

# DS : Algèbre Générale

## Structures Algébriques

Samedi 26 Septembre 2026 (Durée : 4 heures)

**Remarques :** Le devoir est constitué d'un seul problème, formé par 6 parties largement dépendantes, qui traitent les notions suivantes :

- ① Sous groupes distingués.
- ② Quotient d'un groupe par un sous groupe.
- ③ Action d'un groupe sur un ensemble.
- ④ Centre, dérivé et abélianisé d'un groupe.
- ⑤ Quelques propriétés du groupe symétrique.
- ⑥ Sous groupes de Sylow.

### Conseils :

- 📖 Si, au cours de l'épreuve, un candidat repère ce qui lui semble être une erreur dans l'énoncé, il le signale sur sa copie et poursuit sa composition en expliquant les raisons de son initiative.
- 📖 Les candidats sont informés que la qualité de la rédaction et de la présentation, ainsi que la clarté et la précision des raisonnements constitueront des éléments importants pour l'appréciation des copies.
- 📖 Il convient en particulier de rappeler avec précision les références des questions abordées.

## Partie A : Sous groupes distingués

- 📖 Dans tout l'énoncé  $(G, .)$  est un groupe, d'élément neutre  $e$ .
- 📖  $H$  est un sous-groupe de  $G$
- 📖 Pour tout  $g \in G$ , on pose  $g.H.g^{-1} = \{x = g.h.g^{-1} \text{ où } h \in H\}$ .
- 📖 On dit que  $H$  est **distingué** dans  $G$  si et seulement si  $g.H.g^{-1} \subset H$ , pour tout  $g \in G$ . On écrit alors  $H \triangleleft G$ .

- ① Montrer que pour tout  $g \in G$ , on a  $g.H.g^{-1}$  est un sous groupes de  $(G, .)$ .
- ② Montrer que si  $H$  est fini et si  $H \triangleleft G$ , alors  $g.H.g^{-1} = H$ , pour tout  $g \in G$ .
  - 📖 **Indication :** Construire une bijection entre  $H$  et  $g.H.g^{-1}$
- ③ Montrer le résultat précédent est encore valable même si  $H$  est infini.
- ④ Soit  $(g, x) \in G^2$ . Montrer que pour  $n \in \mathbb{Z}$ , on a  $(g.x.g^{-1})^n = g.x^n.g^{-1}$ .
- ⑤ En déduire que si  $H$  est monogène, alors  $g.H.g^{-1}$  l'est aussi.
- ⑥ En déduire que si  $H$  est cyclique, alors  $g.H.g^{-1}$  l'est aussi.
- ⑦ Montrer que l'intersection quelconque d'une famille de sous-groupes distingués de  $G$  est aussi un sous-groupe distingué de  $G$ .
- ⑧ Montrer que l'image réciproque d'un groupe distingué par un morphisme est aussi groupe distingué.

- ⑨ **a** Montrer que l'image directe d'un groupe distingué par un morphisme surjectif est aussi groupe distingué.
- b** Montrer à l'aide d'un contre exemple que le résultat de la question précédente n'est plus valable si on enlève l'hypothèse surjectif.
- 🔑 **Indication** : On pourra utiliser après avoir justifier que  $\{id, (12)\}$  n'est pas distingué dans  $S_3$  et
- ⑩ Si  $H \triangleleft G$  et  $K \triangleleft G$ , montrer que  $H.K = \{h.k \text{ tel que } h \in H, k \in K\}$  est un sous-groupe de  $(G, \cdot)$  et distingué dans  $G$ .

## Partie B : Quotient d'un groupe par un sous groupe

On définit sur  $G$  la relation suivante :  $x\mathcal{R}y \Leftrightarrow \exists h \in H \text{ tel que } y = x.h$ .

- ① Vérifier que  $\mathcal{R}$  est une relation d'équivalence.
- 🔑 On pose alors  $G/H = \{\dot{x} \text{ tel que } x \in G\}$ , appelé ensemble quotient de  $G$  par  $H$ .
- 🔑 On note  $[G : H] = \text{card}(G/H)$ , appelé **indice de  $H$  dans  $G$** .
- ② Montrer que pour tout  $x \in G$ , on a  $\dot{x} = x.H = \{y = x.h \text{ tel que } h \in H\}$ .
- ③ En déduire que dans  $G/G$ , il n'y a une seule classe d'équivalence.
- ④ Déterminer les classes d'équivalence dans  $G/\{e\}$ .  
En déduire que  $G/\{e\}$  et  $G$  sont équipotents.  
Autrement dit : Définissez une application bijective entre  $G/\{e\}$  et  $G$ .
- ⑤ Montrer que  $H$  et  $\dot{x}$  sont de même cardinal, pour tout  $x \in G$ .
- ⑥ **Théorème de Lagrange**. On suppose que  $G$  est fini. Montrer que :
- a**  $G/H$  est fini.
- b**  $\text{card}(G) = [G : H].\text{card}(H)$  et que  $\text{card}(H)$  divise  $\text{card}(G)$ .
- c**  $o(x)$  divise  $\text{card}(G)$  et que  $x^{\text{card}(G)} = e$ , pour tout  $x \in G$ .
- ⑦ En déduire que tout groupe fini de cardinal premier est cyclique.

- ⑧ On suppose dans cette question que  $H \triangleleft G$ . Pour  $(x, y) \in G^2$ , on pose  $\dot{x}.\dot{y} = \overline{x.y}$ .
- a** Montrer que la formule  $\dot{x}.\dot{y} = \overline{x.y}$  est bien définie.
- b** Démontrer alors que  $(G/H, \cdot)$  est un groupe.
- ⑨ **Application** :
- a** Soit  $H$  un sous-groupe de  $G$  tel que  $[G : H] = 2$ . Montrer que  $H \triangleleft G$ .
- b** La réciproque est-elle vraie.

## Partie C : Action d'un groupe sur un ensemble

Soit  $X$  un ensemble non vide. On appelle **action** de  $G$  sur  $X$  toute loi externe, autrement une application  $G \times X \longrightarrow X$ , vérifiant les deux propriétés suivantes :

$$(g, x) \longmapsto g * x$$

$$\forall x \in X, \quad e * x = x$$

$$\forall g, h \in G, \forall x \in X, \quad (g.h) * x = g * (h * x)$$

Dans ce cas, pour tout  $x \in X$

$$\mathcal{O}(x) = \{y = g * x \text{ tel que } g \in G\} \subset X, \text{ désigne l'orbite de } x.$$

$$\text{Stab}(x) = \{g \in G \text{ tel que } g * x = x\} \subset G, \text{ est le stabilisateur de } x.$$

- ① Montrer que pour tout  $x \in X$ ,  $\text{Stab}(x)$  est un sous-groupe de  $(G, \cdot)$ .
- ② Montrer que  $x\mathcal{R}y \iff \exists g \in G, y = g * x$  définit une relation d'équivalence sur  $X$ .
- ③ Montrer que pour tout  $x \in X$ , on a  $\dot{x} = \mathcal{O}(x)$ .
- ④ On suppose dans cette question que  $X$  est fini.  
On note  $X/\mathcal{R} = \{x_1, \dots, x_r\}$  l'ensemble des classes d'équivalence de  $\mathcal{R}$ , deux à deux distinctes.  
Justifier que  $\text{card}(X) = \sum_{i=1}^r \mathcal{O}(x_i)$  (**Formule des orbites**).

- ⑤ On suppose dans cette question que  $G$  est fini et  $G$  agit sur  $X$ . Fixons  $x \in X$   
On pose  $H = \text{Stab}(x)$ , et on considère l'application :  $f : G/H \rightarrow \mathcal{O}(x)$  .  
$$\dot{g} = gH \mapsto g * x$$

- a** Montrer que  $f$  est bien définie  
**b** Montrer que  $f$  est bijective.  
**c** En déduire que  $\text{card}(\mathcal{O}(x)) = \frac{\text{card}(G)}{\text{card}(\text{Stab}(x))}$ . (**Formule Orbite-Stabilisateur**)

### Partie D : Centre, dérivé et abélianisé d'un groupe

- ☞ On pose  $Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$ , appelé **centre** de  $G$ .  
☞ Pour  $x, y \in G$ , on note  $[x, y] = xyx^{-1}y^{-1}$  le **commutateur** de  $x$  et  $y$ .  
☞ On appelle **groupe dérivé** de  $G$ , noté  $D(G)$  ou  $[G, G]$ , le sous-groupe engendré par tous les commutateurs de  $G$ .

- ① Vérifier que  $Z(G)$  est un sous-groupe de  $(G, \cdot)$ , et que  $Z(G) \triangleleft G$ .  
② **a** Montrer que si le groupe quotient  $G/Z(G)$  est cyclique, alors  $G$  est abélien.  
**b** La réciproque de ce résultat est-elle vraie ?  
③ On suppose dans cette question que  $G$  est fini.  
On pose  $f : G \times G \rightarrow G$   
$$(g, x) \mapsto g * x = g.x.g^{-1}$$

- a** Montrer que  $G$  agit sur lui-même grâce à l'application  $f$ .  
**b** Que vaut  $\dot{x} = \mathcal{O}(x)$  pour  $x \in Z(G)$ .  
**c** Que vaut  $\dot{x} = \mathcal{O}(x)$  pour  $x \notin Z(G)$ .  
Justifier que dans ce cas  $\text{Stab}(x) \neq G$ .  
**d** On note  $\{x_1, \dots, x_k\}$  l'ensemble des classes d'équivalence de  $\mathcal{R}$ , deux à deux distinctes, vérifiant  $x_i \notin Z(G)$ .

