
ACTIONS DE GROUPES

Chapitre 2

Ce polycopié est très largement inspiré du polycopié utilisé par mon prédécesseur K. Koufany, que je remercie pour son travail de rédaction.

Table des matières

1. Actions de groupes	1
2. Orbites et stabilisateurs	3
3. Équation des classes, Formule de Burnside	6
4. Théorème de Cauchy	9
5. Théorème de Noether	11
6. Produit semi-direct	12

Dans ce chapitre, G désigne un groupe multiplicatif d'élément neutre e et E un ensemble non vide. L'ensemble des bijections de E sur E sera noté $\mathcal{S}(E)$ et on l'appellera **groupe des permutations** de E .

1. Actions de groupes

Définition 1.1. — On dit que G **opère à gauche** sur E si on a une application

$$\begin{aligned} G \times E &\rightarrow E \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

vérifiant :

- $\forall x \in E, e \cdot x = x$;
- $\forall g, g' \in G, \forall x \in E, g \cdot (g' \cdot x) = (gg') \cdot x$.

Une telle application est aussi appelée **action à gauche** du groupe G sur l'ensemble E .

On peut définir de manière analogue la notion d'action à droite :

Définition 1.2. — On dit que G **opère à droite** sur E si on a une application

$$\begin{aligned} G \times E &\rightarrow E \\ (g, x) &\mapsto x \cdot g \end{aligned}$$

vérifiant :

- $\forall x \in E, x \cdot e = x$;
- $\forall g, g' \in G, \forall x \in E, (x \cdot g) \cdot g' = x \cdot (gg')$.

Une telle application est aussi appelée **action à droite** du groupe G sur l'ensemble E .

Remarque 1.3. — Il n'y a pas de différence conceptuelle entre les actions à gauche et les actions à droite. Plus précisément, si $(g, x) \mapsto g \cdot x$ est une action à gauche, alors on peut définir une action à droite par $x \cdot g := g^{-1} \cdot x$. En effet, on aura avec cette définition

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

alors que

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

où pour la dernière égalité on a utilisé le fait que $(g, x) \mapsto g \cdot x$ est une action à gauche. L'égalité des deux termes calculés montre que $(g, x) \mapsto x \cdot g$ est bien une action à droite.

Par la suite, lorsqu'on parlera d'action, sans préciser s'il s'agit d'une action à droite ou à gauche, ce sera de manière sous-entendue une action à gauche.

Remarque 1.4. — Supposons que G opère à gauche sur E . Pour $g \in G$, l'application

$$\begin{aligned} \varphi(g) : E &\rightarrow E \\ x &\mapsto g \cdot x \end{aligned}$$

est alors une bijection de E sur E , c'est-à-dire $\varphi(g) \in \mathcal{S}(E)$. En effet, de l'égalité $e \cdot x = x$ pour tout $x \in E$, on déduit que $\varphi(e) = Id_E$ et avec l'égalité $g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e \cdot x = x$ et $g^{-1} \cdot (g \cdot x) = x$, on déduit que $\varphi(g) \circ \varphi(g^{-1}) = \varphi(g^{-1}) \circ \varphi(g) = Id_E$, ce qui signifie que $\varphi(g)$ est bijective d'inverse $\varphi(g^{-1})$.

De plus avec $g \cdot (g' \cdot x) = (gg') \cdot x$, pour tous g, g', x , on déduit que $\varphi(gg') = \varphi(g) \circ \varphi(g')$, c'est-à-dire que l'application φ est un morphisme de groupes de G dans $\mathcal{S}(E)$. Le noyau de ce morphisme est le noyau de l'action à gauche de G sur E .

Réciproquement, un tel morphisme φ définit une action à gauche de G sur E de la manière suivante

$$g \cdot x = \varphi(g)(x).$$

Exemple 1.5. — 1. G agit sur lui-même par **translations à gauche** :

$$(g, x) \in G \times G \mapsto g \cdot x = gx \in G$$

et par **translations à droite** :

$$(g, x) \in G \times G \mapsto x \cdot g = xg \in G.$$

2. G agit sur lui-même par **conjugaisons** (c'est une action à gauche) :

$$(g, x) \in G \times G \mapsto g \cdot x = gxg^{-1} \in G.$$

3. Un groupe G agit sur tout sous-groupe distingué H par conjugaisons

$$(g, x) \in G \times H \mapsto g \cdot x = gxg^{-1} \in H.$$

4. Le groupe des permutations $\mathcal{S}(E)$ agit naturellement sur E par

$$(\sigma, x) \in \mathcal{S}(E) \times E \mapsto \sigma \cdot x = \sigma(x) \in E.$$

2. Orbites et stabilisateurs

Définition 2.1. — Soit G un groupe opérant sur un ensemble non vide E . Pour tout $x \in E$, le sous-ensemble de E

$$G \cdot x = \{g \cdot x ; g \in G\},$$

est appelé **orbite** de x sous l'action de G . On le note parfois \mathcal{O}_x .

On considère la relation définie sur E par

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

Pour tout $x \in E$, on a $x = e \cdot x$, donc $x \mathcal{R} x$.

Si $x \mathcal{R} y$, il existe $g \in G$ tel que $y = g \cdot x$, ou encore $x = g^{-1} \cdot y$ d'où $y \mathcal{R} x$.

Si $x \mathcal{R} y$ et $y \mathcal{R} z$, alors $y = g_1 \cdot x$ et $z = g_2 \cdot y$, pour $g_1, g_2 \in G$. Donc $z = g_2 \cdot (g_1 \cdot x) = (g_2 g_1) \cdot x$, d'où $x \mathcal{R} z$.

