GROUPES

par David Blottière, le 11 septembre 2023 à 06h47

CORRIGÉ DM 1

PROBLÈME 1 — ACTION D'UN GROUPE ET THÉORÈME DE CAUCHY

I — Action d'un groupe

Soit E un ensemble fini et soit $(G,*)$ un groupe fini, 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) $\forall\, x\in E,\quad e_G\cdot x = x$

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

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

Q1. — Soit $x\in E$. Le *stabilisateur de x* est l'ensemble $\mathrm{Stab}(x)$ défini par :

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

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

- D'après la propriété (A1) de l'action de groupe, $e_G\in\mathrm{Stab}(x)$.
- Soit $(g_1,g_2)\in G^2$. Alors :

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

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

- Soit $g\in\mathrm{Stab}(x)$. Alors :

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

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

Conclusion. La partie $\mathrm{Stab}(x)$ 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 :

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

Q2. — 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 :

$$\begin{array}{rcll} g_1 \cdot x_1 = g_2 \cdot x_2 & \Longrightarrow & g_1^{-1} \cdot (g_1 \cdot x_1) = g_1^{-1} \cdot (g_2 \cdot x_2) & \\ & \Longrightarrow & \left(g_1^{-1} * g_1\right) \cdot x_1 = \left(g_1^{-1} * g_2\right) \cdot x_2 & [(A2)] \\ & \Longrightarrow & e_G \cdot x_1 = \left(g_1^{-1} * g_2\right) \cdot x_2 & \\ & \Longrightarrow & x_1 = \left(g_1^{-1} * g_2\right) \cdot x_2 & [(A1)]\,. \end{array}$$

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

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

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

■

Q3. — Soient $\mathcal{O}(x_1), \ldots, \mathcal{O}\left(x_p\right)$ une liste exhaustive et sans répétition de toutes les orbites. Justifier :

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

et en déduire une expression de $\mathrm{Card}\,(E)$ en fonction des cardinaux des orbites $\mathcal{O}(x_1), \ldots, \mathcal{O}\left(x_p\right)$.

• Comme chacun des ensembles $\mathcal{O}(x_1), \ldots, \mathcal{O}\left(x_p\right)$ 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 $\mathcal{O}(x_1), \ldots, \mathcal{O}\left(x_p\right)$ est une liste exhaustive de toutes les orbites, il existe $i \in [\![1, p]\!]$ 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 $(i, j) \in [\![1, p]\!]^2$ tel que $\mathcal{O}(x_i) \cap \mathcal{O}\left(x_j\right) \neq \emptyset$. D'après la question précédente, il vient $\mathcal{O}(x_i) = \mathcal{O}\left(x_j\right)$. Comme la liste $\mathcal{O}(x_1), \ldots, \mathcal{O}\left(x_p\right)$ 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 :

$$\mathrm{Card}\,(E) = \sum_{k=1}^{p} \mathrm{Card}\,(\mathcal{O}(x_k))\,.$$

■

Q4. — 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 savons qu'il y a une correspondance entre les relations d'équivalence sur E d'une part et les partitions de E d'autre part. Nous l'appliquons pour répondre à la question.
• Nous définissons la relation $\sim$ sur E par, pour tout $(x, y) \in E^2$:

$$x \sim y \quad :\Longleftrightarrow \quad \mathcal{O}(x) = \mathcal{O}\left(y\right)$$

Il est clair que la relation $\sim$ ainsi définie est une relation d'équivalence sur E, dont les classes d'équivalences sont les orbites.
• On peut démontrer, grâce à (A1) et (A2), pour tout $(x, y) \in E^2$:

$$\mathcal{O}(x) = \mathcal{O}\left(y\right) \iff \left(\exists\, g \in G,\ y = g \cdot x\right) \qquad [\text{relation d'équivalence usuelle pour les actions de groupes}]$$

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

■

II — Formule des classes

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

Q5. — On considère l'application τ définie par :

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

Justifier :

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

Comme τ 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 :

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

■

Q6. — Soit $y \in \mathcal{O}(x)$. Démontrer que les ensembles $\mathrm{Stab}(x)$ et $\tau^{-1}\left(\{y\}\right)$ 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 :

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

est bien définie et bijective.

