Facultat de Matemàtiques i Estadística
Examen final d'Estructures Algebraiques
19 de gener de 2017

Problema 1. El *grup derivat* G' d'un grup G es defineix com el subgrup generat per tots els elements de la forma $aba^{-1}b^{-1}$ per a tots els elements $a, b \in G$.

1. Demostreu que G' és normal a G i que el quocient G/G' és abelià.
2. Demostreu que tot subgrup normal $H \lhd G$ amb quocient G/H abelià conté G'.
3. Demostreu que $G' = \{1\}$ si, i només si, G és abelià.
4. Calculeu el grup derivat del grup simètric $\mathfrak{S}_n$ per a tot n.
5. Demostreu que si H és un subgrup normal de G aleshores el seu derivat H' també és normal a G.
6. Demostreu que tot subgrup normal minimal d'un grup resoluble és abelià.

En el darrer apartat "subgrup normal minimal" vol dir un subgrup normal no trivial que no contingui cap altre subgrup normal no trivial diferent d'ell mateix: un subgrup $H \lhd G$ tal que si $K \subseteq H$ amb $K \lhd G$ aleshores $K = \{1\}$ o bé $K = H$.

Solució:

1. El conjugat d'un generador $aba^{-1}b^{-1}$ per un element $g \in G$ és

$$g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$$

   i és també un dels generadors del grup. Per tant en conjugar un element de G' s'obté un element que també és de G' i això diu que $G' \lhd G$. Donats elements $a, b \in G$ l'element $g = a^{-1}b^{-1}ab$ és de G' i es té

$$bG'aG' = baG' = bagG' = abG' = aG'bG'$$

   i per tant grup quocient G/G' de les classes laterals mòdul el subgrup G' és un grup abelià.

2. Per a tot parell d'elements $a, b \in G$ es té

$$aHbH = bHaH \Rightarrow abH = baH \Rightarrow Hab = Hba \Rightarrow ab(ba)^{-1} = aba^{-1}b^{-1} \in H.$$

   Per tant, tots els generadors de G' pertanyen a H i $G' \subseteq H$.

3. El derivat d'un grup abelià està generat per elements $aba^{-1}b^{-1} = 1$ i per tant és el grup trivial. Recíprocament, si un grup no és abelià conté dos elements a i b que no commuten i aleshores l'element $aba^{-1}b^{-1} \in G'$ no és el neutre.

4. El derivat del grup simètric $\mathfrak{S}_n$ és un subgrup normal amb quocient $\mathfrak{S}_n/\mathfrak{S}'_n$ abelià. Si $n \geqslant 5$ els únics subgrups normals del simètric són el trivial, el total i l'alternat. El derivat no pot ser trivial ja que el grup no és abelià. Per altra banda tot generador de $\mathfrak{S}'_n$ és de la forma $\sigma\tau\sigma^{-1}\tau^{-1}$, i a partir d'aquesta expressió és clar que és una permutació parell. Per tant el derivat només conté permutacions parells i ha de ser

per tant l'alternat $\mathfrak{A}_n$. Si $n = 4$ a més dels altres tres $\mathfrak{S}_4$ conté un altre subgrup normal, que és el grup V_4; com que el quocient $\mathfrak{S}_4/V_4 \simeq \mathfrak{S}_3$ no és abelià aquest grup no pot ser el derivat i pel mateix argument d'abans el derivat és $\mathfrak{A}_4$. Si $n = 3$ els únics subgrups normals són els mateixos que per a $n \geqslant 5$, i pel mateix raonament el derivat és l'alternat $\mathfrak{A}_3 \simeq C_3$. Finalment, si $n = 2$ el grup $\mathfrak{S}_2 \simeq C_2$ és abelià i el seu derivat és el grup trivial, que és el grup alternat corresponent $\mathfrak{A}_2 = \{1\}$. Per tant, en tots els casos el grup derivat és l'alternat: $\mathfrak{S}_n' = \mathfrak{A}_n$.

