

## Un corrigé du devoir surveillé n°1

|                                                                   |    |
|-------------------------------------------------------------------|----|
| 1. Questions de cours .....                                       | 1  |
| 2. Tirs successifs d'un archer sur une cible .....                | 1  |
| 3. Nombre de points fixes d'une permutation .....                 | 2  |
| 4. Structure de l'ensemble des applications lipschitziennes ..... | 3  |
| 5. Racine carrée de $-I_n$ dans $\mathcal{M}_n(\mathbb{R})$ ..... | 4  |
| 6. Action d'un groupe et théorème de Cauchy .....                 | 7  |
| 6.1. Action d'un groupe .....                                     | 7  |
| 6.2. Formule des classes .....                                    | 8  |
| 6.3. Théorème de Cauchy .....                                     | 10 |

### 1. Questions de cours

- Q1.** Énoncer, puis démontrer l'inégalité de Markov.
- Q2.** Soient  $K$  un corps,  $E$  un  $K$ -espace vectoriel de dimension finie,  $F$  un  $K$ -espace vectoriel et  $f : E \longrightarrow F$  un isomorphisme. Démontrer que  $F$  est de dimension finie, de même dimension que  $E$ .
- Q3.** Énoncer, puis démontrer la version géométrique du théorème du rang.
- Q4.** Soient  $K$  un corps,  $E, F, G$  des  $K$ -espaces vectoriels de dimension finie,  $\mathcal{E} = (e_1, \dots, e_n)$  une base de  $E$ ,  $\mathcal{F} = (f_1, \dots, f_m)$  une base de  $F$ ,  $\mathcal{G} = (g_1, \dots, g_p)$  une base de  $G$ ,  $u \in \mathcal{L}(E, F)$  et  $v \in \mathcal{L}(F, G)$ . Démontrer que :

$$\text{Mat}_{\mathcal{G}, \mathcal{G}}(v \circ u) = \text{Mat}_{\mathcal{F}, \mathcal{G}}(v) \times \text{Mat}_{\mathcal{E}, \mathcal{F}}(u).$$

### 2. Tirs successifs d'un archer sur une cible

Un archer tire sur  $n$  cibles ( $n \geq 2$ ).

À chaque tir, il a la probabilité  $p \in ]0, 1[$  de toucher la cible et les tirs sont supposés indépendants.

Il tire une première fois sur chaque cible et l'on note  $X$  le nombre de cibles atteintes lors de ce premier jet.

L'archer tire ensuite une seconde fois sur les cibles restantes et l'on note  $Y$  le nombre de cibles touchées lors de cette tentative.

- Q5.** Déterminer la loi de  $X$ .

Pour tout  $k \in \llbracket 0, n \rrbracket$ , soit  $X_k$  la variable aléatoire valant 1 si l'archer touche la  $k$ -ième cible lors de la première série de tirs et 0 sinon. D'après l'énoncé, les variables aléatoires  $X_1, \dots, X_n$  sont mutuellement indépendantes et suivent toutes la loi  $\mathcal{B}(p)$ . Ainsi :

$$X = \sum_{k=1}^n X_k \sim \mathcal{B}(n, p).$$

Nous en déduisons que  $X(\Omega) = \llbracket 0, n \rrbracket$  et que :

$$\forall k \in \llbracket 0, n \rrbracket \quad \mathbf{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

- Q6.** Soit  $k \in \llbracket 0, n \rrbracket$ . Calculer, pour tout  $i \in \llbracket 0, n \rrbracket$ ,  $\mathbf{P}(Y = i | X = k)$ .

Si l'événement  $(X = k)$  est réalisé, alors l'archer tirera  $n - k$  flèches lors de la deuxième série de tirs. Comme précédemment, on justifie que :

$$Y / (X = k) \sim \mathcal{B}(n - k, p).$$

Ainsi :

$$\forall i \in \llbracket 0, n \rrbracket \quad \mathbf{P}(Y = i | X = k) = \begin{cases} 0 & \text{si } i > n - k \\ \binom{n-k}{i} p^i (1-p)^{n-k-i} & \text{sinon.} \end{cases}$$

- Q7.** Déterminer la loi de la variable  $Z = X + Y$ .

- L'ensemble des valeurs prises par la variable  $Z$  est  $Z(\Omega) = \llbracket 0, n \rrbracket$ .
- Soit  $j \in \llbracket 0, n \rrbracket$ . D'après la formule des probabilités totales, relativement au système complet d'événement  $((X = k))_{k \in \llbracket 0, n \rrbracket}$  :

$$\mathbf{P}(Z = j) = \sum_{k=0}^n \mathbf{P}(X + Y = j, X = k) = \sum_{k=0}^n \mathbf{P}(Y = j - k, X = k) .$$

Puisque  $Y$  prend des valeurs positives ou nulles :

$$\mathbf{P}(Z = j) = \sum_{k=0}^j \mathbf{P}(Y = j - k, X = k) = \sum_{k=0}^j \mathbf{P}(Y = j - k | X = k) \mathbf{P}(X = k) .$$

D'après Q5 et Q6 :

$$\mathbf{P}(Z = j) = \sum_{k=0}^j \binom{n-k}{j-k} p^{j-k} (1-p)^{n-j} \binom{n}{k} p^k (1-p)^{n-k} .$$

Comme :

$$\forall k \in \llbracket 0, j \rrbracket \quad \binom{n-k}{j-k} \binom{n}{k} = \frac{(n-k)!}{(j-k)! (n-j)!} \frac{n!}{k! (n-k)!} \frac{j!}{j!} = \binom{n}{j} \binom{j}{k}$$

il vient :

$$\mathbf{P}(Z = j) = \binom{n}{j} p^j (1-p)^{2n-j} \sum_{k=0}^j \binom{j}{k} \left( \frac{1}{1-p} \right)^j .$$

En appliquant la formule du binôme de Newton, nous obtenons :

$$\mathbf{P}(Z = j) = \binom{n}{j} p^j (1-p)^{2n-j} \left( 1 + \frac{1}{1-p} \right)^j = \binom{n}{j} ((2-p)p)^j (1-p)^{2n-2j} = \binom{n}{j} q^j (1-q)^{n-j}$$

où  $q := (2-p)p$ .

- Finalement  $Z \sim \mathcal{B}(n, (2-p)p)$ .

**Q8.** Donner les valeurs de  $\mathbf{E}(Z)$  et  $\mathbf{V}(Z)$ .

D'après le cours sur la loi binomiale et Q7,  $\mathbf{E}(Z) = n(2-p)p$  et  $\mathbf{V}(Z) = n(2-p)p(1-p)^2$ .

