Correction du DM n°14

Exercice 1

Soit $(a,b) \in \mathbb{Z}^2$. Alors :

$$\begin{aligned} a \top b &= a^2 + b^2 \\ &= b^2 + a^2 \\ &= b \top a \end{aligned}$$

c'est-à-dire : $\boxed{\top \text{ est commutative.}}$

Soit $(a,b,c) \in \mathbb{Z}^3$. D'une part :

$$\begin{aligned} a \top (b \top c) &= a \top (b^2 + c^2) \\ &= a^2 + (b^2 + c^2)^2 \\ &= a^2 + b^4 + 2b^2c^2 + c^4 \end{aligned}$$

et d'autre part :

$$\begin{aligned} (a \top b) \top c &= (a^2 + b^2) \top c \\ &= (a^2 + b^2)^2 + c^2 \\ &= a^4 + 2a^2b^2 + b^4 + c^2 \end{aligned}$$

On ne trouve pas la même chose : montrons que la loi n'est pas associative (il faut un contre-exemple explicite !). Il suffit de voir que $0 \top (0 \top 2) = 16$ et $(0 \top 0) \top 2 = 4$ pour conclure :

$\boxed{\text{La loi n'est pas associative.}}$

Montrons qu'il n'y a pas d'élément neutre. Soit $a \in \mathbb{Z}$. $2 \top a = 4 + a^2 \geqslant 4$ donc $2 \top a \neq 2$: il n'existe aucun élément a tel que $2 \top a = 2$ donc

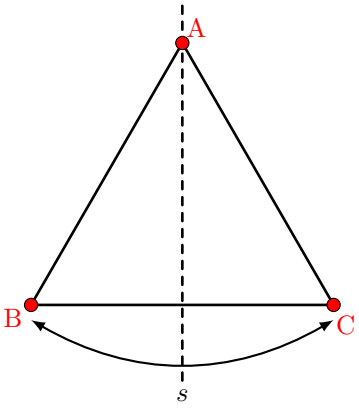
$\boxed{\text{La loi n'admet pas d'élément neutre.}}$

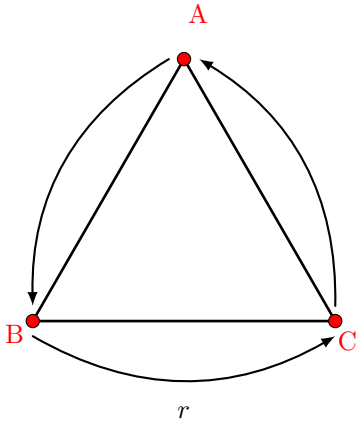
Dès lors $\boxed{\text{Aucun élément n'est symétrisable.}}$

> Rappelons que parler d'élément symétrisable n'a de sens que lorsqu'il existe un élément neutre.

Exercice 2 :

1





2

- L'identité laisse les trois sommets invariants.
- r envoie A sur B, B sur C et C sur A.
- r^2 envoie A sur C, C sur B et B sur A.
- s laisse A invariant et échange B et C.
- $s \circ r$ (attention au sens de la composition : on applique r puis on applique s) envoie A sur C, B est laissé invariant et C est envoyé sur A.
- $s \circ r^2$ envoie A sur B, B sur A et laisse C invariant.

Les six éléments sont bien distincts.

3 Donnons la table de la composition. Précisons que ce qui se trouve à la ligne f et la colonne g est $f \circ g$ dans cet ordre. Par exemple, $r \circ s$ envoie A sur B, B sur A, et laisse C invariant donc $r \circ s = s \circ r^2$. Idem pour les autres.

$\circ$	Id	r	r^2	s	$s \circ r$	$s \circ r^2$
Id	Id	r	r^2	s	$s \circ r$	$s \circ r^2$
r	r	r^2	Id	$s \circ r^2$	s	$s \circ r$
r^2	r^2	Id	r	$s \circ r$	$s \circ r^2$	s
s	s	$s \circ r$	$s \circ r^2$	Id	r	r^2
$s \circ r$	$s \circ r$	$s \circ r^2$	s	r^2	Id	r
$s \circ r^2$	$s \circ r^2$	s	$s \circ r$	r	r^2	Id

4 La composition est associative, la loi est interne d'après la table précédente, Id est un élément neutre (comme la loi n'est pas commutative, il faut vérifier qu'il y a un neutre à gauche et à droite, qui sont évidemment égaux d'après le cours), et tout élément admet un inverse (comme la loi n'est pas commutative, il faut vérifier que tout élément admet un inverse à gauche et à droite, qui sont évidemment égaux d'après le cours). De plus, la loi est associative : par exemple, $r \circ s \neq s \circ r$.

D_3 est un groupe non abélien.

> Il est isomorphe à S_3, le groupe des permutations de $[\![1\,;3]\!]$. C'est le plus petit groupe (au sens du cardinal) non abélien (à isomorphisme près).

Exercice 3 :

1 Montrons que $\mathrm{Stab}(x)$ est un sous-groupe de G.

- $exe^{-1} = exe = x$ donc $e \in \mathrm{Stab}(x)$: $\mathrm{Stab}(x)$ est non vide.
- Soient g_1 et g_2 deux éléments de $\mathrm{Stab}(x)$.

$$\begin{aligned}
(g_1g_2)x(g_1g_2)^{-1} &= (g_1g_2)x({g_2}^{-1}{g_1}^{-1}) && \text{(On change l'ordre quand on inverse)}\\
&= g_1(g_2x{g_2}^{-1}){g_1}^{-1} && \text{(Loi associative)}\\
&= g_1x{g_1}^{-1} && (\text{car } g_2 \in \mathrm{Stab}(x))\\
&= x && (\text{car } g_1 \in \mathrm{Stab}(x))
\end{aligned}$$

  En d'autres termes, $g_1g_2 \in \mathrm{Stab}(x)$: $\mathrm{Stab}(x)$ est stable par produit.
- $g_1 \in \mathrm{Stab}(x)$ donc $g_1x{g_1}^{-1} = x$. En multipliant à gauche par ${g_1}^{-1}$ et à droite par g_1, on obtient $x = {g_1}^{-1}xg_1$ donc ${g_1}^{-1} \in \mathrm{Stab}(x)$: $\mathrm{Stab}(x)$ est stable par inverse.

$\boxed{\text{Stab}(x) \text{ est un sous-groupe de G.}}$

> Vous aurez peut-être reconnu l'ensemble $\text{Z}_x = \{g \in \text{G} \,|\, gx = xg\}$. On le note différemment car la notion de stabilisateur peut se généraliser.

2

- Soit $x \in \text{G}$. $exe^{-1} = x$ donc $x \sim x$: $\sim$ est transitive.
- Soient x et y dans G tels que $x \sim y$. Alors il existe $g \in \text{G}$ tel que $gxg^{-1} = y$. En multipliant à gauche par g^{-1} et à droite par g, il vient : $x = g^{-1}yg$ donc $x = (g^{-1})^{-1}yg^{-1}$, c'est-à-dire que $y \sim x$: $\sim$ est symétrique.
- Soient x, y, z dans G tels que $x \sim y$ et $y \sim z$: il existe g_1 et g_2 dans G tels que ${g_1}xg_1{}^{-1} = y$ et ${g_2}yg_2{}^{-1} = z$ donc

$$\begin{aligned} z &= g_2g_1x{g_1}^{-1}{g_2}^{-1} \\ &= g_2g_1x(g_2g_1)^{-1} \end{aligned}$$

ce qui prouve que $x \sim z$: $\sim$ est transitivie.

$\boxed{\sim \text{ est bien une relation d'équivalence.}}$

3 D'après le cours, les classes d'équivalence forment une partition de l'ensemble.

$\boxed{\text{Les orbites forment une partition de G.}}$

En particulier, une seule contient le neutre. Attention, cela n'en fait pas un sous-groupe pour autant (du moins, pas pour l'instant) ! Mais cela suffit à affirmer que les autres n'en sont pas. Par conséquent, il existe au plus une classe d'équivalence, celle de e, qui soit un sous-groupe. Déterminons $\text{O}(e)$, l'orbite de e. Par définition :

$$\text{O}(e) = \{geg^{-1} \,|\, g \in \text{G}\}$$

Or, pour tout $g \in \text{G}$, $geg^{-1} = e$ donc $\text{O}(e) = \{e\}$ qui est évidemment un sous-groupe de G.