5. El subgrup derivat H' és normal a H i es vol veure que també és normal a G. El raonament és el mateix que el que s'ha fer per veure que el derivat és normal en el grup: donats elements h i $k \in H$ el conjugat per un element $g \in G$ del generador $hkh^{-1}k^{-1}$ de H' és l'element

$$g(hkh^{-1}k^{-1})g^{-1} = (ghg^{-1})(gkg^{-1})(ghg^{-1})^{-1}(gkg^{-1})^{-1}.$$

   Com que H és normal a G els conjugats ghg^{-1} i gkg^{-1} també pertanyen a H i l'expressió anterior és un dels generadors de H'.

6. Sigui $H \lhd G$ un subgrup normal minimal. Com que G és resoluble aleshores H també ho és. Suposi's que H no és abelià. Sigui $K \lhd H$ l'últim subgrup d'una torre normal abeliana: és un subgrup propi de H amb quocient H/K abelià. Per l'apartat 2 es té $H' \subseteq K$. Per l'apartat 5 H' és un subgrup normal de G, no trivial perquè H no és abelià. Així H' és un subgrup normal no trivial de G contingut estrictament en el subgrup normal H, i per tant H no és minimal.

Problema 2. L'objectiu d'aquest problema és trobar totes les solucions enteres de l'equació $Y^2 = X^3 - 2$.

L'anell $A = \mathbb{Z}[\sqrt{-2}] = \{a+b\sqrt{-2} : a, b \in \mathbb{Z}\}$ és un anell euclidià amb norma euclidiana $N(a + b\sqrt{-2}) = a^2 + 2b^2$, que és multiplicativa: $N(\alpha\beta) = N(\alpha)N(\beta)$. Això s'ha vist a classe i ho podeu fer servir sense haver de justificar-ho.

1. Demostreu que les unitats de A són els elements de norma 1: $A^* = \{\alpha \in A : N(\alpha) = 1\}$ i digueu quines són aquestes unitats.
2. Demostreu que els únics enters $y \in \mathbb{Z}$ per als quals $y+\sqrt{-2}$ és el cub d'algun element de A són $y = \pm 5$.
3. Sigui y un enter senar. Calculeu el màxim comú divisor a A dels elements $y + \sqrt{-2}$ i $y - \sqrt{-2}$.
4. Demostreu, argumentat cada pas, que les úniques solucions de l'equació $Y^2 = X^3-2$ a l'anell $\mathbb{Z}$ dels nombres enters són $(X, Y) = (3, 5)$ i $(3, -5)$.

Solució:

1. Si α és invertible i β és el seu invers aleshores $\alpha\beta = 1 \Rightarrow N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1 \Rightarrow N(\alpha) = N(\beta) = 1$. Recíprocament, si $\alpha = a + b\sqrt{-2}$ té norma $N(\alpha) = 1$ aleshores agafant $\beta = a - b\sqrt{-2}$ es té $1 = N(\alpha) = a^2 + 2b^2 = \alpha\beta$ i per tant β és l'invers de α. Es unitats es troben resolent l'equació $a^2 + 2b^2 = 1$ a $\mathbb{Z}$, que clarament té com a úniques solucions $(a, b) = (\pm 1, 0)$ i per tant les unitats són $A^* = \{\pm 1\}$.
2. Sigui $y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2}$. Igualant les parts imaginàries s'obté $1 = b(3a^2 - 2b^2)$ que té com a úniques solucions $(a, b) = (\pm 1, 1)$. Per tant la part real és $y = a(a^2 - 6b^2) = \pm 5$.

3. Si $\alpha \mid \beta$ a l'anell A aleshores $N(\alpha) \mid N(\beta)$ a $\mathbb{Z}$. Tots dos elements $y+\sqrt{-2}$ i $y-\sqrt{-2}$ tenen norma y^2+2, i per tant tot divisor seu $a+b\sqrt{-2}$ té norma a^2+2b^2 un divisor de y^2+2. Per altra banda, tot divisor comú divideix també la seva diferència, que és $2\sqrt{-2}$, i per tant la seva norma a^2+2b^2 divideix $N(2\sqrt{-2})=8$. Així, la norma a^2+2b^2 divideix tant y^2+2, que és un nombre senar, com 8 i ha de dividir el màxim comú divisor d'aquests dos nombres, que és 1. Es dedueix que $a^2+2b^2=1$ i, per tant, que els únics divisors comuns són $a+b\sqrt{-2}=\pm 1$, que són les unitats de l'anell $\mathbb{Z}[\sqrt{-2}]$. Els dos elements $y+\sqrt{-2}$ i $y-\sqrt{-2}$ tenen màxim comú divisor 1: són relativament primers.

