ESTRUCTURES ALGEBRAIQUES

EXAMEN FINAL. 8 de gener de 2021

Problema 1. *(4 pts)*

a) *(0.5 pts)* Demostreu que el polinomi $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ és irreductible.

b) *(1 pt)* Sigui z una arrel de $f(x)$ en $\overline{\mathbb{F}_2}$ i sigui $\mathbb{F} = \mathbb{F}_2(z)$. Demostreu que $\mathbb{F}^* = \langle z \rangle$.

c) *(0.5 pts)* Considereu l'aplicació:

$$\begin{array}{ccc} \mathbb{Z}/32\mathbb{Z} \times \mathbb{F} & \longrightarrow & \mathbb{F} \\ (a, x) & \longrightarrow & a * x := x^{2^a}. \end{array}$$

Demostreu que l'aplicació anterior defineix una acció del grup additiu $\mathbb{Z}/32\mathbb{Z}$ sobre el cos $\mathbb{F}$.

d) *(0.75 pts)* Descriviu les òrbites de l'acció anterior.

e) *(0.5 pts)* Determineu el subgrup d'isotropia de z.

f) *(0.75 pts)* Demostreu que per a cada $a \in \mathbb{Z}/32\mathbb{Z}$ el conjunt $(F)^a = \{x \in \mathbb{F} : a * x = x\}$ és un subcòs de F. Identifiqueu el subòs $(F)^2$.

Problema 2. *(3.5 pts)*

a) *(1.5 pts)* Demostreu que, llevat d'isomorfisme hi ha un únic grup abeliá d'ordre 100 els elements del qual tenen tots ordre divisor de 10.

b) *(2 pts)* Determineu l'ordre maximal d'un element de S_5. Proveu que si $\sigma \in S_5$ és un element d'ordre maximal aleshores el centralitzador és $C_{S_5}(\sigma) = \langle \sigma \rangle$.

Problema 3. *(1.5 pts)* Sigui A un domini d'ideals principals, i sigui $f : M \longrightarrow N$ un isomorfisme entre dos A-mòduls M, N finitament generats. Denotem per $T(M), T(N)$ els submòduls de torsió respectius.

a) *(1 pt)* Demostreu que $f(T(M)) = T(N)$.

b) *(0.5 pts)* Demostreu que existeixen dos mòduls lliures M', N' del mateix rang tals que $M \simeq M' \oplus T(M)$ i $N \simeq N' \oplus T(N)$.

Problema 4. *(1 pt)* Responeu una de les tres qüestions següents- (No podeu triar una qüestió si és una de les que heu plantejat en el vostre treball.)

a) Digueu quins nombres reals cal construir per poder fer la quadratura del cercle i la duplicació del cub. Són constructibles amb regle i compàs? I amb origami? (Justifiqueu les vostres respostes.)

b) Doneu l'expansió p-àdica de $\frac{1}{2}$ a $\mathbb{Z}_7$ i $\mathbb{Z}_{11}$.

c) Sigui K un cos i $f(x) \in K[x]$ un polinomi de grau n. Proveu que els discriminats de $f(x)$ i $f(\beta x)$ satisfàn la relació següent: :

$$\Delta(f(\beta x)) = \beta^{n(n-1)} \Delta(f(x)).$$

ESTRUCTURES ALGEBRAIQUES

EXAMEN FINAL. 8 de gener de 2021

Problema 1.

a) Demostreu que el polinomi $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ és irreductible.

b) Sigui z una arrel de $f(x)$ en $\overline{\mathbb{F}_2}$ i sigui $\mathbb{F} = \mathbb{F}_2(z)$.

c) Demostreu que $\mathbb{F}^* = \langle z \rangle$.

d) Considereu l'aplicació:

$$\begin{array}{ccc} \mathbb{Z}/32\mathbb{Z} \times \mathbb{F} & \longrightarrow & \mathbb{F} \\ (a, x) & \longrightarrow & a * x := x^{2^a}. \end{array}$$

Demostreu que l'aplicació anterior defineix una acció del grup additiu $\mathbb{Z}/32\mathbb{Z}$ sobre el cos $\mathbb{F}$.

e) Descriviu les òrbites de l'acció anterior.

f) Determineu el subgrup d'isotropia de z.

g) Demostreu que per a cada $a \in \mathbb{Z}/32\mathbb{Z}$ el conjunt $(F)^a = \{x \in \mathbb{F} : a * x = x\}$ és un subcòs de F. Identifiqueu el subòs $(F)^2$.

