

# Leçon 101 - Groupe opérant sur un ensemble. Exemples et Applications.

## Extrait du rapport de jury

Le matériel théorique en accord avec le programme doit être présenté, accompagné d'illustrations pertinentes. Il faut pouvoir dégager l'intérêt des notions introduites avec des exemples d'actions bien choisies pour obtenir des informations soit sur un ensemble  $X$  donné, soit sur un groupe  $G$  donné et faire apparaître des sous-groupes intéressants de  $G$  comme stabilisateurs. Par ailleurs, la présentation doit illustrer comment l'étude des orbites de certaines actions revient à classifier certains objets, soit en trouvant un représentant simple de chaque orbite, soit en dégagant des invariants caractérisant les orbites. Les actions de groupes interviennent aussi efficacement dans des problèmes de dénombrements, notamment via la formule de Burnside. Les exemples peuvent être internes à la théorie des groupes (action naturelle de  $\mathfrak{S}_n$  sur  $[1; n]$ , action par translation ou par conjugaison, etc). Mais il est souhaitable d'emprunter aussi à d'autres domaines (action sur des anneaux, des espaces de matrices ou des espaces de polynômes, représentations de groupes, groupes d'isométries, etc). La géométrie fournit aussi de nombreux exemples pertinents (groupes d'isométries d'un polygone dans le plan ou d'un solide ou d'un polygone régulier dans l'espace).

Pour aller plus loin, on peut aborder l'action de  $\mathrm{PGL}_2(\mathbb{K})$  sur la droite projective menant au birapport ou celle de  $\mathrm{SL}_2(\mathbb{Z})$  sur le demi-plan de Poincaré ou les preuves par actions de groupes des théorèmes de Sylow ou encore d'autres actions donnant lieu à des isomorphismes exceptionnels. Il est aussi possible de s'intéresser aux aspects topologiques ou différentiels liés à certaines actions.

## Présentation de la leçon

Je vais vous présenter la leçon 101 intitulée : "Groupe opérant sur un ensemble. Exemples et applications". La théorie des actions de groupes permet d'étudier les interactions entre ensembles et ainsi d'obtenir des propriétés sur le groupe agissant ou l'ensemble sur lequel il agit. Historiquement, les premières opérations apparaissent naturellement en géométrie dès l'antiquité (rotations, symétries, etc.) puis plus tard avec action du groupe de permutations sur les racines d'un polynôme par Lagrange, avant de prendre conscience de la structure de groupe derrière cette opération par Galois.

Dans une première partie on s'intéresse à la théorie générale des actions de groupe sur un ensemble en commençant par en donner la définition de deux manières différentes : en tant qu'application ou de morphisme ce qui offre plus de richesse. On introduit ensuite la notion d'action fidèle qui donne le théorème de Cayley puis d'action transitive ainsi que quelques exemples classiques. On donne dans une deuxième sous-partie la notion de stabilisateur et d'orbite qui partitionne l'espace et on finit par l'équation au classe ainsi que la relation orbite-stabilisateur qui permet faire du dénombrement. On termine cette première partie avec les formules combinatoires telles que la formule de Burnside ainsi que le cas des  $p$ -groupes dont on verra plus loin la puissance des résultats que l'on peut obtenir dessus!

Dans une deuxième partie on s'intéresse aux actions sur les groupes finis dans le but de mieux comprendre la structure interne du groupe. On commence par parler de différents types d'actions (les plus usuelles) avec l'action par translation qui donne le théorème de Lagrange (simple mais assez puissant), puis l'action par conjugaison qui permet de dire des choses sur les  $p$ -groupes et enfin l'action par translation des classes qui donnent quelques isomorphismes. Dans une deuxième sous-partie, on s'intéresse aux théorèmes de Sylow avec l'étude des  $p$ -groupes. Le théorème de Sylow est fondamental car il permet de donner des informations sur un groupe à partir de son cardinal uniquement. La puissance de ce théorème s'explique par le fait qu'il permet par exemple de montrer qu'un groupe est simple ou cyclique mais également qu'il apporte une réciproque partielle au théorème de Lagrange pour les sous-groupes d'ordre premier!

