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

Bibou

Soit G un groupe agissant sur un ensemble X et notons $x \underset{G}{\equiv} y$ pour $x, y \in X$ lorsqu'il existe $g \in G$ pour lequel $y = g \cdot x$.

a) Vérifier que $\underset{G}{\equiv}$ est une relation d'équivalence sur X.

- Réflexivité : pour tout $x \in X$, $x \underset{G}{\equiv} x$ puisque $x = 1 \cdot x$ ✓
- Symétrie : si $x \underset{G}{\equiv} y$, alors il existe $g \in G$ pour lequel $y = g \cdot x$. En multipliant de part et d'autre par g^{-1}, on obtient
$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = 1 \cdot x = x,$$
ce qui signifie que $y \underset{G}{\equiv} x$ ✓
- Transitivité : si $x \underset{G}{\equiv} y$ et $y \underset{G}{\equiv} z$, alors il existe $g, h \in G$ pour lesquels $y = g \cdot x$ et $z = h \cdot y$. Alors $z = h \cdot (g \cdot x) = (hg) \cdot x$, ce qui prouve que $x \underset{G}{\equiv} z$ ✓

b) Pour $x \in X$, montrer que le stabilisateur $\mathrm{Stab}_G(x)$ est un sous-groupe de G.

Par définition, $\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\} \subseteq G$.

- Stabilité par 1 : $1 \in \mathrm{Stab}_G(x)$ puisque $1 \cdot x = x$ ✓
- Stabilité par $^{-1}$: si $g \in \mathrm{Stag}_G(x)$, alors $g \cdot x = x$. En multipliant de par et d'autre par g^{-1}, on obtient
$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = 1 \cdot x,$$
ce qui montre que $g^{-1} \in \mathrm{Stab}_G(x)$ ✓
- Stabilité par $\cdot$: si $g, h \in \mathrm{Stab}_G(x)$, alors
$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x,$$
ce qui montre que $gh \in \mathrm{Stab}_G(x)$ ✓

c) Soit $\Omega := \{\,(h, x) \in G \times X \mid h \cdot x = x\,\}$. Vérifier que la formule
$$g \cdot (h, x) := (hg^{-1},\, g \cdot x)$$
définit une action de G sur Ω pour laquelle tous les stabilisateurs sont triviaux.

La formule définit bien une action :

- $1 \cdot (h, x) = (h1^{-1},\, 1 \cdot x) = (h, x)$ ✓
- $g_1 \cdot (g_2 \cdot (h, x)) = g_1 \cdot (hg_2^{-1},\, g_2 \cdot x) = ((hg_2^{-1})g_1^{-1},\, g_1 \cdot (g_2 \cdot x)) = (h(g_1 g_2)^{-1},\, (g_1 g_2)x) = (g_1 g_2) \cdot (h, x)$ ✓

et si $g \in \mathrm{Stab}_G(h, x)$, c'est-à-dire
$$g \cdot (h, x) = (hg^{-1}, g \cdot x) = (h, x),$$
alors $hg^{-1} = h$ et $g \cdot x = x$, et la première égalité implique que $g = 1$.

Gluglu

a) Soit A un anneau commutatif pour lequel $2 \in A^\times$ et $a, b, c, x \in A$ avec $a \in A^\times$. Démontrer que

$$ax^2 + bx + c = 0 \iff (2ax + b)^2 = b^2 - 4ac,$$

de sorte que $ax^2 + bx + c = 0 \iff x = (2a)^{-1}(-b + \delta)$ où $\delta^2 = \Delta := b^2 - 4ac$.

Il s'agit de se convaincre que la formule usuelle pour les racines d'un polynôme de second degré (ainsi que sa démonstration) reste valable à ce niveau de généralité.

Pour la première étape, on développe :

$$(2ax + b)^2 + 4ac - b^2 = 4a^2x^2 + 4abx + 4ac = 4a(ax^2 + bx + c)$$

or, puisque par hypothèse $4a$ est inversible, on conclut que cette expression est bien nulle si et seulement si $ax^2 + bx + c$ l'est.

