

Facultat de Matemàtiques i Estadística
Examen extraordinari d'Estructures Algebraiques
6 de juliol de 2017

Problema 1. Sigui G un grup simple no abelià d'ordre divisible per un primer p . Demostreu que si k és el nombre de p -subgrups de Sylow de G aleshores G és isomorf a un subgrup de \mathfrak{S}_k .

Deduïu que no hi ha grups simples d'ordres 12, 24, 36, 48, 72, 80 ni 96.

SOLUCIÓ: Sigui X el conjunt dels p -subgrups de Sylow de G , que té k elements. Ha de ser $k > 1$ ja que si $k = 1$ el grup simple G seria un p -grup i l'únic p -grup simple és el grup cíclic d'ordre p , que és abelià. Com que tots els p -subgrups de Sylow són conjugats, el grup G opera transitivament per conjugació en el conjunt X . Aquesta acció dona un homomorfisme no trivial $G \rightarrow \text{Perm}(X) \simeq \mathfrak{S}_k$ que, per ser G simple, ha de tenir nucli trivial. Pel teorema d'isomorfisme es dedueix que G és isomorf a un subgrup de \mathfrak{S}_k .

Tot subgrup de \mathfrak{S}_k té ordre dividint $k!$. Si un grup amb $|G| = 12, 24, 48$ o 96 fos simple el nombre de 2-Sylow seria 3 i $|G| \nmid 6 = |\mathfrak{S}_3|$. Si un grup amb $|G| = 36$ o 72 fos simple el nombre de 3-Sylow seria 4 i $|G| \nmid 24 = |\mathfrak{S}_4|$. Si un grup amb $|G| = 80$ fos simple el nombre de 2-Sylow seria 5 i $80 \nmid 120 = |\mathfrak{S}_5|$.

Problema 2. Sigui \mathbb{F}_q un cos finit de q elements i sigui A un anell íntegre infinit.

1. Doneu un polinomi $f(X) \in \mathbb{F}_q[X]$ diferent de zero tal que $f(a) = 0$ per a tot $a \in \mathbb{F}_q$.
2. Doneu un polinomi $f(X_1, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n]$ diferent del polinomi zero tal que $f(a_1, \dots, a_n) = 0$ per a tota n -tupla $(a_1, \dots, a_n) \in \mathbb{F}_q^n$.
INDICACIÓ: inspireu-vos en l'apartat anterior.
3. Demostreu que l'únic polinomi $f(X) \in A[X]$ tal que $f(a) = 0$ per a tot $a \in A$ és el polinomi zero.
4. Demostreu que l'únic polinomi $f(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$ tal que $f(a_1, \dots, a_n) = 0$ per a tota n -tupla $(a_1, \dots, a_n) \in A^n$ és el polinomi zero.
INDICACIÓ: feu servir l'apartat anterior.
5. Doneu un anell B de cardinal infinit i un polinomi no nul $f(X) \in B[X]$ tal que $f(a) = 0$ per a tot $a \in B$.
INDICACIÓ: Agafeu un producte cartesià d'infinites còpies d'un anell finit.

SOLUCIÓ:

1. $F(X) = X^p - X$ s'anul·la en tots els elements a de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ gràcies al petit teorema de Fermat: $a^p \equiv a \pmod{p}$ per a tot $a \in \mathbb{Z}$.
2. Inspirant-se en l'exemple anterior es pot agafar com a $f(X_1, \dots, X_n)$ qualsevol múltiple no nul d'un polinomi $X_i^p - X_i$ per a alguna de les variables i ; per exemple aquest polinomi mateix, o qualsevol combinació lineal d'aquests polinomis.
3. Tot anell íntegre està contingut en algun cos (per exemple el seu cos de fraccions). Sigui K un cos que conté A . Tot polinomi $f(X) \in A[X]$ es pot veure també com un polinomi amb coeficients a K , i, com tot polinomi a coeficients en un cos, si és

no nul pot tenir només un nombre finit d'arrels $a \in A \subseteq K$. Si A és infinit no tots els seus elements poden ser arrels d'un polinomi no nul. Per tant si $f(a) = 0$ per a tot $a \in A$ ha de ser $f = 0$.