Dans une troisième partie on s'intéresse aux actions de groupe en algèbre linéaire afin d'en déduire des propriétés sur l'espace. On commence par le cas de l'action par translation (à gauche et à droite) qui donnent des résultats sur les orbites et justifient la méthode du pivot de Gauss. On passe ensuite à l'action de Steinitz en en donnant la définition et en décrivant les orbites. On continue en "renforçant" cette action avec l'action par conjugaison qui donne énormément de résultats, notamment dans le cadre de la réduction avec les propriétés de diagonalisabilité et de trigonalisabilité qui sont des propriétés de classes et où ces problèmes se ramènent à chercher un représentant diagonalisable/trigonalisable ou non. On termine enfin avec le dénombrement des endomorphismes nilpotents sur un corps fini qui fait intervenir la décomposition de Fitting et un type d'action différent des trois précédentes.

On conclut enfin cette leçon avec une dernière partie où l'on donne d'autres ap-

plications à d'autres domaines : tout d'abord en algèbre commutative avec le théorème de Wedderburn puis en géométrie. En effet, les actions permettent de décrire (à l'isomorphisme près) les isométries de l'espace laissant invariantes un solide de Platon.

## Plan général

### I - Action de groupe sur un ensemble

- 1 - Action de groupe : double approche et vocabulaire
- 2 - Orbites et stabilisateurs
- 3 - Les formules combinatoires

### II - Actions sur les groupes finis

- 1 - Différents types d'actions
- 2 - Le cas particulier des  $p$ -groupes

### III - Application des actions de groupes en algèbre linéaire

- 1 - Action par translation : pivot de Gauss
- 2 - Action de Steinitz
- 3 - Action par conjugaison
- 4 - Dénombrement des endomorphismes nilpotents sur un corps fini

### IV - Application à d'autres domaines

- 1 - En algèbre commutative
- 2 - En géométrie

## Cours détaillé

Dans toute cette leçon, on considère un groupe  $(G, *)$  de neutre noté  $e_G$ ,  $n, m \in \mathbb{N}^*$  et  $X$  un ensemble quelconque non vide.

## I Action de groupe sur un ensemble

### I.1 Action de groupe : double approche et vocabulaire

#### Définition 1 : Action de groupe [Berhuy, p.169] :

On appelle **action de  $G$  sur  $X$**  toute application  $\cdot : G \times X \rightarrow X$  vérifiant les propriétés suivantes :

\* Pour tout  $x \in X$ ,  $e_G \cdot x = x$ . \* Pour tous  $g, g' \in G$ ,  $g \cdot (g' \cdot x) = (gg') \cdot x$ .

On suppose désormais que  $G$  agit sur  $X$  via une action de groupe notée " $\cdot$ ".

#### Remarque 2 : [Berhuy, p.170]

La donnée d'une action de  $G$  sur  $X$  est équivalente à la donnée d'un morphisme de groupes de  $G$  dans  $\mathfrak{S}_X$ . En effet,  $G$  agit sur  $X$  via  $\cdot$  si, et seulement si, l'application

$$\Psi : \begin{array}{c} G \longrightarrow \mathfrak{S}_X \\ g \longmapsto \sigma_g \end{array} \quad \begin{array}{c} X \longrightarrow X \\ x \longmapsto g \cdot x \end{array}$$

est un morphisme de groupes.

#### Définition 3 : Action fidèle [Berhuy, p.170] :

On dit que  $G$  agit **fidèlement** sur  $X$  lorsque :

$$\forall g \in G, (\forall x \in X, g \cdot x = x \implies g = e_G)$$

#### Remarque 4 : [Berhuy, p.170]

Lorsque  $G$  agit fidèlement sur  $X$ , le morphisme  $\Psi$  associé à l'action " $\cdot$ " est alors injectif.

#### Théorème 5 : Théorème de Cayley [Berhuy, p.177] :

Si  $G$  est d'ordre  $n$ , alors  $G$  est isomorphe à un sous-groupe de  $\mathfrak{S}_n$ .

#### Définition 6 : Action transitive [Berhuy, p.170] :

On dit que  $G$  agit **transitivement** sur  $X$  lorsque pour tous  $x, x' \in X$ , il existe  $g \in G$  tel que  $x' = g \cdot x$ .