Solució:

a) Si el polinomi fos reductible hauria de tenir un factor de grau 1 o 2. Com $f(0) = f(1) = 1$, no té factors lineals. Per altra banda, l'únic polinomi de grau 2 irreductible sobre $\mathbb{F}_2[x]$ és $x^2 + x + 1$, que no divideix $f(x)$.

b) El grau de l'extensió és $[\mathbb{F} : \mathbb{F}_2] = \deg f = 4$, així que $\mathbb{F}^*$ té 15 elements. L'ordre multiplicatiu de z només pot ser 1, 3, 5, o 15. Està clar que no és 1. Si $z^n = 1$, llavors $f \mid x^n - 1$ i per tant, no pot ser $n = 3$ perquÃ¨ $\deg f = 4$. Tampoc pot ser $n = 5$, perquÃ¨ $xf(x) \neq x^5 - 1 \neq (x+1)f(x)$.

c) Tenim que $0 * x = x^{2^0} = x$ per a tot $x \in \mathbb{F}$. Donats $a, b \in \mathbb{Z}/32\mathbb{Z}$ tenim

$$a * (b * x) = a * x^{2^b} = (x^{2^b})^{2^a} = x^{2^b 2^a} = x^{2^{a+b}} = (a+b) * x.$$

d) Per descriure les òrbites, el més fàcil és tenir en compte que, per l'apartat b), $\mathbb{F}^* = \{1, z, z^2, \ldots, z^{15}\}$. Calculem algunes potències de z:

$$\begin{array}{lll} z^{16} = z, & z^{24} = z^{16} z^8 = z^9, & z^{28} = z^{16} z^{12} = z^{13} \\ z^{56} = z^8 z^{48} = z^8 z^3 = z^{11}, & z^{112} = z^{22} = z^7, & z^{20} = z^{16} z^4 = z^5. \end{array}$$

Amb això veiem que les òrbites són

$$\begin{array}{ll} \{0\}, & \{1\}, \\ \{z, z^2, z^4, z^8\}, & \{z^3, z^6, z^9, z^{12}\}, \\ \{z^5, z^{10}\}, & \{z^7, z^{11}, z^{13}, z^{14}\}. \end{array}$$

e) Tenint en compte l'apartat anterior, el subgrup d'isotropia de z és el subgrup $\langle 4 \rangle$.

f) Atés que $\operatorname{char}\mathbb{F} = 2$, tenim que per a qualssevol $x, y \in \mathbb{F}$, $(x+y)^2 = x^2 + y^2$, i per tant $a*(x+y) = a*x + a*y$. Per altra banda, és evident que $a*(xy) = (a*x)(a*y)$ i $a*(x^{-1}) = (a*x)^{-1}$. Aquestes igualtats proven que si $x, y \in (F)^a$, llavors $x+y, xy, x^{-1} \in (F)^a$.

El el subòs $(F)^2$ està format pels elements $x \in \mathbb{F}$ tals que $x^4 = x$ i per tant és el subcòs de 4 elements que hi ha dins de $\mathbb{F}$, que és $\{0, 1, z^5, z^{10}\}$.

Problema 2.

a) Demostreu que, llevat d'isomorfisme hi ha un únic grup abeliá d'ordre 100 els elements del qual tenen tots ordre divisor de 10.

b) Determineu l'ordre maximal d'un element de S_5. Proveu que si $\sigma \in S_5$ és un element d'ordre maximal aleshores el centralitzador és $C_{S_5}(\sigma) = \langle\sigma\rangle$.

Solució: Solució:

a) Pel teorema de classificació, un grup abelià d'ordre 100 serà isomorf al producte cartesià d'un grup H_5 d'ordre 25 i un grup H_2 d'ordre 4. El primer pot ser isomorf a $\mathbb{Z}/25\mathbb{Z}$ o a $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ i el segon pot ser isomorf a $\mathbb{Z}/4\mathbb{Z}$ o a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Si H_5 té un element a d'ordre 25, aleshores $(a, 0)$ té ordre 25 a $H_5 \times H_2$. Si H_2 té un element b d'ordre 4, aleshores $(0, b)$ té ordre 4 a $H_5 \times H_2$.