### 3. Nombre de points fixes d'une permutation

Soit  $n \in \mathbf{N}^*$ . On munit  $\mathfrak{S}_n$  de la probabilité uniforme. Soit  $X$  la variable aléatoire définie par :

$$X \left| \begin{array}{ll} \mathfrak{S}_n & \longrightarrow \llbracket 0, n \rrbracket \\ \sigma & \longmapsto |\{k \in \llbracket 1, n \rrbracket : \sigma(k) = k\}| . \end{array} \right.$$

Pour tout  $i \in \llbracket 1, n \rrbracket$ , on définit la variable  $X_i$  par :

$$X_i \left| \begin{array}{ll} \mathfrak{S}_n & \longrightarrow \llbracket 0, n \rrbracket \\ \sigma & \longmapsto \begin{cases} 1 & \text{si } \sigma(i) = i \\ 0 & \text{sinon} . \end{cases} \end{array} \right.$$

**Q9.** Soit  $i \in \llbracket 1, n \rrbracket$ . Déterminer la loi de  $X_i$ , son espérance et sa variance.

- La variable aléatoire  $X_i$  prend ses valeurs dans  $\{0, 1\}$ . Elle suit donc une loi de Bernoulli.
- Comme  $\mathfrak{S}_n$  est muni de la probabilité uniforme :

$$\mathbf{P}(X_i = 1) = \frac{|\{X_i = 1\}|}{|\mathfrak{S}_n|} = \frac{|\{X_i = 1\}|}{n!} .$$

- L'application :

$$\left| \begin{array}{ll} (X_i = 1) & \longrightarrow \mathfrak{S}(\llbracket 1, n \rrbracket \setminus \{i\}) \\ \sigma & \longmapsto \sigma|_{\llbracket 1, n \rrbracket \setminus \{i\}} \end{array} \right.$$

est bien définie et bijective. Ainsi  $|(X_i = 1)| = (n-1)!$ .

- D'après ce qui précède,  $\mathbf{P}(X_i = 1) = \frac{1}{n}$  et donc :

$$X_i \sim \mathcal{B}\left(\frac{1}{n}\right) \quad \mathbf{E}(X_i) = \frac{1}{n} \quad \mathbf{V}(X_i) = \frac{1}{n} \left(1 - \frac{1}{n}\right) = \frac{n-1}{n^2}.$$

**Q10.** Soient  $i$  et  $j$  des éléments distincts de  $\llbracket 1, n \rrbracket$ . Calculer  $\mathbf{Cov}(X_i, X_j)$ .

- D'après la définition de la covariance et la question précédente :

$$\mathbf{Cov}(X_i, X_j) = \mathbf{E}(X_i X_j) - \mathbf{E}(X_i) \mathbf{E}(X_j) = \mathbf{E}(X_i X_j) - \frac{1}{n^2}.$$

- La variable aléatoire  $X_i X_j$  prend les valeurs 0 et 1. Elle suit donc une loi de Bernoulli.
- Comme  $\mathfrak{S}_n$  est muni de la probabilité uniforme :

$$\mathbf{P}(X_i X_j = 1) = \frac{|(X_i = 1, X_j = 1)|}{|\mathfrak{S}_n|} = \frac{|(X_i = 1, X_j = 1)|}{n!}.$$

- L'application :

$$\left| \begin{array}{ll} (X_i = 1, X_j = 1) & \longrightarrow \mathfrak{S}(\llbracket 1, n \rrbracket \setminus \{i, j\}) \\ \sigma & \longmapsto \sigma|_{\llbracket 1, n \rrbracket \setminus \{i, j\}} \end{array} \right.$$

est bien définie et bijective. Ainsi  $|(X_i = 1, X_j = 1)| = (n-2)!$ .

- D'après ce qui précède,  $\mathbf{P}(X_i = 1, X_j = 1) = \frac{1}{n(n-1)}$  et donc :

$$X_i X_j \sim \mathcal{B}\left(\frac{1}{n(n-1)}\right) \quad \mathbf{E}(X_i X_j) = \frac{1}{n(n-1)}.$$

- Finalement :

$$\mathbf{Cov}(X_i, X_j) = \frac{1}{n(n-1)} - \frac{1}{n^2} = \frac{1}{n^2(n-1)}.$$

**Q11.** Déterminer l'espérance et la variance de  $X$ .

- Observons que  $X = \sum_{i=1}^n X_i$ .

- Par linéarité de l'espérance et Q9 :

$$\mathbf{E}(X) = \sum_{i=1}^n \mathbf{E}(X_i) = \sum_{i=1}^n \frac{1}{n} = 1.$$

- D'après le cours :

$$\mathbf{V}(X) = \sum_{i=1}^n \mathbf{V}(X_i) + 2 \sum_{1 \leq i < j \leq n} \mathbf{Cov}(X_i, X_j).$$

Grâce à Q9 et Q10, nous obtenons :

$$\mathbf{V}(X) = \sum_{i=1}^n \frac{n-1}{n^2} + 2 \sum_{1 \leq i < j \leq n} \frac{1}{n^2(n-1)} = \frac{n-1}{n} + 2 \times \frac{1}{n^2(n-1)} \times \frac{n(n-1)}{2} = 1.$$

#### 4. Structure de l'ensemble des applications lipschitziennes

Soient  $a$  et  $b$  des réels tels que  $a < b$  et  $\text{Lip}([a, b], \mathbf{R})$  l'ensemble des applications lipschitziennes de  $[a, b]$  dans  $\mathbf{R}$ .

**Q12.** Démontrer que  $\mathcal{C}^1([a, b], \mathbf{R}) \subset \text{Lip}([a, b], \mathbf{R})$ .

Soit  $f \in \mathcal{C}^1([a, b], \mathbf{R})$ .

- La fonction  $f'$  est continue sur le segment  $[a, b]$ . D'après le théorème des bornes atteintes, la fonction  $f'$  est bornée sur  $[a, b]$ , d'où :

$$\exists k \in \mathbf{R}_+ \quad \forall t \in [a, b] \quad |f'(t)| \leq k.$$

- Soient  $x$  et  $y$  des éléments de  $[a, b]$  tels que  $x < y$ . D'après le théorème fondamental de l'analyse :

$$|f(x) - f(y)| = \left| \int_x^y f'(t) dt \right| \leq \int_x^y |f'(t)| dt \leq \int_x^y k dt = k(y - x) = k|x - y|.$$

La fonction  $f$  est donc  $k$ -lipschitzienne.

*Remarque.* On peut donner une preuve alternative reposant sur le théorème des accroissements finis.

**Q13.** Démontrer que  $\text{Lip}([a, b], \mathbf{R})$  est un sous-espace vectoriel de  $\mathcal{F}([a, b], \mathbf{R})$ .