• Caractère bien défini de δ. Pour tout $h \in \mathrm{Stab}(x)$:

$$\begin{array}{rcll} \tau(g*h) & = & (g*h)\cdot x & \\ & = & g\cdot(h\cdot x) & [(A2)] \\ & = & g\cdot x & [h\in\mathrm{Stab}(x)] \\ & = & y. & \end{array}$$

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

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

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

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

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

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

Nous observons que :

$$\begin{array}{rcll} k\cdot x = g\cdot x & \Longrightarrow & g^{-1}\cdot(k\cdot x) = g^{-1}\cdot(g\cdot x) & \\ & \Longrightarrow & \left(g^{-1}*k\right)\cdot x = (g^{-1}*g)\cdot x & [(A2)] \\ & \Longrightarrow & \left(g^{-1}*k\right)\cdot x = e_G\cdot x & \\ & \Longrightarrow & \left(g^{-1}*k\right)\cdot x = x & [(A1)]. \end{array}$$

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

■

Q7. — En déduire la formule des classes, qui s'énonce comme suit :

$$\mathrm{Card}\left(\mathscr{O}(x)\right) = \frac{\mathrm{Card}\,(G)}{\mathrm{Card}\left(\mathrm{Stab}(x)\right)}.$$

D'après la question 5 :

$$\mathrm{Card}\,(G) = \sum_{y\in\mathscr{O}(x)} \mathrm{Card}\left(\tau^{-1}(\{y\})\right).$$

D'après la question 6 :

$$\forall\, y\in\mathscr{O}(x),\quad \mathrm{Card}\left(\tau^{-1}(\{y\})\right) = \mathrm{Card}\left(\mathrm{Stab}(x)\right).$$

Ainsi :

$$\mathrm{Card}\,(G) = \sum_{y\in\mathscr{O}(x)} \mathrm{Card}\left(\mathrm{Stab}(x)\right) = \mathrm{Card}\left(\mathscr{O}(x)\right)\cdot\mathrm{Card}\left(\mathrm{Stab}(x)\right).$$

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

$$\mathrm{Card}\left(\mathscr{O}(x)\right) = \frac{\mathrm{Card}\,(G)}{\mathrm{Card}\left(\mathrm{Stab}(x)\right)}.$$

■

III — Théorème de Cauchy

Soient $(\Gamma,*)$ un groupe fini de cardinal n. Soit p un diviseur premier de n. Nous nous proposons de démontrer que Γ possède un élément d'ordre p (théorème de Cauchy).

Posons :

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

où e_Γ désigne le neutre du groupe $(\Gamma,*)$.

Q8. — Démontrer que E est un ensemble fini, de cardinal n^{p-1}.

Nous démontrons que l'application :

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

est bijective, ce qui livrera le résultat car $\mathrm{Card}\left(\Gamma^{p-1}\right) = n^{p-1}$.
• Injectivité de π. Soit $\gamma = (\gamma_1,\gamma_2,\ldots,\gamma_p)\in E$ et $\lambda = (\lambda_1,\lambda_2,\ldots,\lambda_p)\in E$ tels que :

$$\pi\left(\gamma_1,\gamma_2,\ldots,\gamma_p\right) = \pi\left(\lambda_1,\lambda_2,\ldots,\lambda_p\right).$$

Nous en déduisons que :

$$\forall\, i\in[\![1,p-1]\!],\quad \gamma_i = \lambda_i$$

puis :

$$(\star)\qquad \gamma_1*\gamma_2*\ldots*\gamma_{p-1} = \lambda_1*\lambda_2*\ldots*\lambda_{p-1}.$$

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

$$(\star\star)\qquad \gamma_p = \left(\gamma_1*\gamma_2*\ldots*\gamma_{p-1}\right)^{-1}\qquad\text{et}\qquad \lambda_p = \left(\lambda_1*\lambda_2*\ldots*\lambda_{p-1}\right)^{-1}.$$