Par conséquent, la relation \mathcal{R} est une relation d'équivalence sur E . La classe d'un élément $x \in E$ est

$$\bar{x} = \{y \in E, x \mathcal{R} y\} = \{y \in E, \exists g \in G, y = g \cdot x\} = G \cdot x.$$

La classe de x pour cette relation coïncide donc avec l'orbite de x sous l'action de G . On en déduit (d'après le chapitre 1) que **les orbites forment une partition** de E ,

$$E = \bigsqcup_{\alpha \in E/G} \alpha.$$

Exemple 2.2. — 1. Pour l'action de $\mathcal{S}(E)$ sur E , il y a une seule orbite. En effet, pour tout $x \in E$ on a

$$\mathcal{S}(E) \cdot x = \{\sigma(x), \sigma \in \mathcal{S}(E)\} = E,$$

puisque pour tout $y \in E$, $y = \tau(x)$, où τ est la transposition $\tau = (x, y)$ si $y \neq x$ et $\tau = Id_E$ si $y = x$.

2. Pour l'action de G sur lui-même par conjugaisons, les orbites sont appelées **classes de conjugaison** :

$$\forall h \in G, G \cdot h = \{ghg^{-1}, g \in G\}.$$

Le groupe G est abélien si, et seulement si, $G \cdot h = \{h\}$ pour tout $h \in G$.

3. Si H est un sous-groupe de G , il agit (à gauche) par translations à droite sur G :

$$(h, g) \in H \times G \mapsto h \cdot g = gh^{-1} \in G.$$

Pour tout $g \in G$, l'orbite de g est la classe modulo H :

$$H \cdot g = \{h \cdot g, h \in H\} = \{gh^{-1}, h \in H\} = \{gk, k \in H\} = gH.$$

L'ensemble de ces orbites est alors l'ensemble quotient G/H des classes à gauche modulo H .

On peut de même définir l'action de H sur G par translation à gauche

$$(h, g) \in H \times G \mapsto h \cdot g = hg \in G,$$

les orbites sont les classes à droite modulo H

$$H \cdot g = \{hg, h \in H\} = Hg.$$

4. Pour tout entier $n \geq 1$, le groupe orthogonal $O_n(\mathbb{R})$ agit naturellement sur \mathbb{R}^n ,

$$\forall A \in O_n(\mathbb{R}), \forall x \in \mathbb{R}^n, A \cdot x = A(x).$$

L'orbite de $x \in \mathbb{R}^n$ est la sphère centrée en 0 et de rayon $\|x\|$: en effet,

$$O_n(\mathbb{R}) \cdot x = \{A(x), A \in O_n(\mathbb{R})\}.$$

Pour tout $y \in O_n(\mathbb{R}) \cdot x$, il existe $A \in O_n(\mathbb{R})$ tel que $y = A(x)$ et $\|y\| = \|A(x)\| = \|x\|$, donc $y \in S(0, \|x\|)$.

Réciproquement, si $y \in S(0, \|x\|)$ avec $x \neq 0$, on a $y \neq 0$ et on peut construire deux bases orthonormées $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et $\mathcal{B}' = (e'_i)_{1 \leq i \leq n}$ de \mathbb{R}^n avec $e_1 = \frac{1}{\|x\|}x$ et $e'_1 = \frac{1}{\|y\|}y$. La matrice de passage A de \mathcal{B} à \mathcal{B}' est alors orthogonale et $y = \|y\|e'_1 = \|x\|A(e_1) = A(\|x\|e_1) = A(x)$, donc $y \in O_n(\mathbb{R}) \cdot x$. Pour $x = 0$, on a $O_n(\mathbb{R}) \cdot 0 = \{0\} = S(0, 0)$.

Pour la réciproque, on peut aussi considérer la symétrie orthogonale par rapport au plan médiateur du segment $[x, y]$, qui est orthogonale et envoie x sur y .

5. Pour des entiers $n \geq 1$, $m \geq 1$, on considère l'action du groupe $G = GL_n(\mathbb{R}) \times GL_m(\mathbb{R})$ sur l'ensemble $E = \mathcal{M}_{n,m}(\mathbb{R})$ des matrices rectangulaires $n \times m$ définie par

$$\forall (P, Q) \in G, \forall A \in E, (P, Q) \cdot A = PAQ^{-1}.$$

Les orbites de cette action sont les ensembles

$$\mathcal{O}_r = \{A \in E, \text{rg}(A) = r\}$$

où r est un entier compris entre 0 et $\min(n, m)$. (Voir TD, feuille 2)

Définition 2.3. — On dit que l'action de G sur E est **transitive** (resp. **simplement transitive**) si pour tout $x, y \in E$, il existe $g \in G$ tel que $y = g \cdot x$ (resp. pour tout $x, y \in E$, il existe un unique $g \in G$ tel que $y = g \cdot x$).

Dans le cas d'une action transitive ou simplement transitive, il y a une seule orbite, à savoir E .

Définition 2.4. — On dit que l'action de G sur E est **fidèle** si le morphisme de groupes

$$\varphi : g \in G \mapsto \varphi(g) : x \mapsto g \cdot x \in \mathcal{S}(E)$$

est injectif. Autrement dit, pour $g \in G$,

$$(\forall x \in E, g \cdot x = x) \iff g = e.$$

Une action fidèle permet d'identifier G à un sous-groupe de $\mathcal{S}(E)$.

Théorème 2.5 (Cayley). — L'action de G sur lui-même par translation à gauche est fidèle et G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.