4. Tota solució (x,y) de l'equació dóna una identitat $y^2+2=x^3$ a $\mathbb{Z}$, la qual dóna la identitat $(y+\sqrt{-2})(y-\sqrt{-2})=x^3$ a l'anell A. Observi's que l'enter y ha de ser senar ja que si fos parell aleshores de la igualtat $y^2+2=x^3$ es deduiria que x també és parell i, per tant, com que tant y^2 com x^3 serien divisibles per 4, 2 també ho seria.

   L'anell A és Euclidià i, per tant factorial. Considerant la descomposició en primers de l'anell A dels tres elements $y+\sqrt{-2}$, $y-\sqrt{-2}$ i x que apareixen en aquesta igualtat. Tot primer apareix a x^3 un nombre de vegades múltiple de 3; com que els dos elements $y+\sqrt{-2}$ i $y-\sqrt{-2}$ són relativament primers per l'apartat anterior, tot factor primer de x és factor només de l'un o de l'altre, però no de tots dos. Per tant, tots els factors primers d'aquests nombres apareixen amb el mateix exponent que a x^3, que és múltiple de 3. Es dedueix que $y+\sqrt{-2}=\varepsilon\pi_1^{3\alpha_1}\cdots\pi_r^{3\alpha_r}$ per a alguna unitat $\varepsilon\in A^*$ i primers $\pi_1,\ldots,\pi_r$ de A; com que $\varepsilon=\pm 1$ és $\varepsilon=\varepsilon^3$ i, per tant, es té $y+\sqrt{-2}=(\varepsilon\pi_1\cdots\pi_r)^3$ és el cub d'algun element de l'anell A.

   Per l'apartat 1 el nombre y ha de ser ± 5 i, per tant, les úniques solucions possibles de l'equació $Y^2=X^3-2$ tenen aquest valor de Y. Per a aquests valors de Y efectivament hi ha solució, amb $X=3$ i, per tant, les solucions són les dues donades a l'enunciat: $(3,5)$ i $(3,-5)$.

Problema 3. Sigui K un cos i $E=K(\alpha)$ una extensió simple de grau n.

1. Demostreu que si n és senar aleshores $K(\alpha^2)=K(\alpha)$.
2. Sigui $K=\mathbb{Q}$ i $\mathrm{Irr}(\alpha,\mathbb{Q};X)=X^3-2X-2\in\mathbb{Q}[X]$. Calculeu $\mathrm{Irr}(\alpha^2,\mathbb{Q};X)$.
3. Demostreu que si $n=2m$ és parell aleshores $K(\alpha^2)\neq K(\alpha)$ si, i només si, $a_{2k+1}=0$ per a tot $0\leqslant k<m$, on $\mathrm{Irr}(\alpha,K;X)=a_0+a_1X+\cdots+a_{n-1}X^{n-1}+X^n$.
4. Siguin r i s enters relativament primers. Demostreu que per a tot $a\in K$ el polinomi $X^{rs}-a$ és irreductible a $K[X]$ si, i només si, ho són els polinomis X^r-a i X^s-a.

Solució:

1. Es té una inclusió d'extensions $K(\alpha^2)\subseteq K(\alpha)$. Per la multiplicativitat dels graus:

$$n=[K(\alpha):K]=[K(\alpha):K(\alpha^2)][K(\alpha^2):K].$$

   Com que α és arrel del polinomi de segon grau $X^2-\alpha^2\in K(\alpha^2)[X]$ el grau de l'extensió $[K(\alpha):K(\alpha^2)]$ només pot ser 1 o 2. No pot ser 2 ja que aquest grau divideix n, que per hipòtesi és senar. Per tant ha de ser 1. Això vol dir que totes dues extensions coincideixen: $K(\alpha^2)=K(\alpha)$.

