

Llicenciatura de Matemàtiques FME  
Examen parcial d'Àlgebra Abstracta  
9 de novembre de 2007

**Problema 1.** Al conjunt producte cartesià  $G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$  es defineix

$$(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 + 5^{x_1}y_2)$$

1. Demostreu que l'operació  $\star$  està ben definida al conjunt  $G$ .
2. Demostreu que  $G$ , amb aquesta operació, és un grup.
3. Comproveu que el grup  $G$  és un grup no abelià d'ordre 55 i doneu un exemple de grup no abelià d'ordre 22.
4. Demostreu que tot grup d'ordre 33 o 77 és cíclic.

SOLUCIÓ: (1.) S'ha de veure que el resultat de la operació no depèn dels representants de  $\mathbb{Z}/5\mathbb{Z}$  i de  $\mathbb{Z}/11\mathbb{Z}$  escollits. La primera coordenada  $x_1 + x_2$  és una suma d'elements de  $\mathbb{Z}/5\mathbb{Z}$  i no porta cap problema. A la segona coordenada  $y_1 + 5^{x_1}y_2$  s'ha de veure que el nombre  $5^{x_1} \in \mathbb{Z}/11\mathbb{Z}$  no depèn de l'enter  $x_1$  que representa un element de  $\mathbb{Z}/5\mathbb{Z}$ , o sigui que  $5^{x_1} \equiv 5^{x_1+5k} \pmod{11}$  per a tot enter  $k \in \mathbb{Z}$ , i això és equivalent a que sigui  $5^5 \equiv 1 \pmod{11}$ , el qual és cert:

$$5^2 = 25 \equiv 3 \pmod{11}, \quad 5^3 = 5 \cdot 5^2 \equiv 5 \cdot 3 = 15 \equiv 4 \pmod{11}, \quad 5^5 = 5^2 \cdot 5^3 \equiv 3 \cdot 4 = 12 \equiv 1 \pmod{11}.$$

(2.) S'ha de comprovar que la operació és associativa, té element neutre i tot element té invers. Associativa:

$$\begin{aligned} ((x_1, y_1) \star (x_2, y_2)) \star (x_3, y_3) &= (x_1 + x_2, y_1 + 5^{x_1}y_2) \star (x_3, y_3) \\ &= ((x_1 + x_2) + x_3, (y_1 + 5^{x_1}y_2) + 5^{x_1+x_2}y_3) = (x_1 + x_2 + x_3, y_1 + 5^{x_1}(y_2 + 5^{x_2}y_3)) \\ &= (x_1, y_1) \star (x_2 + x_3, y_2 + 5^{x_2}y_3) = (x_1, y_1) \star ((x_2, y_2) \star (x_3, y_3)) \end{aligned}$$

L'element neutre és  $(0, 0)$  ja que

$$(x, y) \star (0, 0) = (x + 0, y + 5^x 0) = (x, y) = (0 + x, 0 + 5^0 y) = (0, 0) \star (x, y).$$

L'invers d'un element  $(x, y)$  és l'element  $(-x, -5^{-x}y) = (4x, 2y) \in G$  ja que

$$\begin{aligned} (x, y) \star (-x, -5^{-x}y) &= (x - x, y + 5^x(-5^{-x}y)) = (0, y - 5^{x-x}y) = (0, 0) \\ &= (-x + x, -5^{-x}y + 5^{-x}y) = (-x, -5^{-x}y) \star (x, y). \end{aligned}$$

(3.) El conjunt  $G$  és el producte cartesià de dos conjunts d'ordres 5 i 11 i, per tant, té ordre 55. Això vol dir que el grup  $G$ , definit a partir d'aquest conjunt, té ordre 55. El grup  $G$  és no abelià ja que no tot parell d'elements commuten. Per exemple:

$$(0, 1) \star (1, 0) = (1, 1 + 5^0 0) = (1, 1) \neq (1, 5) = (1, 0 + 5^1 1) = (1, 0) \star (0, 1)$$

ja que  $1 \not\equiv 5 \pmod{11}$ .

Un exemple de grup d'ordre 22 no abelià és el grup diedral  $D_{22}$  (de fet, és l'únic grup no abelià d'aquest ordre, llevat d'isomorfisme).

(4.) Sigui  $G$  un grup d'ordre 33. El nombre  $n_3$  de 3-Sylows és  $\equiv 1 \pmod{3}$  i divideix 11, per tant, com que  $11 \not\equiv 1 \pmod{3}$  és igual a 1. El nombre  $n_{11}$  de 11-Sylows és  $\equiv 1 \pmod{11}$  i divideix 3, per tant

ha de ser també igual a 1. Així,  $G$  té un únic 3-SyLOW  $H_3$  i un únic 11-SyLOW  $H_{11}$ , que, com que tots els  $p$ -SyLows són conjugats, són subgrups normals de  $G$ .

