GROUPE OPÉRANT SUR UN ENSEMBLE. EXEMPLES ET APPLICATIONS

SOMMAIRE

1. Définition d'une opération d'un groupe *G* sur un ensemble *X*.

<u>1.1. Définition</u>

Soit G un groupe (de loi notée multiplicativement) et X un ensemble (non vide). On dit que G <u>opère</u> sur X si l'on se donne un morphisme θ du groupe G dans le groupe des bijection Bij (X) de l'ensemble X :

$$\theta : G \longrightarrow \mathrm{Bij}\,(X)$$

On a donc, (θ étant un morphisme de groupes) :

$$\theta(gh) = \theta(g) \circ \theta(h)$$

Et en particulier : $\theta(1) = Id_X$

(1 désigne l'élément neutre de G)

<u>1.1. (bis) Définition</u> (Variante)

Soit G un groupe et X un ensemble (non vide).

On dit que G <u>opère</u> (à gauche) sur X si l'on se donne une application : $\varphi : G \times X \longrightarrow X$, $(g, x) \longmapsto g \,.\, x$

ayant les deux propriétés suivantes :

$$\forall (g, h) \in G^2, \forall x \in X,\ g \,.\, (h \,.\, x) = (gh) \,.\, x$$

$$1 \,.\, x = x$$

Noter la similitude entre la loi . et la loi o.

Montrons que ces deux définitions sont bien équivalentes :

Supposons le morphisme θ donné.

Posons $\boxed{g \,.\, x = \theta(g)(x)}$. On a alors :

$\forall (g, h) \in G^2, \forall x \in X$:

$$g \,.\, (h \,.\, x) = \theta(g)(\theta(h)(x)) = \theta(g) \circ \theta(h)\ (x) = \theta(gh)(x) = (gh) \,.\, x \quad \text{et} \quad 1 \,.\, x = \theta(1)(x) = Id_X(x) = x.$$

L'application ainsi construite satisfait bien les conditions de la variante.

Réciproquement, supposons φ donnée.

En notant, pour tout $g \in G$, $\theta(g)$ l'application $X \longrightarrow X$, $x \longmapsto g \,.\, x$, on obtient un morphisme θ de G dans Bij (X).

En effet :

$$\forall x \in X : \theta(gh)(x) = (gh) \,.\, x = g \,.\, (h \,.\, x) = \theta(g)(\theta(h)(x)) = \theta(g) \circ \theta(h)\ (x) \quad \text{(donc } \theta \text{ est un morphisme)}$$

$\forall g \in G, \forall x \in X$: $\theta(g)\theta(g^{-1})(x) = \theta(1)(x) = 1 \,.\, x = x$

D'où : $\theta(g)\theta(g^{-1}) = Id_X$

Donc $\theta(g) \in \mathrm{Bij}\,(X)$ et $\theta(g)^{-1} = \theta(g^{-1})$

<u>1.2. Exemples</u> :

1. S_n opère sur $[\![1, n]\!]$: $S_n \times [\![1, n]\!] \longrightarrow [\![1, n]\!]$, $(\sigma, x) \longmapsto \sigma \,.\, x = \sigma(x)$

   On a bien :

$$\forall (\sigma, \sigma') \in S_n^2, \forall x \in [\![1, n]\!], \sigma' \,.\, (\sigma \,.\, x) = \sigma' \,.\, \sigma(x) = \sigma'(\sigma(x)) = \sigma' \circ \sigma(x) = (\sigma' \circ \sigma) \,.\, x$$

$$Id \,.\, x = Id(x) = x$$

2. Soit $\sigma \in S_n$. Notons $<\sigma> = \{\sigma^n, n \in \mathbb{Z}\}$ le sous-groupe de S_n engendré par σ.

   Alors $<\sigma>$ opère aussi sur $[\![1, n]\!]$: $<\sigma> \times [\![1, n]\!] \longrightarrow [\![1, n]\!]$

$$(\sigma^n, x) \mapsto \sigma^n \cdot x = \sigma^n(x)$$

On a bien : $\forall (m, n) \in \mathbb{Z}^2, \sigma^m \cdot (\sigma^n \cdot x) = \sigma^m \cdot \sigma^n(x) = \sigma^m(\sigma^n(x)) = \sigma^m \circ \sigma^n(x) = (\sigma^m \circ \sigma^n) \cdot x$

$$Id \cdot x = Id(x) = x$$

3. $GL_n(\mathbb{R})$ opère sur $\mathbb{R}^n$: $\forall u \in GL_n(\mathbb{R}), \forall x \in \mathbb{R}^n, u \cdot x = u(x)$.