Justifier la formule suivante :  $\text{card}(G) = \text{card}(Z(G)) + \sum_{i=1}^k \frac{\text{card}(G)}{\text{card}(\text{Stab}(x_i))}$

- ④ On suppose  $G$  est fini, avec  $\text{card}(G) = p^\alpha$ , où  $p$  nombre premier et  $\alpha \in \mathbb{N}^*$ .  
Montrer alors que  $\text{card}(Z(G)) \neq 1$ .  
⑤ En déduire que tout groupe d'ordre  $p^2$  (où  $p$  est un nombre premier) est abélien.  
⑥ Démontrer que  $D(G) \triangleleft G$ .  
⑦ Montrer que  $G/D(G)$  est groupe abélien, appelé le **groupe abélianisé** de  $G$ .  
⑧ Soit  $N \triangleleft G$ . Montrer que  $G/N$  est abélien si et seulement si  $D(G) \subset N$ .  
⑨ Conclure un résultat.

### Partie E : Quelques propriétés du groupe symétrique

- ☞ On rappelle que  $\mathfrak{S}_n = \{\sigma : [1, n] \rightarrow [1, n] \text{ bijective}\}$  et que  $(\mathfrak{S}_n, \circ)$  est un groupe fini de cardinal  $n!$ , appelé **groupe symétrique d'ordre  $n$** . Dans la suite  $\circ$  est notée  $\cdot$ .  
☞ On rappelle aussi que  $\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \text{ tel que } \varepsilon(\sigma) = 1\}$  est un sous groupe de  $(\mathfrak{S}_n, \cdot)$ , appelé **groupe alterné**.

- ① **Une formule de conjugaison dans  $(\mathfrak{S}_n, \circ)$ .**  
**a** Soit  $n \geq 2, \sigma \in \mathfrak{S}_n$  et  $1 \leq i \neq j \leq n$ .  
Montrer que  $\sigma.(i \ j).\sigma^{-1} = (\sigma(i) \ \sigma(j))$ .  
**b** Donner puis justifier une formule générale pour  $\sigma.\tau.\sigma^{-1}$ , quand  $\tau$  est un  $k$ -cycle.  
② **Transitivité de la distinction.**  
Considérons  $G = \mathfrak{S}_4, H = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$  et  $K = \{\text{id}, (12)(34)\}$   
**a** Vérifier que  $H \triangleleft G$  et que  $K \triangleleft H$ .  
**b** Montrer que  $K$  n'est pas distingué dans  $G$   
☞ Indication : Calculer  $\tau(12)(34)\tau^{-1}$ , où  $\tau = (13)$   
**c** Conclure un résultat.

③ On suppose  $n \geq 2$ .

**a** Montrer que l'application  $f : \mathfrak{A}_n \rightarrow \mathfrak{S}_n \setminus \mathfrak{A}_n$  est bijective.  
 $\sigma \mapsto (1\ 2) \cdot \sigma$

**b** En déduire que  $\text{card}(\mathfrak{A}_n) = \frac{n!}{2}$ .

**c** En déduire que  $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$ .

④ On prend  $n = 3$ .

**a** Donner tous les sous groupes de  $\mathfrak{S}_3$ .

**b** Parmi ces groupes, déterminer ceux qui sont distingués dans  $\mathfrak{S}_3$ .

⑤ Montrer que pour  $n \geq 3$ , on a  $D(\mathfrak{S}_n) = \mathfrak{A}_n$ .

 Indication : On pourra utiliser, après avoir justifié la formule suivante :  
 $(i\ j) \cdot (j\ k) = (i\ j\ k)$  quand  $i, j, k$  deux à deux distincts.

⑥ On considère  $a, b, c, d$  des éléments distincts de  $\{1, \dots, n\}$ . Exprimer les produit  $(a\ b)(c\ d)$  et  $(a\ b)(a\ c)$  sous la forme d'un unique 3-cycle.

⑦ Justifier que tout  $\sigma \in \mathfrak{A}_n$  peut s'écrire comme produit d'un nombre pair de transpositions.

⑧ Montrer que pour  $n \geq 5$ , les 3-cycles engendrent  $\mathfrak{A}_n$ .

⑨ En déduire que  $\mathfrak{A}_n$  est un groupe simple pour tout  $n \geq 5$ .

## Partie F : Sous groupes de Sylow.

On suppose dans cette partie que  $G$  est fini, tel que  $n = \text{card}G \geq 2$ .  
Soit  $p$  est un nombre premier qui divise  $n$ .

  $\alpha = \max\{k \in \mathbb{N}^* \text{ tel que } p^k \text{ divise } n\}$ , appelé  **$p$ -valuation** de  $n$ .

 Un sous groupe  $H$  de  $G$  est dit  **$p$ -sous groupe de Sylow** de  $G$  si et seulement si  $\text{card}(H) = p^\alpha$ .

 Considérons l'ensemble  $\mathcal{E} = \{S \subset G \text{ tel que } \text{card}(S) = p^\alpha\}$

① Montrer que  $\alpha$  est bien définie.

② On pose  $\text{card}(G) = p^\alpha \cdot m$ , avec  $p \nmid m$ . Justifier que  $\text{card}(\mathcal{E}) = \binom{p^\alpha m}{p^\alpha}$ .

③ Justifier que  $\binom{p^\alpha m}{p^\alpha} = \prod_{k=0}^{p^\alpha-1} \frac{p^\alpha m - k}{p^\alpha - k}$ .

④ Démontrer que  $p$  ne divise aucun rapport  $\frac{p^\alpha m - k}{p^\alpha - k}$ .

 **Indication** : Pour tout  $0 \leq k < p^\alpha$ , écrivez  $k = p^j r$  avec  $p \nmid r$  et  $j < \alpha$ .

⑤ En déduire que  $p$  ne divise pas  $\text{card}(\mathcal{E})$ .

⑥ Soit  $f : G \times \mathcal{E} \rightarrow \mathcal{E}$   
 $(g, S) \mapsto g * S = gS = \{gs \mid s \in S\}$   
Montrer que  $f$  est bien définie et qu'elle définit une action de  $G$  sur  $\mathcal{E}$ .

⑦ Montrer qu'il existe une partie  $S_0 \in \mathcal{E}$  telle que  $p$  ne divise pas  $\text{card}(\text{Orb}(S_0))$ .

⑧ En déduire que  $\text{Stab}_G(S_0)$  est un  $p$ -sous groupe de Sylow de  $G$ .

⑨ Énoncer un résultat (connu sous le nom du **1<sup>er</sup> théorème de Sylow**).

Fin

## Corrigé

### Partie A : Sous groupes distingués

① Montrons que pour tout  $g \in G$ ,  $gHg^{-1}$  est un sous-groupe de  $(G, \cdot)$ .

✎ **Non vide** :  $H$  est un sous-groupe de  $G$ , donc  $e \in H$ . Ains  $g \cdot e \cdot g^{-1} = e \in gHg^{-1}$ .

✎ **Stabilité par produit et passage à l'inverse** : Soient  $x, y \in gHg^{-1}$ . Il existe  $h_1, h_2 \in H$  tels que  $x = gh_1g^{-1}$  et  $y = gh_2g^{-1}$ .

$$x \cdot y^{-1} = (gh_1g^{-1}) \cdot (gh_2g^{-1})^{-1} = gh_1g^{-1} \cdot gh_2^{-1}g^{-1} = g(h_1h_2^{-1})g^{-1}$$

Comme  $H$  est un sous-groupe de  $G$ ,  $h_1h_2^{-1} \in H$ . Ainsi,  $x \cdot y^{-1} \in gHg^{-1}$ .

**Conclusion** :  $gHg^{-1}$  est un sous-groupe de  $(G, \cdot)$ .

② Montrons que si  $H$  est fini et  $H \triangleleft G$ , alors  $gHg^{-1} = H$  pour tout  $g \in G$ .

Considérons l'application  $\phi_g : H \rightarrow gHg^{-1}$  définie par  $\phi_g(h) = ghg^{-1}$ .

✎  $\phi_g$  est injective : Si  $\phi_g(h_1) = \phi_g(h_2)$ , alors  $gh_1g^{-1} = gh_2g^{-1}$ . En multipliant à gauche par  $g^{-1}$  et à droite par  $g$ , on obtient  $h_1 = h_2$ .

✎ Par définition de  $gHg^{-1}$ ,  $\phi_g$  est surjective, c'est donc une **bijection**.

Par conséquent,  $\text{Card}(gHg^{-1}) = \text{Card}(H)$ . Comme  $H \triangleleft G$ , on a  $gHg^{-1} \subset H$ . Or  $gHg^{-1}$  et  $H$  sont finis de même cardinal, donc  $gHg^{-1} = H$ .

③ Montrons que le résultat reste vrai si  $H$  est infini.

Soit  $g \in G$ . Puisque  $H \triangleleft G$ , on a  $gHg^{-1} \subset H$ . Appliquons cette propriété à l'élément  $g^{-1} \in G$  :

$$g^{-1}H(g^{-1})^{-1} \subset H \implies g^{-1}Hg \subset H$$

En multipliant cette inclusion à gauche par  $g$  et à droite par  $g^{-1}$ , on obtient :

$$g(g^{-1}Hg)g^{-1} \subset gHg^{-1} \implies H \subset gHg^{-1}$$

Par double inclusion,  $gHg^{-1} = H$  pour tout  $g \in G$ .

④ Montrons que pour  $n \in \mathbb{Z}$ ,  $(gxg^{-1})^n = gx^n g^{-1}$ .

✎ **Pour  $n = 0$**  :  $(gxg^{-1})^0 = e$  et  $gx^0 g^{-1} = geg^{-1} = e$ .

