$\mathscr{M}$athématiques $\mathcal{C}\,i\,\mathbf{R}^2$

— Riri —

a) Étant donné un corps $\mathbf{F}$, on munit l'ensemble $\mathbf{F}^3$ de la loi de composition

$$(a,\, b,\, c) \star (a',\, b',\, c') := (aa',\, ab' + bc',\, cc').$$

Montrer que $(\mathbf{F}^3,\, \star)$ est un monoïde et préciser quels sont ses éléments symétrisables.

On doit vérifier les deux propriétés :

- Associativité : pour $A = (a,\, b,\, c)$, $A' = (a',\, b',\, c')$, $A'' = (a'',\, b'',\, c'')$ trois éléments de $\mathbf{F}^3$, on a :

$$\begin{aligned}(A \star A') \star A'' &= (aa',\, ab' + bc',\, cc') \star (a'',\, b'',\, c'') \\ &= \big((aa')a'',\, (aa')b'' + (ab' + bc')c'',\, (cc')c''\big) \\ &= \big(a(a'a''),\, a(a'b'' + b'c'') + b(c'c''),\, c(c'c'')\big) \\ &= (a,\, b,\, c) \star (a'a'',\, a'b'' + b'c'',\, c'c'')\big) \\ &= A \star (A' \star A'') \checkmark\end{aligned}$$

- Existence d'un neutre : si on cherche les composantes $(x,\, y,\, z)$ de celui-ci, on voit qu'on doit avoir en particulier

$$\begin{cases} a = ax \\ b = ay + bz \\ c = cz \end{cases} \qquad \text{pour tous } a,\, b,\, c \in \mathbf{F},$$

ce qui force $x = z = 1$, $y = 0$. Avec ces valeurs, on vérifie qu'on a bien

$$(1,\, 0,\, 1) \star A = A = A \star (1,\, 0,\, 1) \qquad \text{pour tout } A \in \mathbf{F}^3.$$

Élements symétrisables : pour $A = (a,\, b,\, c) \in \mathbf{F}^3$, cherchons à résoudre l'équation $A \star (x,\, y,\, z) = (1,\, 0,\, 1)$, soit

$$\begin{cases} 1 = ax \\ 0 = ay + bz \\ 1 = cz \end{cases}$$

Les premières et troisièmes équations nous disent qu'on doit avoir $a, c \neq 0$ et $x = \frac{1}{a}$, $z = \frac{1}{c}$; la seconde nous donne alors $y = -\frac{b}{ac}$. Par ailleurs, on vérifie qu'avec ces valeurs on a également

$$(\tfrac{1}{a},\, -\tfrac{b}{ac},\, \tfrac{1}{c}) \star (a,\, b,\, c) = (1,\, 0,\, 1),$$

de sorte que l'on peut conclure :

$$(a,\, b,\, c) \in (\mathbf{F}^3)^\star \iff a, c \in \mathbf{F}^\times = \mathbf{F} \setminus \{0\}.$$

b) Soit $(G,\, \cdot)$ un groupe, $(M,\, *)$ un monoïde et $\varphi : G \to M$ un morphisme. Montrer que, pour $x, y \in G$, on a

$$\varphi(x) = \varphi(y) \iff \exists_{z \in \operatorname{Ker}\varphi} \quad y = z \cdot x.$$

[*Indication* : s'il existe un tel z, on peut l'exprimer simplement en termes de x et y …]

On se rappelle que $\operatorname{Ker}\varphi = \{\, g \in G \mid \varphi(g) = 1_M \,\}$. De là :

($\Leftarrow$) Si $y = z \cdot x$ avec $z \in \operatorname{Ker}\varphi$, alors

$$\varphi(y) = \varphi(z \cdot x) = \varphi(z) * \varphi(x) = 1_M * \varphi(x) = \varphi(x).$$

($\Rightarrow$) Inversement : posons $z := y \cdot x^{-1}$, de sorte que $y = z \cdot x$. Si $\varphi(x) = \varphi(y)$, alors

$$\varphi(z) = \varphi(y) * \varphi(x^{-1}) = \varphi(y) * \varphi(x)^{-1} = 1_M,$$

donc effectivement $z \in \operatorname{Ker}\varphi$.

— Fifi —

a) Sachant que $473 = 11 \cdot 43$, résoudre à l'aide du théorème des restes chinois la congruence

$$x^2 + 14x + 5 \underset{473}{\equiv} 0.$$

Puisque $2 \wedge 473 = 1$, on peut utiliser la formule habituelle pour les racines d'un polynôme de second degré et commencer par déterminer les racines carrés δ du discriminant

$$\Delta = 14^2 - 4 \cdot 5 = 176 \begin{cases} \underset{11}{\equiv} 0 \\ \underset{43}{\equiv} 4. \end{cases}$$

Les modules 11 et 43 étant tous deux premiers, on sait qu'il n'y a que les seules possibilités pour $\Delta \equiv \delta^2$ sont

$$\begin{cases} \delta \underset{11}{\equiv} 0 \\ \delta \underset{43}{\equiv} \pm 2 \end{cases}$$

Or : puisque $1 = 4 \cdot 11 - 1 \cdot 43$, la version explicite du théorème des restes chinois nous dit que

$$\begin{cases} y \underset{11}{\equiv} a \\ y \underset{43}{\equiv} b \end{cases} \iff y \underset{473}{\equiv} -43a + 44b,$$

on trouve donc

$$\delta \underset{473}{\equiv} \pm 88$$

et, puisque $237 \cdot 2 \equiv 1$,

$$x \underset{473}{\equiv} 237(-14 \pm 88) \equiv 37 \text{ ou } 422.$$

b) Quel sont l'ordre et le pré-ordre (multiplicatifs) de 2 dans $\mathbf{Z}/1892\mathbf{Z}$?