4. Soit E un $\mathbb{K}$-espace vectoriel. Alors le groupe $\mathbb{K}^*$ opère sur E :

$$\forall \lambda \in \mathbb{K}^*, \forall x \in E, \lambda \cdot x = \lambda x$$

5. Le groupe additif $\mathbb{R}$ opère sur $\mathbb{C}$:

$$\forall \theta \in \mathbb{R}, \forall z \in \mathbb{C}, \theta \cdot z = \mathbf{e}^{\mathbf{i}\theta} z.$$

(Note : ici, l'élément e tel que $e \cdot z = z$ n'est pas unique)

1.3. Remarques :

1. En général $g_1 \cdot x = g_2 \cdot x$ n'entraîne pas $g_1 = g_2$.

   En effet, dans S_4, considérons $\sigma_1 = (1, 2)$ et $\sigma_2 = (1, 3)$.

   On a : $\sigma_1(4) = \sigma_2(4)$ $(= 4)$ et pourtant $\sigma_1 \neq \sigma_2$.

   Cependant, cela est vrai si le morphisme $\theta : G \longrightarrow \text{Bij}(X)$ est **injectif**.

2. Si H est un sous groupe de G, et si G opère sur X, alors H opère aussi sur X (restriction de φ à $H \times X$)

2. Orbites et stabilisateurs.

Sur X, on considère la relation : $x \sim y \iff \exists g \in G$ tel que $y = g \cdot x$

C'est une relation d'équivalence :

- Réflexivité : $x = 1 \cdot x$ d'où $x \sim x$.
- Symétrie :

  Si $x \sim y$, i.e. $\exists g \in G$ tel que $y = g \cdot x$, alors $\exists h \in G$ tel que $x = h \cdot y$.

  (Il suffit de choisir $h = g^{-1}$. En effet, $h \cdot y = g^{-1} \cdot y = g^{-1} \cdot g \cdot x = (g^{-1}g) \cdot x = 1 \cdot x = x$). Donc $y \sim x$.
- Transitivité : Si $x \sim y$ et $y \sim z$ alors on a : $y = g \cdot x$ et $z = h \cdot y$ d'où $z = h \cdot g \cdot x = (hg) \cdot x$ d'où $x \sim z$.

2.1. Définition

On appelle G-orbite de x (ou plus simplement orbite de x) la classe d'équivalence de x pour la relation définie ci-dessus :

$$\text{Orb}_G(x) = \{y \in X \text{ pour lesquels } \exists g \in G \text{ tels que } y = g \cdot x\} = \{g \cdot x, \text{ où } g \in G\} = G \cdot x$$

Pour tout $x \in X$, l'application

$$\begin{aligned} f_x : G &\longrightarrow X \\ g &\longmapsto g \cdot x \end{aligned}$$

s'appelle l'application d'orbite de x.

2.2. Exemples :

1. $G = S_n$. Il n'y a qu'une G-orbite.

   En effet, soit $x \in [\![1 ; n]\!]$.

$$\forall y \in [\![1, n]\!], \exists \sigma \in S_n \text{ telle que } y = \sigma(x)$$

(On peut par exemple choisir la transposition $\sigma = (x, y)$)

D'où : $$\mathrm{Orb}_G(x) = [\![1, n]\!] = X$$

2. Soit $\sigma \in S_n$. Considérons le sous-groupe $G = <\sigma>$ engendré par σ.

   On sait que : $$<\sigma> = \{\sigma^n, n \in \mathbb{Z}\}.$$

   Soit $x \in [\![1 ; n]\!]$.

   On a : $$\mathrm{Orb}_{<\sigma>}(x) = <\sigma> \cdot x = \{\sigma^n(x), n \in \mathbb{Z}\}.$$

   Par exemple, dans S_4, choisissons $\sigma = (1, 2, 4)$.