$\boxed{\text{Parmi les orbites, seule O}(e) \text{ est un sous-groupe de G, et celle-ci est égale à } \{e\}.}$

4 Soit $x \in \text{G}$. Soit

$$\varphi : \begin{cases} \text{G} \longrightarrow \text{O}(x) \\ g \longmapsto gxg^{-1} \end{cases}$$

φ est surjective par définition de $\text{O}(x)$. Soit $y \in \text{O}(x)$. Cherchons le nombre d'antécédents de y par φ. Il existe donc $g_1 \in \text{G}$ tel que $y = \varphi(g_1) = {g_1}x{g_1}^{-1}$. Soit $g_2 \in \text{G}$. Cherchons quand ${g_2}x{g_2}^{-1} = y$. Travaillons par équivalences :

$$\begin{aligned} {g_2}x{g_2}^{-1} = y &\iff {g_2}x{g_2}^{-1} = {g_1}x{g_1}^{-1} \\ &\iff {g_1}^{-1}{g_2}x{g_2}^{-1}g_1 = x \\ &\iff {g_1}^{-1}{g_2}x\left({g_1}^{-1}g_2\right)^{-1} = x \\ &\iff {g_1}^{-1}g_2 \in \text{Stab}(x) \\ &\iff \exists g \in \text{Stab}(x), {g_1}^{-1}g_2 = g \\ &\iff \exists g \in \text{Stab}(x), g_2 = g_1g \end{aligned}$$

En d'autres termes, les antécédents de y par φ sont exactement les g_1g avec $g \in \text{Stab}(x)$. Dès lors, la fonction

$$f : \begin{cases} \text{Stab}(x) \longrightarrow \varphi^{-1}(\{y\}) \\ g \longmapsto g_1g \end{cases}$$

est surjective. Montrons qu'elle est injective. Attention, ce n'est pas un morphisme de groupes ! Soient g et g' tels que $f(g) = f(g')$ alors $g_1g = g_1g'$ donc (en multipliant par ${g_1}^{-1}$ à gauche) $g = g'$: f est injective donc bijective, si bien que

$\mathrm{Card}\,(\varphi^{-1}(\{y\})) = \mathrm{Card}\,(\mathrm{Stab}(x))$. Finalement, tout élément de $\mathrm{O}(x)$ admet $\mathrm{Card}\,(\mathrm{Stab}(x))$ antécédents par φ, et on conclut avec le lemme des bergers.

$$\boxed{\mathrm{Card}\,(\mathrm{G}) = \mathrm{Card}\,(\mathrm{O}(x)) \times \mathrm{Card}\,(\mathrm{Stab}(x))}$$

5 Supposons que $\mathrm{Card}\,(\mathrm{O}(x)) = 1$. Alors $\mathrm{O}(x) = \{x\}$ puisque $x \in \mathrm{O}(x)$ (un élément est toujours équivalent à lui-même puisqu'une relation d'équivalence est réflexive). Soit $g \in \mathrm{G}$. Alors $gxg^{-1} \in \mathrm{O}(x)$ donc $gxg^{-1} = x$ donc (en multipliant par g à droite) $gx = xg$: x commute avec tout élément de g, $x \in \mathrm{Z(G)}$.

Réciproquement, supposons que $x \in \mathrm{Z(G)}$. Soit $y \in \mathrm{O}(x)$: il existe $g \in \mathrm{G}$ tel que $y = gxg^{-1}$. Or, x et g commutent donc $y = xgg^{-1} = x$ donc $\mathrm{O}(x) \subset \{x\}$ et l'inclusion réciproque est immédiate d'après ce qui précède, donc $\mathrm{O}(x) = \{x\}$ et en particulier $\mathrm{Card}\,(\mathrm{O}(x)) = 1$.

$$\boxed{\text{On a l'équivalence voulue.}}$$

6 D'après la question 3, G est l'union disjointe des classes d'équivalence :

$$\mathrm{G} = \bigcup_{\mathrm{O}(x)} \mathrm{O}(x)$$

L'union étant disjointe, le cardinal de l'union est la somme des cardinaux :

$$\mathrm{Card}\,(\mathrm{G}) = \sum_{\mathrm{O}(x)} \mathrm{Card}\,(\mathrm{O}(x))$$

Mettons à part les orbites à un élément :

$$\begin{aligned}\mathrm{Card}\,(\mathrm{G}) &= \sum_{\mathrm{O}(x)\,|\,\mathrm{Card}\,(\mathrm{O}(x))=1} \mathrm{Card}\,(\mathrm{O}(x)) + \sum_{\mathrm{O}(x)\,|\,\mathrm{Card}\,(\mathrm{O}(x))\neq 1} \mathrm{Card}\,(\mathrm{O}(x)) \\ &= \sum_{\mathrm{O}(x)\,|\,\mathrm{Card}\,(\mathrm{O}(x))=1} 1 + \sum_{\mathrm{O}(x)\,|\,\mathrm{Card}\,(\mathrm{O}(x))\neq 1} \mathrm{Card}\,(\mathrm{O}(x))\end{aligned}$$

Or, quand le terme sommé ne dépend pas de l'indice de sommation, comme c'est le cas dans la première somme, la somme est égal au terme sommé, ici 1, multiplié par le nombre de termes, ici le nombre d'orbites à un élément donc le cardinal de Z(G) d'après la question précédente, ce qui permet de conclure.

$$\boxed{\mathrm{Card}\,(\mathrm{G}) = \mathrm{Card}\,(\mathrm{Z(G)}) + \sum_{\mathrm{O}(x)\,|\,\mathrm{Card}\,(\mathrm{O}(x))\neq 1} \mathrm{Card}\,(\mathrm{O}(x))}$$

D'après la question 4, le cardinal d'une orbite divise le cardinal de G qui est une puissance de p, disons p^n, par hypothèse, donc le cardinal d'une orbite est de la forme p^k avec $k \leqslant n$ (p est premier). Par conséquent, lorsqu'une orbite n'est pas réduite à un élément, son cardinal est divisible par p ce qui est le résultat voulu.

$$\boxed{\mathrm{Card}\,(\mathrm{G}) \equiv \mathrm{Card}\,(\mathrm{Z(G)})[p]}$$

7.(a) On sait que Z(G) est un sous-groupe de G donc est non vide, mais c'est à la bordure du programme, donc il suffit de dire que $e \in \mathrm{Z(G)}$ car e commute avec tous les éléments de G.

$$\boxed{\mathrm{Card}\,(\mathrm{Z(G)}) \neq 0}$$

7.(b) $\mathrm{Card}\,(\mathrm{Z(G)}) = p$ et $\mathrm{Card}\,(\mathrm{G}) = p^2$ donc $\mathrm{Z(G)} \neq \mathrm{G}$:

$$\boxed{\text{Il existe } x \in \mathrm{Z(G)}.}$$

Soit $g \in \mathrm{Z(G)}$. Alors $gx = xg$ donc $gxg^{-1} = x$ si bien que $g \in \mathrm{Stab}(x)$, c'est-à-dire que $\mathrm{Z(G)} \subset \mathrm{Stab}(x)$. De plus, $xxx^{-1} = x$ donc $x \in \mathrm{Stab}(x)$. Or, $x \notin \mathrm{Z(G)}$ donc cette inclusion est stricte. L'inclusion $\mathrm{Stab}(x)$ est immédiate. Cependant, $x \notin \mathrm{Z(G)}$ donc il existe $g \in \mathrm{G}$ tel que $xg \neq gx$ donc $x \neq gxg^{-1}$: $g \notin \mathrm{Stab}(x)$, donc la dernière inclusion est encore stricte.

$$\boxed{\text{Il existe } x \in \mathrm{Z(G)} \text{ et on a } \mathrm{Z(G)} \subsetneq \mathrm{Stab}(x) \subsetneq \mathrm{G}}$$

D'après la question 4, $\mathrm{Card}\,(\mathrm{Stab}(x))$ divise $\mathrm{Card}\,(\mathrm{G}) = p^2$ donc $\mathrm{Card}\,(\mathrm{Stab}(x)) = 1, p$ ou p^2 : or, $\mathrm{Card}\,(\mathrm{Z(G)}) = p$ donc $\mathrm{Card}\,(\mathrm{Stab}(x)) > p$ donc $\mathrm{Card}\,(\mathrm{Stab}(x)) = p^2$ ce qui est absurde puisque $\mathrm{Stab}(x) \neq \mathrm{G}$.

Le cardinal de Z(G) ne peut pas être égal à p.

7.(c) On en déduit que Card $(\mathrm{Z(G)}) = p^2$ donc $\mathrm{Z(G)} = \mathrm{G}$: tous les éléments de G commutent avec tout le monde, c'est-à-dire que

G est abélien.

Problème

Partie I. Crochet de Lie et exemple de dérivation

1 Si a et b commutent, alors $ab = ba$ donc

Si a et b commutent, $[a, b] = 0$.

2.(a) $[a, b] = ab - ba$ et $[b, a] = ba - ab$, si bien que

$$[a, b] = -[b, a].$$

2.(b) On a :

$$\begin{aligned}
[a, b + c] &= a(b + c) - (b + c)a \\
&= ab + ac - ba - ca && \text{(Le produit est distributif par rapport à la somme)} \\
&= ab - ba + ac - ca && \text{(La somme est commutative)} \\
&= [a, b] + [a, c]
\end{aligned}$$

$$[a, b + c] = [a, b] + [a, c]$$

2.(c) Notons $\mathrm{S} = [a, [b, c]] + [b, [c, a]] + [c, [a, b]]$.

$$\begin{aligned}
\mathrm{S} &= [a, bc - cb] + [b, ca - ac] + [c, ab - ba] \\
&= a(bc - cb) - (bc - cb)a + b(ca - ac) - (ca - ac)b + c(ab - ba) - (ab - ba)c \\
&= abc - acb - bca + cba + bca - bac - cab + acb + cab - cba - abc + bac
\end{aligned}$$

Finalement $$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$$

3 Soit $(x, y) \in \mathrm{A}^2$. D'une part :

$$\begin{aligned}
d_a(x + y) &= a(x + y) - (x + y)a \\
&= ax + ay - xa - ya \\
&= (ax - xa) + (ay - ya) \\
&= d_a(x) + d_a(y)
\end{aligned}$$

D'autre part $$\begin{aligned}
xd_a(y) + d_a(x)y &= x(ay - ya) + (ax - xa)y \\
&= xay - xya + axy - xay \\
&= axy - xya \\
&= d_a(xy)
\end{aligned}$$