Si un grup té tots els  $p$ -SyLows normals aleshores és el seu producte directe. En el nostre cas això vol dir que  $G \simeq H_3 \times H_{11}$ . Els grups  $H_3$  i  $H_{11}$  tenen nombre d'elements primer i per tant són cíclics d'ordres 3 i 11, respectivament, i el seu producte serà també cíclic, gràcies al teorema xinès.

Sense fer servir el producte directe: es fa operar  $H_{11}$  sobre  $H_3$  per conjugació (com que  $H_3$  és normal, aquesta acció està ben definida). L'estabilitzador de cada element de  $H_3$  és un subgrup de  $H_{11}$ , que ha de tenir un o onze elements. Com que l'índex d'aquest subgrup és el nombre d'elements de l'òrbita, i  $H_3$  només té tres elements, la òrbita ha de tenir necessàriament un sol element i el subgrup estabilitzador és el total. Per tant, cada element de  $H_{11}$  commuta amb cada element de  $H_3$ . Com que  $G = H_3 \cdot H_{11}$  (el producte dels dos subgrups és un grup perquè són normals, i és el total ja que el seu ordre divideix 33 i és més gran que 11), i els elements de l'un commuten amb els de l'altre, el grup és commutatiu. L'únic grup commutatiu de 33 elements és el cíclic.

El cas del grup de 77 elements es fa exactament igual.

El motiu pel qual hi ha grups no abelians d'ordres  $2 \cdot 11$  i  $5 \cdot 11$  i en canvi no n'hi ha d'ordres  $3 \cdot 11$  ni  $7 \cdot 11$  és que  $11 \equiv 1 \pmod{2}$  i  $11 \equiv 1 \pmod{5}$  i, en canvi,  $11 \not\equiv 1 \pmod{3}$  i  $11 \not\equiv 1 \pmod{7}$ . En general, si  $p, q$  són dos primers diferents amb  $p < q$  tals que  $q \not\equiv 1 \pmod{p}$  tot grup d'ordre  $pq$  és abelià (i, per tant, cíclic). Es demostra exactament igual que el cas particular de  $pq = 33$  que s'acaba de fer. Si, en canvi, és  $q \equiv 1 \pmod{p}$  aleshores existeix un grup no abelià d'ordre  $pq$ , que es pot construir de manera semblant a com s'ha fet en l'apartat 1. Es tria un element  $a \in (\mathbb{Z}/q\mathbb{Z})^*$  que tingui ordre  $p$  (n'hi ha algun perquè  $(\mathbb{Z}/q\mathbb{Z})^*$  és un grup cíclic d'ordre  $q-1$  i  $p$  divideix aquest ordre) i es defineix al conjunt producte cartesià  $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$  la operació

$$(x_1, x_2) \star (y_1, y_2) = (x_1 + x_2, y_1 + a^{x_1} x_2),$$

que està ben definida i dóna al conjunt  $G$  estructura de grup no commutatiu (totes aquestes afirmacions es comproven igual que als apartats 1., 2. i 3.).

**Problema 2.** Calculeu tots els  $p$ -subgrups de SyLOW del grup simètric  $S_5$ .

SOLUCIÓ: Atès que  $|S_5| = 5! = 8 \cdot 3 \cdot 5$  hi ha 2-SyLows (d'ordre 8), 3-SyLows (d'ordre 3) i 5-SyLows (d'ordre 5). Tot i que no cal per fer el problema, els resultats sobre el nombre de SyLows ens poden ajudar. Es té

$$\begin{aligned} n_2 &\equiv 1 \pmod{2}, & n_2 &| 15 & \Rightarrow & n_2 &\in \{1, 3, 5, 15\} \\ n_3 &\equiv 1 \pmod{3}, & n_3 &| 40 & \Rightarrow & n_3 &\in \{1, 4, 10, 40\} \\ n_5 &\equiv 1 \pmod{5}, & n_5 &| 24 & \Rightarrow & n_5 &\in \{1, 6\} \end{aligned}$$

*Càlcul dels 3-SyLOW.* Són subgrups d'ordre 3, per tant, grups cíclics generats per un element d'ordre 3, que a  $S_5$  només pot ser un cicle de longitud 3. N'hi haurà tants com cicles de longitud 3 partit per 2, ja que a cada subgrup d'ordre 3 hi ha dos cicles diferents, a part de la identitat. Així, el nombre de 3-SyLows és

$$\frac{5 \cdot 4 \cdot 3 (\text{un per cada lloc del cicle})}{3 (\text{permutacions cicles donen el mateix cicle}) \cdot 2 (\text{a cada grup n'hi ha dos})} = 10.$$

Tots ells són conjugats d'un, per exemple, del grup  $\langle (1, 2, 3) \rangle$  generat pel cicle  $(1, 2, 3)$ .