   On a : $$\sigma^2 = (1, 4, 2) \text{ et } \sigma^3 = Id.$$

   On a donc : $$<\sigma> = \{Id ; (1, 2, 4) ; (1 ; 4 ; 2)\}.$$

   $$\mathrm{Orb}_{<\sigma>}(1) = \{1 ; 2 ; 4\} \ (= \mathrm{Orb}_{<\sigma>}(2) = \mathrm{Orb}_{<\sigma>}(4)) \text{ et } \mathrm{Orb}_{<\sigma>}(3) = \{3\}$$

   Il y a donc 2 $<\sigma>$-orbites.

3. $G = GL_n(\mathbb{R})$.

   Soit $x \in \mathbb{R}^n$.

   $$\mathrm{Orb}_{GL_n(\mathbb{R})}(x) = GL_n(\mathbb{R}) \cdot x$$

   Si $x = 0$ alors $\mathrm{Orb}_{GL_n(\mathbb{R})}(0) = \{0\}$. (En effet, pour tout $u \in GL_n(\mathbb{R})$, $u(0) = 0$).

   Si $x \neq 0$ alors $\mathrm{Orb}_{GL_n(\mathbb{R})}(x) = \mathbb{R}^n \setminus \{0\}$. (En effet, $\forall y \in \mathbb{R}^n \setminus \{0\}$, $\exists u \in GL_n(\mathbb{R})$ tel que $y = u(x)$)

<u>2.3. Conséquence</u> : puisque une orbite est une classe d'équivalence, l'ensemble des orbites de X constitue une partition de X et l'on peut écrire {orbites} = ${}^{X}\!/_{G}$.

<u>2.4. Définition</u>

On dit que l'action de G sur X est <u>transitive</u> si elle n'a qu'une seule orbite :

$$\forall x, y \in X, \exists g \in G \text{ tel que } y = g \cdot x$$

C'est-à-dire : $$\forall x \in X,\ G \cdot x = X$$

Par exemple, si σ est une permutation circulaire, alors l'action de $<\sigma>$ sur $[\![1, n]\!]$ est transitive.

Remarquons qu'en général, l'élément g n'est pas unique. (Voir remarque 1.3.1)

<u>2.5. Théorème</u>

G opère transitivement sur $X \Leftrightarrow \forall x \in X$, l'application d'orbite f_x de x est surjective.

<u>Démonstration</u> :

Supposons que G opère transitivement sur X.

Soit $x \in X$. Montrons que f_x est surjective.

Soit $y \in X$. Comme G opère transitivement sur X :

$$\exists g \in G \text{ tel que : } y = g \cdot x = f_x(g)$$

Donc f_x est surjective.

Réciproquement, si pour tout $x \in X$, l'application f_x est surjective, alors :

$$\forall y \in X, \exists g \in G \text{ tel que : } y = f_x(g) = g \,.\, x$$

Donc G opère transitivement sur X.

<u>2.6. Définition</u>

L'action de G sur X est dite <u>libre</u> (ou <u>fidèle</u>) lorsque pour tout $x \in X$, l'application d'orbite f_x de x est injective.

<u>2.7. Conséquence importante</u>. Si G opère librement sur X, alors on a :

$$g_1 \,.\, x = g_2 \,.\, x \Rightarrow g_1 = g_2$$

(ou de manière équivalente : $g \,.\, x = x \Rightarrow g = 1$ (poser $g = g_1^{-1} g_2$ pour se ramener à la situation précédente).

Ainsi G s'identifie à l'orbite $G \,.\, x$.

<u>2.8. Définition</u>

On dit que G opère sur X de façon <u>simplement transitive</u> si, pour tout $x \in E$, l'application d'orbite f_x de x est bijective : $\forall x, y \in X, \exists\, !\, g \in G$ tel que $y = g \,.\, x$

Autrement dit, G opère sur X de façon simplement transitive si l'action est libre et transitive.

<u>2.9. Exemples</u> :

1. S_n opère transitivement sur $X = [\![1, n]\!]$: $\forall x, y \in [\![1, n]\!], \exists\, \sigma \in S_n$ tel que $y = \sigma(x)$.

   (La transposition $\sigma = (x, y)$ convient).

   Remarquons que pour $n \geqslant 3$, l'élément σ n'est pas unique.