Per tant, l'única possibilitat és $G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. En aquest grup tots els elements tenen ordre divisor de 10 perquè $10(x, y) = (10x, 10y) = (0, 0)$.

b) L'ordre d'un element de S_5 és el mínim comú múltiple de les longituds dels cicles disjunts en què descompon. Les descomposcions en cicles disjunts poden ser dels tipus següents (corresponenets a les particions de 5):

$$(5),\quad (4)(1),\quad (3)(2),\quad (3)(1)(1),\quad (2)(2)(1),\quad (2)(1)(1)(1),\quad (1)(1)1)(1)(1)$$

Els ordres corresponents són: $5, 4, 6, 3, 2, 2, 1$. Per tant, els elements d'ordre maximal són els que descomponen com a producte d'un cicle d'ordre 3 i una transposició, que tene ordre 6.

Sabem que el centralitzador $C_{S_5}(\sigma) = \{g \in S_5 : g\sigma g^{-1} = \sigma\} = \{g \in S_5 : g\sigma = \sigma g\}$ conté $\langle\sigma\rangle$. Per veure que són iguals només cal veure que el centralitzador té cardinal 6, o índex 20.

El centralitzador és el grup d'isoptropia de σ en l'acció per conjugació de S_5 sobre si mateix. Per tant, $[S_5 : C_{S_5}(\sigma)]$ és el cardinal de l'òrbita de σ, és a dir, el nombre de conjugats de σ. Atès que dos elements de S_5 són conjugats si, i només si, tenen el mateix tipus de descomposició en cicles disjunts, només cal comptar els elements de S_5 de la forma $(3)(2)$. Però com que un cop donat el cicle de longitud 3, la transposició queda determinada, només cal comptar els cicles de longitud 3 de S_5:

$$\frac{5 \cdot 4 \cdot 3}{3} = 20.$$

Problema 3. Sigui A un domini d'ideals principals, i sigui $f : M \longrightarrow N$ un isomorfisme entre dos A-mòduls M, N finitament generats. Denotem per $T(M), T(N)$ els submòduls de torsió respectius.

a) Demostreu que $f(T(M)) = T(N)$.

b) Demostreu que existeixen dos mòduls lliures M', N' del mateix rang tals que $M \simeq M' \oplus T(M)$ i $N \simeq N' \oplus T(N)$.

Solució:

a) Per definició, donat $m \in T(M)$ existeix $a \in A \setminus \{0\}$ tal que $am = 0$. Per tant,

$$af(m) = f(am) = f(0) = 0,$$

perquÃ¨ f és un morfisme de mòduls. Per tant $f(m) \in T(N)$ i deduim que $f(T(M)) \subseteq T(N)$.

Per altra banda, com que f és exhaustiu, donat $n \in T(N)$, existeix $m \in M$ tal que $f(m) = n$. Com que $n \in T(N)$, tenim $a \in A \setminus \{0\}$ tal que

$$0 = an = af(m) = f(am).$$

Com que f és també injectiu, $am = 0$. Per tant, $m \in T(M)$ i $T(N) \subseteq f(T(M))$. Això conclou la prova que $f(T(M)) = T(N)$.

b) Com que M i N són finitament generats i A és un domini d'ideals principals, $M/T(M)$ i $N/T(N)$ són A-mòduls lliures. Això implica $M/T(M) \simeq A^r$ i $N/T(N) \simeq A^s$. Ara bé, per la primera part de l'exercici, el nucli del morfisme exhaustiu

$$M \xrightarrow{f} N \longrightarrow N/T(N),$$

és precisament $T(M)$. Això implica que f dóna lloc a un isomorfisme $A^r \simeq M/T(M) \simeq N/T(N) \simeq A^s$ que implica $r = s$. Per tant $M' := M/T(M)$ i $N' := N/T(N)$ són mòduls lliures del mateix rang. Això conclou l'exercici, ja que

$$M \simeq M/T(M) \oplus T(M) = M' \oplus T(M), \qquad N \simeq N/T(N) \oplus T(N) = N' \oplus T(N).$$

Problema 4. Responeu una de les tres qüestions següents. (No podeu triar una qüestió si és una de les que heu plantejat en el vostre treball.)

a) Digueu quins nombres reals cal construir per poder fer la quadratura del cercle i la duplicació del cub. Són constructibles amb regle i compàs? I amb origami? (Justifiqueu les vostres respostes.)

b) Doneu l'expansió p-àdica de $\frac{1}{2}$ a $\mathbb{Z}_7$ i $\mathbb{Z}_{11}$.

c) Sigui K un cos i $f(x) \in K[x]$ un polinomi de grau n. Proveu que els discriminats de $f(x)$ i $f(\beta x)$ satisfàn la relació següent: :

$$\Delta(f(\beta x)) = \beta^{n(n-1)} \Delta(f(x)).$$