Démonstration. — Pour $g \in G$, on a $g \cdot x = gx = x$ pour tout $x \in G$ si, et seulement si, $g = e$, donc φ est injectif. \square

Définition 2.6. — Soit G opérant sur un ensemble non vide E . Pour tout $x \in E$, le sous-ensemble de G

$$G_x = \{g \in G, g \cdot x = x\},$$

est le **stabilisateur** de x sous l'action de G .

On vérifie facilement que ces stabilisateurs G_x sont des sous-groupes de G (en général non distingués).

Théorème 2.7. — Soit G un groupe opérant sur un ensemble non vide E . Pour tout $x \in E$, l'application

$$\begin{aligned} \varphi_x : G/G_x &\rightarrow G \cdot x \\ \bar{g} = gG_x &\mapsto g \cdot x \end{aligned}$$

est bien définie et bijective. Dans le cas où G est fini, on a

$$\text{card}(G \cdot x) = [G : G_x] = \frac{|G|}{|G_x|} \quad (1)$$

donc le cardinal de toute orbite $G \cdot x$ divise l'ordre de G .

Démonstration. — Soit $\bar{g} \in G/G_x$ et soient g_1, g_2 deux représentants de \bar{g} . Donc $\bar{g}_1 = \bar{g}_2 = \bar{g}$ et $g_2^{-1}g_1 \in G_x$. Par conséquent, $g_1 \cdot x = g_2 \cdot x$. Cela signifie que l'application φ_x est bien définie.

Pour tout $g, h \in G$, l'égalité $g \cdot x = h \cdot x$ équivaut à $(h^{-1}g) \cdot x = x$, soit $h^{-1}g \in G_x$ ou encore $\bar{g} = \bar{h}$ dans G/G_x . On déduit que l'application φ_x est bien injective. La surjectivité étant évidente, l'ensemble quotient G/G_x est donc en bijection avec l'orbite $G \cdot x$. Dans le cas où le groupe G est fini, on a

$$\text{card}(G \cdot x) = \text{card}(G/G_x) = [G : G_x] = \frac{|G|}{|G_x|}.$$

□

Exemple 2.8. — Soit E un ensemble non vide de cardinal n . L'action $\mathcal{S}(E)$ sur E est transitive (il y a une seule orbite), donc $\mathcal{S}(E) \cdot x = E$ pour tout $x \in E$. Le stabilisateur de $x \in E$ est $\mathcal{S}(E)_x = \{\sigma \in \mathcal{S}(E), \sigma(x) = x\}$ et l'application qui associe à $\sigma \in \mathcal{S}(E)_x$ sa restriction à $F = E \setminus \{x\}$ réalise un isomorphisme de $\mathcal{S}(E)_x$ sur $\mathcal{S}(F)$. On a donc $\text{card}(\mathcal{S}(E)_x) = \text{card}(\mathcal{S}(F))$ et

$$\begin{aligned} \text{card}(\mathcal{S}(E)) &= \text{card}(\mathcal{S}(E) \cdot x) \text{card}(\mathcal{S}(E)_x) \\ &= \text{card}(E) \text{card}(\mathcal{S}(F)) = n \text{card}(\mathcal{S}(F)) \end{aligned}$$

On conclut alors par récurrence que $\text{card}(\mathcal{S}(E)) = n!$.

3. Équation des classes, Formule de Burnside

Théorème 3.1. — Soit G un groupe fini opérant sur un ensemble fini E . En notant $G \cdot x_1, \dots, G \cdot x_r$ toutes les orbites deux à deux distinctes, on a

$$\text{card}(E) = \sum_{i=1}^r \text{card}(G \cdot x_i) = \sum_{i=1}^r \frac{|G|}{|G_{x_i}|} \quad (\text{Equation des classes}) \quad (2)$$

et le nombre d'orbites est donné par

$$r = \frac{1}{|G|} \sum_{g \in G} \text{card}(\text{Fix}(g)) \quad (\text{Formule de Burnside}) \quad (3)$$

où $\text{Fix}(g) = \{x \in E, g \cdot x = x\}$.

Démonstration. — Comme E est fini, on a un nombre fini d'orbites $G \cdot x_1, \dots, G \cdot x_r$ qui forment une partition de E . Donc

$$\text{card}(E) = \text{card}\left(\bigcup_{i=1}^r G \cdot x_i\right) = \sum_{i=1}^r \text{card}(G \cdot x_i)$$

En utilisant la bijection de G/G_{x_i} sur $G \cdot x_i$, on déduit que

$$\text{card}(E) = \sum_{i=1}^r \text{card}(G \cdot x_i) = \sum_{i=1}^r \frac{|G|}{|G_{x_i}|}$$

d'où l'équation des classes.

Pour montrer la formule de Burnside, il suffit de calculer de deux façons le cardinal de l'ensemble

$$F = \{(g, x) \in G \times E ; g \cdot x = x\}$$

On a, d'une part,

$$\begin{aligned} \text{card}(F) &= \sum_{g \in G} \sum_{x \in E} \text{card}\{(g, x) ; g \cdot x = x\} \\ &= \sum_{g \in G} \text{card}(\text{Fix}(g)). \end{aligned}$$

D'autre part,

$$\begin{aligned} \text{card}(F) &= \sum_{x \in E} \text{card}(G_x) = \sum_{x \in E} \frac{|G|}{\text{card}(G \cdot x)} \\ &= \sum_{i=1}^r \sum_{x \in G \cdot x_i} \frac{|G|}{\text{card}(G \cdot x)} \\ &= |G| \sum_{i=1}^r \sum_{x \in G \cdot x_i} \frac{1}{\text{card}(G \cdot x)} \\ &= |G| \sum_{i=1}^r 1 \quad (\text{car } G \cdot x = G \cdot x_i) \\ &= r |G|. \end{aligned}$$

D'où la formule de Burnside. □

Remarque 3.2. — Si G est un groupe opérant sur un ensemble E , on note alors

$$\text{Fix}(G) = \{x \in E, G \cdot x = \{x\}\},$$

l'ensemble des éléments de E dont l'orbite est réduite à un point.