- La fonction nulle sur  $[a, b]$  est bien lipschitzienne (elle est  $k$ -lipschitzienne pour tout  $k \geq 0$ , comme toute fonction constante).
- Soient  $f_1, f_2 \in \text{Lip}([a, b], \mathbf{R})$  et  $\lambda_1, \lambda_2 \in \mathbf{R}$ . Par hypothèse :

$$\exists k_1 \in \mathbf{R}_+ \quad \forall (x, y) \in [a, b]^2 \quad |f_1(x) - f_1(y)| \leq k_1 |x - y|$$

et :

$$\exists k_2 \in \mathbf{R}_+ \quad \forall (x, y) \in [a, b]^2 \quad |f_2(x) - f_2(y)| \leq k_2 |x - y|.$$

Soit  $(x, y) \in [a, b]^2$ . D'après l'inégalité triangulaire :

$$|(\lambda_1 f_1 + \lambda_2 f_2)(x) - (\lambda_1 f_1 + \lambda_2 f_2)(y)| \leq |\lambda_1| |f_1(x) - f_1(y)| + |\lambda_2| |f_2(x) - f_2(y)|.$$

Comme  $f_1$  est  $k_1$ -lipschitzienne et  $f_2$  est  $k_2$ -lipschitzienne, nous en déduisons que :

$$|(\lambda_1 f_1 + \lambda_2 f_2)(x) - (\lambda_1 f_1 + \lambda_2 f_2)(y)| \leq (|\lambda_1| k_1 + |\lambda_2| k_2) |x - y|.$$

La fonction  $\lambda_1 f_1 + \lambda_2 f_2$  est donc  $(|\lambda_1| k_1 + |\lambda_2| k_2)$ -lipschitzienne.

## 5. Racine carrée de $-I_n$ dans $\mathcal{M}_n(\mathbf{R})$

Soient  $E$  un  $\mathbf{R}$ -espace de dimension finie non nulle et  $f \in \mathcal{L}(E)$  un endomorphisme tel que  $f^2 = -\text{id}_E$ .

**Q14.** Justifier que  $f$  est bijective et préciser  $f^{-1}$ .

- soit  $x \in E$ . Comme  $f$  est linéaire, de  $f(f(x)) = -x$ , nous déduisons :

$$f \circ (-f)(x) = f(-f(x)) = -f(f(x)) = -(-x) = x.$$

Ainsi  $f \circ (-f) = \text{id}_E$ .

- De manière analogue, nous établissons  $(-f) \circ f = \text{id}_E$ .
- Nous avons démontré que  $f$  est bijective, de bijection réciproque  $-f$ .

**Q15.** Démontrer que  $E$  est de dimension paire.

Par propriété du déterminant :

$$\det(f)^2 = \det(f^2) = \det(-\text{id}_E) = (-1)^{\dim(E)} \times \det(\text{id}_E) = (-1)^{\dim(E)}.$$

Comme  $f$  est un endomorphisme d'un  $\mathbf{R}$ -espace vectoriel de dimension finie, son déterminant est un nombre réel, d'où :

$$\det(f)^2 \geq 0.$$

De cette étude, nous déduisons que  $\dim(E)$  est paire.

Soit  $p \in \mathbb{N}^*$  tel que  $\dim(E) = 2p$ .

**Q16.** Démontrer que pour tout vecteur  $a$  non nul de  $E$ , la famille  $(a, f(a))$  est libre.

Fixons un vecteur non nul  $a$  de  $E$  et considérons des réels  $\lambda, \mu$  tels que :

$$(L_1) \quad \lambda a + \mu f(a) = 0_E.$$

En appliquant  $f$ , il vient :

$$(L_2) \quad -\mu a + \lambda f(a) = 0_E.$$

Nous en déduisons :

$$(\lambda L_1 - \mu L_2) \quad (\lambda^2 + \mu^2) a = 0_E.$$

Comme le vecteur  $a$  est non nul, il vient :

$$\lambda^2 + \mu^2 = 0_{\mathbb{R}}.$$

Une somme de nombres réels positifs est nulle si et seulement si tous ses termes sont nuls. Ainsi  $\lambda = \mu = 0$ .

**Q17.** Démontrer qu'il existe des vecteurs non nuls  $a_1, \dots, a_p$  de  $E$  tels que :

$$E = \bigoplus_{i=1}^p \text{Vect}(\{a_i, f(a_i)\}).$$

- Comme  $E$  n'est pas de dimension nulle, nous pouvons choisir un vecteur  $a_1$  non nul dans  $E$ .
- Soient  $k \in \llbracket 1, p-1 \rrbracket$ . Supposons construits des vecteurs non nuls  $a_1, \dots, a_k$  de  $E$  tels que les sous-espaces vectoriels :

$$\text{Vect}(a_1, f(a_1)), \dots, \text{Vect}(a_k, f(a_k))$$

soient en somme directe. D'après Q16, comme les vecteurs  $a_1, \dots, a_k$  sont non nuls :

$$\dim\left(\bigoplus_{i=1}^k \text{Vect}(a_i, f(a_i))\right) = 2k < 2p = \dim(E).$$

Nous pouvons donc choisir un vecteur  $a_{k+1}$  dans  $E \setminus \bigoplus_{i=1}^k \text{Vect}(a_i, f(a_i))$ . Nous allons démontrer que les espaces :

$$\text{Vect}(a_1, f(a_1)), \dots, \text{Vect}(a_k, f(a_k)), \text{Vect}(a_{k+1}, f(a_{k+1}))$$

sont en somme directe. Soient :

$$x_1 \in \text{Vect}(a_1, f(a_1)), \dots, x_k \in \text{Vect}(a_k, f(a_k)), x_{k+1} \in \text{Vect}(a_{k+1}, f(a_{k+1}))$$

tels que  $x_1 + \dots + x_k + x_{k+1} = 0_E$ . Comme  $x_{k+1} \in \text{Vect}(a_{k+1}, f(a_{k+1}))$ , il existe des réels  $\lambda_{k+1}, \mu_{k+1}$  tels que :

$$x_{k+1} = \lambda_{k+1} a_{k+1} + \mu_{k+1} f(a_{k+1}).$$

Nous savons donc que :

$$(L_1) \quad \lambda_{k+1} a_{k+1} + \mu_{k+1} f(a_{k+1}) + \sum_{i=1}^k x_i = 0_E.$$

En appliquant  $f$ , il vient :

$$(L_2) \quad -\mu_{k+1} a_{k+1} + \lambda_{k+1} f(a_{k+1}) + \sum_{i=1}^k f(x_i) = 0_E.$$

En combinant les lignes  $L_1$  et  $L_2$  (cf.  $\lambda_{k+1} L_1 - \mu_{k+1} L_2$ ), il vient :

$$(*) \quad (\lambda_{k+1}^2 + \mu_{k+1}^2) a_{k+1} + \sum_{i=1}^k \underbrace{\lambda_{k+1} x_i + \mu_{k+1} f(x_i)}_{\in \text{Vect}(a_i, f(a_i))} = 0_E \quad [\text{Vect}(a_i, f(a_i)) \text{ est stable par } f].$$