✎ **Pour  $n \in \mathbb{N}^*$**  : Par récurrence, pour  $n = 1$ ,  $gxg^{-1} = gx^1 g^{-1}$ . Si vrai pour  $n$ , alors :  
 $(gxg^{-1})^{n+1} = (gxg^{-1})^n (gxg^{-1}) = (gx^n g^{-1})(gxg^{-1}) = gx^n (g^{-1}g) x g^{-1} = gx^{n+1} g^{-1}$

✎ **Pour  $n < 0$**  : Posons  $m = -n \in \mathbb{N}^*$ . On a :

$$(gxg^{-1})^n = ((gxg^{-1})^{-1})^m = (gx^{-1}g^{-1})^m = g(x^{-1})^m g^{-1} = gx^{-m} g^{-1} = gx^n g^{-1}$$

⑤ Montrons que si  $H$  est monogène, alors  $gHg^{-1}$  l'est aussi.

Si  $H$  est monogène, il existe  $a \in H$  tel que  $H = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ . Alors :

$$gHg^{-1} = \{ga^n g^{-1} \mid n \in \mathbb{Z}\} = \{(gag^{-1})^n \mid n \in \mathbb{Z}\} = \langle gag^{-1} \rangle$$

$gHg^{-1}$  est engendré par  $gag^{-1}$ , donc  $gHg^{-1}$  est monogène.

⑥ Montrons que si  $H$  est cyclique, alors  $gHg^{-1}$  l'est aussi.

Un groupe est cyclique s'il est monogène et fini. Si  $H$  est cyclique,  $H$  est monogène donc  $gHg^{-1}$  est monogène d'après la question précédente. De plus,  $\text{Card}(gHg^{-1}) = \text{Card}(H) < +\infty$  (via la bijection  $\phi_g$ ). Ainsi,  $gHg^{-1}$  est fini et monogène, donc cyclique.

⑦ Montrons que l'intersection de sous-groupes distingués est distinguée.

Soit  $(H_i)_{i \in I}$  une famille de sous-groupes distingués de  $G$ .

Soit  $H = \bigcap_{i \in I} H_i$ .  $H$  est un sous-groupe de  $G$  (intersection de sous-groupes).

Soit  $g \in G$  et  $x \in gHg^{-1}$ . Il existe  $h \in H$  tel que  $x = ghg^{-1}$ .

Pour tout  $i \in I$ ,  $h \in H_i$ . Comme  $H_i \triangleleft G$ ,  $ghg^{-1} \in H_i$ . Donc  $x \in H_i$  pour tout  $i \in I$ , c'est-à-dire  $x \in \bigcap_{i \in I} H_i = H$ . Ainsi  $gHg^{-1} \subset H$ , donc  $H \triangleleft G$ .

- ⑧ Soit  $f : G \rightarrow G'$  morphisme de groupe et  $K \triangleleft G'$ .  
On sait que  $f^{-1}(K)$  est bien un sous-groupe de  $G$  (résultat du cours).  
 $f^{-1}(K)$  est distingué dans  $G$  : Soient  $g \in G$  et  $x \in f^{-1}(K)$ . Montrons que  $gxg^{-1} \in f^{-1}(K)$ .

Calculons l'image de  $gxg^{-1}$  par  $f$  :

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1}$$

Or :

- $f(g) \in G'$ ,
- $f(x) \in K$  (car  $x \in f^{-1}(K)$ ).

Puisque  $K \triangleleft G'$ , le sous-groupe  $K$  est stable par conjugaison par tout élément de  $H$ .

Par conséquent :

$$f(g)f(x)f(g)^{-1} \in K \implies f(gxg^{-1}) \in K$$

Ce qui prouve que  $gxg^{-1} \in f^{-1}(K)$ .

- ⑨ **a** Soit  $f : G \rightarrow G'$  morphisme de groupe surjectif et  $H \triangleleft G$ .  
On sait que  $f(H)$  est bien un sous-groupe de  $G'$  (résultat du cours).  
Montrons que  $f(H) \triangleleft G'$ .  
Soit  $y \in G'$  et  $z \in f(H)$ . Puisque  $f$  est surjectif, il existe  $x \in G$  tel que  $y = f(x)$ .  
Puisque  $z \in f(H)$ , il existe  $h \in H$  tel que  $z = f(h)$ . On calcule le conjugué de  $z$  par  $y$  :

$$yzy^{-1} = f(x)f(g)f(x)^{-1} = f(xhx^{-1})$$

Comme  $H \triangleleft G$  et  $x \in G, h \in H$ , on a  $xhx^{-1} \in H$ . Par conséquent,  $f(xhx^{-1}) \in f(H)$ , donc  $yzy^{-1} \in f(H)$ .  $f(H)$  est donc bien distingué dans  $H$ .

- b** Prenez le groupe symétrique  $\mathfrak{S}_3$  et le sous-groupe  $H = \{id, (12)\}$ .  
On a  $H$  n'est pas distingué dans  $\mathfrak{S}_3$ , car  $(13)(12)(13)^{-1} = (32)$  (calcul déjà fait pareil en TD).  
Prenez  $f : H \rightarrow \mathfrak{S}_3$  comme morphisme de groupe.  $H$  est un sous-groupe distingué de lui-même ( $N \triangleleft N$ ). Pourtant, son image  $f(H) = H$  n'est pas distinguée dans  $\mathfrak{S}_3$ .

- ⑩ Montrons que si  $H \triangleleft G$  et  $K \triangleleft G$ , alors  $HK$  est un sous-groupe distingué.

- Non-Vide** : Comme  $H$  et  $K$  sont des sous-groupes de  $G$ , leurs éléments neutres sont  $e \in H$  et  $e \in K$ . Ainsi :

$$e = e \cdot e \in HK \implies HK \neq \emptyset$$

- Stabilité par produit** : Soient  $x, y \in HK$ . Par définition, il existe  $(h_1, h_2) \in H^2$  et  $(k_1, k_2) \in K^2$  tels que :

$$x = h_1k_1 \quad \text{et} \quad y = h_2k_2$$

Calculons le produit  $x \cdot y$  :

$$xy = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$$

Puisque  $H \triangleleft G$ , pour tout  $g \in G$ , on a  $gHg^{-1} = H$ , ce qui implique que  $gH = Hg$ . En particulier pour  $g = k_1$ , on a  $k_1H = Hk_1$ .

Ainsi, il existe  $h_3 \in H$  tel que  $k_1h_2 = h_3k_1$ . En substituant :

$$xy = h_1(h_3k_1)k_2 = (h_1h_3)(k_1k_2)$$

Comme  $H$  et  $K$  sont des sous-groupes de  $G$ ,  $h_1h_3 \in H$  et  $k_1k_2 \in K$ . Il s'ensuit que  $xy \in HK$ .

- Stabilité par passage à l'inverse** : Soit  $x = hk \in HK$  (avec  $h \in H$  et  $k \in K$ ). Son inverse dans  $G$  s'écrit :

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1}$$

Comme  $H \triangleleft G$ , la propriété  $Hk^{-1} = k^{-1}H$  garantit qu'il existe  $h' \in H$  tel que :

$$k^{-1}h^{-1} = h'k^{-1}$$

Puisque  $h' \in H$  et  $k^{-1} \in K$  (car  $K$  est un sous-groupe), on en déduit que  $x^{-1} \in HK$ .

- Distingué** : Soit  $g \in G$  et  $x \in HK$ . On écrit  $x = hk$  avec  $h \in H$  et  $k \in K$ .

$$gxg^{-1} = g(hk)g^{-1} = (ghg^{-1})(gkg^{-1})$$

Comme  $H \triangleleft G$ ,  $ghg^{-1} \in H$ . Comme  $K \triangleleft G$ ,  $gkg^{-1} \in K$ . Ainsi,  $gxg^{-1} \in HK$ . Donc  $g(HK)g^{-1} \subset HK$ , d'où  $HK \triangleleft G$ .

On conclut que  $HK$  est un sous-groupe distingué de  $G$ .

## Partie B : Quotient d'un groupe par un sous groupe

### ① Vérification que $\mathcal{R}$ est une relation d'équivalence

Pour montrer que  $\mathcal{R}$  est une relation d'équivalence sur  $G$ , il faut vérifier trois propriétés :

- (a) **Réflexivité** : Soit  $x \in G$ . Comme  $H$  est un sous-groupe de  $G$ , son élément neutre  $e \in H$ . On a  $x = x \cdot e$ , donc  $x\mathcal{R}x$ .
- (b) **Symétrie** : Soient  $x, y \in G$  tels que  $x\mathcal{R}y$ . Il existe  $h \in H$  tel que  $y = x \cdot h$ . En multipliant par  $h^{-1}$  à droite (avec  $h^{-1} \in H$  car  $H$  est un sous-groupe), on obtient  $x = y \cdot h^{-1}$ . D'où  $y\mathcal{R}x$ .
- (c) **Transitivité** : Soient  $x, y, z \in G$  tels que  $x\mathcal{R}y$  et  $y\mathcal{R}z$ . Il existe  $h_1, h_2 \in H$  tels que  $y = x \cdot h_1$  et  $z = y \cdot h_2$ . Ainsi :

$$z = (x \cdot h_1) \cdot h_2 = x \cdot (h_1 \cdot h_2)$$

Comme  $h_1 \cdot h_2 \in H$ , il s'ensuit que  $x\mathcal{R}z$ .

**Conclusion** :  $\mathcal{R}$  est bien une relation d'équivalence sur  $G$ .

### ② Description des classes d'équivalence

Par définition, la classe d'équivalence d'un élément  $x \in G$ , notée  $\dot{x}$ , est :

$$\dot{x} = \{y \in G \mid x\mathcal{R}y\} = \{y \in G \mid \exists h \in H, y = x \cdot h\} = \{x \cdot h \mid h \in H\} = x \cdot H$$

Ainsi, pour tout  $x \in G$ , on a  $\dot{x} = x \cdot H$ .