En posant $\delta := 2ax + b$ et $\Delta := b^2 - 4ac$, on constate que les racines x de l'équation du second degré correspondent bien aux valeurs de δ qui sont des racines carrées de Δ, et on exprime x en terme de δ par

$$x = (2a)^{-1}(-b + \delta).$$

Notez que l'on n'affirme ni ne suppose rien sur le *nombre* de racines carrées de Δ dans A qui peut être a priori n'importe quel entier positif sans que ça n'invalide l'argument présenté ici.

b) Déterminer toutes les solutions $x \in \mathbf{Z}_{497}$ à l'équation $x^2 + 3x + 4 = 0$. [*Indication* : $497 = 7 \cdot 71$]

D'après la question précédente (et les réflexes du lycée bien internalisés), on doit commencer par déterminer les racines carrées de

$$\Delta = 3^2 - 4 \cdot 4 = -7$$

dans $\mathbf{Z}_{497}$. Pour se simplifier la vie, exploitons l'isomorphisme d'anneaux fourni par le théorème des restes chinois

$$\mathbf{Z}_{497} \simeq \mathbf{Z}_7 \times \mathbf{Z}_{71}$$

sous lequel $\Delta = -7$ correspond au couple $(0, 64)$, dont les racines carrées sont $(0, \pm 8)$, qui correspondent à $\pm 63 \in \mathbf{Z}_{497}$. Il y a donc deux solutions :

$$\frac{-3 \pm 63}{2} = 30 \text{ et } -33.$$

c) Soit $(x_n)_{n=0}^{\infty}$ la suite d'éléments de $\mathbf{Z}_{497}$ définie par $x_0 = 1$, $x_1 = 30$ et $x_n = -3x_{n-1} - 4x_{n-2}$ pour $n \geqslant 2$. Donner une formule explicite pour x_n et en déduire la période de la suite.

L'équation caractéristique de l'équation de récurrence est exactement l'équation de la question précédente : on sait que sa solution générale est de la forme

$$x_n = A \cdot 30^n + B \cdot (-33)^n,$$

et en imposant les conditions initiales, on constate qu'il s'agit en fait de $x_n = 30^n$.

La période de la suite est l'ordre multplicatif de 30 dans $\mathbf{Z}_{497}$; pour le calculer, exploitons encore le théorème des restes chinois.

- $\mathrm{ord}_7(30) = \mathrm{ord}_7(2) = 3$ comme on le voit facilement puisque $2^3 \underset{7}{\equiv} 1$
- $\mathrm{ord}_7 1(30)$: on sait qu'il s'agit d'un diviseur de $\phi(71) = 70 = 2 \cdot 5 \cdot 7$, et en les testant un par un on voit que le plus petit qui fonctionne est 7.

Conclusion : $\mathrm{ord}_{497}(30) = \mathrm{PPCM}(3, 7) = 21$.

Yoyo

Un *carré magique* à coefficents dans un corps $\mathbf{F}$ est une matrice 3×3 dont les sommes des coefficients de chaque ligne, chaque colonne et chacune des deux diagonales principales sont égales.

a) Vérifier que l'ensemble $\mathrm{Mag}(\mathbf{F})$ des carrés magiques à coefficients dans $\mathbf{F}$ est un sous-espace vectoriel de $\mathcal{M}_3(\mathbf{F})$.

Il y a plusieurs façons de rédiger, voici sans doute la plus concise :

- Si φ et ψ sont deux applications linéaires d'un $\mathbf{F}$-espace vectoriel V dans $\mathbf{F}$, alors le sous-ensemble
$$\{v \in V \,|\, \varphi(v) = \psi(v)\}$$
est un sous-espace vectoriel de V (puisqu'il s'agit du noyau de l'application linéaire $\varphi - \psi$) ;
- l'intersection de sous-espaces est un sous-espace ;
- $\mathrm{Mag}(\mathbf{F})$ est donc un sous-espace de $\mathcal{M}_3(\mathbf{F})$, étant l'ensemble sur lequel les 8 applications linéaires « somme des lignes », « somme des colonnes » et « somme des diagonales » coïncident.

b) Déterminer la dimension de ce sous-espace et en déduire dans le cas d'un corps fini que $|\mathrm{Mag}(\mathbf{F})| = q^3$ si $|\mathbf{F}| = q$.