   Par exemple, avec $\sigma = (1, 2)$ et $\sigma' = (1, 2, 3)$, on a $\sigma(1) = \sigma'(1) = 2$)

2. $GL_n(\mathbb{R})$ sur $\mathbb{R}^n \setminus \{0\}$.

3. Définition d'un espace affine : soit A un ensemble et E un espace vectoriel. On dit que A est un espace affine (attaché à E) si le groupe $(E, +)$ opère de façon simplement transitive sur A au moyen de l'application φ suivante :

$$\begin{aligned} \varphi : E \times A &\longrightarrow A \\ (\vec{u}, M) &\longmapsto \vec{u} \,.\, M = M + \vec{u} \end{aligned}$$

   Conséquences :

   Comme φ est une opération :

$$(M + \vec{u}) + \vec{v} = \vec{v} \,.\, (M + \vec{u}) = \vec{v} \,.\, \vec{u} \,.\, M = (\vec{v} + \vec{u}) \,.\, M = (\vec{u} + \vec{v}) \,.\, M = M + (\vec{u} + \vec{v})$$

$$M + \vec{0} = \vec{0} \,.\, M = M$$

   En outre, comme φ opère de façon simplement transitive :

   $\forall M, N \in A, \exists\, !\, \vec{u} \in E$ tel que $N = M + \vec{u}$ (notation $\vec{u} = \overrightarrow{MN}$)

   En particulier, pour $M = N$, on a : $\exists\, !\, \vec{u} \in E$ tel que $M = M + \vec{u}$, et comme $M + \vec{0} = M$, on a :

$$M = M + \vec{u} \iff \vec{u} = \vec{0}$$

Soit O un point fixé de A. L'application $\varphi_O : E \longrightarrow A$, $\vec{u} \mapsto O + \vec{u}$ est bijective.

Donc le choix d'un point O de A permet d'identifier E à A.

2.10. Définition

Soit $x \in X$. On appelle stabilisateur de x dans G le sous-groupe S_x de G défini par :

$$S_x = \{g \in G \text{ tels que } g \,.\, x = x\}$$

S_x s'appelle encore le groupe d'isotropie de x dans G.

2.11. Remarque : S_x est un bien un sous groupe de G :

- $1 \in S_x$ puisque $1 \,.\, x = x$
- Si $g, h \in S_x$ alors $(gh) \,.\, x = g \,.\, h \,.\, x = g \,.\, x = x$ donc $gh \in S_x$.
- Si $g \in S_x$ alors $g \,.\, x = x$. On a donc $g^{-1} \,.\, x = g^{-1} \,.\, g \,.\, x = 1 \,.\, x = x$ donc $g^{-1} \in S_x$.

2.12. Exemples :

1. Le stabilisateur S_2 de 2 dans le groupe S_4 est $S_2 = \{Id\ ;\ (1, 3)\ ;\ (1, 4)\ ;\ (3, 4)\ ;\ (1, 3, 4)\ ;\ (1, 4, 3)\}$.
2. Plus généralement, dans S_n, le stabilisateur de n est S_{n-1}.

Cas particulier : si $x \in X$ est tel que $S_x = G$ alors, pour tout $g \in G$, on a $g \,.\, x = x$. On dit alors que x est un point fixe pour l'opération de G sur X. (C'est le cas de $0 \in \mathbb{R}^n$ pour $GL_n(\mathbb{R})$)

Rappels :

Deux éléments x et y d'un groupe G sont dits conjugués s'il existe $g \in G$ tel que $y = i_g(x) = gxg^{-1}$.

Plus généralement, deux sous-groupes G_1 et G_2 de G sont conjugués s'il existe $g \in G$ tel que $G_2 = i_g(G_1) = gG_1g^{-1}$.

(cela signifie que $\exists g \in G$ tel que $\forall h \in G_1$, $ghg^{-1} \in G_2$)

2.13. Proposition

$$y \in \mathrm{Orb}_G(x) \Rightarrow S_x \text{ et } S_y \text{ sont conjugués}$$

Démonstration :

Soit $y \in \mathrm{Orb}_G(x)$, donc : $\exists g \in G$ tel que $y = g \,.\, x$

Soit $h \in S_y$: $h \,.\, y = y$.