### ③ Car pour tout $x \in G$ , on a $\dot{x} = x \cdot G = G$

### ④ Pour tout $x \in G$ , on a $\dot{x} = x \cdot \{e\} = \{x\}$ . L'application bijective sera $f: G \rightarrow G/\{e\}$ . $x \mapsto \{x\}$

### ⑤ Cardinal de la classe $\dot{x}$

Considérons l'application :

$$f: H \rightarrow x \cdot H \\ h \mapsto x \cdot h$$

**Injectivité** : Soient  $h_1, h_2 \in H$ . Si  $f(h_1) = f(h_2)$ , alors  $x \cdot h_1 = x \cdot h_2$ . En multipliant à gauche par  $x^{-1}$ , on obtient  $h_1 = h_2$ .

**Surjectivité** : Par définition de  $x \cdot H$ , tout élément  $y \in x \cdot H$  s'écrit  $y = x \cdot h = f(h)$  pour un certain  $h \in H$ .

$f$  est une bijection entre  $H$  et  $\dot{x} = x \cdot H$ . Donc  $\text{card}(\dot{x}) = \text{card}(H)$  pour tout  $x \in G$ .

### ⑥ Théorème de Lagrange (Cas $G$ fini)

**a** Puisque  $G/H$  est une partition de l'ensemble fini  $G$ ,  $G/H$  est un ensemble fini.

**b** La relation d'équivalence  $\mathcal{R}$  induit une partition de  $G$  en classes d'équivalence disjointes deux à deux :

$$G = \bigsqcup_{\dot{x} \in G/H} \dot{x}$$

En passant au cardinal et sachant que toutes les classes ont même cardinal  $\text{card}(H)$  :

$$\text{card}(G) = \sum_{\dot{x} \in G/H} \text{card}(\dot{x}) = \sum_{\dot{x} \in G/H} \text{card}(H) = \text{card}(G/H) \times \text{card}(H).$$

D'où  $\text{card}(G) = [G : H] \times \text{card}(H)$ , et puisque  $[G : H]$  est un entier, il s'ensuit que  $\text{card}(H)$  divise  $\text{card}(G)$ .

**c** Soit  $x \in G$  et  $K = \langle x \rangle$  le sous-groupe engendré par  $x$ .

Par le théorème de Lagrange appliqué à  $K$ ,  $\text{card}(K) = o(x)$  divise  $\text{card}(G)$ . Il existe donc  $k \in \mathbb{N}^*$  tel que  $\text{card}(G) = k \cdot o(x)$ . D'où :  $x^{\text{card}(G)} = x^{k \cdot o(x)} = (x^{o(x)})^k = e^k = e$ .

### ⑦ Groupes d'ordre premier

Soit  $G$  un groupe fini tel que  $\text{card}(G) = p$  où  $p$  est premier. Soit  $x \in G \setminus \{e\}$ . Le sous-groupe engendré  $K = \langle x \rangle$  a un cardinal  $o(x) > 1$  qui divise  $p$ . Puisque  $p$  est premier,  $o(x) = p = \text{card}(G)$ , ce qui signifie que  $G = \langle x \rangle$ .  $G$  est donc un groupe cyclique.

### ⑧ Structure de groupe sur $G/H$ quand $H \triangleleft G$

On suppose désormais que  $H$  est un sous-groupe distingué de  $G$  ( $H \triangleleft G$ ).

**a** le produit des classes est bien défini Soient  $(x_1, y_1)$  et  $(x_2, y_2)$  tels que  $\dot{x}_1 = \dot{x}_2$  et  $\dot{y}_1 = \dot{y}_2$ . Il existe  $h_1, h_2 \in H$  tels que  $x_2 = x_1 h_1$  et  $y_2 = y_1 h_2$ . Calculons le produit :

$$x_2 y_2 = (x_1 h_1)(y_1 h_2) = x_1 (h_1 y_1) h_2$$

Comme  $H \triangleleft G$ ,  $h_1 y_1 \in Hy_1 = y_1 H$ , il existe  $h_3 \in H$  tel que  $h_1 y_1 = y_1 h_3$ . Ainsi :

$$x_2 y_2 = x_1 (y_1 h_3) h_2 = (x_1 y_1) (h_3 h_2)$$

Comme  $h_3 h_2 \in H$ ,  $x_2 y_2 \in (x_1 y_1) \cdot H$ , c'est-à-dire  $\overline{x_2 y_2} = \overline{x_1 y_1}$ . La loi est bien définie.

**b**  $(G/H, \cdot)$  est un groupe

- ☞ **Associativité** : Héritée directement de l'associativité dans  $G$ .
- ☞ **Élément neutre** : La classe  $\dot{e} = H$  sert d'élément neutre :  $\dot{x} \cdot \dot{e} = \overline{x\dot{e}} = \dot{x}$ .
- ☞ **Symphonique (Inverse)** : Pour tout  $\dot{x} \in G/H$ , le symétrique est  $\overline{x^{-1}}$  car  $\dot{x} \cdot \overline{x^{-1}} = \overline{xx^{-1}} = \dot{e}$ .

**9 Applications**

**a** Tout sous-groupe d'indice 2 est distingué

Soit  $H$  un sous-groupe de  $G$  tel que  $[G : H] = 2$ .  
Il y a exactement 2 classes d'équivalence :  $\dot{e} = e.H = H$  et l'autre sera forcément  $G \setminus H$ , puisque les deux classes d'équivalence forment une partition de  $G$ .  
Pour tout  $g \in G$ , on distingue deux cas :

- ☞ Si  $g \in H$ ,  $gH = H$ , donc  $gHg^{-1} = Hg^{-1} = H$ , car  $g^{-1} \in H$ .
- ☞ Si  $g \notin H$ , alors  $\dot{g} = gH = G \setminus H$ , or  $Hg \cap H = \emptyset$  (puisque  $g \notin H$ , d'où  $Hg \subset G \setminus H = gH$ , d'où  $gHg^{-1} \subset H$ ).

Ainsi,  $gHg^{-1} \subset H$  pour tout  $g \in G$ , ce qui prouve que  $H \triangleleft G$ .

**b** La réciproque est fausse en général.

Un sous-groupe distingué  $H \triangleleft G$  n'a pas nécessairement un indice égal à 2.

**Contre-exemple** : Dans  $G = \mathbb{Z}/6\mathbb{Z}$ , le sous-groupe  $H = \{\bar{0}, \bar{3}\}$  est distingué ( $\mathbb{Z}/6\mathbb{Z}, +$ ), car le groupe est abélien. Mais son indice est  $[G : H] = \frac{6}{2} = 3 \neq 2$ .

**Partie C : Action d'un groupe sur un ensemble**

**1**  $\text{Stab}(x)$  est un sous-groupe de  $(G, \cdot)$

Soit  $x \in X$ .

- (a) **Non-vide** : Par la propriété neutre de l'action,  $e * x = x$ . Ainsi  $e \in \text{Stab}(x)$ , donc  $\text{Stab}(x) \neq \emptyset$ .
- (b) **Stabilité par produit et passage à l'inverse** : Soient  $g, h \in \text{Stab}(x)$ . On a  $g * x = x$  et  $h * x = x$ .  
Montrons que  $g \cdot h^{-1} \in \text{Stab}(x)$  : Comme  $h * x = x$ , en faisant agir  $h^{-1}$  à gauche :  
$$h^{-1} * (h * x) = h^{-1} * x \implies (h^{-1} \cdot h) * x = h^{-1} * x \implies e * x = h^{-1} * x \implies h^{-1} * x = x$$

On en déduit :

$$(g \cdot h^{-1}) * x = g * (h^{-1} * x) = g * x = x$$

Donc  $g \cdot h^{-1} \in \text{Stab}(x)$ .

**Conclusion** :  $\text{Stab}(x)$  est un sous-groupe de  $(G, \cdot)$ .

**2**  $\mathcal{R}$  est une relation d'équivalence sur  $X$

On définit  $x\mathcal{R}y \iff \exists g \in G, y = g * x$ .

- (a) **Réflexivité** : Soit  $x \in X$ . On a  $x = e * x$  avec  $e \in G$ , donc  $x\mathcal{R}x$ .
- (b) **Symétrie** : Soient  $x, y \in X$  tels que  $x\mathcal{R}y$ . Il existe  $g \in G$  tel que  $y = g * x$ . En faisant agir  $g^{-1}$  :

$$g^{-1} * y = g^{-1} * (g * x) = (g^{-1} \cdot g) * x = e * x = x$$

Puisque  $g^{-1} \in G$ , on a  $y\mathcal{R}x$ .

- (c) **Transitivité** : Soient  $x, y, z \in X$  tels que  $x\mathcal{R}y$  et  $y\mathcal{R}z$ . Il existe  $g, h \in G$  tels que  $y = g * x$  et  $z = h * y$ . Ainsi :

$$z = h * (g * x) = (h \cdot g) * x$$

Comme  $h \cdot g \in G$ , on a  $x\mathcal{R}z$ .

**Conclusion :**  $\mathcal{R}$  est bien une relation d'équivalence sur  $X$ .

**③ Description de la classe d'équivalence**  $\dot{x} = \mathcal{O}(x)$

Soit  $x \in X$ . La classe d'équivalence de  $x$  modulo  $\mathcal{R}$  est définie par :

$$\dot{x} = \{y \in X \mid x\mathcal{R}y\} = \{y \in X \mid \exists g \in G, y = g * x\} = \{g * x \mid g \in G\} = \mathcal{O}(x)$$

Ainsi, la classe d'équivalence de tout élément  $x$  correspond exactement à son orbite  $\mathcal{O}(x)$ .