De $(\star)$ et $(\star\star)$ nous déduisons $\gamma_p = \lambda_p$, puis $\gamma = \lambda$.
• Surjectivité de π. Soit $(\gamma_1,\gamma_2,\ldots,\gamma_{p-1})\in\Gamma^{p-1}$. On remarque que :

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

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

■

Soit $c \in S_p$ le cycle de longueur p défini par :

$$c := \begin{pmatrix} 1 & 2 & \dots & p-1 & p \end{pmatrix}$$

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

$$\forall\, k \in [\![1, p-1]\!], \quad c(k) = k+1.$$

On note $G := \langle c \rangle$ le sous-groupe de $(S_p, \circ)$ engendré par c.

Q9. — Démontrer que $\mathrm{Card}\,(G) = p$.

Le cycle c est de longueur p, donc a pour ordre p dans le groupe $(S_p, \circ)$. D'après le cours :

$$\mathrm{Card}\,(\langle c \rangle) = \mathrm{ord}(c) = p.$$

■

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

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

Q10. — Soit $\gamma := (\gamma_1, \gamma_2, \dots, \gamma_p) \in E$. Démontrer que :

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

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

$$G = \langle c \rangle = \left\{ c^k \,:\, k \in [\![0, p-1]\!] \right\}.$$

Par conséquent, il nous faut établir que :

$$\forall\, k \in [\![0, p-1]\!], \quad c^k \cdot \gamma \in E.$$

- 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 :

$$\begin{array}{rcll} \gamma_2 * \gamma_3 * \dots * \gamma_{p-2} * \gamma_{p-1} * \gamma_p * \gamma_1 & = & \gamma_2 * \gamma_3 * \dots * \gamma_{p-2} * \gamma_{p-1} * \left(\gamma_1 * \gamma_2 * \dots * \gamma_{p-2} * \gamma_{p-1}\right)^{-1} * \gamma_1 & [\gamma \in E] \\ & = & \gamma_2 * \gamma_3 * \dots * \gamma_{p-2} * \gamma_{p-1} * \gamma_{p-1}^{-1} * \gamma_{p-2}^{-1} * \dots * \gamma_2^{-1} * \gamma_1^{-1} * \gamma_1 & \\ & = & e_\Gamma & \end{array}$$

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

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

- Clairement :

$$c^0 \cdot \gamma = \mathrm{id}_{[\![1,]\!]p} \cdot \gamma = \gamma \in E.$$

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

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

et de $(\star)$, nous déduisons :

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

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

$$\forall\, k \in [\![0, p-1]\!], \quad c^k \cdot \gamma \in E.$$

■

Q11. — D'après la question précédente, l'application ρ définie par :

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

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 $\mathrm{id}_{[\![1,p]\!]}$. Soit $\gamma=(\gamma_1,\gamma_2,\ldots,\gamma_p)\in E$.

$$\mathrm{id}_{[\![1,p]\!]}\cdot\gamma := \left(\gamma_{\mathrm{id}_{[\![1,p]\!]}(1)},\gamma_{\mathrm{id}_{[\![1,p]\!]}(2)},\ldots,\gamma_{\mathrm{id}_{[\![1,p]\!]}(p)}\right)=(\gamma_1,\gamma_2,\ldots,\gamma_p)=\gamma$$

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

$$\begin{array}{rcl} \sigma_1\cdot(\sigma_2\cdot\gamma) & = & \sigma_1\cdot\left(\gamma_{\sigma_2(1)},\gamma_{\sigma_2(2)},\ldots,\gamma_{\sigma_2(p)}\right) \\ & = & \left(\gamma_{\sigma_1(\sigma_2(1))},\gamma_{\sigma_1(\sigma_2(2))},\ldots,\gamma_{\sigma_1(\sigma_2(p))}\right) \\ & = & \left(\gamma_{\sigma_1\circ\sigma_2(1)},\gamma_{\sigma_1\circ\sigma_2(2)},\ldots,\gamma_{\sigma_1\circ\sigma_2(p)}\right) \\ & = & (\sigma_1\circ\sigma_2)\cdot(\gamma_1,\gamma_2,\ldots,\gamma_p) \\ & = & (\sigma_1\circ\sigma_2)\cdot\gamma \end{array}$$