Donc : $(hg) \,.\, x = g \,.\, x$

D'où : $g^{-1}hg \in S_x$.

Bilan : $\exists g \in G$ tel que $\forall h \in S_y$, $g^{-1}hg \in S_x$, donc S_x et S_y sont conjugués.

On a donc $S_y = gS_xg^{-1}$ et comme $y = g \,.\, x$, on a : $S_{g.\,x} = gS_xg^{-1}$.

3. Groupe opérant sur lui même

Dans les cas d'étude suivants, on a $G = X$.

3.1. G opère sur lui même par translation à gauche

$$\begin{aligned} G \times G &\to G \\ (g, x) &\mapsto g \,.\, x = gx \end{aligned}$$

On obtient bien une opération ($1 \,.\, x = 1x = x$ et $g \,.\, (h \,.\, x) = g \,.\, (hx) = ghx = (gh) \,.\, x$)

Comme G est un groupe, $\forall x, y \in G, \exists\,!\, g \in G$ tel que $y = gx$ (on choisit $g = yx^{-1}$)

Il n'y a donc qu'une seule G-orbite (G lui même). L'opération est donc simplement transitive.

D'autre part, pour tout $x \in G$, on a $S_x = \{g \in G$ tels que $gx = x\}$.

Or, $gx = x$ équivaut à $g = 1$. Donc le stabilisateur S_x de tout élément x est réduit à $\{1\}$.

3.2. G opère sur lui même par translation à droite

$$\begin{aligned} G \times G &\to G \\ (g, x) &\mapsto g \,.\, x = xg^{-1} \end{aligned}$$

Remarque : pourquoi ne pas avoir choisi $g \,.\, x = xg$? Car, cela ne définit pas d'opération :

$$g \,.\, (h \,.\, x) = g \,.\, (xh) = xhg = (hg) \,.\, x \text{ et non } (gh) \,.\, x$$

Tandis qu'en choisissant $g \,.\, x = xg^{-1}$, on définit bien une opération :

$$1 \,.\, x = x1^{-1} = x \quad \text{et} \quad g \,.\, (h \,.\, x) = g \,.\, (xh^{-1}) = xh^{-1}g^{-1} = x(gh)^{-1} = (gh) \,.\, x$$

Comme G est un groupe, $\forall x, y \in G, \exists\,!\, g \in G$ tel que $y = xg^{-1}$ (on choisit $g^{-1} = x^{-1}y$ c'est-à-dire $g = y^{-1}x$)

Il n'y a donc qu'une seule G-orbite (G lui même). L'opération est donc simplement transitive.

D'autre part, pour tout $x \in G$, on a $S_x = \{g \in G$ tels que $xg^{-1} = x\}$.

Or, $xg^{-1} = x$ équivaut à $g^{-1} = 1$ c'est-à-dire $g = 1$. Donc le stabilisateur S_x de tout élément x est réduit à $\{1\}$.

3.3. G opère sur lui même par conjugaison (ou automorphisme intérieur)

$$\begin{aligned} G \times G &\to G \\ (g, x) &\mapsto g \,.\, x = gxg^{-1} \end{aligned}$$

On obtient bien une opération ($1 \,.\, x = 1x1^{-1} = x$ et $g \,.\, (h \,.\, x) = g \,.\, (hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = (gh) \,.\, x$)

$$\mathrm{Orb}_G(x) = \{y \in G \text{ pour lesquels } \exists g \in G \text{ tel que } y = gxg^{-1}\} = GxG^{-1}$$

(C'est ce qu'on appelle la classe de conjugaison de x)

D'autre part, pour tout $x \in G$, on a :

$$S_x = \{g \in G \text{ tels que } gxg^{-1} = x\} = \{g \in G \text{ tels que } gx = xg\} = Z_G(x) = \text{centralisateur de } x \text{ dans } G.$$

3.4. Théorème de Cayley

Tout groupe fini G d'ordre n est isomorphe à un sous-groupe de S_n.

Démonstration :

On fait opérer G sur lui même par translation à gauche :

$$\begin{aligned} \varphi : G \times G &\to G \\ (g, x) &\mapsto g \,.\, x = gx \end{aligned}$$

On a vu (3.2.) que cette opération est simplement transitive.