**④ Formule des orbites ( $X$  fini)**

Puisque  $\mathcal{R}$  est une relation d'équivalence sur l'ensemble fini  $X$ , l'ensemble des classes d'équivalence  $X/\mathcal{R} = \{\dot{x}_1, \dots, \dot{x}_r\}$  constitue une partition de  $X$ . Par conséquent,  $X$  est la réunion disjointe des orbites disjointes  $\mathcal{O}(x_i)$  :

$$X = \bigsqcup_{i=1}^r \mathcal{O}(x_i)$$

En passant au cardinal, la somme des cardinaux des parties de la partition donne le cardinal de l'ensemble total :

$$\text{card}(X) = \sum_{i=1}^r \text{card}(\mathcal{O}(x_i)) \quad (\text{Formule des orbites})$$

**⑤ Formule Orbite-Stabilisateur**

On suppose  $G$  fini, et  $x \in X$  fixé. Soit  $H = \text{Stab}(x)$ . Considérons l'application :

$$\begin{aligned} f : G/H &\longrightarrow \mathcal{O}(x) \\ \dot{g} = gH &\longmapsto g * x \end{aligned}$$

**a**  $f$  est bien définie Soient  $g_1, g_2 \in G$  tels que  $\dot{g}_1 = \dot{g}_2$ , c'est-à-dire  $g_1H = g_2H$ . Il existe  $h \in H = \text{Stab}(x)$  tel que  $g_2 = g_1 \cdot h$ . Calculons l'image de  $g_2H$  par  $f$  :

$$f(\dot{g}_2) = g_2 * x = (g_1 \cdot h) * x = g_1 * (h * x)$$

Comme  $h \in \text{Stab}(x)$ ,  $h * x = x$ . D'où :

$$f(\dot{g}_2) = g_1 * x = f(\dot{g}_1)$$

L'image ne dépend pas du choix du représentant de la classe, donc  $f$  est bien définie.

**b**  $f$  est bijective

**Injectivité :** Soient  $\dot{g}_1, \dot{g}_2 \in G/H$  tels que  $f(\dot{g}_1) = f(\dot{g}_2)$ .

$$g_1 * x = g_2 * x \implies g_2^{-1} * (g_1 * x) = g_2^{-1} * (g_2 * x) \implies (g_2^{-1} \cdot g_1) * x = e * x = x$$

Ainsi,  $g_2^{-1} \cdot g_1 \in \text{Stab}(x) = H$ , ce qui implique  $g_1H = g_2H$ , d'où  $\dot{g}_1 = \dot{g}_2$ .  $f$  est injective.

**Surjectivité :** Soit  $y \in \mathcal{O}(x)$ . Par définition de l'orbite, il existe  $g \in G$  tel que  $y = g * x = f(\dot{g})$ . Tout élément de l'orbite admet donc un antécédent dans  $G/H$ .  $f$  est surjective.

**c Conclusion (Formule Orbite-Stabilisateur)** Puisque  $f : G/H \longrightarrow \mathcal{O}(x)$  est une bijection, leurs cardinaux sont égaux :

$$\text{card}(\mathcal{O}(x)) = \text{card}(G/H) = [G : H]$$

Or, d'après le théorème de Lagrange appliqué au sous-groupe  $H = \text{Stab}(x)$  du groupe fini  $G$  :

$$\text{card}(G/H) = \frac{\text{card}(G)}{\text{card}(H)} = \frac{\text{card}(G)}{\text{card}(\text{Stab}(x))}$$

D'où la Formule Orbite-Stabilisateur :

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

## Partie D : Centre, dérivé et abélianisé d'un groupe

### ① $Z(G)$ est un sous-groupe distingué de $G$

☞ **Sous-groupe :**

☞  $e \in Z(G)$  car pour tout  $x \in G$ ,  $ex = x = xe$ . Donc  $Z(G) \neq \emptyset$ .

☞ Soient  $g_1, g_2 \in Z(G)$ . Pour tout  $x \in G$  :

$$(g_1 g_2^{-1})x = g_1(x^{-1}g_2)^{-1} = g_1(g_2 x^{-1})^{-1} = g_1 x g_2^{-1} = x(g_1 g_2^{-1})$$

Ainsi,  $g_1 g_2^{-1} \in Z(G)$ , ce qui prouve que  $Z(G)$  est un sous-groupe de  $G$ .

☞ **Distingué ( $Z(G) \triangleleft G$ ) :** Pour tout  $g \in G$  et  $z \in Z(G)$ , on a  $gzg^{-1} = zgg^{-1} = ze = z \in Z(G)$ . Par conséquent,  $Z(G) \triangleleft G$ .

### ② **a** Si $G/Z(G)$ est cyclique, alors $G$ est abélien

Supposons que  $G/Z(G)$  est cyclique, engendré par une classe  $\bar{a} = aZ(G)$  avec  $a \in G$ . Chaque classe d'équivalence s'écrit de la forme  $\bar{x} = \bar{a}^k = \overline{a^k}$  pour un entier  $k \in \mathbb{Z}$ . Ainsi, tout élément  $x \in G$  s'écrit sous la forme  $x = a^k z_1$  avec  $k \in \mathbb{Z}$  et  $z_1 \in Z(G)$ .

Soient  $x, y \in G$ . Il existe  $k, m \in \mathbb{Z}$  et  $z_1, z_2 \in Z(G)$  tels que :

$$x = a^k z_1 \quad \text{et} \quad y = a^m z_2$$

Calculons leur produit. Comme  $z_1, z_2 \in Z(G)$ , on a :

$$xy = (a^k z_1)(a^m z_2) = a^k a^m z_1 z_2 = a^{k+m} z_1 z_2$$

De même :

$$yx = (a^m z_2)(a^k z_1) = a^m a^k z_2 z_1 = a^{m+k} z_1 z_2 = xy$$

Puisque tous les éléments commutent,  $G$  est un groupe abélien.

**b** Si  $G$  est abélien, alors  $Z(G) = G$ , et donc  $G/Z(G) = G/G = \{\bar{e}\}$  est bien cyclique car réduit à l'élément neutre.

### ③ **a** Pour montrer que $f$ définit une action de groupe de $G$ sur lui-même (action par conjugaison), il faut vérifier deux propriétés :

☞ **Élément neutre :** Soit  $e$  l'élément neutre de  $G$ . Pour tout  $x \in G$ ,

$$e * x = e \cdot x \cdot e^{-1} = x$$

☞ **Associativité mixte :** Soient  $g, h \in G$  et  $x \in G$ .

$$g*(h*x) = g*(h \cdot x \cdot h^{-1}) = g \cdot (h \cdot x \cdot h^{-1}) \cdot g^{-1} = (g \cdot h) \cdot x \cdot (h^{-1} \cdot g^{-1}) = (g \cdot h) \cdot x \cdot (g \cdot h)^{-1} =$$

L'application  $f$  définit donc bien une action de  $G$  sur lui-même.

**b** L'orbite d'un élément  $x \in G$  est définie par  $\mathcal{O}(x) = \{g * x \mid g \in G\} = \{g \cdot x \cdot g^{-1} \mid g \in G\}$ .

Si  $x \in Z(G)$  (le centre de  $G$ ), alors par définition du centre,  $x$  commute avec tous les éléments de  $G$ .

Ainsi, pour tout  $g \in G$ ,  $g \cdot x \cdot g^{-1} = x \cdot g \cdot g^{-1} = x$ .

Par conséquent,

$$\dot{x} = \mathcal{O}(x) = \{x\}$$

L'orbite de  $x$  est un singleton.

**c** ☞ Pour  $x \notin Z(G)$ , l'orbite est l'ensemble des conjugués de  $x$  dans  $G$

$$\dot{x} = \mathcal{O}(x) = \{g \cdot x \cdot g^{-1} \mid g \in G\}$$

☞ Le stabilisateur de  $x$  est donné par :

$$\text{Stab}(x) = \{g \in G \mid g * x = x\} = \{g \in G \mid g \cdot x \cdot g^{-1} = x\} = \{g \in G \mid g \cdot x = x \cdot g\}$$

(il s'agit du centralisateur de  $x$  dans  $G$ ).

Puisque  $x \notin Z(G)$ , il existe au moins un élément  $g_0 \in G$  qui ne commute pas avec  $x$  ( $g_0 \cdot x \neq x \cdot g_0$ ). Donc  $g_0 \notin \text{Stab}(x)$ , ce qui prouve que :

$$\text{Stab}(x) \neq G$$

**d** Les orbites forment une partition du groupe  $G$ . Ainsi, le cardinal de  $G$  est la somme des cardinal des orbites distinctes :

$$\text{card}(G) = \sum_{x \in \mathcal{R}} \text{card}(\mathcal{O}(x))$$

où  $\mathcal{R}$  est un système de représentants des orbites.

On sépare cette somme en deux parties :

☞ **Les éléments du centre  $Z(G)$**  : D'après la question b), pour chaque  $x \in Z(G)$ , la classe d'équivalence comporte un seul élément, c'est-à-dire  $\text{card}(\mathcal{O}(x)) = 1$ . La réunion de ces orbites fournit exactement  $Z(G)$ , d'où une contribution égale à  $\text{card}(Z(G))$ .

