* \Leftrightarrow N(\alpha) = 1$; trobeu totes les unitats de l'anell $\mathbb{A}$.
3. Tots els elements no nuls de $\mathbb{A}$ descomponen com a producte d'irreductibles.
4. $2, 3, 1 + \sqrt{-5}$ i $1 - \sqrt{-5}$ són irreductibles no primers.
5. N no és una norma euclidiana a $\mathbb{A}$.

Solució:

1. L'aplicació N és multiplicativa: $N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2$. Si $\alpha \mid \beta$, sigui $\beta = \alpha q$. Aleshores $N(\beta) = N(\alpha)N(q)$ i per tant $N(\alpha) \mid N(\beta)$.
2. Sigui $\alpha \in \mathbb{A}^*$. Sigui $\beta = \alpha^{-1}$. Aleshores $\alpha\beta = 1 \Rightarrow N(\alpha)N(\beta) = N(1) = 1$; com que $N(\alpha)$ és un enter positiu ha de ser $N(\alpha) = 1$. Recíprocament, si $N(\alpha) = 1$ es té $\alpha\overline{\alpha} = 1$ i per tant $\overline{\alpha} = \alpha^{-1}$, de manera que $\alpha \in \mathbb{A}^*$.

   L'equació $a^2 + 5b^2$ admet les úniques solucions $(a, b) = (\pm 1, 0)$ i per tant les unitats de l'anell $\mathbb{A}$ són els dos nombres enters ± 1.
3. Per inducció sobre $N(\alpha)$. Si $N(\alpha) = 1$ aleshores α és una unitat, que és un producte buit d'irreductibles. Suposi's demostrat per a tots els elements no nuls de norma menor que la d'un element α. Si α és irreductible aleshores $\alpha = \alpha$ és una descomposició en producte d'irreductibles. En cas contrari existeix una descomposició $\alpha = \beta\gamma$ en la qual ni β ni γ són unitats. Aleshores $N(\alpha) = N(\beta)N(\gamma)$ amb $N(\beta) > 1$

i $N(\gamma) > 1$; per tant $N(\beta) < N(\alpha)$ i $N(\gamma) < N(\alpha)$. Per hipòtesi d'inducció β i γ són producte d'irreductibles i, per tant $\alpha = \beta\gamma$ també ho és.

Alternativa: reducció a l'absurd. Suposi's que no és cert i sigui α un element que no descompon en producte d'irreductibles de norma mínima. Aleshores α no és un irreductible i per tant descompon de la forma $\alpha = \beta\gamma$ amb $\beta, \gamma \notin \mathbb{A}^*$. Però aleshores β i γ tenen norma estrictament menor que α i algun dels dos no descompon en producte d'irreductibles, ja que si tots dos descomponguessin α també ho faria (en el producte).

4. Suposi's que es té una descomposició $2 = \alpha\beta$ amb α i β no unitats. Aleshores $N(\alpha)N(\beta) = N(2) = 4$ i ha de ser $N(\alpha) = N(\beta) = 2$. Però l'equació $a^2 + 5b^2 = 2$ no té solucions amb $a, b \in \mathbb{Z}$, i per tant la descomposició no pot existir. Anàlogament es prova en els demés casos: si $3 = \alpha\beta$ hauria de ser $N(\alpha) = N(\beta) = 3$, i l'equació $a^2 + 5b^2$ no té solució; si $1 \pm \sqrt{-5} = \alpha\beta$ hauria de ser $N(\alpha) = 2$ i $N(\beta) = 3$, o al revés, i les equacions corresponents no tenen solució. Per tant, aquests quatre elements són irreductibles.

   En canvi no són primers. En efecte, es té la igualtat $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}) = 6$. Per tant, 2 divideix el producte $(1+\sqrt{-5})(1-\sqrt{-5})$. Però 2 no divideix cap dels dos factors, ja que si fos així $N(2) = 4$ dividiria $N(1 \pm \sqrt{-5}) = 6$. El mateix argument prova que els altres tampoc són primers.

5. Com que tot anell euclidià és factorial, si N fos una norma euclidiana aleshores $\mathbb{A}$ seria un anell factorial, i en un anell factorial tots els irreductibles són primers, però a l'apartat anterior s'ha vist que això no és cert a l'anell $\mathbb{A}$.

Problema 4. Sigui E/K una extensió de cossos, i sigui A un anell tal que $K \subseteq A \subseteq E$. Demostreu que, si E/K és algebraica, aleshores A és un cos, però que, si E/K no és algebraica, existeix algun anell A amb $K \subseteq A \subseteq E$ que no és un cos.