En conclusion $\boxed{d_a \text{ est bien une dérivation sur A.}}$

Partie II. Propriétés des dérivations

1 Par définition d'une dérivation, $\delta(0+0) = \delta(0) + \delta(0)$ donc $\delta(0) = \delta(0) + \delta(0)$ si bien que $\delta(0) = 0$. De plus, $\delta(1 \times 1) = 1\delta(1) + \delta(1)1$ c'est-à-dire que $\delta(1) = \delta(1) + \delta(1)$. Finalement :

$$\boxed{\delta(0) = \delta(1) = 0}$$

2.a Par définition d'une dérivation, $\delta(x - x) = \delta(x) + \delta(-x)$. Or, $x - x = 0$ et $\delta(0) = 0$ si bien que $\delta(x) + \delta(-x) = 0$. Il en découle que :

$$\boxed{\delta(-x) = -\delta(x)}$$

2.(b) D'après la question 1, $\delta(xx^{-1}) = \delta(1) = 0$. Par définition d'une dérivation :

$$\delta(xx^{-1}) = 0 = x\delta(x^{-1}) + \delta(x)x^{-1}$$

Dès lors $$x\delta(x^{-1}) = -\delta(x)x^{-1}$$

Finalement (x étant inversible) $$\boxed{\delta(x^{-1}) = -x^{-1}\delta(x)x^{-1}}$$

3.(a) Montrons par récurrence que pour tout $n \geqslant 1$:

$$\delta(x_1 \dots x_n) = \delta(x_1)x_2 \dots x_n + x_1\delta(x_2)x_3 \dots x_n + \dots + x_1 \dots x_{n-1}\delta(x_n)$$

> Attention, l'anneau n'étant pas commutatif, on ne peut pas écrire comme sur $\mathbb{R}$:
>
> $$\delta(x_1 \dots x_n) = \sum_{i=1}^{n} \delta(x_i) \prod_{j \neq i} x_j$$

- Si $n \geqslant 1$, notons H_n :

  « $\forall (x_1, \dots, x_n) \in \mathrm{A}^n, \delta(x_1 \dots x_n) = \delta(x_1)x_2 \dots x_n + x_1\delta(x_2)x_3 \dots x_n + \dots + x_1 \dots x_{n-1}\delta(x_n)$ »
- Si $x_1 \in \mathrm{A}$, $\delta(x) = \delta(x)$ donc H_1 est trivialement vraie.
- Soit $n \geqslant 1$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Soit $(x_1, \dots, x_{n+1}) \in \mathrm{A}^{n+1}$. Par définition d'une dérivation (en posant $x = x_1 \dots x_n$) :

$$\begin{aligned}
\delta(x_1 \dots x_{n+1}) &= x_1 \dots x_n\delta(x_{n+1}) + \delta(x_1 \dots x_n)x_{n+1} \\
&= x_1 \dots x_n\delta(x_{n+1}) + \delta(x_1)x_2 \dots x_nx_{n+1} + x_1\delta(x_2)x_3 \dots x_nx_{n+1} + \dots + x_1 \dots x_{n-1}\delta(x_n)x_{n+1} \qquad \text{(HR)} \\
&= \delta(x_1)x_2 \dots x_nx_{n+1} + x_1\delta(x_2)x_3 \dots x_nx_{n+1} + \dots + x_1 \dots x_{n-1}\delta(x_n)x_{n+1} + x_1 \dots x_n\delta(x_{n+1})
\end{aligned}$$

  c'est-à-dire que H_{n+1} est vraie.
- D'après le principe de récurrence, H_n est vraie pour tout $n \geqslant 1$.

$$\boxed{\forall (x_1, \dots, x_n) \in \mathrm{A}^n, \delta(x_1 \dots x_n) = \delta(x_1)x_2 \dots x_n + x_1\delta(x_2)x_3 \dots x_n + \dots + x_1 \dots x_{n-1}\delta(x_n)}$$

3.(b) D'après la question précédente, en prenant les x_i tous égaux à x (et donc les x_i commutent, mais attention, ils ne commutent pas forcément avec $\delta(x)$) :

$$\boxed{\delta(x^n) = \delta(x)x^{n-1} + x\delta(x)x^{n-2} + x^2\delta(x)x^{n-3} + \dots + x^{n-1}\delta(x)}$$

Si x et $\delta(x)$ commutent : $$\boxed{\delta(x^n) = nx^{n-1}\delta(x)}$$

4.(a) On a déjà vu que 0 et 1 appartiennent à C_δ (question 1). Il suffit donc de prouver que C_δ est stable par somme, par opposé et par produit. Soient x et y deux éléments de C_δ i.e. tels que $\delta(x) = \delta(y) = 0$.

- $\delta(-x) = -\delta(x)$ d'après la question 2.(a) donc $\delta(-x) = 0$: $-x \in \mathrm{C}_\delta$, C_δ est stable par opposé.
- $\delta(x+y) = \delta(x) + \delta(y) = 0$ donc $x + y \in \mathrm{C}_\delta$: C_δ est stable par somme, c'est un sous-groupe de A.
- $\delta(xy) = x\delta(y) + \delta(x)y = x \times 0 + 0 \times y = 0$ puisque 0 est absorbant : $xy \in \mathrm{C}_\delta$, C_δ est stable par produit.

$\boxed{\mathrm{C}_\delta \text{ est un sous-anneau de A.}}$

4.(b) A étant un corps, il est supposé commutatif (dans cette question uniquement), donc C_δ l'est aussi. Il suffit donc de prouver que $\mathrm{C}_\delta \backslash \{0\}$ est stable par inverse, puisqu'on sait déjà que C_δ est un sous-anneau de A. Soit donc $x \neq 0$ dans C_δ. D'après la question 2.(b) :

$$\delta(x^{-1}) = -x^{-1}\delta(x)x^{-1}$$

Or, $\delta(x) = 0$ et 0 est absorbant donc $\delta(x^{-1}) = 0$ ce qui permet de conclure.

$\boxed{\text{Si A est un corps alors } \mathrm{C}_\delta \text{ est un sous-corps de A.}}$

Partie III. Manipulations de dérivations

1.(a) Soient x et y dans A. δ_1 et δ_2 étant des dérivations, d'une part :

$$\begin{aligned}(\delta_1+\delta_2)(x+y) &= \delta_1(x+y) + \delta_2(x+y)\\ &= \delta_1(x) + \delta_1(y) + \delta_2(x) + \delta_2(y)\\ &= \delta_1(x) + \delta_2(x) + \delta_1(y) + \delta_2(y)\\ &= (\delta_1+\delta_2)(x) + (\delta_1+\delta_2)(y)\end{aligned}$$

et d'autre part

$$\begin{aligned}(\delta_1+\delta_2)(xy) &= \delta_1(xy) + \delta_2(xy)\\ &= x\delta_1(y) + \delta_1(x)y + x\delta_2(y) + \delta_2(x)y\\ &= x(\delta_1(y)+\delta_2(y)) + (\delta_1(x)+\delta_2(x))y \qquad \text{(Distributivité)}\\ &= x(\delta_1+\delta_2)(y) + (\delta_1+\delta_2)(x)y\end{aligned}$$

Finalement $\boxed{\delta_1 + \delta_2 \text{ est une dérivation.}}$

1.(b) Soient x et y deux éléments de A. D'une part :

$$\begin{aligned}[\delta_1,\delta_2](x+y) &= \delta_1(\delta_2(x+y)) - \delta_2(\delta_1(x+y))\\ &= \delta_1(\delta_2(x)+\delta_2(y)) - \delta_2(\delta_1(x)+\delta_1(y)) \qquad (\delta_2 \text{ et } \delta_1 \text{ dérivations})\\ &= \delta_1(\delta_2(x)) + \delta_1(\delta_2(y)) - \delta_2(\delta_1(x)) - \delta_2(\delta_1(y)) \qquad \text{(idem)}\\ &= [\delta_1,\delta_2](x) + [\delta_1,\delta_2](y)\end{aligned}$$

D'autre part :

$$\begin{aligned}[\delta_1,\delta_2](xyy) &= \delta_1(\delta_2(xy)) - \delta_2(\delta_1(xy))\\ &= \delta_1(x\delta_2(y)+\delta_2(x)y) - \delta_2(x\delta_1(y)+\delta_1(x)y)\\ &= x\delta_1(\delta_2(y)) + \delta_1(x)\delta_2(y) + \delta_2(x)\delta_1(y) + \delta_1(\delta_2(x))y - x\delta_2(\delta_1(y)) - \delta_2(x)\delta_1(y) - \delta_1(x)\delta_2(y) - \delta_2(\delta_1(x))y\\ &= x\delta_1(\delta_2(y)) + \delta_1(\delta_2(x))y - x\delta_2(\delta_1(y)) - \delta_2(\delta_1(x))y\\ &= x[\delta_1,\delta_2](y) + [\delta_1,\delta_2](x)y\end{aligned}$$

En conclusion $\boxed{[\delta_1, \delta_2] \text{ est une dérivation.}}$

2.(a) Soit $x \in \mathrm{A}$.

$$\begin{aligned}[\delta, d_a] &= \delta(d_a(x)) - d_a(\delta(x)) \\ &= \delta(ax - xa) - a\delta(x) + \delta(x)a \\ &= a\delta(x) + \delta(a)x - x\delta(a) - \delta(x)a - a\delta(x) + \delta(x)a \\ &= \delta(x)x - x\delta(a) \\ &= d_{\delta(a)}(x)\end{aligned}$$

x étant quelconque $\boxed{[\delta, d_a] = d_{\delta(a)}}$

2.(b) D'après la question précédente, avec $\delta = d_b$:

$$\begin{aligned}[d_b, d_a] &= d_{d_b(a))} \\ &= d_{ba-ab} \\ &= d_{[b,a]}\end{aligned}$$