Encore une fois le plus simple est d'exploiter le théorème des restes chinois qui nous dit que

$$\mathbf{Z}/1892\mathbf{Z} \;\cong\; (\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/11\mathbf{Z}) \times (\mathbf{Z}/43\mathbf{Z})$$

qui nous permet de travailler séparément modulo 4, 11 et 43 :

- Modulo 4 : $1 \overset{\cdot 2}{\mapsto} 2 \overset{\cdot 2}{\mapsto} 0 \overset{\cdot 2}{\mapsto} 0 \overset{\cdot 2}{\mapsto} \cdots$, pré-cycle de longueur 2, cycle de longueur 1 ;
- Modulo 11 : puisque $2 \wedge 11 = 1$ et que 11 est premier, on sait d'après Lagrange que le pré-ordre est 0 et que l'ordre de 2 divise $\Phi(11) = 10$. Or :

  $$2^1 \underset{11}{\equiv} 2, \quad 2^2 \underset{11}{\equiv} 4, \quad 2^5 \underset{11}{\equiv} -1$$

  donc forcément l'ordre multiplicatif de 2 modulo 11 est 10 (c'est un élément primitif) ;
- Modulo 43 : par le même argument, on sait que l'ordre de 2 divise $\Phi(43) = 42$; en testant les diviseurs propres maximaux de 42 on voit

  $$2^{21} \underset{43}{\equiv} -1, \quad 2^{14} \underset{43}{\equiv} 1, \quad 2^6 \underset{43}{\equiv} 21,$$

  ce qui nous apprend que l'ordre de 2 est un diviseur de 14 qui ne divise ni 6 ni 21 ; c'est donc 14.

En remettant tout ensemble, on trouve

$$\text{pré-ordre} = \max(2, 0, 0) = 2, \quad \text{ordre} = \text{PPCM}(1, 10, 14) = 70.$$

— Loulou —

On travaille dans le corps $\mathbf{F}_9 = \{\, a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbf{F}_3 \,\}$ obtenu en adjoignant à $\mathbf{F}_3$ un élément α tel que $\alpha^2 = \alpha + 1$.

Problème d'énoncé ! ! Celui-ci n'est pas sûr s'il veut travailler dans le corps à 9 ou à 27 éléments, voici donc des choses intelligentes qui peuvent être dites dans chacun des cas.

a) Montrer que l'application $\varphi : \mathbf{F}_9 \to \mathbf{F}_9$ définie par $\varphi(x) := x^3$ est $\mathbf{F}_3$-linéaire. Quel est son noyau ? Son image ?

Dans les deux cas, appelant $\mathbf{F}$ le corps en question : l'application φ est linéaire car

$$\varphi(x+y) = (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 = x^3 + y^3 = \varphi(x) + \varphi(y)$$

puisque $3 = 0$ dans $\mathbf{F}$; et par ailleurs

$$\varphi(\lambda x) = (\lambda x)^3 = \lambda^3 x^3 = \lambda x^3$$

puisque $\lambda^3 = \lambda$ pour tout $\lambda \in \mathbf{F}_3$.

Dans les deux cas Ker $\varphi = \{0\}$, et en raisonnant sur la forme normale de φ qui nous dit que

$$\dim \operatorname{Ker} \varphi + \dim \operatorname{Im} \varphi = \dim \mathbf{F},$$

on conclut que $\operatorname{Im} \varphi = \mathbf{F}$; il s'agit d'un automorphisme de $\mathbf{F}$.

Versions matricielles : pour $\mathbf{F} = \mathbf{F}_9$, appelant α un élément tel que $\alpha^2 = \alpha + 1$, on a par rapport à la base $(1, \alpha)$:

$$[\varphi] = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}.$$

Pour $\mathbf{F} = \mathbf{F}_{27}$, appelant cette fois α un élément pour lequel $\alpha^3 = \alpha + 1$, on a par rapport à la base $(1, \alpha, \alpha^2)$:

$$[\varphi] = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

et on peut vérifier les affirmations précédentes par réduction de Gauss.

b) Trouver un élément $\beta \in \mathbf{F}_9$ satisfaisant $\beta^3 = \beta + \alpha$. Quelle est la matrice de φ par rapport à la base $(1, \alpha, \beta)$?

Dans les deux cas on peut voir ça comme un système d'équations linéaires à résoudre pour les coordonnées de β :

$$(\varphi - \mathrm{id})(\beta) = \alpha.$$

Pour $\mathbf{F} = \mathbf{F}_9$: avec la base de la question précédentes on cherche à résoudre

$$\left[\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 1 & 1 \end{array}\right]$$

qui n'a pas de solution ; et d'ailleurs $\mathbf{F}$ n'a pas de bases à 3 éléments car il est de dimension 2 sur $\mathbf{F}_3$. Autre façon de dire : écrivant $\beta = x + y\alpha$ avec $x, y \in \mathbf{F}^3$, on remarque que

$$\beta^3 - \beta = y(1+\alpha)$$

et que ceci ne peut jamais être égal à α.

Pour $\mathbf{F} = \mathbf{F}_{27}$: cette fois-ci le système s'écrit sous forme matricielle

$$\left[\begin{array}{ccc|c} 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

ce qui nous donne

$$\beta = a + \alpha - \alpha^2 \qquad \text{avec } a \in \mathbf{F}_3 \text{ quelconque.}$$

Peu importe la valeur de a, la relation $\beta^3 = \beta + \alpha$ nous donne directement les coordonées de $\varphi(\beta)$ dans la base $(1, \alpha, \beta)$ ce qui nous donne la représentation matricielle

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

On obtient bien sûr le même résultat en utilisant une matrice de passage :

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$