*Càlcul dels 5-SyLOW.* Anàlogament al cas anterior, els 5-SyLows són subgrups d'ordre 5, per tant, grups cíclics generats per elements d'ordre 5, que han de ser cicles de longitud 5. El mateix tipus de càlcul que abans ens diu que n'hi ha

$$\frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{5 \cdot 4} = 6.$$

Tots ells són conjugats d'un, per exemple del grup generat pel cicle  $(1, 2, 3, 4, 5)$ .

*Càlcul dels 2-Sylow.* Els 2-Sylow tenen 8 elements i són tots conjugats d'un d'ells. El grup  $S_4$  conté tres subgrups isomorfs al grup diedral d'ordre 8, que són

$$\langle(1, 2, 3, 4), (1, 3)\rangle, \langle(1, 2, 4, 3), (1, 4)\rangle, \langle(1, 3, 2, 4), (1, 2)\rangle,$$

i com que  $S_5$  conté subgrups isomorfs a  $S_4$ , aleshores conté subgrups isomorfs al diedral. En particular, tots els seus 2-sylows són isomorfs al diedral (els grups conjugats són isomorfs).

Hi ha almenys cinc subgrups diferents a  $S_5$  que són isomorfs a  $S_4$ , que són els subgrups que deixen fix un dels cinc nombres 1, 2, 3, 4, 5, respectivament, diguem-los  $G_1, G_2, G_3, G_4, G_5$ . Els tres subgrups diedrals continguts en cadascun d'aquests cinc subgrups són diferents, ja que el diedral de  $S_4$  no deixen fix cap element i per tant els diedrals de  $G_i$  només deixen fix l'element  $i$  i cap altre element  $j$ , i per tant no poden coincidir amb cap dels tres diedrals de cap altre  $G_j$ . Així, el grup  $S_5$  conté al menys 15 diedrals d'ordre 8. Com que aquest és el màxim nombre possible de diedrals, ja els tenim tots.

Tots els 2-Sylows de  $S_5$  s'obtenen conjugant-ne un d'ells qualsevol.

**Problema 3.** Doneu exemples del següent, justificant tot el que calgui:

1. Un anell  $A$  i polinomis  $f, g \in A[X]$  tals que  $\deg(f) = \deg(g) = \deg(fg) = 2$ .
2. Dos anells  $A, B$  que no siguin cossos i dos cossos  $K, L$  amb  $A \subset K \subset B \subset L$ .
3. Dos polinomis  $f, g \in K[X, Y]$  que tinguin tots dos grau 2 en la variable  $X$  i grau 3 en la variable  $Y$  tals que  $f$  és primer i que  $g$  no ho és, on  $K$  és un cos qualsevol.
4. Un anell  $A$  i un ideal  $\mathfrak{a} \subseteq A$  que no sigui principal.
5. Dos polinomis  $f(X), g(X)$  de grau 3 irreductibles a l'anell  $\mathbb{Z}[X]$  tals que les seves reduccions  $\overline{f}(X), \overline{g}(X)$  mòdul 5 siguin l'una irreductible i l'altra reductible a l'anell  $\mathbb{F}_5[X]$ .
6. Un polinomi  $f(X, Y)$  de  $\mathbb{Z}[X, Y]$  de grau total 3 que sigui irreductible a  $\mathbb{Q}[X, Y]$  però no sigui primitiu ni a  $(\mathbb{Z}[X])[Y]$  ni a  $(\mathbb{Z}[Y])[X]$ .

SOLUCIÓ: (1.) Com que en un anell íntegre val la fórmula  $\deg(fg) = \deg f + \deg g$  és clar que l'anell no pot ser íntegre. Per exemple, en un anell no íntegre qualsevol  $A$ , si  $a, b \neq 0$  són elements amb  $ab = 0$  aleshores els polinomis  $f(X) = aX^2 + 1$  i  $g(X) = bX^2$  són de grau 2 i tenen  $fg(X) = abX^4 + bX^2 = bX^2$  també de grau 2. Es poden donar exemples més concrets es. Per exemple, a l'anell  $\mathbb{Z}/4\mathbb{Z}$  els polinomis  $f = 2X^2 + X + 1$  i  $g = f = 2X^2 + X + 1$  tenen  $fg = 4X^4 + 4X^3 + 5X^2 + 2X + 1 = X^2 + 2X + 1$ ; a  $\mathbb{Z}/6\mathbb{Z}$  els polinomis  $f = 2X^2$  i  $g = 3X^2 + 2$  tenen  $fg = 6X^4 + 4X^2 = 4X^2$ , etc.