■

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

Q12. — Justifier que :

$$\mathscr{O}(\gamma)=\left\{c^k\cdot\gamma\ :\ k\in[\![0,p-1]\!]\right\}.$$

Par définition :

$$\mathscr{O}(\gamma):=\{g\cdot\gamma\ :\ g\in G\}.$$

Nous avons déjà observé à la question 10 que :

$$G=\langle c\rangle=\left\{c^k\ :\ k\in[\![0,p-1]\!]\right\}.$$

Nous en déduisons que :

$$\mathscr{O}(\gamma)=\left\{c^k\cdot\gamma\ :\ k\in[\![0,p-1]\!]\right\}.$$

■

Q13. — Démontrer que $\mathrm{Card}\left(\mathscr{O}(\gamma)\right)$ est égal à 1 ou p.

D'après la question 7, $\mathrm{Card}\left(\mathscr{O}(\gamma)\right)$ est un diviseur positif de $\mathrm{Card}(G)=p$ premier. Donc $\mathrm{Card}\left(\mathscr{O}(\gamma)\right)\in\{1,p\}$. ■

Q14. — Démontrer :

$$\mathrm{Card}\left(\mathscr{O}(\gamma)\right)=1 \quad\Longrightarrow\quad \gamma_1^p=e_\Gamma.$$

Supposons que $\mathrm{Card}\left(\mathscr{O}(\gamma)\right)=1$. Comme :

$$\mathscr{O}(\gamma)=\{\gamma,c\cdot\gamma,c^2\cdot\gamma,\ldots,c^{p-1}\cdot\gamma\} \qquad \text{[question 12]}$$

il vient :

$$\forall\, k\in[\![1,p-1]\!],\quad \gamma=c^k\cdot\gamma$$

i.e.

$$\forall\, k\in[\![1,p-1]\!],\quad (\gamma_1,\gamma_2,\ldots,\gamma_p)=\left(\gamma_{c^k(1)},\gamma_{c^k(2)},\ldots,\gamma_{c^k(p)}\right)=\left(\gamma_{k+1},\gamma_{c^k(2)},\ldots,\gamma_{c^k(p)}\right).$$

En observant les premières composantes des p-uplets ci-dessus, nous obtenons :

$$\gamma_1 = \gamma_2 = \ldots = \gamma_p.$$

Comme $\gamma \in E$:

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

■

Q15. — En déduire que Γ possède un élément d'ordre p.

- D'après la question 3 :

$$(\star) \qquad \mathrm{Card}\,(E) = \sum_{i=1}^{r} \mathrm{Card}\left(\mathcal{O}\left(\gamma_i\right)\right)$$

où $\mathcal{O}\left(\gamma_1\right), \mathcal{O}\left(\gamma_2\right), \ldots, \mathcal{O}\left(\gamma_r\right)$ est une liste exhaustive et sans répétition des orbites de l'action de G sur E définie en Q11.
- La question 8 nous permet de réécrire $(\star)$:

$$(\star\star) \qquad n^{p-1} = \sum_{i=1}^{r} \mathrm{Card}\left(\mathcal{O}\left(\gamma_i\right)\right)$$

- Nous observons que :

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

vérifie :

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

Son orbite est donc :

$$\mathcal{O}\left(\lambda\right) = \left\{\lambda, c \cdot \lambda, c^2 \cdot \lambda, \ldots, c^{p-1} \cdot \lambda\right\} = \{\lambda\} \qquad [\text{question 12.}]$$

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

$$(\star\star\star) \qquad n^{p-1} = 1 + \sum_{i=2}^{r} \mathrm{Card}\left(\mathcal{O}\left(\gamma_i\right)\right)$$