En séparant dans la formule des classes les orbites réduites à un point des autres, celle-ci s'écrit :

$$\text{card}(E) = \text{card}(\text{Fix}(G)) + \sum_{\substack{i=1 \\ \text{card}(G \cdot x_i) \geq 2}}^r \frac{|G|}{|G_{x_i}|}, \quad (4)$$

la somme étant nulle si toutes les orbites sont réduites à un point.

Définition 3.3. — Soit $p \geq 2$ un nombre premier. On appelle p -groupe tout groupe d'ordre p^α , où α est un entier naturel non nul.

Corollaire 3.4. — Si $p \geq 2$ est un nombre premier et G un p -groupe opérant sur un ensemble fini E , alors

$$\text{card}(\text{Fix}(G)) \equiv \text{card}(E) \pmod{p}.$$

Démonstration. — Notons $|G| = p^\alpha$ avec $\alpha \geq 1$. Si $G \cdot x_i$ est une orbite non réduite à un point (s'il en existe), alors

$$2 \leq \text{card}(G \cdot x_i) = \frac{|G|}{|G_{x_i}|}.$$

On en déduit qu'il existe un entier β_i , $0 \leq \beta_i < \alpha$ tel que $|G_{x_i}| = p^{\beta_i}$ et $\text{card}(G \cdot x_i) = p^{\alpha - \beta_i}$ avec $1 \leq \alpha - \beta_i \leq \alpha$. Il en résulte que

$$\text{card}(E) = \text{card}(\text{Fix}(G)) + \sum_{\substack{i=1 \\ \text{card}(G \cdot x_i) \geq 2}}^r \text{card}(G \cdot x_i) \equiv \text{card}(\text{Fix}(G)) \pmod{p}$$

□

Corollaire 3.5. — Soit G un groupe fini que l'on fait agir sur lui-même par conjugaison ($g \cdot h = ghg^{-1}$ pour $(g, h) \in G \times G$). En notant $G \cdot h_1, \dots, G \cdot h_r$ toutes les orbites deux à deux distinctes, on a

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\substack{i=1 \\ \text{card}(G \cdot h_i) \geq 2}}^r \text{card}(G \cdot h_i) \\ &= |Z(G)| + \sum_{\substack{i=1 \\ \text{card}(G \cdot x_i) \geq 2}}^r \frac{|G|}{|G_{h_i}|}, \end{aligned}$$

où $Z(G)$ est le centre de G .

Démonstration. — Une orbite $G \cdot h$ est réduite à un point si et seulement si $G \cdot h = \{h\}$, ou encore $ghg^{-1} = h$ pour tout $g \in G$, ce qui signifie $h \in Z(G)$. Ainsi $\text{Fix}(G) = Z(G)$. Le corollaire se déduit alors de la formule (4). □

Exemple 3.6. — Soit G un groupe d'ordre 21 qui agit sur un ensemble E à 20 éléments. On suppose que G ne fixe aucun élément de E . Combien y a-t-il d'orbites pour cette action?

Si \mathcal{O} est une orbite de l'action de G sur E , alors $\text{card}(\mathcal{O})$ divise $|G| = 21$. Donc $\text{card}(\mathcal{O}) \in \{1, 3, 7, 21\}$. Comme G ne fixe aucun élément de E , $\text{card}(\mathcal{O}) \neq 1$. Les orbites étant une partition de E , donc $\text{card}(\mathcal{O}) \neq 21$ (car $21 > 20$). Soit n le nombre d'orbites de cardinal 3 et m le nombre d'orbites de cardinal 7. On a alors (équation des classes) $3n + 7m = 20$. Modulo 3 cette équation est réduite à $m \equiv 2[3]$ et modulo 7 elle est réduite à $n \equiv 2[7]$. Donc les seules valeurs possibles sont $n = 2$ et $m = 2$. Il y a donc deux orbites à 3 éléments et deux orbites à 7 éléments.

Théorème 3.7. — Soit G un p -groupe, d'ordre p^α . Alors $|Z(G)| \geq p$.

Démonstration. — Soit G un groupe d'ordre $|G| = p^\alpha$. On fait agir G sur lui-même par conjugaison. On a alors $\text{Fix}(G) = Z(G)$ et d'après le Corollaire 3.4, on a

$$|Z(G)| = \text{card}(\text{Fix}(G)) \equiv |G| \pmod{p}.$$

Comme $e \in Z(G)$, on a $|Z(G)| \geq 1$, et on conclut que $|Z(G)| \geq p$ et que $Z(G)$ est non trivial. \square

Théorème 3.8. — Tout groupe d'ordre p^2 avec p un nombre premier est abélien.

Démonstration. — Comme $Z(G)$ est un sous-groupe de G , on a d'après le théorème de Lagrange $|Z(G)| \in \{1, p, p^2\}$. D'après théorème 3.7 on a $|Z(G)| \neq 1$, donc $|Z(G)| = p$ ou $|Z(G)| = p^2$.

