Àlex Batlle Casellas

3.28. Considerem a $\mathbb{Z}$ les operacions

$$a \oplus b = a + b - 6;$$

$$a \odot b = ab + \alpha(a+b) + 42,$$

on $\alpha \in \mathbb{Z}$.

1) **Comproveu que $(\mathbb{Z}, \oplus)$ és un grup commutatiu.**
Per ser un grup commutatiu, l'operació $\oplus$ ha de complir les propietats associativa i commutativa i ha de tenir element neutre i invers per tots els elements de $\mathbb{Z}$. Comprovem-ho:

- Associativa: comprovem que $\forall a, b \in \mathbb{Z},\ a \oplus (b \oplus c) = (a \oplus b) \oplus c = a \oplus b \oplus c$.

$$a \oplus (b \oplus c) = a + (b \oplus c) - 6 = a + (b + c - 6) - 6 =$$

$$(a + b - 6) + c - 6 = (a \oplus b) + c - 6 = (a \oplus b) \oplus c.\square$$

- Commutativa: comprovem que $\forall a, b \in \mathbb{Z},\ a \oplus b = b \oplus a$.

$$a \oplus b = a + b - 6 = b + a - 6 = b \oplus a.\square$$

- Existència del neutre: suposem que $\exists e \in \mathbb{Z} :\ a \oplus e = a$ i el trobem.

$$a \oplus e = a \iff a + e - 6 = a \iff e - 6 = 0 \iff e = 6.$$

En ser $\oplus$ commutativa, ens podem estalviar comprovar per l'altre costat.

- Existència de l'invers: suposem que $\exists a' \in \mathbb{Z} :\ a \oplus a' = e$ i el trobem.

$$a \oplus a' = e \iff a + a' - 6 = 6 \iff a' = 12 - a.$$

2) **Demostreu que l'operació $\odot$ és associativa si, i només si, $\alpha = -6$ o $\alpha = 7$.**
L'operació $\odot$ serà associativa quan $a \odot (b \odot c) = (a \odot b) \odot c = a \odot b \odot c$. Veiem què passa quan igualem les expressions per cada un dels costats de la tesi:

- $a \odot (b \odot c) = a(b \odot c) + \alpha(a + b \odot c) + 42 = a(bc + \alpha(b+c) + 42) + \alpha(a + bc + \alpha(b+c) + 42) + 42$
- $(a \odot b) \odot c = (a \odot b)c + \alpha(a \odot b + c) + 42 = (ab + \alpha(a+b) + 42)c + \alpha(ab + \alpha(a + b) + 42 + c) + 42$

En igualar,

$$a(bc + \alpha(b+c) + 42) + \alpha(a + bc + \alpha(b+c) + 42) + 42$$

$$= (ab + \alpha(a+b) + 42)c + \alpha(ab + \alpha(a+b) + 42 + c) + 42.$$

Treiem els 42 d'ambdós costats i desenvolupem els productes amb la distributivitat del producte sobre la suma usual:

$$abc + a\alpha b + a\alpha c + 42a + a\alpha + bc\alpha + \alpha^2 b + \alpha^2 c + 42\alpha =$$

$$abc + c\alpha a + c\alpha b + 42c + ab\alpha + \alpha^2 a + \alpha^2 b + 42\alpha + c\alpha.$$

Cancel·lant els termes iguals,

$$42a + a\alpha + c\alpha^2 = 42c + a\alpha^2 + c\alpha,$$

i ara reescrivint com una equació de segon grau en α queda:

$$(c - a)\alpha^2 + (a - c)\alpha + 42(a - c) = 0.$$

Aquesta equació la dividim entre $(c - a)$, que és diferent de zero ja que si $a = c$, $(a \odot b) \odot a = a \odot (b \odot a)$ si $\odot$ és commutativa. Ho podem veure ràpid:

$$a \odot b = ab + \alpha(a + b) + 42 = ba + \alpha(b + a) + 42 = b \odot a.$$

Per tant, com que $a \neq c$, dividim;

$$\alpha^2 - \alpha - 42 = 0,$$

i calculem les solucions amb la fórmula pel càlcul de les arrels dels polinomis de segon grau:

$$\alpha = \frac{1 \pm \sqrt{1 - 4(-42)}}{2}$$
$$\alpha_1 = -6 \qquad \alpha_2 = 7.$$

Per tant, seguint el curs de les implicacions i tal com volíem demostrar, $\odot$ només és associativa quan $\alpha = -6$ o $\alpha = 7$.$\square$