- Si toutes les orbites $\mathcal{O}\left(\gamma_2\right), \ldots, \mathcal{O}\left(\gamma_r\right)$ ont cardinal p, alors la classe du membre de gauche de $(\star\star\star)$ dans $\mathbb{F}_p$ est $\overline{0}$, alors que la classe du membre de droite de $(\star\star\star)$ dans $\mathbb{F}_p$ est $\overline{1}$. Donc il existe $i \in [\![2, p]\!]$ tel que :

$$\mathrm{Card}\left(\mathcal{O}\left(\gamma_i\right)\right) \neq p.$$

D'après la question 13 :

$$\mathrm{Card}\left(\mathcal{O}\left(\gamma_i\right)\right) = 1.$$

Alors, comme nous l'avons vu dans la question 14, il existe $\kappa \in \Gamma$ tel que :

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

Puisque p est premier, l'ordre de κ est donc 1 ou p.
- Nous démontrons que l'ordre de κ n'est pas 1, en raisonnant par l'absurde, ce qui permettra de conclure. Supposons $\mathrm{ord}(\kappa) = 1$, i.e. $\kappa = e_\Gamma$. Alors :

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

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

PROBLÈME 2 — UN THÉORÈME DE SYLOW

Ce sujet a été posé à l'oral X-MP-2021.

Soit $(G,*)$ un groupe fini de cardinal $p^\alpha \cdot m$, avec p premier, $\alpha \in \mathbf{N}^*$, $m \geqslant 2$ et $p \wedge m = 1$. On se propose de démontrer que G possède un sous-groupe de cardinal p^α (théorème de Sylow).

Si $g \in G$ et A est une partie de G, alors on pose :

$$g * A := \{g * a : a \in A\}.$$

Soit E une partie de G de cardinal p^α. On pose :

$$G(E) := \{g \in G : g * E = E\} \qquad et \qquad \mathcal{O}(E) := \{g * E : g \in G\}.$$

Q16. — Démontrer que $G(E)$ est un sous-groupe de G et que $\mathrm{Card}\,(G(E)) \leqslant p^\alpha$.

Une action de groupe est présente en filigrane dans cet énoncé. Nous la mettons en lumière ci-dessous, pour ensuite pouvoir appliquer les résultats du problème 1.

• Cardinal de $g * A$, où $(g,A) \in G \times \mathscr{P}(G)$. Soient A une partie de G et $g \in G$. Les applications :

$$\varphi \left| \begin{array}{ccc} A & \longrightarrow & g*A \\ a & \longmapsto & g*a \end{array} \right. \quad \text{et} \quad \psi \left| \begin{array}{ccc} g*A & \longrightarrow & A \\ b & \longmapsto & g^{-1}*b \end{array} \right.$$

sont bien définies et vérifient $\psi \circ \varphi = \mathrm{id}_A$ et $\varphi \circ \psi = \mathrm{id}_{g*A}$. Les ensembles A et $g * A$ sont donc équipotents. Ainsi $\mathrm{Card}\,(A) = \mathrm{Card}\,(g * A)$.

• Définition de l'action de groupe. Soit X l'ensemble des parties de G possédant p^α éléments. D'après le point précédent, l'application :

$$\rho \left| \begin{array}{ccc} G \times X & \longrightarrow & X \\ (g,A) & \longmapsto & g*A \end{array} \right.$$

est bien définie.

• Vérification de la propriété (A1). Soit A une partie de G à p^α éléments. Alors :

$$e_G * A := \{e_G * a : a \in A\} = \{a : a \in A\} = A.$$

• Vérification de la propriété (A2). Soient $(g_1,g_2) \in G^2$ et A une partie de G à p^α éléments. Démontrons que les parties $g_1 * (g_2 * A)$ et $(g_1 * g_2) * A$ de G à p^α éléments sont égales. Il suffit d'établir que $g_1 * (g_2 * A) \subset (g_1 * g_2) * A$. Soit $h \in g_1 * (g_2 * A)$. Alors il existe $k \in g_2 * A$ tel que :

$$h = g_1 * k.$$

Comme $k \in g_2 * A$, il existe $a \in A$ tel que :

$$k = g_2 * a.$$

Avec l'associativité de la loi $*$ du groupe G, nous calculons :

$$h = g_1 * (g_2 * a) = (g_1 * g_2) * a.$$

Puisque $a \in A$, il vient $h \in (g_1 * g_2) * A$.