Supposons $|Z(G)| = p$. Soit $x \in G \setminus Z(G)$. On considère encore l'action de G sur lui-même par conjugaison. D'une part, $x \in G_x$, d'autre part $Z(G) \subset G_x$. Donc $|G_x| \geq p + 1$. Or d'après le théorème de Lagrange, $|G_x|$ divise p^2 , donc $G_x = G$ ce qui conduit à la contradiction $x \in Z(G)$. Ainsi $|Z(G)| = p^2$ et par suite $Z(G) = G$, autrement dit G est abélien. \square

4. Théorème de Cauchy

Le but de ce paragraphe est de démontrer le Théorème 4.4. Pour cela, on introduit des notations et on montre des résultats préliminaires.

Soit G un groupe fini d'ordre $n \geq 2$ et p un nombre premier. On pose

$$E = \{(g_1, g_2, \dots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = e\}.$$

L'application $(g_1, \dots, g_{p-1}) \mapsto (g_1, \dots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1})$ réalise une bijection de G^{p-1} sur E , donc

$$\text{card}(E) = n^{p-1}.$$

Considérons $H = \langle \sigma \rangle = \{Id, \sigma, \dots, \sigma^{p-1}\}$ le sous-groupe du groupe symétrique \mathcal{S}_p engendré par le p -cycle $\sigma = (1, 2, \dots, p)$.

Lemme 4.1. — H agit sur E par

$$\sigma^k \cdot (g_1, \dots, g_p) = (g_{\sigma^k(1)}, \dots, g_{\sigma^k(p)}) \quad (5)$$

Démonstration. — Pour $(g_1, \dots, g_p) \in E$, on a $g_2 \cdots g_p g_1 = g_1^{-1} g_1 = e$, donc

$$(g_{\sigma(1)}, \dots, g_{\sigma(p)}) = (g_2, \dots, g_p, g_1) \in E.$$

Il en résulte que pour tout entier k , $0 \leq k \leq p-1$, $(g_{\sigma^k(1)}, \dots, g_{\sigma^k(p)}) \in E$ et l'application (5) est bien définie. Cette application définit bien une action puisque

$$Id \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p)$$

et

$$\begin{aligned} \sigma^j \cdot (\sigma^k \cdot (g_1, \dots, g_p)) &= \sigma^j \cdot (g_{\sigma^k(1)}, \dots, g_{\sigma^k(p)}) \\ &= (g_{\sigma^{j+k}(1)}, \dots, g_{\sigma^{j+k}(p)}) \\ &= \sigma^{j+k} \cdot (g_1, \dots, g_p) = (\sigma^j \circ \sigma^k) \cdot (g_1, \dots, g_p). \end{aligned}$$

□

Lemme 4.2. — Soit $g_1, \dots, g_p \in G$. Alors, $(g_1, \dots, g_p) \in \text{Fix}(H)$ si et seulement si $g_1 = g_2 = \dots = g_p = g$ avec $g \in G$ tel que $g^p = e$.

Démonstration. — D'une part, si $(g_1, \dots, g_p) \in \text{Fix}(H)$, alors

$$(g_1, g_2, \dots, g_{p-1}, g_p) = \sigma \cdot (g_1, g_2, \dots, g_{p-1}, g_p) = (g_2, g_3, \dots, g_p, g_1),$$

de sorte que $g_1 = g_2, g_2 = g_3, \dots, g_{p-1} = g_p, g_p = g_1$ et on peut noter g cet élément. De plus, la relation $g_1 \cdots g_p = e$ donne alors $g^p = e$.

D'autre part, si $(g_1, \dots, g_p) = (g, \dots, g)$ avec $g^p = e$, alors $(g_1, \dots, g_p) \in E$ et (g_1, \dots, g_p) est bien fixé par $H = \{\sigma^k\}$. □

Lemme 4.3. — On a

$$\text{Fix}(H) = \{x \in E ; H \cdot x = \{x\}\} \neq \emptyset$$

et $\text{card}(\text{Fix}(H))$ est divisible par p si p est un diviseur premier de n .

Démonstration. — Il suffit de remarquer grâce au Lemme 4.2 que $x = (e, \dots, e)$ est dans $\text{Fix}(H)$ pour déduire que $\text{Fix}(H)$ est non vide. Comme H est un p -groupe (il est d'ordre p) on a d'après le corollaire 3.4,

$$\text{card}(\text{Fix}(H)) \equiv \text{card}(E) \pmod{p}$$

avec $\text{card}(E) = n^{p-1}$ divisible par p comme n , ce qui entraîne que $\text{card}(\text{Fix}(H))$ est également divisible par p . □

Théorème 4.4 (Cauchy). — Si G est un groupe fini d'ordre $n \geq 2$, alors pour tout diviseur premier p de n , il existe dans G un élément d'ordre p (et donc un sous-groupe d'ordre p).

Démonstration. — On utilise les notations ci-dessus. De $\text{card}(\text{Fix}(H)) \geq 1$ et $\text{card}(\text{Fix}(H))$ divisible par p , on déduit que $\text{card}(\text{Fix}(H)) \geq p \geq 2$. Du Lemme 4.2, on déduit qu'il existe $g \neq e$ tel que $g^p = e$, ce qui signifie que g est d'ordre p . □

5. Théorème de Noether

Soit G un groupe. On fait agir G sur l'ensemble de ses sous-groupes par conjugaison :

$$\forall g \in G, \forall H \leq G, \quad g \cdot H = gHg^{-1}.$$

Le stabilisateur d'un sous-groupe H pour cette action sera noté N_H ,

$$N_H = \{g \in G \mid gHg^{-1} = H\},$$

et sera appelé le **normalisateur** de H dans G . C'est un sous-groupe de G , il contient H et on a $H \triangleleft N_H$.