Solució: Suposi's que E/K és algebraica. S'ha de veure que, per a tot element no nul $\alpha \in A \setminus \{0\}$, l'invers $\alpha^{-1} \in E$ també pertany a A. Com que $\alpha \in E$ i E/K és algebraica, α és arrel d'algun polinomi no nul a coeficients en K. Sigui $P(X) = \mathrm{Irr}(\alpha, K; X)$ el polinomi irreductible, amb $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ i $a_0 \neq 0$ ja que $\alpha \neq 0$. Aleshores

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \quad \Rightarrow \quad \alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_2\alpha + a_1) = -a_0$$

$$\Rightarrow \alpha\beta = 1 \quad \text{amb} \quad \beta = \left(\frac{-1}{a_0}\alpha^{n-1} + \frac{-a_{n-1}}{a_0}\alpha^{n-2} + \cdots + \frac{-a_2}{a_0}\alpha + \frac{-a_1}{a_0}\right).$$

L'invers de $\beta = \alpha^{-1}$ és una combinació lineal de potències de α a coeficients en K, i per tant pertany a l'anell A. Alternativament, a classe s'ha vist que quan α és algebraic sobre K aleshores $K[\alpha] = K(\alpha)$. En aquest cas, $\alpha^{-1} \in K[\alpha] \subseteq A$.

Si l'extensió E/K no és algebraica, sigui $\alpha \in E$ un element transcendent sobre K. Aleshores l'anell $A = K[\alpha] = \{P(\alpha) : P(X) \in K[X]\}$ és un subanell de E que conté K i no és un cos, ja que α no és invertible en aquest anell. En efecte, si fos $\alpha^{-1} = P(\alpha)$ aleshores es tindria $\alpha P(\alpha) - 1 = 0$ i α seria arrel d'un polinomi no nul a coeficients en K, en contradicció amb la seva transcendència.

Problema 5. Calculeu el grau, un element primitiu $\alpha \in E$ i el seu polinomi irreductible $\mathrm{Irr}(\alpha, K; X)$, per a les extensions E/K següents:

1. $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$,
2. $\mathbb{Q}(e^{\pi i/8}, i+\sqrt{2}+\sqrt{-2})/\mathbb{Q}$,
3. $\mathbb{F}_5(\sqrt[4]{2},\sqrt[2]{3})/\mathbb{F}_5$,
4. $\mathbb{F}_7(\sqrt[4]{2},\sqrt[2]{3})/\mathbb{F}_7$.

Solució:

1. Com que $\sqrt{2}\notin\mathbb{Q}(\sqrt{3})$ ja que elevant al quadrat la igualtat $\sqrt{2}=a+b\sqrt{3}$ amb $a,b\in\mathbb{Q}$ es tindria que $\sqrt{3}\in\mathbb{Q}$, i com que $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt{3},\sqrt{3})$, es dedueix que l'extensió és de grau 4. Sigui $\alpha=\sqrt{2}+\sqrt{3}$. Com que $(\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3})=-1$ es té $\alpha^{-1}=\sqrt{3}-\sqrt{2}$ i per tant $\sqrt{2}=\frac{1}{2}(\alpha-\alpha^{-1}), \sqrt{3}=\frac{1}{2}(\alpha+\alpha^{-1})$. Es dedueix que $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$ i α és un element primitiu de l'extensió. Elevant al quadrat es té $\alpha^2=2+3+2\sqrt{6}$; per tant, $\alpha^2-5=2\sqrt{6}\Rightarrow\alpha^4-10\alpha^2+25=24$ i α és arrel del polinomi X^4-10X^2+1. Aquest polinomi és $\mathrm{Irr}(\alpha,\mathbb{Q};X)$.
2. Sigui $\zeta=e^{\pi i/8}=e^{2\pi i/16}$, que és una arrel 16-ena primitiva de la unitat. Com que $i=\zeta^4=e^{\pi i/2}$ i $\frac{1+i}{\sqrt{2}}=\zeta^2=e^{\pi i/4}$ es dedueix que $i+\sqrt{2}+\sqrt{-2}=\zeta^4+(1+\zeta^4)\zeta^{-2}+\zeta^4(1+\zeta^4)\zeta^{-2}$. Per tant $\mathbb{Q}(\zeta,i+\sqrt{2}+\sqrt{-2})=\mathbb{Q}(\zeta)$. L'extensió és simple amb element primitiu ζ. El polinomi irreductible d'una arrel primitiva de la unitat és el ciclotòmic, per tant $\mathrm{Irr}(\zeta,\mathbb{Q};X)=\Phi_{16}(X)=X^8+1$. L'extensió té grau 8.
3. Sigui $\alpha=\sqrt[4]{2}$ a $E=\mathbb{F}_5(\sqrt[4]{2},\sqrt{3})$. Aleshores $\alpha^2=\sqrt{2}$ i $\alpha^{-2}=(\sqrt{2})^{-1}=\sqrt{3}$. Per tant, l'extensió és simple generada per α, $E=\mathbb{F}_5(\alpha)$. Com que 3 no és un quadrat a $\mathbb{F}_5$ i l'extensió conté la subextensió $\mathbb{F}_5(\sqrt{3})\simeq\mathbb{F}_{25}$ de grau 2, ha de tenir grau 2 o 4. Si tingués grau 2 aleshores seria isomorfa a $\mathbb{F}_{25}$ i per tant tot element no nul d'aquesta extensió tindria potència 24-ena igual a 1. Com que $\alpha^4=2\Rightarrow\alpha^8=4=-1\Rightarrow\alpha^{24}=-1\neq1$ es dedueix que l'extensió ha de ser de grau 4, i per tant isomorfa al cos $\mathbb{F}_{625}$. α és arrel del polinomi X^4-2, de grau 4, que ha de ser per tant el seu polinomi irreductible.
4. Com que $X^4-2=(X^2-3)(X^2+3)=(X^2-3)(X-2)(X-5)$. De les arrels quartes de 2 n'hi ha dues que ja pertanyen a $\mathbb{F}_7$, que són 2 i 5, i unes altres dues que no hi pertanyen, que són $\pm\sqrt{3}$. Com que l'extensió que es demana ja conté $\sqrt{3}$ sempre es té $\mathbb{F}_7(\sqrt[4]{2},\sqrt{3})=\mathbb{F}_7(\sqrt{3})$, sigui quina sigui l'arrel quarta de 2 triada. Per tant l'extensió és igual a $\mathbb{F}_7(\sqrt{3})\simeq\mathbb{F}_{49}$, de grau 2. Un element primitiu és $\alpha=\sqrt{3}$ i el seu polinomi irreductible és X^2-3.