• $G(E)$ est un sous-groupe de $(G,*)$. Nous reconnaissons que $G(E)$ est le stabilisateur de E pour l'action de groupe ρ introduite ci-dessus, i.e. :

$$G(E) = \mathrm{Stab}(E).$$

D'après la question 1, $G(E)$ est un sous-groupe de $(G,*)$.

• $\mathrm{Card}\,(G(E)) \leqslant p^\alpha$. La partie E possédant p^α éléments, elle est non vide. Nous pouvons donc considérer un élément a de E, puis l'application :

$$f \left| \begin{array}{ccc} G(E) & \longrightarrow & E \\ g & \longmapsto & g*a \end{array} \right.$$

qui est bien définie puisque, par définition de $G(E)$, pour tout $(g,a)\in G(E)\times E$, $g*a\in g*E=E$. Comme, pour tout $(g_1,g_2)\in G(E)^2$:

$$\begin{array}{rll} g_1*a=g_2*a & \Longrightarrow & (g_1*a)*a^{-1}=(g_2*a)*a^{-1} \quad \left[a \text{ est un élément du groupe } (G,*)\right] \\ & \Longrightarrow & g_1*\left(a*a^{-1}\right)=g_2*\left(a*a^{-1}\right) \quad \left[\text{associativité de la loi } * \text{ du groupe } G\right] \\ & \Longrightarrow & g_1*e_G=g_2*e_G \\ & \Longrightarrow & g_1=g_2 \end{array}$$

l'application f est injective, d'où :

$$\text{Card}\,(G(E))\leqslant \text{Card}\,(E)=p^\alpha.$$

■

Q17. — Démontrer que :

$$\text{Card}\,(G)=\text{Card}\,(G(E))\cdot\text{Card}\,(\mathscr{O}(E)).$$

Nous reconnaissons que $\mathscr{O}(E)$ est l'orbite de E sous le groupe G, pour l'action ρ introduite à la question 16. D'après la question 7 :

$$\text{Card}\,(G)=\text{Card}\,(\text{Stab}(E))\cdot\text{Card}\,(\mathscr{O}(E))=\text{Card}\,(G(E))\cdot\text{Card}\,(\mathscr{O}(E)).$$

■

Q18. — Démontrer que les trois assertions suivantes sont équivalentes.

(a) p ne divise pas $\text{Card}\,(\mathscr{O}(E))$.

(b) $\text{Card}\,(G(E))=p^\alpha$

(c) $\text{Card}\,(\mathscr{O}(E))=m$

(a)$\Longrightarrow$(b). Supposons que p ne divise pas $\text{Card}\,(\mathscr{O}(E))$, i.e. que $v_p\text{Card}\,(\mathscr{O}(E))=0$. D'après la question 17 :

$$\alpha \underset{p\wedge m=1}{=} v_p\left(\text{Card}\,(G)\right)=v_p\left(\text{Card}\,(G(E))\right)+v_p\left(\text{Card}\,(\mathscr{O}(E))\right)=v_p\left(\text{Card}\,(G(E))\right).$$

Ainsi p^α divise $\text{Card}\,(G(E))$, d'où $p^\alpha\leqslant\text{Card}\,(G(E))$. Or d'après la question 16, $p^\alpha\geqslant\text{Card}\,(G(E))$. Ainsi $\text{Card}\,(G(E))=p^\alpha$.
(b)$\Longrightarrow$(c). Cette implication est conséquence de la question 17.
(c)$\Longrightarrow$(a). Cette implication est conséquence de $p\wedge m=1$. ■

Q19. — On note X l'ensemble des parties de G de cardinal p^α. Déterminer le cardinal de X, puis établir que p ne divise pas $\text{Card}\,(X)$.