(2.) Si  $k$  és un cos qualsevol, es pot posar

$$A = k[X], \quad K = k(X), \quad B = k(X)[Y], \quad L = k(X, Y).$$

Un altre exemple possible seria  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{Q}[\pi] \subset \mathbb{R}$ , fent servir que  $\pi$  és transcendent sobre  $\mathbb{Q}$ , o també  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{Q}[X] \subset \mathbb{Q}(X)$ , etc. Cap exemple on apareguin cossos finits pot funcionar, ja que un subanell d'un cos finit és sempre un cos (un anell íntegre finit és un cos).

(3.) Polinomi primer  $f(X, Y) = X^2 - Y^3$ . Justificació:  $K[X, Y] = (K[X])[Y]$  amb  $K[X]$  anell factorial. El polinomi  $f$ , com a polinomi en la variable  $Y$ , és de grau 3, té terme independent  $X^2$  i terme de grau màxim  $-1$ . Per tant és primitiu, i gràcies a l'estudi fet a teoria dels elements primers d'un anell de polinomis  $A[X]$  a coeficients en un anell factorial (basat en el lema de Gauss) sabem que la seva irreductibilitat a  $K[X][Y]$  equival a la irreductibilitat a  $K(X)[Y]$  (ara amb coeficients en un cos). Un polinomi de grau 3 a coeficients en un cos és irreductible si, i només si, no té arrels. Per Ruffini, les úniques arrels a  $K(X)$  d'aquest polinomi tenen numerador que divideix  $X^2$  i denominador que divideix

$-1$ , i per tant són polinomis de la forma  $a \in K$  o bé  $aX$  o  $aX^2$  amb  $a \in K^*$ , amb  $a \in K$ . Substituint a  $f$  es veu que  $f(X, a)$ ,  $f(X, aX)$  i  $f(X, aX^2)$  mai són zero (tenen graus 2, 3 i 6, respectivament). El mateix argument es pot aplicar mirant  $f$  com a element de  $(K[Y])[X]$ .

Un altre polinomi primer és  $f(X, Y) = X(X+1) + Y^3$ . Justificació:  $K[X, Y] = (K[X])[Y]$  amb  $K[X]$  anell factorial.  $X$  és un primer de l'anell  $K[X]$  i  $f$  és  $X$ -Eisenstein (també és  $(X+1)$ -Eisenstein).

Un polinomi no primer pot ser  $g(X, Y) = X^2Y^3 = (XY)(XY^2)$  o qualsevol cosa per l'estil.

(4.) Se n'han fet exemples, amb la justificació corresponent, a classe de problemes: l'ideal  $(X, Y)$  generat per  $X$  i  $Y$  a l'anell  $K[X, Y]$  no és principal, o l'ideal  $(2, X)$  generat per 2 i  $X$  a  $\mathbb{Z}[X]$  no és principal.

(5.) Els polinomis de grau 3 a coeficients en un cos són irreductibles si, i només si, no tenen arrels al cos.  $f(X) = X^3 + 2$  és irreductible a  $\mathbb{Z}[X]$  per ser primitiu i irreductible a  $\mathbb{Q}[X]$  (Eisenstein o Ruffini). La seva reducció mòdul 5 segueix sent irreductible ja que cap enter satisfà la congruència  $X^3 \equiv -2 \pmod{5}$  (es comprova: només s'ha de fer per 5 casos). El polinomi  $g(X) = X^3 + 2X + 2$  també és irreductible a  $\mathbb{Z}[X]$  (mateixos arguments) però la seva reducció mòdul 5 no ho és ja que  $X = 1$  és òbviament una arrel mòdul 5.

(6.) Qualsevol polinomi de la forma  $af(X, Y)$  amb un enter  $a \neq 0, \pm 1$  i  $f \in \mathbb{Z}[X, Y]$  un polinomi irreductible a  $\mathbb{Q}[X, Y]$  funciona. Per exemple,  $2X^3 + 2Y$  o també  $2X^3 + 4$ , etc. Els arguments per a la irreductibilitat de  $X^3 + Y$  o de  $X^3 + 2$  o de coses semblants són anàlegs als de la secció 3. i es basen en Ruffini o en Eisenstein.