Problema 6. Digueu si els nombres complexos següents són o no construïbles amb regle i compàs, justificant la vostra resposta:

1. $\sqrt[3]{3}$,
2. $\sqrt{\frac{1}{2}\sqrt{2}-\frac{1}{5}\sqrt[4]{5}}$,
3. $e^{2\pi i/255}+e^{2\pi i/257}$,
4. $\zeta+\zeta^{10}$, on $\zeta=e^{2\pi i/11}$,
5. $\zeta+\zeta^3+\zeta^9$, on $\zeta=e^{2\pi i/13}$.

Solució:

1. El polinomi irreductible de $\sqrt[3]{3}$ sobre $\mathbb{Q}$ és el polinomi $X^3 - 3$. Per tant l'extensió $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}]$ té grau 3. Per tant $\sqrt[3]{3}$ no és construïble ja que els nombres construïbles generen extensions de grau potència de 2.
2. És construïble ja que tot nombre complex que es pugui obtenir a partir de nombres racionals fent sumes, restes, productes, quocients i arrels quadrades és construïble. El nombre donat s'obté fent l'arrel quadrada de 2, l'arrel quadrada de l'arrel quadrada de 5, multiplicant per racionals i restant, i finalment fent l'arrel quadrada del resultat.
3. $257 = 2^8+1$ és un primer de Fermat i, per tant, $e^{2\pi i/257}$ és construïble. $255 = 3\cdot 5\cdot 17$, i els tres factors $3 = 2 + 1$, $5 = 2^2 + 1$ i $17 = 2^4 + 1$ són primers de Fermat; per tant, el polígon regular de 255 costats és construïble i això és el mateix que dir que $e^{2\pi i/255}$ és construïble. Com que la suma de construïbles és construïble, el nombre donat ho és.
4. El subgrup $H = \{1, 10\} \subset (\mathbb{Z}/11\mathbb{Z})^*$ té índex 5 a $(\mathbb{Z}/11\mathbb{Z})^*$. Per tant, l'extensió $\mathbb{Q}(\zeta^H)$ té grau 5 sobre $\mathbb{Q}$ i això implica que el nombre ζ^H no és construïble, ja que els nombres construïbles generen extensions de grau potència de 2.
5. El subgrup $H = \{1, 3, 9\} \subset (\mathbb{Z}/13\mathbb{Z})^*$ té índex 4 a $(\mathbb{Z}/13\mathbb{Z})^*$. Per tant, l'extensió $\mathbb{Q}(\zeta^H)$ té grau 4 sobre $\mathbb{Q}$. El subgrup $K = \{1, 3, 4, 9, 10, 12\}$ conté H com a subgrup d'índex 2 i ell mateix té índex 2 a $(\mathbb{Z}/13\mathbb{Z})^*$. Per tant, es té una torre d'extensions $\mathbb{Q} \subseteq \mathbb{Q}(\zeta^K) \subseteq \mathbb{Q}(\zeta^H)$ on cada salt és una extensió de grau 2. Això assegura que el nombre ζ^H és construïble.