3) **Demostreu que l'operació $\odot$ té element neutre si, i només si, $\alpha = -6$ o $\alpha = 7$.**
Si existeix un element neutre, $\exists e \in \mathbb{Z} : a \odot e = a$. Per tant, ho escrivim:

$$a \odot e = ae + \alpha(a + e) + 42 = a.$$

Si el trobem, haurem demostrat que existeix. Per fer-ho, intentem resoldre l'equació:

$$a(e + \alpha) + e\alpha + 42 = a.$$

Com que estem utilitzant la suma i el producte usuals, la única solució possible es troba solucionant el sistema:

$$e + \alpha = 1$$
$$e\alpha + 42 = 0$$

D'aquí tenim $e = 1 - \alpha$ i $(1 - \alpha)\alpha + 42 = 0$. Aquesta equació ja la tenim solucionada (apartat 2) i per tant, veiem que e existeix només quan $\alpha = -6$ o $\alpha = 7$.$\square$

4) **Per a quins valors de α és $(\mathbb{Z}, \oplus, \odot)$ un anell?**
Per a que $(\mathbb{Z}, \oplus, \odot)$ sigui un anell necessitem que $(\mathbb{Z}, \oplus$ sigui grup abelià i que $\odot$ sigui associativa, tingui element neutre i sigui distributiva respecte $\oplus$. Com ja hem vist, $\oplus$ només és associativa i té neutre quan $\alpha = -6$ o $\alpha = 7$. Per ser distributiva, volem que $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$. Ho desenvolupem per ambdós costats:

(1) $a \odot (b \oplus c) = a(b \oplus c) + \alpha(a + b \oplus c) + 42 = ab + ac - 6a + \alpha(a + b + c - 6) + 42,$
(2) $(a \odot b) \oplus (a \odot c) = (ab + \alpha(a + b) + 42) \oplus (ac + \alpha(a + c) + 42) =$
$ab + ac + \alpha(a + b) + \alpha(a + c) + 42 + 42 - 6.$

Ara igualem ambdós resultats i veiem què li ha de passar a α:

$$ab + ac - 6a + \alpha(a + b + c - 6) + 42 = ab + ac + \alpha(a + b) + \alpha(a + c) + 42 + 42 - 6$$

$$-6a + a\alpha - 6\alpha = 2a\alpha + 36,$$

$$-a\alpha - 6\alpha = 6a + 36,$$

$$-\alpha(a + 6) = 6(a + 6) \implies \alpha = -6.$$

Per tant, $(\mathbb{Z}, \oplus, \odot)$ és un anell per $\alpha = -6$.

3.36. Considereu les permutacions de $\mathfrak{S}_5$ següents:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}$$

1) **Descompsoeu les tres permutacions en producte de cicles.**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1,3,4)(2,5).$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} = (1,5)(2,3,4).$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} = (1,3,4,5).$$

2) **Calculeu $\sigma\tau\rho$ i $\sigma\rho^2$.**

$$\sigma\tau\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}.$$

$$\sigma\rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}.$$

3) **Trobeu la signatura de τ i de ρ^{-1}.**
Es pot descomposar τ en tres transposicions:

$$\tau = (1,5)(2,3)(3,4),$$

i per tant $\mathscr{E}(\tau) = (-1)^3 = -1$.
Per descompondre ρ^{-1}, primer hem de trobar aquesta permutació. Seguint el recorregut de ρ, només cal intercanviar les files i reordenar per obtenir la inversa. Ho fem:

$$\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}.$$

Per tant, si ara descomposem ρ^{-1} en producte de transposicions en podem trobar la signatura:

$$\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} = (1,5,4,3).$$

Per tant, $\mathscr{E}(\rho^{-1}) = (-1)^1 = -1$.

3.39. **Demostra que si τ_1 i τ_2 són dues transposicions diferents, aleshores $\tau_1\tau_2$ és d'ordre 2 o 3.**

Si són dues transposicions diferents, això vol dir que $\tau_1 = (i, j) \neq \tau_2 = (k, l)$. Aleshores,

$$\tau_1 \cap \tau_2 = \begin{cases} \emptyset, & \text{si } \tau_1 \text{ i } \tau_2 \text{ no comparteixen cap element igual,} \\ \{j\}, & \text{ja que sense pèrdua de generalitat podem suposar que si} \\ & \tau_1 \text{ i } \tau_2 \text{ comparteixen un element aquest pot ser } j. \end{cases}$$

Si no comparteixen cap element, la composició de τ_1 i τ_2 és la següent:

$$\tau_1\tau_2 = (i, j)(k, l) = \begin{pmatrix} i & j & k & l \\ j & i & l & k \end{pmatrix},$$

que per definició té ordre igual al mínim comú múltiple dels ordres de ls transposicions composades (que són cicles disjunts). En aquest cas,

$$\operatorname{ord}(\tau_1\tau_2) = \operatorname{mcm}(\operatorname{ord}\tau_1, \operatorname{ord}\tau_2) = \operatorname{mcm}(2, 2) = 2.$$

En el cas que tinguin un element comú, suposem (sense pèrdua de generalitat) $j = k$ i en composar:

$$\tau_1\tau_2 = (i, j)(j, l) = \begin{pmatrix} i & j & l \\ j & l & i \end{pmatrix}$$

veiem que $\operatorname{ord}(\tau_1\tau_2) = 3$.

$\square$