Par symétrie des rôles entre a et b on a le résultat voulu

$$\boxed{[d_a, d_b] = d_{[a,b]}}$$

Exercice 4 - Le Dobble

1

- Il y a évidemment q droites verticales puisqu'une droite verticale d'équation $x = c$ est entièrement déterminée par le choix de $c \in \mathbb{K}$ et il y a $\mathrm{Card}\,(\mathbb{K}) = q$ choix possibles.
- Ensuite, une droite non verticale d'équation $y = ax + b$ est entièrement déterminée par le choix de a et le choix de b, il y a q choix possibles pour chacun donc, d'après le principe multiplicatif, il y a q^2 droites non verticales, ce qui fait bien $q^2 + q$ droites possibles, quand nous aurons montré que toutes les droites sont bien deux à deux distinctes.
- Tout d'abord, si $a_1 \neq a_2$ alors les droites verticales d'équation $x = a_1$ et $x = a_2$ sont distinctes car la première contient le point $(a_1, 0)$ et pas la deuxième : les droites verticales sont donc bien deux à deux distinctes.
- Si $a_1 \in \mathbb{K}$ et si a et b appartiennent à $\mathbb{K}$, montrons que la droite d'équation $x = a_1$ et la droite (non verticale) d'équation $y = ax + b$ sont distinctes. Si $a_1 \neq 0$, la droite non verticale ne contient pas le point $(0, b)$ mais l'autre le contient, donc elles sont distinctes, et si $a_1 = 0$, la droite verticale ne contient pas le point $(1, a + b)$ alors que l'autre le contient. Dans tous les cas, les deux droites sont distinctes.
- Soient $(a_1, b_1) \neq (a_2, b_2)$ deux couples distincts. Si $b_1 \neq b_2$, la droite d'équation $y = a_1x + b_1$ ne contient pas le point $(0, b_2)$ contrairement à la droite d'équation $y = a_2x + b_2$, et si $b_1 = b_2$ alors $a_1 \neq a_2$ donc la première contient le point $(1, a_1 + b_1)$ et pas la deuxième (car $a_2 \neq a_1$ et $b_2 = b_1$).

$$\boxed{\text{Il y a bien } q^2 + q \text{ droites dans } \mathbb{K}^2.}$$

2 Soit $u = (x_1, y_1) \in \mathbb{K}^2$. Alors u appartient à une unique droite verticale, celle d'équation $x = x_1$. Il suffit donc de prouver que u appartient à q droites non verticales. Soit $(a, b) \in \mathbb{K}^2$. Alors u appartient à la droite d'équation $y = ax + b$ si et seulement si $y_1 = ax_1 + b$. Dès lors, pour tout $a \in \mathbb{K}$ (q choix possibles), un seul b convient ($b = y_1 - ax_1$). Il y a donc q droites non verticales qui conviennent u.

$$\boxed{\text{Tout point de } \mathbb{K}^2 \text{ appartient à exactement } q + 1 \text{ droites.}}$$

3 Soient donc $u_1 = (x_1, y_1)$ et $u_2 = (x_2, y_2)$ deux points distincts de $\mathbb{K}^2$.

- Si $x_1 = x_2$: alors u_1 et u_2 appartiennent à la droite d'équation $x = x_1$, d'où l'existence. De plus, ils n'appartiennent à aucune autre droite non verticale. Enfin, si $(a, b) \in \mathbb{K}^2$, supposons que u_1 et u_2 appartiennent à la droite d'équation $y = ax + b$, si bien que $y_1 = ax_1 + b$ et $y_2 = ax_2 + b$ et $x_1 = x_2$ donc $y_1 = y_2$ ce qui est absurde puisque les points sont distincts. Aucune droite non verticale ne contient ces deux points ensemble, d'où l'unicité.
- Si $x_1 \neq x_2$ alors u_1 et u_2 ne sont pas sur une même droite verticale (tous les points d'une même droite verticale ont la même abscisse). Analyse : soit donc $(a, b) \in \mathbb{K}^2$ tel que u_1 et u_2 appartiennent à la droite d'équation $y = ax + b$. Alors $y_1 = ax_1 + b$ et $y_2 = ax_2 + b$ donc, par différence, $y_1 - y_2 = a(x_1 - x_2)$. Or, $x_1 - x_2 \neq 0$ et on est sur un corps donc cet élément est inversible si bien que $a = (y_1 - y_2) * (x_1 - x_2)^{-1}$ et $b = y_1 - ax_1$. Synthèse : si on pose $a = (y_1 - y_2) * (x_1 - x_2)^{-1}$ et $b = y_1 - ax_1$ alors u_1 et u_2 appartiennent à la droite d'équation $y = ax + b$. En effet :

$$ax_1 + b = a * x_1 + y_1 - a * x_1$$

$$= y_1$$

et idem pour l'autre : d'où l'existence et l'unicité.

Par deux points distincts passe une et une seule droite.

4 Tout point ordinaire appartient à $q + 1$ droites ordinaires et n'est pas sur la droite à l'infini, donc le résultat est prouvé pour les points ordinaires.

I_v appartient uniquement aux q droites verticales et à la droite à l'infini, ce qui fait encore $q + 1$ droites. Enfin, si I est un point à l'infini différent de I_v, il existe q tel que $I = I_a$, si bien que I appartient uniquement aux q droites obliques de coefficient directeur a et à la droite à l'infini.

Chaque point (à l'infini ou non) appartient à $q + 1$ droites (à l'infini ou non).

5 On a déjà répondu à cette question lorsque les deux points ne sont pas à l'infini et la droite n'est pas à l'infini. Il reste donc à étudier trois cas cas : deux points pas à l'infini mais la droite à l'infini, un seul point à l'infini, ou les deux points à l'infini.

- Si les deux points ne sont pas à l'infini, ils n'appartiennent pas (par définition) à la droite à l'infini.
- Soient $u = (x_1, y_1)$ un point « ordinaire » et soit I_v le point à l'infini vertical. Puisque u est un point « ordinaire », il n'appartient pas à la droite infinie. I appartient à la droite verticale d'équation $x = x_1$ donc les deux points appartiennent à cette même droite, d'où l'existence. Cependant, par définition, I_v n'appartient à aucune droite oblique donc à aucune des autres droites auxquelles u appartient (question 2 : u appartient à une droite verticale et q droites obliques), d'où l'unicité.
- Soient $u = (x_1, y_1)$ un point « ordinaire » et soit I un point à l'infini non vertical : il existe donc $a \in \mathbb{K}$ tel que $I = I_a$. On sait (question 2) que u appartient à une unique droite oblique de coefficient directeur a donc cette droite contient les deux points, d'où l'existence. Et puisque I_a n'appartient qu'à des droites de coefficient directeur a (sauf la droite infinie mais u n'est pas sur cette droite), I_a n'appartient à aucune autre droite qui passe par u, d'où l'unicité.
- Soient I et J deux points infinis distincts. Si I est vertical et J non, alors I n'appartient qu'aux droites verticales et à la droite infinie, et J n'appartient à aucune droite verticale et la droite infinie, donc par ces deux points ne passe que la droite infinie. Si aucun des deux n'est égal à I_v, alors il existe $a \neq b$ tels que $I = I_a$ et $J = I_b$. I n'appartient qu'aux droites de coefficient directeur a et la droite infinie, et idem pour I_b (coefficient directeur b) donc seule la droite infinie contient ces deux points.

Par deux points (à l'infini ou non) passe exactement une droite (à l'infini ou non).

6 Commençons par les points.

- On a q^2 points ordinaires.
- Il y a $q + 1$ points à l'infini : I_v puis tous les points I_a avec $a \in \mathbb{K}$ donc q choix possibles.

Il y a donc $q^2 + q + 1$ points (à l'infini ou non).

Ensuite, on a déjà prouvé qu'il y avait $q^2 + q$ droites ordinaires, auxquelles il faut rajouter la droite à l'infini.

Il y a donc $q^2 + q + 1$ droites (à l'infini ou non).

Problème - Actions de groupes

Partie I. Notion de loi externe etc.

1.(a) Soit $u = (u_1, \dots, u_n) \in \mathbb{R}^n$. Puisque le neutre de $\mathbb{R}_+^*$ (pour la loi $\times$) est 1, la condition (C_1) devient : $1.u = u$, ce qui est le cas par définition de la loi. De plus, pour tous g_1 et g_2 dans $\mathbb{R}_+^*$,

$$\begin{aligned} g_1.(g_2.u) &= g_1.(g_2 \times u_1, \dots, g_2 \times u_n) \\ &= (g_1. \times g_2 \times u_1, \dots, g_1 \times g_2 \times u_n) && \text{associativité du produit} \\ &= (g_1 \times g_2).u \end{aligned}$$

c'est-à-dire que la condition (C_2) est vérifiée.

L'ensemble $\mathbb{R}_+^*$ agit sur l'ensemble $\mathbb{R}^n$ pour cette loi externe.

1.(b) L'ensemble $\mathbb{R}$ étant un groupe pour l'addition, le neutre est 0 donc la condition (C_1) devient : $\forall u \in \mathbb{R}^n, 0.u = u$ ce qui n'est pas le cas car $0.u = (0, \dots, 0)$.

$\mathbb{R}$ n'agit pas sur $\mathbb{R}^n$ pour cette loi externe.

> Cependant, cette loi externe est tout de même utile : elle munira $\mathbb{R}^n$ d'une structure de $\mathbb{R}$-espace vectoriel, cf. chapitre 28.