Théorème 5.1 (Théorème de Noether). — Soient G un groupe, H, K deux sous-groupes de G tels que $K \subset N_H$.

(a) On a $HK = KH$ et c'est le sous-groupe de G engendré par H et K .

(b) $H \cap K$ est un sous-groupe distingué de K et H est un sous-groupe distingué de HK .

(c) Les groupes HK/H et $K/(H \cap K)$ sont isomorphes.

Démonstration. — (a) Soit $h \in H$ et $k \in K$. On a $hk = k(k^{-1}hk) \in KH$ car $K \subset N_H$. De même $kh = (khk^{-1})k \in KH$. On a donc $HK = KH$.

De plus, HK est un sous-groupe de G . En effet, soit $h, h' \in H$ et $k, k' \in K$. Comme $kh' \in KH = HK$, il existe $h'' \in H$ et $k'' \in K$ tels que $kh' = h''k''$. D'où

$$(hk)(h'k') = h(kh')k' = h(h''k'')k = (hh'')(k''k') \in HK.$$

D'autre part,

$$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK.$$

Le sous-groupe HK contient à la fois H et K , donc $HK \supset \langle H \cup K \rangle$. Or ce sous-groupe contient tous les éléments hk de HK , par conséquent, $\langle H \cup K \rangle \supset HK$. Ainsi $HK = \langle H \cup K \rangle$.

(b) Pour $h \in H \cap K$ et $k \in K$, on a $khk^{-1} \in H$ car $K \subset N_H$ et $khk^{-1} \in K$ car K est un sous-groupe de G . Ainsi $khk^{-1} \in H \cap K$ et $H \cap K$ est distingué dans K .

Comme $H, K \subset N_H$, $HK \subset N_H$ et donc H est distingué dans HK .

(c) Considérons la surjection canonique $p : HK \rightarrow HK/H$ qui associe à tout $x \in HK$ la classe \bar{x} de x modulo H . Soit $f = p|_K$ la restriction de p à K . Alors f est un morphisme de groupes de K dans $HK/H = KH/H$. Ce morphisme est surjectif car tout élément de KH/H est de la forme $\overline{kh} = \bar{k}$. De plus, si $k \in K$ alors

$$k \in \text{Ker } f \iff \bar{k} = \bar{e} \iff k \in H \iff k \in H \cap K$$

Donc $\text{Ker } f = H \cap K$. Par le théorème de factorisation canonique (Théorème 8.9 du chapitre 1), on obtient un isomorphisme de $K/(H \cap K)$ sur HK/H . \square

6. Produit semi-direct

Ce paragraphe n'est plus au programme, vous pouvez toutefois le consulter pour votre culture personnelle.

Soient K et H deux groupes et supposons que K opère sur H ,

$$\begin{aligned} K \times H &\rightarrow H \\ (k, h) &\mapsto k \cdot h \end{aligned}$$

D'après la remarque 1.4, pour tout $k \in K$

$$\begin{aligned} \alpha_k : H &\rightarrow H \\ h &\mapsto k \cdot h \end{aligned}$$

est une bijection de H sur H , $\alpha_k \in \mathcal{S}(H)$. Soit

$$\begin{aligned} \alpha : K &\rightarrow \mathcal{S}(H) \\ k &\mapsto \alpha_k \end{aligned}$$

le morphisme de groupes associé à cette action.

Si pour tout $k \in K$, α_k est un automorphisme de H , $\alpha_k \in \text{Aut}(H)$, alors l'action de K sur H vérifie la condition supplémentaire

$$\forall k \in K, \forall h, h' \in H, \alpha_k(hh') = \alpha_k(h)\alpha_k(h') \quad (6)$$

On dira alors $\alpha : k \mapsto \alpha_k$ est une action par automorphismes du groupe K sur le groupe H .

Réciproquement, toute action de K sur H vérifiant la condition (6) est telle que, pour tout $k \in K$, $\alpha_k \in \text{Aut}(H)$ c'est-à-dire que

$$(6) \iff \text{Im}(\alpha) \leq \text{Aut}(H).$$

Exemple 6.1. — (1) Soit G un groupe considéré comme opérant sur lui-même par conjugaison

$$\begin{aligned} G \times G &\rightarrow G \\ (g, h) &\mapsto g \cdot h = ghg^{-1} \end{aligned}$$

Pour tout $g \in G$ et tout $h \in G$, on a $\alpha_g(h) = ghg^{-1}$, donc $\alpha_g \in \text{Aut}(G)$. La condition (6) est donc vérifiée.

(2) On remarquera que l'action d'un groupe G sur lui-même par translations à gauche

$$\begin{aligned} G \times G &\rightarrow G \\ (g, h) &\mapsto g \cdot h = gh \end{aligned}$$

ne vérifie pas la condition (6), puisqu'une translation de G n'est pas un automorphisme, en général.

(3) Soient $(A, +, \times)$ un anneau unitaire et A^\times le groupe multiplicatif des éléments inversibles de A . Considérons l'action du groupe A^\times sur le groupe abélien $(A, +)$,

$$\begin{aligned} A^\times \times (A, +) &\rightarrow (A, +) \\ (u, a) &\mapsto u \cdot a = ua \end{aligned}$$

Cette action vérifie la condition (6), puisque $\alpha_u \in \text{Aut}((A, +))$ pour tout $u \in A^\times$.