4. Inducció sobre el nombre n de variables. Si $n = 1$ l'apartat anterior diu que l'enunciat es compleix. Suposi's demostrat fins a un $n \geq 1$. Tot polinomi en $n + 1$ variables $f(X_1, \dots, X_n, X_{n+1})$ és de la forma

$$f(X_1, \dots, X_n, X_{n+1}) = \sum_{k=0}^d f_k(X_1, \dots, X_n) X_{n+1}^k, \quad f_k(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$$

on k és el grau de f en la variable X_{n+1} . Sigui $(a_1, \dots, a_n) \in A^n$ una n -tupla qualsevol. En substituir les variables X_i pels valors a_i el polinomi f es converteix en un polinomi en una variable $f(a_1, \dots, a_n, X_{n+1})$ amb coeficients $f_i(a_1, \dots, a_n) \in A$. La hipòtesi assegura que aquest polinomi s'anul·la en substituir la variable X_{n+1} per cada element $a \in A$ i, per l'apartat anterior, això vol dir que és el polinomi zero: tots els coeficients són zero. Per tant, per a cada índex i es té $f_i(a_1, \dots, a_n) = 0$ per a tota n -tupla d'elements de A i, per hipòtesi d'inducció això implica que cada polinomi $f_i(X_1, \dots, X_n)$ és el polinomi zero. Per tant f és el polinomi zero.

5. Es considera l'anell $A = \prod_{n=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$, format per les successions $a = (a_1, a_2, a_3, \dots)$ d'elements $a \in \mathbb{Z}/2\mathbb{Z}$ amb la suma i producte component a component. Com que a $\mathbb{Z}/2\mathbb{Z}$ el quadrat de tot element coincideix amb ell mateix, es té $a^2 = a$ per a tot $a \in A$ i, per tant, tots els infinits elements de A són arrels del polinomi de segon grau $X^2 - X \in A[X]$.

Problema 3. Trobeu les relacions d'inclusió que hi ha entre els cossos $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(i, \sqrt{3})$, $\mathbb{Q}(\sqrt{-3} - \sqrt{3})$ i $\mathbb{Q}(i + \sqrt{-3})$.

SOLUCIÓ: Les extensions $\mathbb{Q}(\sqrt{3})$ i $\mathbb{Q}(\sqrt{-3})$ són extensions de grau 2 diferents, i per tant cap de les dues està continguda en l'altra.

Les altres tres extensions són totes tres de grau 4 i són iguals. És a dir, els nombres $\alpha = \sqrt{-3} - \sqrt{3}$ i $\beta = i + \sqrt{-3}$ són tots dos elements primitius de l'extensió $K = \mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(i, \sqrt{-3}) = \mathbb{Q}(\sqrt{-3}, \sqrt{3})$. En efecte, està clar que $\alpha \in K$ i $\beta \in K$.

D'altra banda es té que $\alpha(\sqrt{-3} + \sqrt{3}) = -3 - 3 = -6 \Rightarrow \sqrt{-3} + \sqrt{3} = -\frac{6}{\alpha}$. Per tant, $\sqrt{-3} = \frac{1}{2}(\alpha - \frac{6}{\alpha})$ i $\sqrt{3} = \frac{1}{2}(-\alpha - \frac{6}{\alpha})$ i es dedueix que $K \subseteq \mathbb{Q}(\alpha)$. Una altra manera d'expressar $\sqrt{-3}$ i $\sqrt{3}$ en funció de α és partir de la igualtat $\alpha + \sqrt{3} = \sqrt{-3}$, elevar al quadrat $\alpha^2 + 2\alpha\sqrt{3} + 3 = -3$, i obtenir $\sqrt{3} = (-6 - \alpha^2)/(2\alpha) \Rightarrow \sqrt{3} = \frac{12}{\alpha} - \frac{6}{\alpha} - \alpha$, i a partir d'aquí obtenir una expressió per a $\sqrt{-3} = \alpha + \sqrt{3}$.

Anàlogament, $\beta(i - \sqrt{-3}) = -1 + 3 = 2 \Rightarrow i - \sqrt{-3} = \frac{2}{\beta}$. Per tant, $i = \frac{1}{2}(\beta + \frac{2}{\beta})$ i $\sqrt{-3} = \frac{1}{2}(\beta - \frac{2}{\beta})$, i també $K \subseteq \mathbb{Q}(\beta)$.

Totes dues extensions quadràtiques estan clarament contingudes en aquesta extensió de grau 4.