1.(c) Il suffit de donner une loi externe modelée sur la question 1.(a), mais version addition, c'est-à-dire :

$$\forall u = (u_1, \dots, u_n) \in \mathbb{R}^n, \forall g \in \mathbb{R}, g.u = (g + u_1, \dots, g + u_n)$$

c'est-à-dire qu'on ajoute g à toutes les coordonnées. La condition (C_1) devient : $\forall u \in \mathbb{R}^n, 0.u = u$, ce qui est le cas, et la condition (C_2) devient :

$$\forall u \in \mathbb{R}^n, \forall (g_1, g_2) \in \mathbb{R}^2, g_1.(g_2.u) = (g_1 + g_2).u$$

et on montre comme dans la question 1.(a) que cette condition est vérifiée.

Avec cette loi externe, $\mathbb{R}$ agit sur $\mathbb{R}^n$.

2 Le neutre de S_n (muni de la composition, donc) est l'identité, et on a bien, pour tout i, $\mathrm{id}\,.x_i = x_{\mathrm{id}\,(i)} = x_i$. En d'autres termes : $\forall x \in X, \mathrm{id}\,.x = x$, c'est-à-dire que la condition (C_1) est vérifiée.
Soient à présent σ_1 et σ_2 deux éléments de S_n et soit $i \in [\![1 ; n]\!]$. Par définition de la loi externe,

$$\begin{aligned} \sigma_1.(\sigma_2.x_i) &= \sigma_1.x_{\sigma_2(i)} \\ &= x_{\sigma_1(\sigma_2(i))} \\ &= x_{\sigma_1 \circ \sigma_2(i)} \\ &= \sigma_1 \circ \sigma_2.x_i \end{aligned}$$

et donc la condition (C_2) est elle-aussi vérifiée :

S_n agit bien sur l'ensemble X : on peut donc faire agir S_n sur tout ensemble à n éléments.

3.(a) Vérifions (C_1) : soit donc $x \in G$. Par définition, $e.x = e * x = x$ par définition du neutre, c'est-à-dire que la condition (C_1) est vérifiée. Soient à présent g_1 et g_2 dans G. Alors :

$$\begin{aligned} g_1.(g_2.x) &= g_1.(g_2 * x) && \text{Définition de la loi externe} \\ &= g_1 * (g_2 * x) && \text{Idem} \\ &= (g_1 * g_2) * x && \text{Associativité de } * \\ &= (g_1 * g_2).x \end{aligned}$$

c'est-à-dire que la condition (C_2) est vérifiée.

Un groupe agit bien sur lui-même par translation à gauche.

3.(b) Précisons qu'il n'y a pas de parenthèses dans l'expression $g * x * g^{-1}$ car la loi est associative. Vérifions (C_1) : soit donc $x \in G$. Par définition, $e.x = e * x * e^{-1}$. Or, $e^{-1} = e$ donc $e.x = e * x * e = x$ par définition du neutre, c'est-à-dire que la condition (C_1) est vérifiée. Soient à présent g_1 et g_2 dans G. Alors :

$$\begin{aligned} g_1.(g_2.x) &= g_1.(g_2 * x * {g_2}^{-1}) \\ &= g_1 * g_2 * x * {g_2}^{-1} * {g_1}^{-1} \\ &= (g_1 * g_2) * x * (g_1 * g_2)^{-1} && \text{On change l'ordre quand on inverse} \\ &= (g_1 * g_2).x \end{aligned}$$

c'est-à-dire que la condition (C_2) est vérifiée.

Un groupe agit bien sur lui-même par conjugaison.

4.(a) Montrons que φ est bien définie, c'est-à-dire que, pour tout g, $\varphi(g)$ est bien une bijection de X dans lui-même. Soit donc $g \in G$.

- Tout d'abord, par définition d'une action de groupe, pour tout x, $g.x \in X$ donc $\varphi(g)$ prend bien un élément de X et renvoie un élément de X donc va bien de X dans X.
- Montrons que $\varphi(g)$ est injective. Soient donc x_1 et x_2 tels que $\varphi(g)(x_1) = \varphi(g)(x_2)$ i.e. $g.x_1 = g.x_2$. En composant par g^{-1} à gauche, il vient :

  $$g^{-1}.(g.x_1) = g^{-1}.(g.x_2)$$

  En utilisant la condition (C_2), on trouve $(g^{-1} * g).x_1 = (g^{-1} * g).x_2$ donc $e.x_1 = e.x_2$ si bien que $x_1 = x_2$ en utilisant la condition (C_1) : $\varphi(g)$ est bien injective.
- Soit $y \in X$. Soit $x = g^{-1}.y$. De même, en utilisant (C_2) puis (C_1), on trouve que $g.x = y$ donc $\varphi(g)(x) = y$: x est un antécédent de y par $\varphi(g)$ donc $\varphi(g)$ est surjective : φ est bien définie.

Montrons enfin que φ est un morphisme de groupes. Soient donc g_1 et g_2 dans G. On veut prouver que $\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$ (rappelons que S_X est un groupe pour la composition, et que $\varphi(g_1)$ et $\varphi(g_2)$ sont des fonctions et même des bijections). Cela découle simplement de la condition (C_2) : en effet, si $x \in X$,

$$\begin{aligned} \varphi(g_1 * g_2)(x) &= (g_1 * g_2).x \\ &= g_1.(g_2.x) && \text{Condition } (C_2) \\ &= \varphi(g_1)(g_2.x) \\ &= \varphi(g_1)(\varphi(g_2)(x)) \\ &= \varphi(g_1) \circ \varphi(g_2)(x) \end{aligned}$$

Les deux fonctions $\varphi(g_1 * g_2)$ et $\varphi(g_1) \circ \varphi(g_2)$ coïncident en tout $x \in X$ donc sont égales, ce qui permet de conclure.

φ est bien définie et est un morphisme de groupes.

4.(b) On pourrait raisonner par double implication, mais on va utiliser la caractérisation de l'injectivité des morphismes de groupes vue en classe. Puisque φ est un morphisme de groupes d'après la question précédente, φ est injective si et seulement si son noyau est réduit au neutre, i.e. $\mathrm{Ker}\,(\varphi) = \{e\}$. Or, par définition, le noyau est l'ensemble des éléments qui ont comme image le neutre du groupe d'arrivée, c'est-à-dire id ici puisque le groupe d'arrivée est S_X. Par conséquent, φ est injective si et seulement si e est le seul élément de G vérifiant $\varphi(g) = \mathrm{id}$ c'est-à-dire : $\forall x \in X, \varphi(g)(x) = g.x = \mathrm{id}\,(x) = x$, c'est-à-dire si et seulement si e est le seul élément de G qui stabilise tous les éléments de X, ce qui est le résultat voulu.

φ est injective si et seulement si e est le seul élément du groupe qui stabilise tous les éléments de l'ensemble.

Partie II. Orbites et stabilisateurs

1 Montrons que c'est une relation d'équivalence.

- Soit $x \in \mathrm{X}$. D'après la condition (C_1), $e.x = x$ donc il existe bien un élément $g \in \mathrm{G}$ tel que $x = g.x$: $x\mathrm{R}x$ donc R est réflexive.
- Soient x et $y \in \mathrm{X}$ tels que $x\mathrm{R}y$. Alors il existe $g \in \mathrm{X}$ tel que $y = g.x$. Dès lors, $g^{-1}.y = g^{-1}.(g.x)$. À l'aide de la condition (C_2) puis de la condition (C_1), on trouve que

$$\begin{aligned} g^{-1}.y &= \left(g^{-1} * g\right).x \\ &= e.x \\ &= x \end{aligned}$$

  donc $y\mathrm{R}x$: R est symétrique.
- Soient $x, y, z \in \mathrm{X}$ tels que $x\mathrm{R}y$ et $y\mathrm{R}z$: il existe g_1 et g_2 (qui n'ont aucune raison d'être égaux) tels que $y = g_1.x$ et $z = g_2.y$ donc, d'après la condition (C_2), $z = (g_2 * g_1).x$ c'est-à-dire que $x\mathrm{R}z$: R est transitive.

R est bien une relation d'équivalence.

2 Montrons donc que $\mathrm{Stab}(x)$ est un sous-groupe de G.

- D'après la condition (C_1), on sait que $e \in \mathrm{Stab}(x)$ donc $\mathrm{Stab}(x)$ est non vide.
- Soient g_1 et $g_2 \in \mathrm{Stab}(x)$. En utilisant la condition (C_2) (mais je vais arrêter de le préciser à chaque fois, idem pour (C_1)) :

$$\begin{aligned} (g_1 * g_2).x &= g_1.(g_2.x) \\ &= g_1.x && \text{car } g_2 \in \mathrm{Stab}(x) \\ &= x && \text{car } g_1 \in \mathrm{Stab}(x) \end{aligned}$$

  c'est-à-dire que $g_1 * g_2 \in \mathrm{Stab}(x)$: $\mathrm{Stab}(x)$ est stable par la loi de G.
- Enfin, soit $g \in \mathrm{Stab}(x)$. Alors $x = g.x$ si bien que, de même que ci-dessus, $g^{-1}.x = x$ donc $g^{-1} \in \mathrm{Stab}(x)$: $\mathrm{Stab}(x)$ est stable par inverse.

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

Cependant, $\omega(x)$ est une partie de X et pas une partie de G donc ce n'est pas un sous-groupe de G, et même si $\mathrm{G} = \mathrm{X}$ (comme par exemple dans la question 3 de la partie I), les orbites étant deux à deux disjointes, une seule contient le neutre donc les autres ne peuvent pas non plus être des sous-groupes de G.

$\omega(x)$ n'est pas (du tout) un sous-groupe de G.