(4) Soit H un groupe et soit K un sous-groupe de $\text{Aut}(H)$. Alors K opère sur H par

$$\begin{aligned} K \times H &\rightarrow H \\ (k, h) &\mapsto k \cdot h = k(h) \end{aligned}$$

et $\alpha_k = k$ pour tout $k \in K$, autrement dit $\text{Im}(\alpha) \leq \text{Aut}(H)$. La condition (6) est donc vérifiée.

Proposition 6.2 (Produit semi-direct de groupes)

Soit $\alpha : k \mapsto \alpha_k$ une action par automorphismes d'un groupe K sur un autre groupe H . Alors $G := H \times K$ muni de la loi de composition interne définie par

$$(h, k)(h', k') = (h\alpha_k(h'), kk') \quad (7)$$

est un groupe non abélien, en général.

Les applications $f : h \mapsto (h, e_K)$ et $g : k \mapsto (e_H, k)$ sont des morphismes injectifs de H et K sur les sous-groupes $H' = H \times \{e_K\}$ et $K' = \{e_H\} \times K$ de G et on a

$$H' \triangleleft G, \quad H' \cap K' = \{e\}, \quad H'K' = G.$$

Démonstration. — On a $\alpha_{e_K} = \text{Id}_H$ car $\alpha \in \text{Hom}(K, \text{Aut}(H))$. Pour tout $k \in K$, on a $\alpha_k(e_H) = e_H$ car $\alpha_k \in \text{Aut}(H)$. On en déduit que pour tout $(h, k) \in H \times K$

$$(h, k)(e_H, e_K) = (h\alpha_k(e_H), ke_K) = (h, k),$$

et

$$(e_H, e_K)(h, k) = (e_H\alpha_{e_K}(h), e_Kk) = (h, k).$$

Ainsi $e := (e_H, e_K)$ est un élément neutre de G . La loi de composition est associative. En effet, comme $\alpha_{kk'} = \alpha_k \circ \alpha_{k'}$, les expressions suivantes sont égales

$$[(h, k)(h', k')](h'', k'') = (h\alpha_k(h'), kk')(h'', k'') = (h\alpha_k(h')\alpha_{kk'}(h''), kk'k'')$$

$$(h, k)[(h', k')(h'', k'')] = (h, k)(h'\alpha_{k'}(h''), k'k'') = (h\alpha_k[h'\alpha_{k'}(h'')], kk'k'').$$

On vérifie aussi que tout $(h, k) \in G$ a pour inverse $(\alpha_{k^{-1}}(h^{-1}), k^{-1})$. Donc $G = H \times K$ est un groupe.

Les applications injectives f et g sont des morphismes car

$$f(h)f(h') = (h, e_K)(h', e_K) = (h\alpha_{e_K}(h'), e_K) = (hh', e_K) = f(hh')$$

$$g(k)g(k') = (e_H, k)(e_H, k') = (e_H \alpha_k(e_H), kk') = (e_H, kk') = g(kk').$$

Soit $(h', e_K) \in H'$ et $(h, k) \in G$, on a

$$\begin{aligned} (h, k)(h', e_K)(h, k)^{-1} &= (h\alpha_k(h'), k)(\alpha_{k^{-1}}(h^{-1}), k^{-1}) \\ &= (h\alpha_k(h')h^{-1}, e_K) \in H' \end{aligned}$$

Donc $H' \triangleleft G$. On en déduit que $H'K'$ est un sous-groupe de $G = H \times K$. D'autre part, tout $(h, k) \in G$ s'écrit $(h, k) = (h, e_K)(e_H, k)$. Par conséquent $G = H'K'$. La dernière affirmation, $H' \cap K' = \{e\}$, est claire. \square

Définition 6.3. — Ce groupe G est appelé le **produit semi-direct** associé à l'action α de K sur H (ou produit semi-direct de H par K). On le note $H \rtimes_{\alpha} K$.

Proposition 6.4 (Produit semi-direct de sous-groupes)

Soient G un groupe et H et K deux sous-groupes de G tels que

$$H \triangleleft G, \quad H \cap K = \{e\}, \quad HK = G.$$

Alors $f : (h, k) \mapsto hk$ de $H \times K$ dans G est un isomorphisme du produit semi-direct $H \rtimes_{\alpha} K$ sur G , où α désigne l'action de K sur H par automorphisme intérieurs, $\alpha : k \mapsto \text{Ad}_{k|_H}$.

Démonstration. — Tout automorphisme intérieur $\text{Ad}_k : g \mapsto kgk^{-1}$ de G laisse stable H car $H \triangleleft G$. Il induit par restriction un automorphisme $\alpha_k = \text{Ad}_{k|_H}$ de H . Ainsi $\text{Im}(\alpha) \leq \text{Aut}(H)$ et la propriété (6) est vérifiée. On en déduit que $H \rtimes_{\alpha} K$ est un produit semi-direct.