☞ **Les éléments hors du centre** : Soit  $\{x_1, \dots, x_k\}$  l'ensemble des classes d'équivalence distinctes associées aux éléments n'appartenant pas au centre ( $x_i \notin Z(G)$ ). D'après le théorème orbite-stabilisateur, pour tout  $x_i$ , on a :

$$\text{card}(\mathcal{O}(x_i)) = [G : \text{Stab}(x_i)] = \frac{\text{card}(G)}{\text{card}(\text{Stab}(x_i))}$$

En rassemblant les deux parties, on obtient directement la formule des orbites :

$$\text{card}(G) = \text{card}(Z(G)) + \sum_{i=1}^k \frac{\text{card}(G)}{\text{card}(\text{Stab}(x_i))}$$

④ D'après la question précédente, l'action de  $G$  sur lui-même par conjugaison fournit l'équation de la classe :

$$\text{card}(G) = \text{card}(Z(G)) + \sum_{i=1}^k \frac{\text{card}(G)}{\text{card}(\text{Stab}(x_i))}$$

où les  $x_i \notin Z(G)$  représentent les classes de conjugaison non ponctuelles.

☞ **Étude des termes de la somme** : Pour tout  $i \in \{1, \dots, k\}$ , comme  $x_i \notin Z(G)$ , son stabilisateur  $\text{Stab}(x_i)$  est un sous-groupe strict de  $G$ .

D'après le théorème de Lagrange,  $\text{card}(\text{Stab}(x_i))$  divise  $\text{card}(G) = p^\alpha$ . Ainsi, il existe un entier  $\beta_i < \alpha$  tel que :

$$\text{card}(\text{Stab}(x_i)) = p^{\beta_i}$$

On en déduit que :

$$\frac{\text{card}(G)}{\text{card}(\text{Stab}(x_i))} = \frac{p^\alpha}{p^{\beta_i}} = p^{\alpha-\beta_i}$$

Puisque  $\beta_i < \alpha$ , on a  $\alpha - \beta_i \geq 1$ , ce qui implique que chaque terme de la somme est un multiple de  $p$  :

$$\frac{\text{card}(G)}{\text{card}(\text{Stab}(x_i))} \equiv 0 \pmod{p}$$

☞ **Passage de l'équation modulo  $p$**  : Puisque  $\text{card}(G) = p^\alpha \equiv 0 \pmod{p}$ , la réduction de l'équation de la classe modulo  $p$  donne :

$$0 \equiv \text{card}(Z(G)) + \sum_{i=1}^k 0 \pmod{p} \implies \text{card}(Z(G)) \equiv 0 \pmod{p}$$

Ainsi,  $\text{card}(Z(G))$  est un multiple de  $p$ .

☞ **Conclusion** : Puisque l'élément neutre  $e$  appartient au centre ( $e \in Z(G)$ ), on a  $\text{card}(Z(G)) \geq 1$ .

Un entier strictement positif divisible par  $p$  ne peut pas être égal à 1 (car  $p \geq 2$ ).

On en conclut que :

$$\text{card}(Z(G)) \geq p \implies \text{card}(Z(G)) \neq 1 \quad \blacksquare$$

#### ⑤ Tout groupe d'ordre $p^2$ est abélien

Soit  $G$  un groupe tel que  $|G| = p^2$  avec  $p$  premier.

N.B : dans la suite  $|G|$  désigne  $\text{card}(G)$ .

☞ Par l'équation de la classe, le centre d'un  $p$ -groupe est non trivial, donc  $|Z(G)| \in \{p, p^2\}$ .

☞ Si  $|Z(G)| = p^2$ , alors  $Z(G) = G$  et  $G$  est abélien.

☞ Si  $|Z(G)| = p$ , alors  $|G/Z(G)| = \frac{p^2}{p} = p$ . Or, tout groupe d'ordre premier est cyclique. Ainsi  $G/Z(G)$  est cyclique, ce qui implique (d'après la question 2) que  $G$  est abélien, d'où  $Z(G) = G$  (contradiction avec  $|Z(G)| = p$ ).

Dans tous les cas,  $G$  est abélien.

#### ⑥ $D(G)$ est distingué dans $G$ ( $D(G) \triangleleft G$ )

Soit  $g \in G$  et  $[x, y] \in S$  un commutateur. Calculons le conjugué :

$$g[x, y]g^{-1} = g(xy x^{-1} y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) = [gxg^{-1}, gyg^{-1}] \in S$$

Le conjugué d'un commutateur est encore un commutateur. Puisque tout élément  $u \in D(G)$  s'écrit comme un produit fini de commutateurs  $u = c_1 c_2 \dots c_k$ , on a :

$$gug^{-1} = (gc_1g^{-1})(gc_2g^{-1}) \dots (gc_kg^{-1}) \in D(G)$$

Donc  $D(G) \triangleleft G$ .

⑦  $G/D(G)$  est un groupe abélien

Puisque  $D(G) \triangleleft G$ , le groupe quotient  $G/D(G)$  est bien défini. Soient  $\bar{x}, \bar{y} \in G/D(G)$ . On a :

$$\bar{x} \cdot \bar{y} \cdot \bar{x}^{-1} \cdot \bar{y}^{-1} = \overline{xyx^{-1}y^{-1}} = \overline{[x, y]}$$

Comme  $[x, y] \in D(G)$ , la classe  $\overline{[x, y]}$  est l'élément neutre de  $G/D(G)$ . Ainsi  $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{e}$ , soit  $\bar{x}\bar{y} = \bar{y}\bar{x}$ . Le quotient  $G/D(G)$  est donc abélien.

⑧  $G/N$  est abélien si et seulement si  $D(G) \subset N$

Soit  $N \triangleleft G$ .

$$\begin{aligned} G/N \text{ est abélien} &\iff \forall x, y \in G, \bar{x}\bar{y} = \bar{y}\bar{x} \text{ dans } G/N \\ &\iff \forall x, y \in G, \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{e} \\ &\iff \forall x, y \in G, \overline{[x, y]} = \bar{e} \text{ dans } G/N \\ &\iff \forall x, y \in G, [x, y] \in N \\ &\iff \langle \{[x, y] \mid x, y \in G\} \rangle \subset N \\ &\iff D(G) \subset N \end{aligned}$$

⑨ Conclusion

Le groupe dérivé  $D(G)$  est le plus petit sous-groupe distingué de  $G$  tel que le quotient  $G/D(G)$  soit abélien.

Tout quotient abélien de  $G$  s'obtient en quotientant par un sous-groupe distingué contenant  $D(G)$ .

Partie E : Quelques propriétés du groupe symétrique

① Une formule de conjugaison dans  $(\mathfrak{S}_n, \circ)$

**a** Conjugaison d'une transposition Soient  $n \geq 2$ ,  $\sigma \in \mathfrak{S}_n$  et  $1 \leq i \neq j \leq n$ . Posons  $\tau = (i \ j)$  et  $\rho = \sigma \circ (i \ j) \circ \sigma^{-1}$ .

Pour déterminer la permutation  $\rho$ , étudions l'image de tout  $k \in \{1, \dots, n\}$  par  $\rho$  :

Si  $k = \sigma(i)$ , alors  $\sigma^{-1}(k) = i$ . Ainsi :

$$\rho(\sigma(i)) = \sigma((i \ j)(i)) = \sigma(j)$$

Si  $k = \sigma(j)$ , alors  $\sigma^{-1}(k) = j$ . Ainsi :

$$\rho(\sigma(j)) = \sigma((i \ j)(j)) = \sigma(i)$$

Si  $k \notin \{\sigma(i), \sigma(j)\}$ , alors  $\sigma^{-1}(k) \notin \{i, j\}$ . D'où  $(i \ j)(\sigma^{-1}(k)) = \sigma^{-1}(k)$ , et :

$$\rho(k) = \sigma(\sigma^{-1}(k)) = k$$

L'application  $\rho = \sigma \circ (i \ j) \circ \sigma^{-1}$  échange  $\sigma(i)$  et  $\sigma(j)$  et laisse tous les autres éléments fixes. C'est donc la transposition  $(\sigma(i) \ \sigma(j))$  :

$$\sigma \cdot (i \ j) \cdot \sigma^{-1} = (\sigma(i) \ \sigma(j)) \quad \blacksquare$$

**b** Formule générale pour la conjugaison d'un  $k$ -cycle

Soit  $\tau = (a_1 \ a_2 \ \dots \ a_k)$  un  $k$ -cycle de  $\mathfrak{S}_n$ . Par un raisonnement analogue, en décomposant  $\tau = (a_1 \ a_2) \dots (a_{k-1} \ a_k)$  (résultat du cours), on obtient :

$$\begin{aligned} \sigma \cdot \tau \cdot \sigma^{-1} &= \sigma \cdot (a_1 \ a_2) \dots (a_{k-1} \ a_k) \cdot \sigma^{-1} \\ &= \sigma \cdot (a_1 \ a_2) \cdot \sigma^{-1} \dots \sigma \cdot (a_{k-1} \ a_k) \cdot \sigma^{-1} \\ &= (\sigma(a_1) \ \sigma(a_2)) \dots (\sigma(a_{k-1}) \ \sigma(a_k)) = (\sigma(a_1) \ \sigma(a_2) \ \dots \ \sigma(a_k)) \end{aligned}$$

② Transitivité de la distinction

Considérons  $G = \mathfrak{S}_4$ ,  $H = \{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$  et  $K = \{\text{id}, (1\ 2)(3\ 4)\}$ .

a Vérifier que  $H \triangleleft G$  et que  $K \triangleleft H$

☞ **Distinction de  $H$  dans  $G$  ( $H \triangleleft G$ ) :**  $H$  est constitué de l'identité et de toutes les double-transpositions de  $\mathfrak{S}_4$ . Soit  $\sigma \in G = \mathfrak{S}_4$  et  $x \in H$ .