Si le couple de réels  $(\lambda_{k+1}, \mu_{k+1})$  est non nul, alors :

$$\lambda_{k+1}^2 + \mu_{k+1}^2 \neq 0_{\mathbb{R}}$$

et (\*) implique  $a_{k+1} \in \bigoplus_{i=1}^k \text{Vect}(a_i, f(a_i))$ , ce qui n'est pas. Donc :

$$\lambda_{k+1} = \mu_{k+1} = 0_{\mathbf{R}}$$

et :

$$x_{k+1} = 0_E.$$

L'identité  $(L_1)$  s'écrit alors :

$$\sum_{i=1}^k x_i = 0_E.$$

Comme les sous-espaces vectoriels :

$$\text{Vect}(a_1, f(a_1)), \dots, \text{Vect}(a_k, f(a_k))$$

sont en somme directe, il vient finalement :

$$x_1 = \dots = x_k = 0_E.$$

- Nous construisons ainsi, par récurrence finie, des vecteurs non nuls  $a_1, \dots, a_p$  tels que les sous-espaces vectoriels :

$$\text{Vect}(a_1, f(a_1)), \dots, \text{Vect}(a_p, f(a_p))$$

sont en somme directe. D'après Q16, comme les vecteurs  $a_1, \dots, a_p$  sont non nuls :

$$\dim\left(\bigoplus_{i=1}^p \text{Vect}(a_i, f(a_i))\right) = 2p = \dim(E).$$

$$\text{Ainsi } \bigoplus_{i=1}^p \text{Vect}(a_i, f(a_i)) = E.$$

**Q18.** Construire une base de  $E$  dans laquelle la matrice de  $f$  est :

$$R := \begin{pmatrix} 0 & -1 & & & \\ 1 & 0 & & & \\ & & 0 & -1 & \\ & & 1 & 0 & \\ & & & \ddots & \\ & & & & 0 & -1 \\ & & & & 1 & 0 \end{pmatrix} = E_{2,1} - E_{1,2} + E_{4,3} - E_{3,4} + \dots + E_{2p,2p-1} - E_{2p-1,2p}$$

- Soit  $i \in \llbracket 1, p \rrbracket$ . D'après Q16,  $(a_i, f(a_i))$  est une base de  $\text{Vect}(a_i, f(a_i))$ .
- Grâce à Q17, nous savons alors que :

$$\mathcal{B} := (a_1, f(a_1), \dots, a_p, f(a_p))$$

est une base de  $E$  (concaténation de bases dans une somme directe).

- Clairement  $\text{Mat}_{\mathcal{B}}(f) = R$ .

**Q19.** Soit  $A \in \mathcal{M}_{2p}(\mathbf{R})$  telle que  $A^2 = -I_{2p}$ . Démontrer que la matrice  $A$  est semblable à la matrice  $R$ .

- Soit  $\mathcal{B}_c$  la base canonique de  $\mathcal{M}_{2p,1}(\mathbf{R})$  et :

$$f_A \left| \begin{array}{ccc} \mathcal{M}_{2p,1}(\mathbf{R}) & \longrightarrow & \mathcal{M}_{2p,1}(\mathbf{R}) \\ X & \longmapsto & AX \end{array} \right.$$

l'application linéaire canoniquement associée à  $A$ , de sorte que  $\text{Mat}_{\mathcal{B}_c}(f_A) = A$ .

- Nous calculons :

$$\text{Mat}_{\mathcal{B}_c}(-\text{id}_{\mathcal{M}_{2p,1}(\mathbf{R})}) = -I_{2p} = A^2 = \text{Mat}_{\mathcal{B}_c}(f_A)^2 = \text{Mat}_{\mathcal{B}_c}(f_A^2).$$

Comme :

$$\text{Mat}_{\mathcal{B}_c}(\cdot) \left| \begin{array}{ccc} \mathcal{L}(\mathcal{M}_{2p,1}(\mathbf{R})) & \longrightarrow & \mathcal{M}_{2p}(\mathbf{R}) \\ u & \longmapsto & \text{Mat}_{\mathcal{B}_c}(u) \end{array} \right.$$

est un isomorphisme de  $\mathbf{R}$ -algèbres (son injectivité suffit ici), il vient :

$$f_A^2 = -\text{id}_{\mathcal{M}_{2p,1}(\mathbf{R})}.$$

• D'après ce qui précède, nous pouvons appliquer Q18 au  $\mathbf{R}$ -espace vectoriel  $\mathcal{M}_{2p,1}(\mathbf{R})$  muni de l'endomorphisme  $f_A$ . Il existe donc une base  $\mathcal{B}$  de  $\mathcal{M}_{2p,1}(\mathbf{R})$  telle que :

$$\text{Mat}_{\mathcal{B}}(f_A) = R.$$

• Par théorème de changement de base :

$$\text{Mat}_{\mathcal{B}_c}(f_A) = P_{\mathcal{B}_c \rightarrow \mathcal{B}} \times \text{Mat}_{\mathcal{B}}(f_A) \times P_{\mathcal{B} \rightarrow \mathcal{B}_c}$$

identité qui se réécrit :

$$A = P \times R \times P^{-1}$$

en posant  $P := P_{\mathcal{B}_c \rightarrow \mathcal{B}} \in \text{GL}_n(\mathbf{R})$ . Les matrices  $A$  et  $R$  sont donc semblables.

## 6. Action d'un groupe et théorème de Cauchy

### 6.1. Action d'un groupe

Soient  $E$  un ensemble fini et  $(G, *)$  un groupe, dont le neutre est noté  $e_G$ . On se donne une application :

$$\rho \left| \begin{array}{ccc} G \times E & \longrightarrow & E \\ (g, x) & \longmapsto & g \cdot x := \rho(g, x) \end{array} \right.$$

vérifiant les deux propriétés suivantes :

$$(A1) \quad \forall x \in E \quad e_G \cdot x = x ;$$

$$(A2) \quad \forall (g_1, g_2) \in G^2 \quad \forall x \in E \quad g_1 \cdot \underbrace{(g_2 \cdot x)}_{\in E} = \underbrace{(g_1 * g_2)}_{\in G} \cdot x.$$

Une telle application  $\rho$  est appelée *action du groupe*  $(G, *)$  sur  $E$ .

**Q20.** Soit  $x \in E$ . Le stabilisateur de  $x$  est l'ensemble  $\text{Stab}(x)$  défini par :

$$\text{Stab}(x) := \{g \in G : g \cdot x = x\} \subset G.$$

Démontrer que  $\text{Stab}(x)$  est un sous-groupe de  $(G, *)$ .

• D'après la propriété (A1) de l'action de groupe,  $e_G \in \text{Stab}(x)$ .

• Soit  $(g_1, g_2) \in G^2$ . Alors :

$$\begin{aligned} (g_1 * g_2) \cdot x &= g_1 \cdot (g_2 \cdot x) && [(A2)] \\ &= g_1 \cdot x && [g_2 \in \text{Stab}(x)] \\ &= x && [g_1 \in \text{Stab}(x)]. \end{aligned}$$

Ainsi  $g_1 * g_2 \in \text{Stab}(x)$ .