ALTERNATIVA: Sigui $a_0+a_1X+\cdots+a_nX^n$ el polinomi irreductible amb $n=2k+1$ senar i $a_n=1$ ja que ha de ser mònic. Separant els termes d'índex parell i senar i traient factor comú d'α en aquests segons es té

$$(a_0+a_2\alpha^2+a_4\alpha^4+\cdots+a_{2k}\alpha^{2k})+\alpha(a_1+a_3\alpha^2+\cdots+a_{2k-1}\alpha^{2(k-1)}+1\alpha^{2k})=0$$

L'expressió $a_1+a_3\alpha^2+\cdots+\alpha^{2k}$ no pot donar zero ja que és un polinomi no nul de grau $2k<n$ (el coeficient de X^{2k} és 1) avaluat en α, que és un element de grau n. Per tant aïllant α es té

$$\alpha=-\frac{a_0+a_2(\alpha^2)+a_4(\alpha^2)^2+\cdots+a_{2k}(\alpha^2)^k}{a_1+a_3(\alpha^2)+\cdots+a_{2k-1}(\alpha^2)^{k-1}+(\alpha^2)^k},$$

que expressa α com un quocient de polinomis a coeficients en K avaluats en α^2. Per tant $\alpha\in K(\alpha^2)\Rightarrow K(\alpha)\subseteq K(\alpha^2)$.

2. Per l'apartat anterior α^2 també té grau 3 sobre $\mathbb{Q}$ i per tant el seu polinomi irreductible té grau 3. Fent servir el polinomi irreductible de α es té:

$$\alpha^3-2\alpha-2=0\Rightarrow\alpha^3-2\alpha=2\Rightarrow(\alpha^3-2\alpha)^2=\alpha^6+4\alpha^2-4\alpha^4=4$$

i es dedueix que α^2 és arrel del polinomi X^3-4X^2+4X-4, que com que és de grau 3 és el polinomi irreductible.

ALTERNATIVA: Del polinomi irreductible de α es dedueix que $\alpha=\frac{2}{\alpha^2-2}$. Substituint aquesta expressió en el polinomi irreductible de α i multiplicant per $(\alpha^2-2)^3$ s'arriba a la mateixa igualtat que abans.

ALTERNATIVA: El polinomi irreductible de α^2 ha de ser de la forma $\mathrm{Irr}(\alpha^2,\mathbb{Q};X)=X^3+aX^2+bX+c$ amb $a,b,c\in\mathbb{Q}$. Aleshores $\alpha^6+a\alpha^4+b\alpha^2+c=0$. Tenint en compte que $\alpha^3-2\alpha-2=0\Rightarrow\alpha^3=2\alpha+2$ és fàcil escriure les potències de α en la base $1,\alpha,\alpha^2$ de $\mathbb{Q}(\alpha)/\mathbb{Q}$ i s'obté $\alpha^4=\alpha\alpha^3=\alpha(2\alpha+2)=2\alpha+2\alpha^2$ i $\alpha^6=\alpha^3\alpha^3=\alpha^3(2\alpha+2)=2\alpha^4+2\alpha^3=4\alpha+4\alpha^2+4\alpha+4=4+8\alpha+4\alpha^2$. Aleshores a partir del polinomi irreductible de α^2 i tenint en compte que $1,\alpha,\alpha^2$ són una $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$ s'obté:

$$\begin{aligned}&\alpha^6+a\alpha^4+b\alpha^2+c=4+8\alpha+4\alpha^2+2a\alpha+2a\alpha^2+b\alpha^2+c\\&=(4+c)+(8+2a)\alpha+(4+2a+b)\alpha^2=0\Leftrightarrow 4+c=8+2a=4+2a+b=0.\end{aligned}$$