L'application f est surjective puisque $HK = G$. Si $hk = h'k'$, alors $kk'^{-1} = h^{-1}h' \in H \cap K = \{e\}$ et par suite $h = h'$ et $k = k'$. Cela prouve que f est injective et donc bijective. Pour tous $(h, k), (h', k') \in H \rtimes_{\alpha} K$, on a

$$\begin{aligned} f(h, k)f(h', k') &= hkh'k' = hkh'k^{-1}kk' = h\alpha_k(h')kk' \\ &= f(h\alpha_k(h'), kk') = f((h, k)(h', k')). \end{aligned}$$

On en déduit que f est un isomorphisme du groupe $H \rtimes_{\alpha} K$ sur G . \square

Définition 6.5. — Soient G un groupe et H et K deux sous-groupes. On dira que G est **produit semi-direct** de H par K si

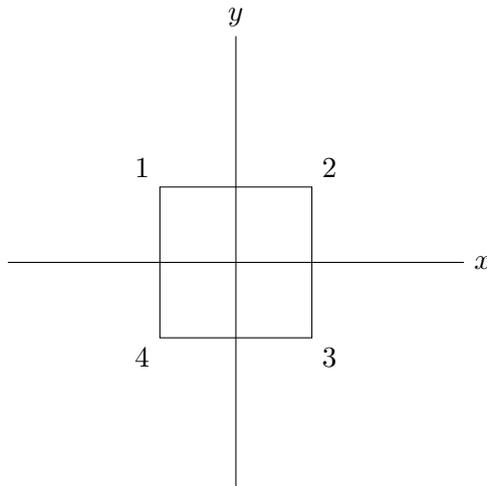
- (a) $H \triangleleft G$
- (b) $H \cap K = \{e\}$
- (c) $HK = G$.

Définition 6.6. — Etant donné un groupe G et $H \triangleleft G$, s'il existe un sous-groupe K de G tel que G est produit semi-direct de H par K , alors K est appelé **complément** de H dans G . Dans ce cas, l'application du théorème de l'isomorphisme donne $G/H \simeq K$.

Remarque 6.7. — L'intérêt de la notion de produit semi-direct de groupes est de fournir une méthode de construction de nouveaux groupes, à partir de groupes connus.

Par analogie avec le cas d'un groupe K opérant sur un groupe H , de telle sorte que le morphisme $\alpha : K \rightarrow \mathcal{S}(H)$ associé à cette action vérifie la condition $\text{Im}(\alpha) \leq \text{Aut}(H)$, on peut envisager l'action d'un groupe G opérant sur un ensemble E muni d'une structure algébrique autre que celle de groupe. En particulier si E est un espace vectoriel, si G opère sur E de telle sorte que le morphisme $\rho : G \rightarrow \mathcal{S}(E)$ associé à cette action vérifie la condition $\text{Im}(\rho) \leq \text{Aut}(E) = \text{GL}(E)$, alors le couple (ρ, E) définit ce qu'on appelle **une représentation linéaire de G** .

Exemple 6.8 (Groupe diédral). — On considère le carré ci-dessous avec de sommets numérotés 1, 2, 3 et 4, centré à l'origine des axes (x) et (y)



Doit D_4 l'ensemble des transformations du carré,

$$D_4 = \{Id, R, R^2, R^3, T_x, T_y, T_{1,3}, T_{2,4}\}$$

où

→ R est la rotation (dans le sens trigonométrique) d'angle $\frac{\pi}{2}$ (donc R^2 est la rotation d'angle π et R^3 est la rotation d'angle $\frac{3\pi}{2}$ et $R^4 = I$ est la rotation d'angle 2π);

→ T_x la réflexion par rapport à l'axe (x) ;

→ T_y la réflexion par rapport à l'axe (y) ;

→ $T_{1,3}$ la réflexion par rapport à la diagonale $(1, 3)$;

→ $T_{2,4}$ la réflexion par rapport à la diagonale $(2, 4)$.

D_4 est un groupe d'ordre 8 appelé groupe des symétries du carrée et sa table de multiplication est

	I	R	R^2	R^3	T_x	$T_{2,4}$	T_y	$T_{1,3}$
I	I	R	R^2	R^3	T_x	$T_{2,4}$	T_y	$T_{1,3}$
R	R	R^2	R^3	I	$T_{2,4}$	T_y	$T_{1,3}$	T_x
R^2	R^2	R^3	I	R	T_y	$T_{1,3}$	T_x	$T_{2,4}$
R^3	R^3	I	R	R^2	$T_{1,3}$	T_x	$T_{2,4}$	T_y
T_x	T_x	$T_{2,4}$	T_y	$T_{1,3}$	I	R^3	R^2	R
$T_{2,4}$	$T_{2,4}$	T_x	$T_{1,3}$	T_y	R	I	R^3	R^2
T_y	T_y	$T_{1,3}$	T_x	$T_{2,4}$	R^2	R	I	R^3
$T_{1,3}$	$T_{1,3}$	T_y	$T_{2,4}$	T_x	R^3	R^2	R	I

On peut remarquer que D_4 est non abélien. De plus si on note $H = \langle R \rangle$ et $K = \langle T_{1,3} \rangle$ alors H est distingué dans D_4 , $H \cap K = \{I\}$ et que

$$HK = \{Id, R, R^2, R^3, T_{1,3}, RT_{1,3}, R^2T_{1,3}, R^3T_{1,3}\} = D_4$$

(Ainsi D_4 est produit semi-direct de H et K)

Soit D_n ($n \geq 3$) le **groupe diédral** d'ordre $2n$, engendré par deux éléments a et b tels que a d'ordre n , b d'ordre 2 et $ba = a^{-1}b$. On pose $H = \langle a \rangle$ et $K = \langle b \rangle$. On a

- $H \triangleleft D_n$, puisque $[D_n, H] = 2$ (tout sous-groupe d'indice 2 est distingué),
- $H \cap K = \{e\}$,
- $HK = \{e, a, a^2, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\} = D_n$.

(donc D_n est produit semi-direct de H par K . L'action associée est $\alpha : K \rightarrow \text{Aut}(H)$, $b \mapsto \alpha_b(a) = bab^{-1} = a$ est l'action triviale).