- Si  $x = \text{id}$ , alors  $\sigma \circ \text{id} \circ \sigma^{-1} = \text{id} \in H$ .
- Si  $x = (a\ b)(c\ d)$  est une double-transposition, d'après la formule de conjugaison :

$$\sigma \circ (a\ b)(c\ d) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$$

Comme  $\sigma$  est une bijection de  $\{1, 2, 3, 4\}$ , le résultat est encore un produit de deux transpositions à supports disjoints dans  $\mathfrak{S}_4$ . C'est donc une double-transposition, d'où  $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d)) \in H$ .

On en déduit que  $H$  est stable par conjugaison par tout élément de  $G$ , donc  $H \triangleleft G$ .

☞ **Distinction de  $K$  dans  $H$  ( $K \triangleleft H$ ) :** Le groupe  $H$  est un groupe abélien, donc tout sous-groupe de  $H$  est distingué dans  $H$ .  $K$  étant un sous-groupe de  $H$ , on a donc directement  $K \triangleleft H$ .

b Montrer que  $K$  n'est pas distingué dans  $G$

Suivons l'indication en prenant  $\tau = (1\ 3) \in G = \mathfrak{S}_4$  et  $x = (1\ 2)(3\ 4) \in K$ . Calculons le conjugué de  $x$  par  $\tau$  :

$$\begin{aligned} \tau \circ (1\ 2)(3\ 4) \circ \tau^{-1} &= (1\ 3) \circ (1\ 2)(3\ 4) \circ (1\ 3) \\ &= (\tau(1)\ \tau(2))(\tau(3)\ \tau(4)) = (3\ 2)(1\ 4) \\ &= (1\ 4)(2\ 3) \end{aligned}$$

Or,  $(1\ 4)(2\ 3) \notin K = \{\text{id}, (1\ 2)(3\ 4)\}$ .

$K$  n'est pas stable par conjugaison par les éléments de  $G$ , donc  $K$  n'est pas distingué dans  $G$ .

c Conclusion

On a construit un exemple où :

$$K \triangleleft H \quad \text{et} \quad H \triangleleft G \quad \text{mais} \quad K \ntriangleleft G$$

**Conclusion :** La relation de "distingué" entre sous-groupes n'est pas transitive. ■

③ ( $n \geq 2$ )

a **Bijection  $f : \mathfrak{A}_n \rightarrow \mathfrak{S}_n \setminus \mathfrak{A}_n$**  Soit  $\tau = (1\ 2)$  la transposition échangeant 1 et 2. Sa signature est  $\varepsilon(\tau) = -1$ . Soit  $f : \mathfrak{A}_n \rightarrow \mathfrak{S}_n \setminus \mathfrak{A}_n$  définie par  $f(\sigma) = \tau \circ \sigma$ .

☞ **Bijektivité :** Considérons l'application  $g : \mathfrak{S}_n \setminus \mathfrak{A}_n \rightarrow \mathfrak{A}_n$  définie par  $g(\rho) = \tau \circ \rho$ . Pour tout  $\rho \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ ,  $\varepsilon(g(\rho)) = (-1) \cdot (-1) = 1$ , donc  $g$  est bien définie. De plus,  $(g \circ f)(\sigma) = \tau \circ (\tau \circ \sigma) = \tau^2 \circ \sigma = \text{id} \circ \sigma = \sigma$ , et de même  $(f \circ g)(\rho) = \rho$ .  $g$  est la réciproque de  $f$ , donc  $f$  est bijective.

b **Cardinal de  $\mathfrak{A}_n$**  Puisque  $f$  est une bijection entre  $\mathfrak{A}_n$  et  $\mathfrak{S}_n \setminus \mathfrak{A}_n$ , leurs cardinaux sont égaux :

$$\text{card}(\mathfrak{A}_n) = \text{card}(\mathfrak{S}_n \setminus \mathfrak{A}_n)$$

Comme  $\mathfrak{A}_n$  et  $\mathfrak{S}_n \setminus \mathfrak{A}_n$  forment une partition de  $\mathfrak{S}_n$ , on a :

$$\text{card}(\mathfrak{S}_n) = \text{card}(\mathfrak{A}_n) + \text{card}(\mathfrak{S}_n \setminus \mathfrak{A}_n) = 2 \cdot \text{card}(\mathfrak{A}_n)$$

D'où :

$$\text{card}(\mathfrak{A}_n) = \frac{\text{card}(\mathfrak{S}_n)}{2} = \frac{n!}{2} \quad \blacksquare$$

c **Distinction de  $\mathfrak{A}_n$  dans  $\mathfrak{S}_n$**  L'indice de  $\mathfrak{A}_n$  dans  $\mathfrak{S}_n$  vaut :

$$[\mathfrak{S}_n : \mathfrak{A}_n] = \frac{\text{card}(\mathfrak{S}_n)}{\text{card}(\mathfrak{A}_n)} = 2$$

Tout sous-groupe d'indice 2 dans un groupe est distingué. Ainsi,  $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$ .

④ Sous-groupes distingués de  $\mathfrak{S}_3$  pour  $n = 3$

a Le groupe symétrique  $\mathfrak{S}_3$  contient  $3! = 6$  éléments :

- ☞ L'identité :  $\text{id}$  (d'ordre 1)
- ☞ Les transpositions :  $(1\ 2), (1\ 3), (2\ 3)$  (d'ordre 2)
- ☞ Les 3-cycles :  $(1\ 2\ 3), (1\ 3\ 2)$  (d'ordre 3)
- ☞ Soit  $H$  un sous-groupe de  $\mathfrak{S}_3$ . D'après le théorème de Lagrange, le cardinal de  $H$  divise  $|\mathfrak{S}_3| = 6$ . Donc  $|H| \in \{1, 2, 3, 6\}$ .

Les seuls sous groupes possibles de  $\mathfrak{S}_3$  sont :

- ☞ Si  $|H| = 1$  :  $H = \{\text{id}\}$ .
- ☞ Si  $|H| = 6$  :  $H = \mathfrak{S}_3$ .
- ☞ Si  $|H| = 2$  :  $H$  est engendré par un élément d'ordre 2, c'est-à-dire une transposition, donc  $H = \{\text{id}, (i\ j)\}$ .

☞ Si  $|H| = 3$ , alors  $H = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\} = \mathfrak{A}_3$ .

**b** ☞  $\{\text{id}\}$  et  $\mathfrak{S}_3$  sont trivialement distingués dans  $\mathfrak{S}_3$ .

☞  $\mathfrak{A}_3$  est distingué dans  $\mathfrak{S}_3$ , selon la question précédente.

☞ Si  $H = \{\text{id}, (i\ j)\}$ . Puisque deux transpositions quelconques sont conjuguées dans  $\mathfrak{S}_3$  (par la formule  $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$ ), si  $H$  contient une transposition, son image par conjugaison doit aussi appartenir à  $H$ . Or  $H$  ne contient qu'un seul élément d'ordre 2. Ainsi, aucun sous-groupe d'ordre 2 ne peut être distingué dans  $\mathfrak{S}_3$ .

**Conclusion :** Les seuls sous-groupes distingués de  $\mathfrak{S}_3$  sont  $\{\text{id}\}$ ,  $\mathfrak{A}_3$  et  $\mathfrak{S}_3$ .

### 5 Groupe dérivé $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 3$

☞ Inclusion  $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$  : Tout commutateur  $[u, v] = uvu^{-1}v^{-1}$  a pour signature  $\varepsilon([u, v]) = \varepsilon(u)\varepsilon(v)\varepsilon(u)^{-1}\varepsilon(v)^{-1} = 1$ . Donc  $[u, v] \in \mathfrak{A}_n$ .  $\mathfrak{A}_n$  étant un groupe, il contient le sous-groupe engendré par les commutateurs, d'où  $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$ .

☞  $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$  : Pour  $n \geq 3$ , tout 3-cycle  $(a\ b\ c)$  s'écrit comme un commutateur de transpositions :

$$\begin{aligned} [(a\ b), (a\ c)] &= (a\ b)(a\ c)(a\ b)^{-1}(a\ c)^{-1} \\ &= (b\ a)(a\ c)(b\ b)(a\ c) \\ &= (b\ a\ c)^2 = (a\ b\ c) \end{aligned}$$

Ainsi, tous les 3-cycles appartiennent à  $D(\mathfrak{S}_n)$ . Comme les 3-cycles engendrent  $\mathfrak{A}_n$  pour  $n \geq 3$ , on a  $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$ .

**Conclusion :**  $D(\mathfrak{S}_n) = \mathfrak{A}_n$  pour tout  $n \geq 3$ .

### 6 Produit de transpositions sous forme de 3-cycles

Soient  $a, b, c, d$  des éléments distincts de  $\{1, \dots, n\}$  :

☞ Produit à supports disjoints :

$$(a\ b)(c\ d) = (a\ c\ b) \circ (a\ c\ d)$$

☞ Produit avec un élément commun :

$$(a\ b)(a\ c) = (a\ c\ b)$$

### 7 Écriture de $\sigma \in \mathfrak{A}_n$

Tout élément  $\sigma \in \mathfrak{S}_n$  se décompose en un produit de transpositions. Si  $\sigma \in \mathfrak{A}_n$ , alors  $\varepsilon(\sigma) = 1$ . Puisque la signature d'une transposition est  $-1$ , la parité du nombre de transpositions dans une décomposition de  $\sigma$  doit être paire pour donner un produit de signatures égal à 1. Ainsi, tout  $\sigma \in \mathfrak{A}_n$  s'écrit comme produit d'un nombre pair de transpositions.

### 8 Engendrement de $\mathfrak{A}_n$ par les 3-cycles ( $n \geq 5$ )

D'après la question 7, tout élément de  $\mathfrak{A}_n$  s'écrit comme produit d'un nombre pair de transpositions. On peut regrouper ces transpositions deux par deux :

☞ Les termes de la forme  $(a\ b)(a\ b) = \text{id}$  sont triviaux.