3.(a) On sait que les classes d'équivalence forment une partition de l'ensemble (cf. cours), c'est-à-dire que X est l'union des orbites et que celles-ci sont deux à deux disjointes. Le résultat découle donc de la question 1 en disant que le cardinal d'une union de parties deux à deux disjointes est la somme des cardinaux.

$$\boxed{\mathrm{Card}\,(\mathrm{X}) = \sum_{\omega(x)} \mathrm{Card}\,(\omega(x))}$$

3.(b) Soit $x \in \mathrm{X}$. Alors $x \in \mathrm{X}^{\mathrm{G}}$ si et seulement si x est fixé par tous les éléments de G, si et seulement si son orbites est réduite à $\{x\}$ (puisque son orbite est constituée des éléments de la forme $g.x$). En d'autres termes, $x \in \mathrm{X}^{\mathrm{G}}$ si et seulement si $\mathrm{Card}\,(\omega(x)) = 1$. Dès lors, d'après la question précédente :

$$\begin{aligned} \mathrm{Card}\,(\mathrm{X}) &= \sum_{\omega(x)\,|\,x \in \mathrm{X}^{\mathrm{G}}} \mathrm{Card}\,(\omega(x)) + \sum_{\omega(x)\,|\,x \notin \mathrm{X}^{\mathrm{G}}} \mathrm{Card}\,(\omega(x)) \\ &= \sum_{\omega(x)\,|\,x \in \mathrm{X}^{\mathrm{G}}} 1 + \sum_{\omega(x)\,|\,x \notin \mathrm{X}^{\mathrm{G}}} \mathrm{Card}\,(\omega(x)) \end{aligned}$$

ce qui permet de conclure (une somme de termes égaux à 1 est égale au nombre de termes de la somme donc, ici, au cardinal de X^{G}).

$$\boxed{\mathrm{Card}\,(\mathrm{X}) = \mathrm{Card}\,(\mathrm{X}^{\mathrm{G}}) + \sum_{\omega(x)\,|\,x\notin \mathrm{X}^{\mathrm{G}}} \mathrm{Card}\,(\omega(x))}$$

4.(a) On pourrait travailler par double inclusion (et ça marcherait très bien), mais on va plutôt raisonner par équivalences. Soit donc $x \in \mathrm{X} = \mathrm{G}$.

$$\begin{aligned} x \in \mathrm{X}^{\mathrm{G}} &\iff \forall g \in \mathrm{G}, g.x = x \\ &\iff \forall g \in \mathrm{G}, g * x * g^{-1} = x \\ &\iff \forall g \in \mathrm{G}, g * x = x * g \\ &\iff x \in \mathrm{Z}(\mathrm{G}) \end{aligned}$$

$$\boxed{\mathrm{X}^{\mathrm{G}} = \mathrm{Z}(\mathrm{G})}$$

4.(b) Soit $x \in \mathrm{G}$. Soit

$$u\colon \begin{cases} \mathrm{G} \longrightarrow \omega(x) \\ g \longmapsto gxg^{-1} \end{cases}$$

u est surjective par définition de $\omega(x)$. Soit $y \in \omega(x)$. Cherchons le nombre d'antécédents de y par u. Il existe donc $g_1 \in \mathrm{G}$ tel que $y = u(g_1) = g_1 x {g_1}^{-1}$. Soit $g_2 \in \mathrm{G}$. Cherchons quand $g_2 x {g_2}^{-1} = y$. Travaillons par équivalences :

$$\begin{aligned} g_2 x {g_2}^{-1} = y &\iff g_2 x {g_2}^{-1} = g_1 x {g_1}^{-1} \\ &\iff {g_1}^{-1} g_2 x {g_2}^{-1} g_1 = x \\ &\iff {g_1}^{-1} g_2 x \left({g_1}^{-1} g_2\right)^{-1} = x \\ &\iff {g_1}^{-1} g_2 \in \mathrm{Stab}(x) \\ &\iff \exists g \in \mathrm{Stab}(x), {g_1}^{-1} g_2 = g \\ &\iff \exists g \in \mathrm{Stab}(x), g_2 = g_1 g \end{aligned}$$

En d'autres termes, les antécédents de y par u sont exactement les $g_1 g$ avec $g \in \mathrm{Stab}(x)$. Dès lors, la fonction

$$f\colon \begin{cases} \mathrm{Stab}(x) \longrightarrow u^{-1}(\{y\}) \\ g \longmapsto g_1 g \end{cases}$$

est surjective. Montrons qu'elle est injective. Attention, ce n'est pas un morphisme de groupes ! Soient g et g' tels que $f(g) = f(g')$ alors $g_1 g = g_1 g'$ donc (en multipliant par ${g_1}^{-1}$ à gauche) $g = g'$: f est injective donc bijective, si bien que $\mathrm{Card}\,(u^{-1}(\{y\})) = \mathrm{Card}\,(\mathrm{Stab}(x))$. Finalement, tout élément de $\omega(x)$ admet $\mathrm{Card}\,(\mathrm{Stab}(x))$ antécédents par u, et on conclut avec le lemme des bergers.

$$\boxed{\mathrm{Card}\,(\mathrm{G}) = \mathrm{Card}\,(\omega(x)) \times \mathrm{Card}\,(\mathrm{Stab}(x))}$$

4.(c) D'après la question précédente, le cardinal d'une orbite divise le cardinal de G qui est égal à p^n donc le cardinal d'une orbite est de la forme p^k avec $k \leqslant n$ (p est premier). Par conséquent, lorsqu'une orbite n'est pas réduite à un élément, son cardinal est divisible par p ce qui est le résultat voulu.

$$\boxed{\mathrm{Card}\,(\mathrm{G}) \equiv \mathrm{Card}\,(\mathrm{Z}(\mathrm{G}))[p]}$$

4.(d) D'après la question précédente, $\mathrm{Card}\,(\mathrm{Z}(\mathrm{G})) \not\equiv 1[p]$ donc Z§G) $\neq \{e\}$.

$$\boxed{\text{Le centre d'un } p\text{-groupe est non trivial.}}$$

Partie III. Théorème de Cauchy

1 Par définition de la loi externe, on a successivement :

$$\boxed{0.x = (x_1, \dots, x_p), 1.x = (x_2, x_3, \dots, x_p, x_1) \qquad \text{et} \qquad 2.x = (x_3, x_4, \dots, x_p, x_1, x_2)}$$

2 Un élément $x = (x_1, \dots, x_p)$ est entièrement déterminé par :

- le choix de $x_1 \in \mathrm{G}$: n choix possibles.
- le choix de $x_2 \in \mathrm{G}$: n choix possibles.
- $\vdots$
- le choix de $x_{p-1} \in \mathrm{G}$: n choix possibles.

Il n'y a alors qu'un seul choix possible pour x_p : puisque $x_1 * \cdots * x_p = e$ alors on a forcément

$$x_p = (x_1 * \cdots * x_{p-1})^{-1} = {x_{p_1}}^{-1} * \cdots * {x_1}^{-1}$$

donc un seul choix possible pour x_p : le principe multiplicatif permet de conclure.

$$\boxed{\mathrm{Card}\,(\mathrm{X}) = n^{p-1}}$$

3 D'après la partie précédente, (avec $\mathbb{Z}/p\mathbb{Z}$ à la place de G puisque c'est le groupe qui agit),

$$\mathrm{Card}\,(\mathrm{Stab}(x)) \times \mathrm{Card}\,(\omega(x)) = \mathrm{Card}\,(\mathbb{Z}/p\mathbb{Z}) = p$$

En particulier, $\mathrm{Card}\,(\omega(x))$ divise p. Or, p est un nombre premier donc :

$$\boxed{\text{Pour tout } x,\ \mathrm{Card}\,(\omega(x)) = p \text{ ou } 1.}$$

4 D'après l'équation aux classes :

$$\mathrm{Card}\,(\mathrm{X}) = \mathrm{Card}\,\left(\mathrm{X}^{\mathbb{Z}/p\mathbb{Z}}\right) + \sum_{\omega(x)\,|\,x \notin \mathrm{X}^{\mathbb{Z}/p\mathbb{Z}}} \mathrm{Card}\,(\omega(x))$$

Soit $x \notin \mathrm{X}^{\mathbb{Z}/p\mathbb{Z}}$. Alors l'orbite de x n'est pas réduite à un élément (voir la partie II) donc est de cardinal p. Dès lors, la somme ci-dessus est divisible par p donc $\mathrm{Card}\,(\mathrm{X}) \equiv \mathrm{Card}\,\left(\mathrm{X}^{\mathbb{Z}/p\mathbb{Z}}\right)\,[p]$. Enfin, n est divisible par p par hypothèse donc n^{p-1} également si bien que $n^{p-1} \equiv 0[p]$. D'où le résultat.

$$\boxed{\mathrm{Card}\,\left(\mathrm{X}^{\mathbb{Z}/p\mathbb{Z}}\right) \equiv 0[p]}$$

5 Notons E le premier ensemble de l'énoncé. Soit

$$h : \begin{cases} \mathrm{E} \longrightarrow \mathrm{X}^{\mathbb{Z}/p\mathbb{Z}} \\ x \longmapsto \underbrace{(x, \dots, x)}_{p \text{ fois}} \end{cases}$$