Encore plusieurs façons de procéder : l'une d'elle consiste à remarquer que $\mathrm{Mag}(\mathbf{F})$ contient au moins les trois matrices linéairement indépendantes
$$\begin{bmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix},$$
la dimension du sous-espace $\mathrm{Mag}(\mathbf{F})$ est donc au moins 3. Or en réduisant explicitement le système d'équations linéaires définissant un carré magique :
$$\begin{cases} a_{i1} + a_{i2} + a_{i3} = s, & i = 1,2,3, \\ a_{1j} + a_{2j} + a_{3j} = s, & j = 1,2,3, \end{cases} \qquad \begin{cases} a_{11} + a_{22} + a_{33} = s, \\ a_{13} + a_{22} + a_{32} = s, \end{cases}$$
on constate qu'une équation est redondante et qu'il est de rang 7, son noyau est donc de dimension $10 - 7 = 3$.

Les carrés magiques sont donc les matrices de la forme
$$\alpha \begin{bmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{bmatrix} + \beta \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix} + \gamma \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad (\alpha, \beta, \gamma \in \mathbf{F})$$
et il y a donc bien $|\mathbf{F}|^3 = q^3$ choix possibles.

c) Considérons que deux carrés magiques sont équivalents s'il ne diffèrent que d'une rotation ou réflexion préservant le carré. Combien y a-t-il alors, en fonction de q, de carrés magiques « vraiment différents » ?

On applique la formule de Cauchy-Frobenius à l'action du groupe diédral $\mathcal{D}_4$ sur l'ensemble $X = \mathrm{Mag}(\mathbf{F})$.
On distingue les éléments selon la structure cyclique de leur action sur les neuf cases :

- $g = 1$: $|X_1| = |\mathrm{Mag}(\mathbf{F})| = q^3$
- g une rotation de 90 degrés : dans la formule ci-dessus on voit qu'on doit avoir $\alpha = \beta = -\alpha = -\beta$ donc $\alpha = \beta = 0$ *sauf* si $2 = 0$ dans $\mathbf{F}$. Donc la plupart du temps $|X_g| = q$.
- g la rotation de 180 degrés : encore $\alpha = \beta = 0$ dans le cas générique, $|X_g| = q$.
- g la réflexion d'axe horizontal : on voit qu'on doit avoir $\alpha = \beta$ donc $|X_g| = q^2$ (axe vertical semblable sauf que $\alpha = -\beta$)
- g une réflexion dans une diagonale : selon la diagonale on a $\alpha = 0$ ou $\beta = 0$, donc encore $|X_g| = q^2$.

Conclusion : lorsque $2 \in \mathbf{F}^\times$,
$$|\mathrm{Mag}(\mathbf{F})/\mathcal{D}_4| = \frac{q^3 + 4q^2 + 3q}{8} = \frac{q(q^2 + 4q + 3)}{8}.$$

Le cas où $2 = 0$ doit être traité séparément, puisqu'alors en reprenant l'analyse ci-dessus :

- $g = 1$: $|X_g| = q^3$
- g une rotation de 90 degrés : $\alpha = \beta$ donc $|X_g| = q^2$
- g la rotation de 180 degrés : elles le sont toutes, $|X_g| = q^3$
- g réflexion horizontale ou verticale : encore $|X_g| = q^2$
- g une réflexion dans une diagonale : encore elles le sont toutes, $|X_g| = q^3$

donc dans ce cas
$$|\mathrm{Mag}(\mathbf{F})/\mathcal{D}_4| = \frac{4q^3 + 4q^2}{8} = \frac{q^2(q+1)}{2}.$$