☞ Les termes de la forme  $(a\ b)(a\ c)$  se réécrivent sous la forme d'un 3-cycle  $(a\ c\ b)$  (question 6).

☞ Les termes de la forme  $(a\ b)(c\ d)$  se réécrivent comme produit de deux 3-cycles  $(a\ c\ b)(a\ c\ d)$  (question 6).

Par conséquent, tout élément de  $\mathfrak{A}_n$  s'écrit comme produit de 3-cycles. Les 3-cycles engendrent donc  $\mathfrak{A}_n$  pour tout  $n \geq 3$  (et en particulier pour  $n \geq 5$ ).

## Partie F : Sous groupes de Sylow.

### ① Définition de $\alpha$

L'ensemble  $K = \{k \in \mathbb{N}^* \mid p^k \text{ divise } n\}$  est :

☞ Non vide : car  $p$  divise  $n$ , donc  $1 \in K$ .

☞ Majoré : en effet, pour tout  $k \in K$ , on a  $p^k \leq n$ , ce qui implique  $k \leq \frac{\ln(n)}{\ln(p)}$ .

$K$  étant une partie non vide et majorée de  $\mathbb{N}$ , elle admet un plus grand élément. Ainsi,  $\alpha = \max(K)$  est bien défini. ■

### ② Cardinal de $\mathcal{E}$

On écrit  $n = \text{card}(G) = p^\alpha m$  avec  $p \wedge m = 1$  (c'est-à-dire que  $p$  ne divise pas  $m$ ). Par définition,  $\mathcal{E}$  est l'ensemble de toutes les parties de  $G$  ayant exactement  $p^\alpha$  éléments. Le nombre de sous-ensembles de taille  $p^\alpha$  parmi un ensemble à  $p^\alpha m$  éléments est donné par le coefficient binomial :

$$\text{card}(\mathcal{E}) = \binom{p^\alpha m}{p^\alpha} \quad \blacksquare$$

### ③ Formule du produit pour $\text{card}(\mathcal{E})$

En utilisant la formule explicite du coefficient binomial :

$$\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!} = \frac{\prod_{k=0}^{p^\alpha m - 1} (p^\alpha m - k)}{\prod_{k=0}^{p^\alpha - 1} (p^\alpha - k)}$$

En regroupant terme à terme pour chaque index  $k \in \{0, 1, \dots, p^\alpha - 1\}$ , on obtient :

$$\text{card}(\mathcal{E}) = \binom{p^\alpha m}{p^\alpha} = \prod_{k=0}^{p^\alpha - 1} \frac{p^\alpha m - k}{p^\alpha - k} \quad \blacksquare$$

### ④ Étude de la simplification des rapports $\frac{p^\alpha m - k}{p^\alpha - k}$

Soit  $k \in \{0, 1, \dots, p^\alpha - 1\}$ .

☞ Si  $k = 0$  :

$$\frac{p^\alpha m - 0}{p^\alpha - 0} = \frac{p^\alpha m}{p^\alpha} = m$$

Puisque  $p \wedge m = 1$ ,  $p$  ne divise pas ce rapport  $m$ .

☞ Si  $1 \leq k < p^\alpha$  : D'après l'indication, on écrit  $k = p^j r$  avec  $p$  ne divisant pas  $r$  et  $j < \alpha$ . Substituons cette écriture dans le numérateur et le dénominateur :

$$\frac{p^\alpha m - k}{p^\alpha - k} = \frac{p^\alpha m - p^j r}{p^\alpha - p^j r} = \frac{p^j (p^{\alpha-j} m - r)}{p^j (p^{\alpha-j} - r)} = \frac{p^{\alpha-j} m - r}{p^{\alpha-j} - r}$$

Comme  $j < \alpha$ ,  $p^{\alpha-j}$  est un multiple de  $p$ . De plus,  $p$  ne divise pas  $r$ .

Ainsi, ni le numérateur ( $p^{\alpha-j} m - r$ ) ni le dénominateur ( $p^{\alpha-j} - r$ ) ne sont divisibles par  $p$ .

Par conséquent, après simplification des puissances de  $p$ , ni le numérateur ni le dénominateur ne contiennent de facteur  $p$ . Ainsi,  $p$  ne divise aucun rapport  $\frac{p^{\alpha-j} m - r}{p^{\alpha-j} - r}$ . ■

### ⑤ Non-divisibilité de $\text{card}(\mathcal{E})$ par $p$

D'après la question 3,  $\text{card}(\mathcal{E})$  est le produit de  $p^\alpha$  fractions. D'après la question 4, chaque terme de ce produit se simplifie sous la forme  $\frac{A_k}{B_k}$  où ni  $A_k$  ni  $B_k$  ne sont divisibles par  $p$ .

En effectuant le produit complet  $\text{card}(\mathcal{E}) = \frac{A}{B}$  sous forme simplifiée, ni le numérateur  $A$  ni le dénominateur  $B$  ne contiennent le facteur premier  $p$ . Par conséquent,  $p$  ne divise pas  $\text{card}(\mathcal{E})$ . ■

### ⑥ Action de $G$ sur $\mathcal{E}$

Soit  $f : G \times \mathcal{E} \rightarrow \mathcal{E}$  définie par  $f(g, S) = gS = \{gs \mid s \in S\}$ .

☞ Bonne définition de  $f$  : Pour tout  $S \in \mathcal{E}$  et tout  $g \in G$ , la translation à gauche  $s \mapsto gs$  est une bijection de  $G$  dans  $G$ . Par conséquent,  $\text{card}(gS) = \text{card}(S) = p^\alpha$ , ce qui prouve que  $gS \in \mathcal{E}$ .

☞ Axiomes d'une action de groupe :

☞ Pour tout  $S \in \mathcal{E}$  :  $e_G S = \{e_G s \mid s \in S\} = S$ .

☞ Pour tous  $g_1, g_2 \in G$  et tout  $S \in \mathcal{E}$  :

$$g_1(g_2 S) = \{g_1(g_2 s) \mid s \in S\} = \{(g_1 g_2)s \mid s \in S\} = (g_1 g_2)S$$

$f$  définit donc bien une action du groupe  $G$  sur l'ensemble  $\mathcal{E}$ . ■

⑦ Existence d'une orbite  $S_0$  non divisible par  $p$

Les orbites de l'action de  $G$  sur  $\mathcal{E}$  forment une partition de  $\mathcal{E}$ . Soient  $\mathcal{O}_1, \dots, \mathcal{O}_N$  ces orbites. On a :

$$\text{card}(\mathcal{E}) = \sum_{i=1}^N \text{card}(\mathcal{O}_i)$$

Si la taille de chaque orbite  $\text{card}(\mathcal{O}_i)$  était divisible par  $p$ , alors la somme  $\text{card}(\mathcal{E})$  le serait également. Or, d'après la question 5,  $p$  ne divise pas  $\text{card}(\mathcal{E})$ .

Il existe donc au moins une partie  $S_0 \in \mathcal{E}$  telle que  $p$  ne divise pas  $\text{card}(\mathcal{O}(S_0))$ . ■

⑧  $\text{Stab}_G(S_0)$  est un  $p$ -sous-groupe de Sylow de  $G$

Considérons la partie  $S_0 \in \mathcal{E}$  obtenue à la question 7. Posons  $H = \text{Stab}_G(S_0) = \{g \in G \mid gS_0 = S_0\}$ .

☞ Conséquence de la formule orbite-stabilisateur :

$$\text{card}(G) = \text{card}(\mathcal{O}(S_0)) \times \text{card}(\text{Stab}_G(S_0)) \implies p^\alpha m = \text{card}(\mathcal{O}(S_0)) \times \text{card}(H)$$

Comme  $p$  ne divise pas  $\text{card}(\mathcal{O}(S_0))$ , tous les facteurs  $p^\alpha$  de  $\text{card}(G)$  doivent se retrouver dans  $\text{card}(H)$ . Donc  $p^\alpha$  divise  $\text{card}(H)$ , ce qui implique que :

$$\text{card}(H) \geq p^\alpha$$

☞ Majoration de  $\text{card}(H)$  : Soit  $s_0 \in S_0$ . Pour tout  $h \in H = \text{Stab}_G(S_0)$ , on a  $hs_0 \in S_0$ . L'application  $h \mapsto hs_0$  est injective de  $H$  dans  $S_0$ . Par conséquent :

$$\text{card}(H) \leq \text{card}(S_0) = p^\alpha$$

Des deux inégalités, on conclut que  $\text{card}(H) = p^\alpha$ . Ainsi,  $H = \text{Stab}_G(S_0)$  est un sous-groupe de  $G$  de cardinal  $p^\alpha$ , c'est-à-dire un  $p$ -sous-groupe de Sylow de  $G$ . ■

⑨ Énoncé du 1<sup>er</sup> théorème de Sylow

1<sup>er</sup> Théorème de Sylow

Soit  $G$  un groupe fini d'ordre  $n$ , et soit  $p$  un nombre premier divisant  $n$ . Si  $\alpha$  est la  $p$ -valuation de  $n$  (c'est-à-dire la plus grande puissance de  $p$  divisant  $n$ ), alors  $G$  possède au moins un sous-groupe d'ordre  $p^\alpha$ .

Un tel sous-groupe est appelé un  $p$ -sous-groupe de Sylow de  $G$ .



**Peter Ludwig Sylow (1832-1918)** : Mathématicien norvégien de premier de devenir professeur d'université sur le tard.

Il est mondialement célèbre en algèbre pour ses trois théorèmes de Sylow publiés de Lagrange pour les groupes finis. Ses outils structurent encore aujourd'hui

FiN