• Détermination de $\text{Card}\,(X)$ et stratégie. D'après le cours, l'ensemble des parties à p^α éléments d'un ensemble à $p^\alpha m$ éléments est $\binom{p^\alpha m}{p^\alpha}$. Ainsi :

$$\text{Card}\,(X)=\binom{p^\alpha m}{p^\alpha}.$$

Pour achever notre réponse à cette question, il nous faut démontrer que p ne divise pas $\binom{p^\alpha m}{p^\alpha}$, i.e. que :

$$\mathscr{P}(\alpha)\ :\ v_p\left(\left(p^\alpha m\right)!\right)=v_p\left(\left(p^\alpha\right)!\right)+v_p\left(\left(p^\alpha m-p^\alpha\right)!\right).$$

• $v_p((ap)!)=a+v_p(a!)$, pour tout $a\in\mathbf{N}^*$. Soit $a\in\mathbf{N}^*$. Nous observons :

$$v_p((ap)!)=\sum_{i=1}^{ap}v_p(i)$$

Comme :

$$[\![1, ap]\!] = \bigsqcup_{i=0}^{a-1} \{1+ip, 2+ip, \ldots, p-1+ip, p+ip\}$$

il vient :

$$v_p((ap)!) = \sum_{i=1}^{ap} v_p(i) = \sum_{i=0}^{a-1} \left(\underbrace{v_p(1+ip)}_{=0} + \underbrace{v_p(2+ip)}_{=0} + \ldots + \underbrace{v_p(p-1+ip)}_{=0} + \underbrace{v_p(p+ip)}_{=1+v_p(i+1)} \right)$$

puis :

$$(\star) \qquad v_p((ap)!) = \sum_{i=0}^{a-1} 1 + \sum_{i=0}^{a-1} v_p(i+1) = a + v_p\left(\prod_{i=0}^{a-1} i \right) = a + v_p(a!).$$

• Initialisation de $\mathscr{P}(\alpha)$ à $\alpha = 0$. L'assertion $\mathscr{P}(0)$ s'écrit :

$$v_p(m!) = \underbrace{v_p(1!)}_{=0} + v_p((m-1)!)$$

Comme $p \wedge m = 1$, $v_p(m) = 0$ et donc :

$$v_p(m!) = v_p(m \cdot (m-1)!) = v_p(m) + v_p((m-1)!) = v_p((m-1)!)$$

ce qui établit $\mathscr{P}(0)$.

• Caractère héréditaire de $\mathscr{P}(\alpha)$. Soit $\alpha \in \mathbf{N}$ tel que $\mathscr{P}(\alpha)$ est vraie. D'après $(\star)$:

$$v_p\left((p^{\alpha+1}m)!\right) - v_p\left((p^{\alpha+1})!\right) - v_p\left((p^{\alpha+1}m - p^{\alpha+1})!\right)$$

égale :

$$p^\alpha m + v_p\left((p^\alpha m)!\right) - \left(p^\alpha + v_p\left((p^\alpha)!\right)\right) - \left(p^\alpha m - p^\alpha + v_p\left((p^\alpha m - p^\alpha)!\right)\right)$$

ou encore, après simplification, égale :

$$v_p\left((p^\alpha m)!\right) - v_p\left((p^\alpha)!\right) - v_p\left((p^\alpha m - p^\alpha)!\right).$$

Grâce à $\mathscr{P}(\alpha)$, ce dernier terme est nul et donc :

$$v_p\left((p^{\alpha+1}m)!\right) = v_p\left((p^{\alpha+1})!\right) + v_p\left((p^{\alpha+1}m - p^{\alpha+1})!\right).$$

■

Q20. — Démontrer que G possède un sous-groupe de cardinal p^α.

• D'après la question 3 :

$$(\star) \qquad \mathrm{Card}(X) = \sum_{k=1}^{r} \mathrm{Card}(\mathscr{O}(E_i))$$

où $\mathscr{O}(E_1), \mathscr{O}(E_2), \ldots, \mathscr{O}(E_r)$ est une liste exhaustive et sans répétition des orbites de l'actions du groupe G sur l'ensemble X définie à la question 16.

• D'après la question 19 et l'identité $(\star)$, il existe $i \in [\![1, r]\!]$ tel que p ne divise pas $\mathrm{Card}(\mathscr{O}(E_i))$.

• D'après les questions 16 et 18, $G(E_i)$ est un sous-groupe de $(G, *)$ de cardinal p^α.

■