- Tout d'abord, h est bien à valeurs dans X : soit en effet $x \in \mathrm{E}$. Alors $x * \cdots * x = x^p = e$ par définition de E donc $h(x) \in \mathrm{E}$.
- Ensuite, pour tout $k \in \mathbb{Z}/p\mathbb{Z}$, $k.h(x) = h(x)$ (les coordonnées de $h(x)$ sont toutes égales donc $h(x)$ est laissé invariant par permutation circulaire, donc par l'action de k.
- h est trivialement injective (si $x_1 \neq x_2$ alors $h(x_1) \neq h(x_2)$ car leurs coordonnées sont toutes distinctes).
- Soit enfin $y \in \mathrm{X}^{\mathbb{Z}/p\mathbb{Z}}$. Si y a deux coordonnées distinctes, disons y_a et y_b alors $(b-a).y$ a pour coordonnée y_b en position a donc $(b-a).y \neq y$ ce qui contredit le fait que $y \in \mathrm{X}^{\mathbb{Z}/p\mathbb{Z}}$. On en déduit que toutes les coordonnées de y sont égales à y_1 donc $y = (y_1, \dots, y_1) = h(y_1)$: h est surjective.

$$\boxed{h : \begin{cases} \mathrm{E} \longrightarrow \mathrm{X}^{\mathbb{Z}/p\mathbb{Z}} \\ x \longmapsto \underbrace{(x, \dots, x)}_{p \text{ fois}} \end{cases} \text{ est une bijection de E dans } \mathrm{X}^{\mathbb{Z}/p\mathbb{Z}}.}$$

6 D'après la question précédente, E et $X^{\mathbb{Z}/p\mathbb{Z}}$ ont le même cardinal donc $\text{Card}\,(E) \equiv 0[p]$ d'après la question 4. Or, $e \in E$ donc $\text{Card}\,(E) \geqslant 1$ et, toujours grâce à la congruence, $\text{Card}\,(E) \neq 1$: il existe donc un élément x différent de e dans E et x vérifie $x^p = e$ par définition de E : d'où le résultat.

$$\boxed{\text{G admet un sous-groupe de cardinal } p.}$$

> Le théorème de Lagrange (HP) vu en classe dit que le cardinal d'un sous-groupe divise le cardinal du groupe. Le problème est que la réciproque est fausse : si d divise n et si G est un groupe de cardinal n, G n'admet pas forcément de sous-groupe de cardinal d. Par exemple, il existe des groupes à 12 éléments n'ayant aucun sous-groupe de cardinal 6. Le théorème de Cauchy (et le premier théorème de Sylow vu dans la suite) peut donc être vu comme une « réciproque partielle » du théorème de Lagrange : si p est un facteur premier de n alors G admet un sous-groupe de cardinal p.

Partie IV. Notion de p-Sylow et premiers résultats

1 Soit donc $\varphi : G_1 \to G_2$ un isomorphisme de groupes, et soit S_1 un p-Sylow de G_1. Notons $S_2 = \varphi(S_1)$. Alors :

- $\text{Card}\,(G_1) = \text{Card}\,(G_2)$ car φ est bijective. Notons $p^\alpha \times m$ avec $m \wedge p = 1$ leur cardinal commun, si bien qu'un p-Sylow est un sous-groupe de cardinal p^α.
- S_2 est un sous-groupe de G_2 (image d'un sous-groupe par un morphisme de groupes).
- $\text{Card}\,(S_1) = \text{Card}\,(S_2)$ (S_1 et S_2 sont en bijection, car φ injective donc est une bijection sur son image et S_2 est l'image de S_1) donc ont le même cardinal p^α donc S_2 est bien un p-Sylow de G_2.

$$\boxed{G_2 \text{ admet un } p\text{-Sylow.}}$$

2 Soient x_1 et x_2 dans G. On a :

$$\begin{aligned}\varphi(x_1x_2) &= ax_1x_2a^{-1}\\ &= ax_1ex_2a^{-1}\\ &= ax_1a^{-1}ax_2a^{-1}\\ &= \varphi(x_1)\varphi(x_2)\end{aligned}$$

c'est-à-dire que φ est un morphisme de groupes. Montrons qu'il est injectif en examinant son noyau. Soit donc $x \in \text{Ker}\,(\varphi)$. Alors $axa^{-1} = e$ donc $ax = a$ (en multipliant par a à droite) donc (tout élément est régulier, ou en multipliant par a^{-1} à gauche) $x = e$: $\text{Ker}\,(\varphi) = \{e\}$ donc φ est injectif entre deux ensembles finis de même cardinal donc est bijectif.

$$\boxed{\varphi \text{ est un automorphisme.}}$$

Notons enfin $T = aSa^{-1}$. T étant l'image de S par φ, on montre comme ci-dessus que c'est un p-Sylow de G (bijectif car injectif donc bijectif sur son image, donc S et T ont le même cardinal).

$$\boxed{aSa^{-1} \text{ est un } p\text{-Sylow de G.}}$$

3 Par double inclusion.

- Soit $x \in g_1(g_2A)$. Alors il existe $y \in g_2A$ tel que $x = g_1y$ et $y \in g_2A$ donc il existe $a \in A$ tel que $y = g_2a$ donc $x = g_1(g_2a) = (g_1g_2)a$ (associativité de la loi) donc $x \in (g_1g_2)A$: d'où l'inclusion $g_1(g_2A) \subset (g_1g_2)A$.
- Réciproquement, soit $x \in (g_1g_2)A$. Alors il existe a tel que $x = (g_1g_2)a = g_1(g_2a)$. Dès lors, $g_2a \in g_2A$ et donc $x \in g_1(g_2A)$, d'où l'inclusion réciproque, d'où l'égalité.

$$\boxed{g_1(g_2A) = (g_1g_2)A}$$

4 Par double inclusion.

- Soit $a \in S$. Alors $a = s * (s^{-1} * a)$. Or, S est un sous-groupe de G donc stable par inverse et par produit donc $s^{-1} \in S$ et $s^{-1} * a \in S$ si bien que $a \in sS$: $S \subset sS$.

- Soit $a \in s\mathrm{S}$: il existe donc $b \in \mathrm{S}$ tel que $a = sb$ et S est stable par produit donc $sb \in \mathrm{S}$, d'où l'inclusion réciproque, d'où l'égalité.

$$\boxed{\text{Si } s \in \mathrm{S} \text{ alors } s\mathrm{S} = \mathrm{S}.}$$

5 Si $\alpha = 0$ alors un groupe de cardinal p^α est un groupe à 1 élément et le seul sous-groupe à un élément de G est $\{e\}$ (car un sous-groupe contient le neutre, donc s'il n'a qu'un élément, c'est que c'est le seul) : G admet un seul « p-Sylow », le singleton $\{e\}$.

$$\boxed{\text{Bref, aucun intérêt.}}$$

> Remarquons que les trois théorèmes de Sylow sont encore vrais dans ce cas, mais appliquer les théorèmes de Sylow quand p ne divise pas le cardinal de G (par exemple s'intéresser aux 2-Sylow d'un groupe à 63 éléments) tient surtout du vice...

Partie V. Lemme-clef et premier théorème de Sylow

1.(a) S est un sous-groupe de G : idem que dans le cours, dans la démonstration du théorème de Lagrange.

$$\boxed{\text{C'est bon.}}$$

1.(b) Raisonnons par double inclusion.

- Soit $x \in \mathrm{cl}(a)$. Alors $a^{-1}x \in \mathrm{S}$: notons donc $s = a^{-1}x \in \mathrm{S}$ si bien que (en multipliant par a à gauche) $x = as \in a\mathrm{S}$ d'où l'inclusion $\mathrm{cl}(a) \subset a\mathrm{S}$.
- Réciproquement, soit $x \in a\mathrm{S}$. Alors il existe $s \in \mathrm{S}$ tel que $x = as$ donc $a^{-1}x = s \in \mathrm{S}$ si bien que $x \sim a$ donc $x \in \mathrm{cl}(a)$, d'où l'inclusion réciproque, d'où l'égalité.

$$\boxed{\mathrm{cl}(a) = a\mathrm{S}}$$

1.(c) On montre aisément que

$$f : \begin{cases} \mathrm{S} \longrightarrow a\mathrm{S} \\ s \longmapsto as \end{cases}$$

est une bijection :surjective par définition, et si $f(s_1) = f(s_2)$ alors, en multipliant par a^{-1} à gauche, on trouve $s_1 = s_2$ donc injective. Les deux ensembles sont en bijection donc ont le même cardinal.

$$\boxed{\mathrm{Card}\,(a\mathrm{S}) = \mathrm{Card}\,(\mathrm{S})}$$

1.(d) D'après la question 1.(b), X est l'ensemble des classes d'équivalence. On cherche donc le nombre de classes d'équivalence. Toujours car les classes d'équivalence forment une partition de G, G est l'union disjointe des classes d'équivalence donc le cardinal de G est la somme des cardinaux des classes d'équivalences. Or, tous ces cardinaux valent $\mathrm{Card}\,(\mathrm{S})$ donc

$$\mathrm{Card}\,(\mathrm{G}) = \sum \mathrm{Card}\,(\mathrm{S})$$

Le terme sommé est constant donc $\mathrm{Card}\,(\mathrm{G})$ est égal à $\mathrm{Card}\,(\mathrm{S})$ multiplié par le nombre de termes c'est-à-dire le nombre de classes d'équivalences, qu'on note k. Or, S est un p-Sylow donc $\mathrm{Card}\,(\mathrm{S}) = p^\alpha$ si bien que $\mathrm{Card}\,(\mathrm{G}) = p^\alpha \times k = p^\alpha \times m$ donc $k = m$.

$$\boxed{\mathrm{Card}\,(\mathrm{X}) = m}$$

2.(a) Par hypothèse, il existe $s \in \mathrm{S}$ tel que $x = asa^{-1}$ donc $x(a\mathrm{S}) = asa^{-1}a\mathrm{S} = as\mathrm{S} = a\mathrm{S}$ d'après la partie question 4 de la IV.