• Soit  $g \in \text{Stab}(x)$ . Alors :

$$\begin{aligned} g^{-1} \cdot x &= g^{-1} \cdot (g \cdot x) && [g \in \text{Stab}(x)] \\ &= (g^{-1} * g) \cdot x && [(A2)] \\ &= e_G \cdot x \\ &= x && [(A1)]. \end{aligned}$$

Ainsi  $g^{-1} \in \text{Stab}(x)$ .

• Conclusion. La partie  $\text{Stab}(x)$  de  $G$  contient son neutre et est stable par la loi et par passage au symétrique. Elle est donc un sous-groupe de  $(G, *)$ .

À tout  $x \in E$ , on associe son orbite  $\mathcal{O}(x)$  définie par :

$$\mathcal{O}(x) := \{g \cdot x : g \in G\} \subset E.$$

**Q21.** Soient  $(x_1, x_2) \in E^2$ . Démontrer que  $\mathcal{O}(x_1) \cap \mathcal{O}(x_2) = \emptyset$  ou  $\mathcal{O}(x_1) = \mathcal{O}(x_2)$ .

Nous supposons  $\mathcal{O}(x_1) \cap \mathcal{O}(x_2) \neq \emptyset$  et en déduisons qu'alors  $\mathcal{O}(x_1) = \mathcal{O}(x_2)$ , ce qui établit le résultat demandé.

- D'après notre hypothèse, nous pouvons considérer un élément  $y \in \mathcal{O}(x_1) \cap \mathcal{O}(x_2)$ . Il existe donc  $(g_1, g_2) \in G^2$  tel que  $y = g_1 \cdot x_1$  et  $y = g_2 \cdot x_2$ .
- Nous observons que :

$$\begin{aligned} g_1 \cdot x_1 = g_2 \cdot x_2 &\implies g_1^{-1} \cdot (g_1 \cdot x_1) = g_1^{-1} \cdot (g_2 \cdot x_2) \\ &\implies (g_1^{-1} * g_1) \cdot x_1 = (g_1^{-1} * g_2) \cdot x_2 \quad [(A2)] \\ &\implies e_G \cdot x_1 = (g_1^{-1} * g_2) \cdot x_2 \\ &\implies x_1 = (g_1^{-1} * g_2) \cdot x_2 \quad [(A1)]. \end{aligned}$$

- Soit  $z \in \mathcal{O}(x_1)$ . Il existe donc  $g \in G$  tel que  $z = g \cdot x_1$ . Comme  $x_1 = (g_1^{-1} * g_2) \cdot x_2$ , il vient grâce à (A2) :

$$z = g \cdot ((g_1^{-1} * g_2) \cdot x_2) = (g * g_1^{-1} * g_2) \cdot x_2 \in \mathcal{O}(x_2).$$

Ainsi  $\mathcal{O}(x_1) \subset \mathcal{O}(x_2)$ .

- En échangeant les rôles de  $x_1$  et  $x_2$ , nous obtenons aussi  $\mathcal{O}(x_2) \subset \mathcal{O}(x_1)$ .

**Q22.** Soient  $\mathcal{O}(x_1), \dots, \mathcal{O}(x_p)$  une liste exhaustive et sans répétition de toutes les orbites. Justifier :

$$E = \bigsqcup_{k=1}^p \mathcal{O}(x_k) \quad [\text{réunion disjointe}]$$

et en déduire une expression de  $\text{card}(E)$  en fonction des cardinaux des orbites  $\mathcal{O}(x_1), \dots, \mathcal{O}(x_p)$ .

- Comme chacun des ensembles  $\mathcal{O}(x_1), \dots, \mathcal{O}(x_p)$  est une partie de  $E$ , l'inclusion  $\supset$  est claire.
- Soit  $x \in E$ . D'après (A1),  $x = e_G \cdot x$  et donc  $x \in \mathcal{O}(x)$ . Comme  $\mathcal{O}(x_1), \dots, \mathcal{O}(x_p)$  est une liste exhaustive de toutes les orbites, il existe  $i \in \llbracket 1, p \rrbracket$  tel que  $\mathcal{O}(x) = \mathcal{O}(x_i)$ . Alors :

$$x \in \mathcal{O}(x) = \mathcal{O}(x_i) \subset \bigcup_{k=1}^p \mathcal{O}(x_k).$$

L'inclusion  $\subset$  est donc établie.

- Soit  $(i, j) \in \llbracket 1, p \rrbracket^2$  tel que  $\mathcal{O}(x_i) \cap \mathcal{O}(x_j) \neq \emptyset$ . D'après la question précédente, il vient  $\mathcal{O}(x_i) = \mathcal{O}(x_j)$ . Comme la liste  $\mathcal{O}(x_1), \dots, \mathcal{O}(x_p)$  de toutes les orbites ne contient aucune répétition, nous en déduisons  $i = j$ . La réunion est donc disjointe.

- Nous avons démontré que  $E = \bigsqcup_{k=1}^p \mathcal{O}(x_k)$ . En considérant les cardinaux, il vient :

$$\text{card}(E) = \sum_{k=1}^p \text{card}(\mathcal{O}(x_k)).$$

**Q23.** Nous savons qu'une relation d'équivalence sur  $E$  livre une partition de  $E$  : celle donnée par les classes d'équivalences. Proposer une relation d'équivalence  $\sim$  sur  $E$  dont la partition de  $E$  associée est celle obtenue à la question précédente.

- Nous définissons la relation  $\sim$  sur  $E$  par, pour tout  $(x, y) \in E^2$  :

$$x \sim y \iff \mathcal{O}(x) = \mathcal{O}(y).$$

Il est clair que la relation  $\sim$  ainsi définie est une relation d'équivalence sur  $E$ . Grâce à Q21, on établit que ses classes d'équivalences sont les orbites.

- On peut démontrer, en outre, grâce à (A1) et (A2), pour tout  $(x, y) \in E^2$  :

$$\mathcal{O}(x) = \mathcal{O}(y) \iff (\exists g \in G, y = g \cdot x).$$

L'exercice est laissé (et vivement conseillé) au lecteur.

## 6.2. Formule des classes

Nous considérons ici un ensemble fini  $E$ , muni d'une action de groupe  $\rho$  par un groupe fini  $(G, *)$  et nous fixons un élément  $x \in E$ .