La solució d'aquestes equacions és $(a,b,c)=(-4,4,-4)$ i, per tant,

$$\mathrm{Irr}(\alpha^2,\mathbb{Q};X)=X^3-4X^2+4X-4.$$

3. Tal com s'ha vist al primer apartat els cossos $K(\alpha^2)$ i $K(\alpha)$ són diferents si, i només si, l'extensió $K(\alpha)/K(\alpha^2)$ té grau 2, que equival què l'extensió $K(\alpha^2)/K$ tingui grau $m=n/2$; o sigui, a què l'element α^2 tingui grau m sobre $\mathbb{Q}$. Si tots els coeficients d'índex senar són zero aleshores

$$\mathrm{Irr}(\alpha,K;X)=a_0+a_2X^2+a_4X^2+\cdots+a_{2m-2}X^{2m-2}+X^{2m}.$$

Per tant si $\beta=\alpha^2$ es té

$$a_0+\alpha^2+a_4\alpha^4+\cdots+a_{2m-2}\alpha^{2m-2}+\alpha^{2m}=0\Rightarrow a_0+\beta+a_4\beta^2+\cdots+a_{2m-2}\beta^{m-1}+\beta^m=0$$

i α^2 és arrel d'un polinomi de grau $m = n/2$ i el seu grau ha de ser m. Recíprocament, si α^2 té grau m sobre $\mathbb{Q}$ és arrel d'un polinomi $b_0 + b_1X + \cdots + b_mX^m$ de grau m i, per tant,

$$b_0 + b_1\alpha^2 + b_2\alpha^4 + \cdots + b_{m-1}\alpha^{2m-2} + \alpha^{2m} = 0.$$

Això vol dir que α és arrel del polinomi mònic de grau $2m = n$

$$b_0 + b_1X^2 + b_2X^4 + \cdots + b_{m-1}X^{2m-2} + X^{2m}.$$

Com que α té grau n sobre $\mathbb{Q}$ aquest polinomi (mònic) ha de ser el seu polinomi irreductible $a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + X^n$. Per tant els coeficients a_{2k} d'índex parell són els b_k i els a_{2k+1} d'índex senar són tots zero.

ALTERNATIVA: Raonant com a la solució alternativa del primer apartat es veu que si $a_{2k+1} \neq 0$ per a algun índex senar $2k+1$ aleshores α es pot posar com a quocient de polinomis a coeficients en K avaluats en α^2 *amb denominador* $\neq 0$. Aquesta condició de que el denominador sigui $\neq 0$, que és essencial, depèn d'una banda de què α té grau n i al denominador apareix un polinomi de grau estrictament inferior, i també de què hi hagi algun coeficient a_{2k+1} que sigui $\neq 0$.

4. Suposi's que el polinomi $X^r - a$ és reductible i sigui $X^r - a = f(X)g(X)$ una descomposició no trivial. Aleshores $X^{rs} - a = (X^s)^r - a = f(X^s)g(X^s)$ és una descomposició no trivial i el polinomi $X^{rs} - a$ també és reductible. Anàlogament si $X^s - a$ és reductible $X^{rs} - a$ també ho és.

   Suposi's que tots dos polinomis $X^r - a$ i $X^s - a$ són irreductibles. Sigui α una arrel del polinomi $X^{rs} - a$. Aleshores α^s és una arrel de $X^r - a$ i, per ser irreductible, es té $[K(\alpha^s) : K] = r$. Anàlogament es veu que $[K(\alpha^r) : K] = s$. Com que $K(\alpha^r)$ i $K(\alpha^s)$ són tots dos subcossos de $K(\alpha)$, per multiplicativitat dels graus $[K(\alpha) : K]$ es divideix tant per r com per s. Com que aquests nombres són relativament primers s'ha de dividir pel seu producte rs, i això assegura que polinomi $X^{rs} - a$ és irreductible.

   ULL! Les arrels s'han d'agafar bé. En general no es pot dir que $K(\sqrt[r]{a}) \subseteq K(\sqrt[rs]{a})$ sense especificar de quines arrels es parla. ja que d'arrels n-èsimes d'un element d'un cos n'hi ha en general n de diferents i el fet d'adjuntar-ne una no vol dir que es tinguin automàticament totes: per exemple a $\mathbb{Q}$ en adjuntar l'arrel real $\sqrt[11]{2}$ el cos $\mathbb{Q}(\sqrt[11]{2})$ només conté aquesta arrel però no cap de les altres 10 arrels onzenes $e^{2\pi i/11}\sqrt[11]{2}$. Així, si $\alpha = \sqrt[rs]{a}$ és una arrel fixada de $X^{rs} - a$ el cos $K(\alpha)$ conté α^s, que és una de les r arrels r-èsimes de a concreta, però pot no contenir les altres $r - 1$.