Or, pour tout $g \in G$, l'application : $\quad \begin{aligned} \theta(g) : G &\to G \\ x &\mapsto g \,.\, x \end{aligned}$

est un endomorphisme de G (1.1.)

Et l'application : $$\begin{aligned}\theta : G &\longrightarrow \mathrm{Bij}(G)\\ g &\longmapsto \theta(g)\end{aligned}$$

est injective. (Car : $\theta(g_1) = \theta(g_2) \Rightarrow \forall x \in G,\ \theta(g_1)(x) = \theta(g_2)(x) \Rightarrow g_1x = g_2x \Rightarrow g_1 = g_2$)

En conséquence, G est isomorphe à $\mathrm{Im}(\theta)$, c'est-à-dire à un sous groupe de $\mathrm{Bij}(G) \cong S_n$.

4. Formule des classes

Dans ce paragraphe, on suppose que X est de cardinal fini.

4.1. Factorisation de l'application d'orbite

Soit $x \in X$. L'application d'orbite $$\begin{aligned}f_x : G &\longrightarrow X\\ g &\longmapsto g \centerdot x\end{aligned}$$

n'est pas injective en général.

Cependant, on a :

$$f_x(g_1) = f_x(g_2) \Rightarrow g_1 \centerdot x = g_2 \centerdot x \Rightarrow (g_2^{-1}g_1 \centerdot x = x) \Rightarrow g_2^{-1}g_1 \in S_x$$

Définissons la relation R_x sur G par : $g_1 \, R_x \, g_2 \Leftrightarrow g_2^{-1}g_1 \in S_x$

On vérifie que R_x est une relation d'équivalence sur G (car le stabilisateur S_x est un sous-groupe de G)

On peut donc définir l'application $\overline{f}_x$ du groupe quotient G/R_x (que l'on notera encore G/S_x) dans X par :

$$\begin{aligned}\overline{f}_x : G/S_x &\longrightarrow X\\ \overline{g} &\longmapsto g \centerdot x\end{aligned}$$

Cette application est bien définie :

En effet, si g_1 et g_2 sont des éléments de $\overline{g}$, alors :

$$g_2^{-1}g_1 \in S_x \Rightarrow g_2^{-1}g_1 \centerdot x = x \Rightarrow g_1 \centerdot x = g_2 \centerdot x \Rightarrow f_x(g_1) = f_x(g_2)$$

On peut donc bien poser $\overline{f}_x(\overline{g}) = f_x(g)$ où g est un représentant quelconque de $\overline{g}$.

De plus, $\overline{f}_x$ est un injective.

En effet :

$$\overline{f}_x(\overline{g}_1) = \overline{f}_x(\overline{g}_2) \Rightarrow g_1 \centerdot x = g_2 \centerdot x \Rightarrow g_1 \, R_x \, g_2 \Rightarrow \overline{g}_1 = \overline{g}_2$$

Donc $\overline{f}_x$ induit un isomorphisme de G/S_x sur $\mathrm{Im}(\overline{f}_x) = \mathrm{Orb}_G(x) = G \centerdot x$.

Donc : G/S_x et $\mathrm{Orb}_G(x)$ sont **isomorphes**

4.2. Formule des classes

Puisque les orbites sous G forment une partition de X, on a :

$$\mathrm{Card}(X) = \sum_{x \in I} \mathrm{Card}(G \centerdot x)$$

Où I est une partie de G contenant exactement un représentant de chaque orbite.

Mais, d'après 4.1., pour tout $x \in G$:

$$\mathrm{Card}(G \centerdot x) = \frac{\mathrm{Card}(G)}{\mathrm{Card}(S_x)}$$

On a donc : $$\text{Card}(X) = \sum_{x\in I} \frac{\text{Card}(G)}{\text{Card}(S_x)}$$

Étudions des cas particuliers :

4.2.a. Formule des classes dans le cas où G opère sur lui-même par conjugaison :

Dans ce cas là, chaque élément x du centre $Z(G)$ définit une orbite réduite à lui même :

En effet, rappelons que : $\text{Orb}_G(x) = G\,.\,x = \{g\,.\,x \text{ où } g \in G\} = \{gxg^{-1} \text{ où } g \in G\}$