$$\boxed{\text{Si } x \in a\mathrm{S}a^{-1} \cap \mathrm{H}, \text{ alors } x(a\mathrm{S}) = a\mathrm{S}}$$

2.(b) Soit $s_1 \in \mathrm{S}$: on a donc $as_1 \in a\mathrm{S}$ donc $xas_1 \in x(a\mathrm{S}) = a\mathrm{S}$: il existe s_2 tel que $xas_1 = as_2$ donc $x = as_2{s_1}^{-1}a^{-1}$ et puisque $s_2{s_1}^{-1} \in \mathrm{S}$ (sous-groupe de G) alors $x \in a\mathrm{S}a^{-1}$ et $x \in \mathrm{H}$ par hypothèse donc x appartient à l'intersection.

$$\boxed{x \in a\mathrm{S}a^{-1} \cap \mathrm{H}}$$

2.(c) $a\mathrm{S}a^{-1}$ est un p-Sylow de G d'après la question 2 de la partie IV et en particulier est un groupe. Une intersection de groupes étant un groupe, $a\mathrm{S}a^{-1} \cap \mathrm{H}$ est un groupe inclus dans $a\mathrm{S}a^{-1}$ donc est un sous-groupe de $a\mathrm{S}a^{-1}$.

$$\boxed{a\mathrm{S}a^{-1} \cap \mathrm{H} \text{ est un sous-groupe de } a\mathrm{S}a^{-1}.}$$

En particulier, d'après le théorème de Lagrange, son cardinal divise $\mathrm{Card}\,(a\mathrm{S}a^{-1}) = p^\alpha$ puisque c'est un p-Sylow de G. p étant premier, les seuls diviseurs de p^α sont les nombres de la forme p^k avec $k \leqslant \alpha$.

$$\boxed{a\mathrm{S}a^{-1} \cap \mathrm{H} \text{ est un } p\text{-groupe.}}$$

3 D'après la question 3.(a) de la partie II,

$$\mathrm{Card}\,(\mathrm{X}) = \sum a\mathrm{S} \in \mathrm{X}\, \mathrm{Card}\,(\omega(a\mathrm{S}))$$

Or, $\mathrm{Card}\,(\mathrm{X}) = m$ et $\mathrm{Card}\,(\omega(a\mathrm{S})) = \mathrm{Card}\,(\mathrm{H})/\,\mathrm{Card}\,(\mathrm{Stab}(a\mathrm{S}))$ (question 4.(b) de la partie II) et $\mathrm{Stab}(a\mathrm{S})$. En d'autres termes :

$$m = \sum a\mathrm{S} \in \mathrm{X} \frac{\mathrm{Card}\,(\mathrm{H})}{\mathrm{Card}\,(a\mathrm{S}a^{-1} \cap \mathrm{H})}$$

Or, $m \wedge p = 1$ donc la somme n'est pas divisible par p : il existe donc au moins un terme de la somme qui n'est pas divisible par p et p est premier donc un nombre non divisible par p est premier avec p.

$$\boxed{\text{Il existe } a \in \mathrm{G} \text{ tel que } \frac{\mathrm{Card}\,(\mathrm{H})}{\mathrm{Card}\,(a\mathrm{S}a^{-1} \cap \mathrm{H})} \wedge p = 1.}$$

4 Soit donc un tel a. $a\mathrm{S}a^{-1} \cap \mathrm{H}$ est un sous-groupe de H (intersection de groupes donc groupe et inclus dans H), c'est un p-groupe (question 2.(c)) de cardinal maximal puisque, en divisant par son cardinal, on obtient un nombre premier avec p : c'est donc un p-Sylow.

$$\boxed{\text{Le lemme clef est démontré.}}$$

Partie VI. Deuxième théorème de Sylow

1 Par définition d'un p-Sylow, S est un p-groupe donc il existe α tel que $\mathrm{Card}\,(\mathrm{S}) = p^\alpha$. Dès lors, un p-Sylow de S est un sous-groupe de S de cardinal p^α, c'est-à-dire S tout entier.

$$\boxed{\text{Le seul } p\text{-Sylow de S est S tout entier.}}$$

2 D'après le lemme-clef (avec $\mathrm{S} = \mathrm{S}_1$ et $\mathrm{H} = \mathrm{S}_2$), il existe $a \in \mathrm{G}$ tel que $a\mathrm{S}_1a^{-1} \cap \mathrm{S}_2$ soit un p-Sylow de S_2, c'est-à-dire S_2 tout entier d'après la question 1. Ainsi, $a\mathrm{S}_1a^{-1} \cap \mathrm{S}_2 = \mathrm{S}_2$ si bien que $\mathrm{S}_2 \subset a\mathrm{S}_1a^{-1}$. Or, ces deux ensembles ont le même cardinal (ce sont tous les deux des p-Sylow, question 2 de la partie IV) donc sont égaux.

$$\boxed{\text{Les } p\text{-Sylow d'un groupe sont tous conjugués.}}$$

Partie VII. Troisième théorème de Sylow

1.(a) D'après l'équation aux classes :

$$\boxed{\mathrm{Card}\,(\mathrm{X}) = \mathrm{Card}\,(\mathrm{X}^\mathrm{S}) + \sum_{\omega(x)\,|\,x \notin \mathrm{X}^\mathrm{S}} \mathrm{Card}\,(\omega(x))}$$

Il suffit de montrer que tous les termes de la somme de droite sont divisibles par p. Or (cf. question 4.(b) de la partie II) le cardinal d'une orbite divise le cardinal du groupe (attention, rien à voir avec le théorème de Lagrange : une orbite n'est pas un sous-groupe, cf. partie II) et si $x \notin \mathrm{X}^\mathrm{S}$, on a déjà vu que cela voulait dire que l'orbite n'était pas réduite à un élément.

Or, $\mathrm{Card}\,(\mathrm{S}) = p^\alpha$ et p est premier donc les seuls diviseurs de p^α sont les p^k avec $k \leqslant \alpha$, et puisque l'orbite n'est pas réduite à un élément, son cardinal est divisible par p, ce qui permet de conclure.

$$\boxed{\mathrm{Card}\,(\mathrm{X}) \equiv \mathrm{Card}\,(\mathrm{X}^\mathrm{S})[p]}$$

1.(b) Analogue à la question 4 de la partie IV.

$$\boxed{\text{C'est bon.}}$$

1.(c) Découle de la définition de X^S : T est invariant par tous les éléments de S c'est-à-dire que, pour tout $s \in \mathrm{S}$, $s\mathrm{T}s^{-1} = \mathrm{T}$.

$$\boxed{\forall s \in \mathrm{S}, s\mathrm{T}s^{-1} = \mathrm{T}}$$

1.(d) Ce sont des p-groupes de cardinal maximal dans G donc dans N : le cardinal de N divise le cardinal de G, théorème de Lagrange, donc la valuation p-adique de $\mathrm{Card}\,(\mathrm{N})$ est inférieure ou égale à α, et puisque N contient des p-groupes de cardinal p^α, on ne peut pas faire mieux !

$$\boxed{\text{S et T sont des } p\text{-Sylow de N.}}$$

D'après le deuxième théorème de Sylow (dans N), il existe $n \in \mathrm{N}$ tel que $n\mathrm{T}n^{-1} = \mathrm{S}$ mais $n\mathrm{T}n^{-1} = \mathrm{T}$ donc $\mathrm{T} = \mathrm{S}$.

$$\boxed{\mathrm{T} = \mathrm{S}}$$

1.(e) On déduit de la question précédente que $\mathrm{X}^\mathrm{S} = \{\mathrm{S}\}$ ($\mathrm{S} \in \mathrm{X}^\mathrm{S}$ et si on prend un élément de X^S, alors il est égal à S d'après la question précédente). En particulier, $\mathrm{Card}\,(\mathrm{X}^\mathrm{S}) = 1$. La question 1.(a) permet de répondre (rappelons que n_p est le nombre de p-Sylow donc le cardinal de X).

$$\boxed{n_p \equiv 1[p]}$$

2 Découle du deuxième théorème de Sylow : pour tout $\mathrm{T} \in \mathrm{X}$, il existe $g \in \mathrm{G}$ tel que $g\mathrm{S}g^{-1} = \mathrm{T}$ donc $g.\mathrm{S} = \mathrm{T}$: T est bien dans l'orbite de S.

$$\boxed{\text{L'orbite de S est X tout entier.}}$$

D'après la partie II, le cardinal de l'orbite divise le cardinal du groupe donc n_p divise $n = p^\alpha \times m$. Or, d'après la question précédente, il existe $u \in \mathbb{Z}$ tel que $n_p - up = 1$ donc, d'après le théorème de Bézout, $n_p \wedge p = 1$ donc, d'après le théorème de Gauß,

$$\boxed{n_p \text{ divise } m}$$

3 Soit donc G un groupe à 63 éléments. $63 = 7 \times 9$ et $7 \wedge 9 = 1$ donc $m = 9$. D'après le troisième théorème de Sylow, le nombre de 7-Sylow divise 9, donc est égal à $1, 3$ ou 9 et est congru à 1 modulo 7.

$$\boxed{\text{Un groupe à 63 éléments comporte un seul 7-Sylow.}}$$

Soit donc S l'unique 7-Sylow de ce groupe. Pour tout $g \in \mathrm{G}$, $g\mathrm{S}g^{-1}$ est un 7-Sylow de G (partie I) donc, puisqu'il n'y en a qu'un, $g\mathrm{S}g^{-1} = \mathrm{S}$: c'est la définition d'un sous-groupe conjugué.

$$\boxed{\text{Un groupe de cardinal 63 n'est pas simple.}}$$