**Q24.** Soit  $\tau$  l'application définie par :

$$\tau \left| \begin{array}{ll} G & \longrightarrow \mathcal{O}(x) \\ g & \longmapsto g \cdot x . \end{array} \right.$$

Justifier que :

$$G = \bigsqcup_{y \in \mathcal{O}(x)} \tau^{-1}(\{y\}) .$$

Comme  $\tau$  est une application de  $G$  dans  $\mathcal{O}(x)$  :

$$G = \tau^{-1}(\mathcal{O}(x)) .$$

De la décomposition  $\mathcal{O}(x) = \bigsqcup_{y \in \mathcal{O}(x)} \{y\}$ , nous déduisons :

$$G = \tau^{-1}\left(\bigsqcup_{y \in \mathcal{O}(x)} \{y\}\right) .$$

Comme les images réciproques respectent les réunions disjointes, nous obtenons finalement :

$$G = \bigsqcup_{y \in \mathcal{O}(x)} \tau^{-1}(\{y\}) .$$

**Q25.** Soit  $y \in \mathcal{O}(x)$ . Démontrer que les ensembles  $\text{Stab}(x)$  et  $\tau^{-1}(\{y\})$  sont équipotents.

Comme  $y \in \mathcal{O}(x)$ , il existe  $g \in G$  tel que  $y = g \cdot x$ . Nous allons démontrer que l'application :

$$\delta \left| \begin{array}{ll} \text{Stab}(x) & \longrightarrow \tau^{-1}(\{y\}) \\ h & \longmapsto g * h \end{array} \right.$$

est bien définie et bijective.

• *Caractère bien défini de  $\delta$ .* Pour tout  $h \in \text{Stab}(x)$  :

$$\begin{aligned} \tau(g * h) &= (g * h) \cdot x \\ &= g \cdot (h \cdot x) \quad [(A2)] \\ &= g \cdot x \quad [h \in \text{Stab}(x)] \\ &= y . \end{aligned}$$

Nous en déduisons que, pour tout  $h \in \text{Stab}(x)$ ,  $g * h \in \tau^{-1}(\{y\})$ .

• *Injectivité de  $\delta$ .* Soit  $(h_1, h_2) \in \text{Stab}(x)^2$  tel que  $\tau(h_1) = \tau(h_2)$ , i.e. tel que :

$$g * h_1 = g * h_2 \quad [\text{identité entre éléments du groupe } (G, *)] .$$

En multipliant à gauche par  $g^{-1}$ , il vient  $h_1 = h_2$ .

• *Surjectivité de  $\delta$ .* Soit  $k \in \tau^{-1}(\{y\})$ . Alors  $\tau(k) = y$ , i.e. :

$$k \cdot x = y = g \cdot x .$$

Nous observons que :

$$\begin{aligned} k \cdot x = g \cdot x &\implies g^{-1} \cdot (k \cdot x) = g^{-1} \cdot (g \cdot x) \\ &\implies (g^{-1} * k) \cdot x = (g^{-1} * g) \cdot x \quad [(A2)] \\ &\implies (g^{-1} * k) \cdot x = e_G \cdot x \\ &\implies (g^{-1} * k) \cdot x = x \quad [(A1)] . \end{aligned}$$

Nous avons établi que  $g^{-1} * k \in \text{Stab}(x)$  et il est clair que  $\delta(g^{-1} * k) = k$ .

**Q26.** En déduire la formule des classes, qui s'énonce comme suit :

$$\text{card}(\mathcal{O}(x)) = \frac{\text{card}(G)}{\text{card}(\text{Stab}(x))} .$$

D'après Q24 :

$$\text{card}(G) = \sum_{y \in \mathcal{O}(x)} \text{card}(\tau^{-1}(\{y\})).$$

D'après la question Q25 :

$$\forall y \in \mathcal{O}(x) \quad \text{card}(\tau^{-1}(\{y\})) = \text{card}(\text{Stab}(x)).$$

Ainsi :

$$\text{card}(G) = \sum_{y \in \mathcal{O}(x)} \text{card}(\text{Stab}(x)) = \text{card}(\mathcal{O}(x)) \cdot \text{card}(\text{Stab}(x)).$$

Comme  $\text{Stab}(x)$  est un sous-groupe de  $G$ , il est non vide. Nous pouvons donc conclure que :

$$\text{card}(\mathcal{O}(x)) = \frac{\text{card}(G)}{\text{card}(\text{Stab}(x))}.$$

### 6.3. Théorème de Cauchy

Soient  $(\Gamma, *)$  un groupe fini de cardinal  $n$  et  $p$  un diviseur premier de  $n$ .  
Nous nous proposons de démontrer que :

$$\exists \gamma \in \Gamma \quad \gamma \neq e_\Gamma \quad \text{et} \quad \gamma^p = e_\Gamma$$

où  $e_\Gamma$  désigne le neutre du groupe  $(\Gamma, *)$ . Il s'agit d'un théorème dû à Cauchy.



Augustin-Louis Cauchy (1789-1857)

Nous introduisons l'ensemble :

$$E := \{(\gamma_1, \gamma_2, \dots, \gamma_p) \in \Gamma^p : \gamma_1 * \gamma_2 * \dots * \gamma_p = e_\Gamma\} \subset \Gamma^p.$$

**Q27.** Démontrer que  $E$  est un ensemble fini, de cardinal  $n^{p-1}$ .

Nous démontrons que l'application :

$$\pi \left| \begin{array}{ccc} E & \longrightarrow & \Gamma^{p-1} \\ (\gamma_1, \gamma_2, \dots, \gamma_p) & \longmapsto & (\gamma_1, \gamma_2, \dots, \gamma_{p-1}) \end{array} \right.$$

est bijective, ce qui livrera le résultat car  $\text{card}(\Gamma^{p-1}) = n^{p-1}$ .

• *Injectivité de  $\pi$ .* Soit  $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_p) \in E$  et  $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_p) \in E$  tels que :

$$\pi(\gamma_1, \gamma_2, \dots, \gamma_p) = \pi(\lambda_1, \lambda_2, \dots, \lambda_p).$$

Nous en déduisons que :

$$\forall i \in \llbracket 1, p-1 \rrbracket, \quad \gamma_i = \lambda_i$$

puis :

$$(*) \quad \gamma_1 * \gamma_2 * \dots * \gamma_{p-1} = \lambda_1 * \lambda_2 * \dots * \lambda_{p-1}.$$

D'après la définition de l'ensemble  $E$  et  $(\gamma, \lambda) \in E^2$  :

$$(**) \quad \gamma_p = (\gamma_1 * \gamma_2 * \dots * \gamma_{p-1})^{-1} \quad \text{et} \quad \lambda_p = (\lambda_1 * \lambda_2 * \dots * \lambda_{p-1})^{-1}.$$

De  $(*)$  et  $(**)$  nous déduisons  $\gamma_p = \lambda_p$ , puis  $\gamma = \lambda$ .

• *Surjectivité de  $\pi$ .* Soit  $(\gamma_1, \gamma_2, \dots, \gamma_{p-1}) \in \Gamma^{p-1}$ . On remarque que :

$$\gamma := (\gamma_1, \gamma_2, \dots, \gamma_{p-1}, (\gamma_1 * \gamma_2 * \dots * \gamma_{p-1})^{-1})$$

appartient à  $E$  et que  $\pi(\gamma) = (\gamma_1, \gamma_2, \dots, \gamma_{p-1})$ .