On a donc : $$x \in Z(G) \Leftrightarrow \text{Orb}_G(x) = \{x\}$$

Par ailleurs :

$$x \in Z(G) \Leftrightarrow \forall y \in G, xy = yx \Leftrightarrow \forall y \in G,\ x = yxy^{-1} \Leftrightarrow \forall y \in G,\ x = y\,.\,x \Leftrightarrow \forall y \in G,\ y \in S_x \Leftrightarrow S_x = G$$

Le formule des classes devient, en posant $I = I' \cup Z(G)$:

$$\text{Card}(G) = \sum_{x\in Z(G)} \frac{\text{Card}(G)}{\text{Card}(S_x)} + \sum_{x\in I'} \frac{\text{Card}(G)}{\text{Card}(S_x)}$$

Et comme pour $x \in Z(G)$, on a : $\text{Card}(G) = \text{Card}(S_x)$:

$$\text{Card}(G) = \text{Card}(Z(G)) + \sum_{x\in I'} \frac{\text{Card}(G)}{\text{Card}(S_x)}$$

4.2.b. Formule des classes dans le cas où G est un p-groupe opérant sur un ensemble X

Soit p un nombre premier. On appelle p-groupe tout groupe d'ordre p^α où $\alpha \in \mathbb{N}^*$.

Soit G un p-groupe d'ordre p^α.

Définissons l'ensemble X^G des points fixes de X par l'opération de G :

$$X^G = \{x \in X \mid \forall g \in G, g\,.\,x = x\} \subset X$$

Comme dans 4.2.a., on a :

$$x \in X^G \Leftrightarrow G\,.\,x = \{x\} \Leftrightarrow S_x = G$$

Par contraposition : $x \notin X^G \Leftrightarrow S_x$ est un sous-groupe strict de G

La formule des classes devient :

$$\text{Card}(X) = \text{Card}(X^G) + \sum_{x\in I'} \frac{\text{Card}(G)}{\text{Card}(S_x)}$$

Donc, d'après le théorème de Lagrange, S_x est d'ordre p^β avec $\beta \in [\![1, \alpha - 1]\!]$.

En conséquence, pour tout $x \in I'$: $$\frac{\text{Card}(G)}{\text{Card}(S_x)} = 0\ [p]$$

D'où : $$\text{Card}(X) = \text{Card}(X^G)\ [p]$$

Conséquences :

1) Le centre d'un p-groupe est non trivial.

2) Tous les groupes d'ordre p^2 sont abéliens.

Démonstration :

On fait opérer G sur lui-même par conjugaison :

Dans ce cas : $$X^G = G^G = Z(G)$$

On a donc : $$\text{Card}(Z(G)) = \text{Card}(G)\ [p] = 0\ [p]$$

Or, $\text{Card}(Z(G)) \geqslant 1$, (car $Z(G)$ contient au moins le neutre), donc :

$$\text{Card}(Z(G)) = p^\gamma \text{ avec } 1 \leqslant \gamma \leqslant \alpha$$

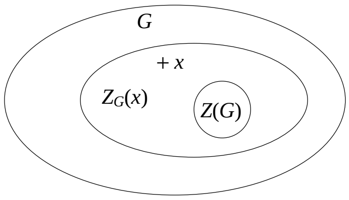
Ce qui prouve 1).

Dans le cas où $\alpha = 2$, le raisonnement ci-dessus montre que :

$$\text{Card}(Z(G)) = p \text{ ou } p^2$$

Supposons $\text{Card}(Z(G)) = p$. Il existe alors $x \in G \setminus Z(G)$.

Mais d'après 3.3. : $S_x = Z_G(x)$



Or, $x \in S_x = Z_G(x)$ et $Z(G) \subset Z_G(x)$.

Donc $\text{Card}(Z_G(x)) \geqslant \text{Card}(Z(G))$.

Mais comme $x \in Z_G(x) \setminus Z(G)$.

On a : $\text{Card}(Z_G(x)) \geqslant p + 1$.

Donc, d'après le théorème de Lagrange : $\text{Card}(Z_G(x)) = p^2$.

Donc $Z_G(x) = G$ et par suite $x \in Z(G)$. Contradiction.

Donc $\text{Card}(Z(G)) = p^2$ et donc G est abélien d'où 2).

Remarque : cela ne fonctionnerait pas avec un groupe d'ordre p^3.