Soit  $c \in \mathfrak{S}_p$  le cycle de longueur  $p$  défini par :

$$c := (1 \quad 2 \quad \dots \quad p-1 \quad p)$$

de sorte que  $c(p) = 1$  et :

$$\forall i \in \llbracket 1, p-1 \rrbracket \quad c(i) = i+1.$$

**Q28.** Démontrer que :

$$G := \{c^k : k \in \llbracket 0, p-1 \rrbracket\}$$

est un sous-groupe du groupe symétrique  $(\mathfrak{S}_p, \circ)$  et que  $\text{card}(G) = p$ .

- Comme  $c^0 = \text{id}_{\llbracket 1, p \rrbracket}$ , l'ensemble  $G$  contient le neutre du groupe  $(\mathfrak{S}_p, \circ)$ .
- Le cycle  $p$  étant de longueur  $p$ , nous savons que :

$$(*) \quad c^p = \text{id}_{\llbracket 1, p \rrbracket}.$$

- Soient  $k, \ell \in \llbracket 0, p-1 \rrbracket$ . La division euclidienne de  $k + \ell$  par  $p$  livre l'existence de  $q \in \mathbb{N}$  et  $r \in \llbracket 0, p-1 \rrbracket$  tels que :

$$k + \ell = qp + r.$$

Nous calculons, grâce à  $(*)$  :

$$c^k \circ c^\ell = c^{k+\ell} = c^{qp+r} = (c^p)^q \circ c^r = c^r \in G.$$

L'ensemble  $G$  est donc stable pour la loi  $\circ$ .

- Soit  $k \in \llbracket 0, p-1 \rrbracket$ .

— Si  $k = 0$ , alors :

$$(c^k)^{-1} = (\text{id}_{\llbracket 1, p \rrbracket})^{-1} = \text{id}_{\llbracket 1, p \rrbracket} \in G.$$

— Si  $k \in \llbracket 1, p-1 \rrbracket$ , alors grâce à  $(*)$  :

$$(c^k)^{-1} = c^{-k} = c^{p-k}.$$

Comme  $p - k \in \llbracket 1, p-1 \rrbracket$  :

$$(c^k)^{-1} = c^{p-k} \in G.$$

L'ensemble  $G$  est donc stable par passage au symétrique.

- La partie  $G$  de  $\mathfrak{S}_p$  contient son élément neutre, est stable pour la loi  $\circ$  et par passage au symétrique. Elle forme donc un sous-groupe de  $(\mathfrak{S}_p, \circ)$ .
- Par définition de  $G$ , l'application :

$$f \left| \begin{array}{ccc} \llbracket 0, p-1 \rrbracket & \longrightarrow & G \\ k & \longmapsto & c^k \end{array} \right.$$

est bien définie et surjective. Nous démontrons son injectivité pour en déduire que  $|G| = p$ .

- Démontrons que l'application  $f$  est injective en raisonnant par l'absurde.

Soient  $k, \ell \in \llbracket 0, p-1 \rrbracket$  tels que :

$$k < \ell \quad \text{et} \quad c^k = f(k) = f(\ell) = c^\ell.$$

En posant  $i := \ell - k$ , nous en déduisons que :

$$1 \leq i \leq p-1 \quad \text{et} \quad c^i = \text{id}_{\llbracket 1, p \rrbracket}.$$

puis :

$$i + 1 = c^i(1) = \text{id}_{\llbracket 1, p \rrbracket}(1) = 1$$

ce qui n'est pas.

Pour tout  $\gamma := (\gamma_1, \gamma_2, \dots, \gamma_p) \in \Gamma^p$  et tout  $\sigma \in \mathfrak{S}_p$ , on définit  $\sigma \cdot \gamma \in \Gamma^p$  par :

$$\sigma \cdot \gamma := (\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \dots, \gamma_{\sigma(p)}) \quad [\text{permutation des composantes de } \gamma].$$

**Q29.** Soit  $\gamma := (\gamma_1, \gamma_2, \dots, \gamma_p) \in E$ . Démontrer que :

$$\forall \sigma \in G \quad \sigma \cdot \gamma \in E.$$

- Comme  $\text{ord}(c) = p$ , nous savons que :

$$G = \langle c \rangle = \{c^k : k \in \llbracket 0, p-1 \rrbracket\}.$$

Par conséquent, il nous faut établir que :

$$\forall k \in \llbracket 0, p-1 \rrbracket \quad c^k \cdot \gamma \in E.$$

- Commençons par démontrer que  $c \cdot \gamma \in E$ . Nous calculons :

$$c \cdot \gamma = (\gamma_2, \gamma_3, \dots, \gamma_{p-1}, \gamma_p, \gamma_1).$$

Comme  $\gamma \in E$  :

$$\begin{aligned} \gamma_2 * \gamma_3 * \dots * \gamma_{p-2} * \gamma_{p-1} * \gamma_p * \gamma_1 &= \gamma_2 * \gamma_3 * \dots * \gamma_{p-2} * \gamma_{p-1} * (\gamma_1 * \gamma_2 * \dots * \gamma_{p-2} * \gamma_{p-1})^{-1} * \gamma_1 \\ &= \gamma_2 * \gamma_3 * \dots * \gamma_{p-2} * \gamma_{p-1} * \gamma_{p-1}^{-1} * \gamma_{p-2}^{-1} * \dots * \gamma_2^{-1} * \gamma_1^{-1} * \gamma_1 \\ &= e_\Gamma \end{aligned}$$

on a bien  $c \cdot \gamma \in E$ . Ainsi :

$$(\star) \quad \text{l'ensemble } E \text{ est stable par l'action de } c.$$

- Clairement :

$$c^0 \cdot \gamma = \text{id}_{\llbracket 1, p \rrbracket} \cdot \gamma = \gamma \in E.$$

Soit  $k \in \llbracket 0, p-2 \rrbracket$  tel que  $c^k \cdot \gamma \in E$ . De :

$$\begin{aligned} c^{k+1} \cdot \gamma &:= (\gamma_{c^{k+1}(1)}, \gamma_{c^{k+1}(2)}, \dots, \gamma_{c^{k+1}(p)}) \\ &= c \cdot (\gamma_{c^k(1)}, \gamma_{c^k(2)}, \dots, \gamma_{c^k(p)}) \\ &= c \cdot (c^k \cdot \gamma) \end{aligned}$$

et de  $(\star)$ , nous déduisons :

$$c^{k+1} \cdot \gamma \in E.$$

D'après ce raisonnement par récurrence finie, il vient :

$$\forall k \in \llbracket 0, p-1 \rrbracket \quad c^k \cdot \gamma \in E.$$

**Q30.** D'après la question précédente, l'application  $\rho$  définie par :

$$\rho \left| \begin{array}{ll} G \times E & \longrightarrow E \\ (\sigma, \gamma) & \longmapsto \sigma \cdot \gamma \end{array} \right.$$

est bien définie. Démontrer qu'elle définit une action du groupe  $G$  sur l'ensemble  $E$ , i.e. que les propriétés (A1) et (A2) de la partie I sont vérifiées.

- Vérification de la propriété (A1). Le neutre du groupe  $G$  est  $\text{id}_{\llbracket 1, p \rrbracket}$ . Soit  $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_p) \in E$ .

$$\text{id}_{\llbracket 1, p \rrbracket} \cdot \gamma := (\gamma_{\text{id}_{\llbracket 1, p \rrbracket}(1)}, \gamma_{\text{id}_{\llbracket 1, p \rrbracket}(2)}, \dots, \gamma_{\text{id}_{\llbracket 1, p \rrbracket}(p)}) = (\gamma_1, \gamma_2, \dots, \gamma_p) = \gamma$$

- Vérification de la propriété (A2). Soient  $(\sigma_1, \sigma_2) \in G^2$  et  $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_p) \in E$ .

$$\begin{aligned} \sigma_1 \cdot (\sigma_2 \cdot \gamma) &= \sigma_1 \cdot (\gamma_{\sigma_2(1)}, \gamma_{\sigma_2(2)}, \dots, \gamma_{\sigma_2(p)}) \\ &= (\gamma_{\sigma_1(\sigma_2(1))}, \gamma_{\sigma_1(\sigma_2(2))}, \dots, \gamma_{\sigma_1(\sigma_2(p))}) \\ &= (\gamma_{\sigma_1 \circ \sigma_2(1)}, \gamma_{\sigma_1 \circ \sigma_2(2)}, \dots, \gamma_{\sigma_1 \circ \sigma_2(p)}) \\ &= (\sigma_1 \circ \sigma_2) \cdot (\gamma_1, \gamma_2, \dots, \gamma_p) \\ &= (\sigma_1 \circ \sigma_2) \cdot \gamma \end{aligned}$$

Fixons un élément  $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_p) \in E$ .

**Q31.** Démontrer que  $\text{card}(\mathcal{O}(\gamma))$  est égal à 1 ou  $p$ .

D'après la question 26,  $\text{card}(\mathcal{O}(\gamma))$  est un diviseur positif de  $\text{card}(G) = p$  premier. Donc  $\text{card}(\mathcal{O}(\gamma)) \in \{1, p\}$ .

**Q32.** Démontrer :

$$\text{card}(\mathcal{O}(\gamma)) = 1 \implies \gamma_1^p = e_\Gamma.$$

Supposons que  $\text{card}(\mathcal{O}(\gamma)) = 1$ . Comme :

$$\mathcal{O}(\gamma) = \{\gamma, c \cdot \gamma, c^2 \cdot \gamma, \dots, c^{p-1} \cdot \gamma\}$$

il vient :

$$\forall k \in \llbracket 1, p-1 \rrbracket \quad \gamma = c^k \cdot \gamma$$

i.e.

$$\forall k \in \llbracket 1, p-1 \rrbracket \quad (\gamma_1, \gamma_2, \dots, \gamma_p) = (\gamma_{c^k(1)}, \gamma_{c^k(2)}, \dots, \gamma_{c^k(p)}) = (\gamma_{k+1}, \gamma_{c^k(2)}, \dots, \gamma_{c^k(p)}) .$$

En observant les premières composantes des  $(p-1)$ -uplets ci-dessus, nous obtenons :

$$\gamma_1 = \gamma_2 = \dots = \gamma_p .$$

Comme  $\gamma \in E$  :

$$e_\Gamma = \gamma_1 * \gamma_2 * \dots * \gamma_p = \gamma_1^p .$$

**Q33.** En déduire qu'il existe  $\kappa \in \Gamma$  tel que  $\kappa \neq e_\Gamma$  et  $\kappa^p = e_\Gamma$ .

• D'après Q22 :

$$(*) \quad \text{card}(E) = \sum_{i=1}^r \text{card}(\mathcal{O}(\gamma_i))$$

où  $\mathcal{O}(\gamma_1), \mathcal{O}(\gamma_2), \dots, \mathcal{O}(\gamma_r)$  est une liste exhaustive et sans répétition des orbites de l'action de  $G$  sur  $E$  définie en Q30.

• Q27 nous permet de réécrire (\*) :

$$(**) \quad n^{p-1} = \sum_{i=1}^r \text{card}(\mathcal{O}(\gamma_i)) .$$

• Nous observons que :

$$\lambda := (e_\Gamma, e_\Gamma, \dots, e_\Gamma) \in E .$$

vérifie :

$$c \cdot \lambda = \lambda .$$

Son orbite est donc :

$$\mathcal{O}(\lambda) = \{\lambda, c \cdot \lambda, c^2 \cdot \lambda, \dots, c^{p-1} \cdot \lambda\} = \{\lambda\} .$$

Cette orbite apparaît donc une et une seule fois dans la liste  $\mathcal{O}(\gamma_1), \mathcal{O}(\gamma_2), \dots, \mathcal{O}(\gamma_r)$  exhaustive et sans répétition de toutes les orbites. Quitte à renuméroter les  $\gamma_1, \dots, \gamma_r$ , on peut supposer que  $\mathcal{O}(\gamma_1) = \mathcal{O}(\lambda)$ . L'identité (\*\*) se réécrit :

$$(***) \quad n^{p-1} = 1 + \sum_{i=2}^r \text{card}(\mathcal{O}(\gamma_i)) .$$

• Si toutes les orbites  $\mathcal{O}(\gamma_2), \dots, \mathcal{O}(\gamma_r)$  ont cardinal  $p$ , alors :

$$0 = 1 \pmod{p} \quad [\text{considérer l'identité (***) modulo } p]$$

ce qui n'est pas. Donc il existe  $i \in \llbracket 2, p \rrbracket$  tel que :

$$\text{card}(\mathcal{O}(\gamma_i)) \neq p .$$

D'après la question 31 :

$$\text{card}(\mathcal{O}(\gamma_i)) = 1 .$$

Alors, comme nous l'avons vu dans la question 32, il existe  $\kappa \in \Gamma$  tel que :

$$\gamma_i = (\kappa, \kappa, \dots, \kappa) \quad \text{et} \quad \kappa^p = e_\Gamma .$$

• Nous démontrons finalement que  $\kappa \neq e_\Gamma$ , en raisonnant par l'absurde, ce qui permettra de conclure au théorème de Cauchy. Supposons donc  $\kappa = e_\Gamma$ . Alors :

$$\gamma_i = (e_\Gamma, e_\Gamma, \dots, e_\Gamma) = \lambda$$

et donc  $\mathcal{O}(\gamma_i) = \mathcal{O}(\lambda) = \mathcal{O}(\gamma_1)$ , ce qui contredit qu'il n'y aucune répétition dans la liste  $\mathcal{O}(\gamma_1), \mathcal{O}(\gamma_2), \dots, \mathcal{O}(\gamma_r)$ .