**Exemple 7 : [Berhuy, p.171]**

- \*  $G$  agit sur lui-même par translation à gauche et cette action est fidèle et transitive.
- \*  $G$  agit sur un sous-groupe  $H$  distingué dans  $G$  par conjugaison (en particulier,  $G$  agit sur lui-même par conjugaison). Cette action n'est cependant pas fidèle en général (par exemple pour  $G$  abélien).
- \* L'action de  $\mathfrak{S}(E)$  sur  $E$  définie par  $(\sigma, x) \mapsto \sigma \cdot x = \sigma(x)$  est une action fidèle et transitive.
- \* On considère  $H$  un sous-groupe quelconque de  $G$  et  $E = G/H$  l'ensemble des classes à gauche modulo  $H$ . L'action de  $G$  sur  $E$  définie par  $(g, \bar{g}') \mapsto g \cdot \bar{g}' = \overline{gg'}$  est bien définie et est transitive.

## I.2 Orbites et stabilisateurs

**Définition 8 : Stabilisateur [Berhuy, p.172] :**

L'ensemble  $\text{Stab}_G(x) = \{g \in G \text{ tq } g \cdot x = x\}$  est appelé **stabilisateur de  $x$  sous l'action de  $G$**  (c'est un sous-groupe de  $G$ ).

**Lemme 9 : [Berhuy, p.172]**

La relation sur  $X$  définie par :

$$x \sim y \text{ lorsqu'il existe } g \in G \text{ tel que } y = g \cdot x$$

est une relation d'équivalence.

**Définition 10 : Orbite [Berhuy, p.173] :**

On considère  $x \in X$ .

L'ensemble  $\text{Orb}(x) = \{g \cdot x, g \in G\}$  est appelé **orbite de  $x$  sous l'action de  $G$**  (c'est la classe d'équivalence de  $x$  pour la relation d'équivalence donnée par le lemme précédent).

**Lemme 11 : Équation aux classes [Berhuy, p.173] :**

Si  $X$  est un ensemble fini et que  $\Omega$  est un système de représentants de  $X$ , on a alors  $\text{Card}(X) = \sum_{\omega \in \Omega} \text{Card}(\text{Orb}(\omega))$ .

**Proposition 12 : [Berhuy, p.174]**

Pour tout  $x \in X$ , l'application suivante est une bijection :

$$f_x : \begin{array}{l} G/\text{Stab}_G(x) \longrightarrow \text{Orb}(x) \\ \bar{g} \longmapsto g \cdot x \end{array}$$

En particulier, si  $G$  est fini, alors pour tout  $x \in X$ , l'ensemble  $\text{Orb}(x)$  est fini, son cardinal divise l'ordre de  $G$  et  $\text{Card}(\text{Orb}(x)) = \frac{\text{Card}(G)}{\text{Card}(\text{Stab}_G(x))}$ .

## I.3 Les formules combinatoires

**Proposition 13 : Formule de Burnside [Berhuy, p.176] :**

Si  $G$  et  $X$  sont finis, que l'on note  $\text{Fix}(g) = \{x \in X \text{ tq } g \cdot x = x\}$  et  $\Omega$  l'ensemble des orbites de  $X$  sous l'action de  $G$ , alors on a l'égalité :

$$\text{Card}(\Omega) = \frac{1}{\text{Card}(G)} \sum_{g \in G} \text{Card}(\text{Fix}(g))$$

**Corollaire 14 : [Caldero (1), p.305]**

Si  $G$  est un groupe non abélien d'ordre  $n$  possédant  $k$  classes de conjugaison, alors la probabilité  $p$  que deux éléments commutent est égale à  $\frac{k}{n}$ .

**Définition 15 :  $p$ -groupe [Berhuy, p.180] :**

On considère  $p$  un nombre premier.

On appelle  **$p$ -groupe** tout groupe fini d'ordre une puissance de  $p$ .

On note désormais  $X^G$  l'ensemble des éléments de  $X$  fixes sous l'action de  $G$ .

**Proposition 16 : [Berhuy, p.181]**

Si  $G$  est un  $p$ -groupe et que  $E$  est fini, alors  $\text{Card}(X) \equiv \text{Card}(X^G) \pmod{p}$ .

De plus, si  $p$  ne divise pas  $\text{Card}(X)$ , alors  $X^G \neq \emptyset$ .

## II Actions sur les groupes finis

### II.1 Différents types d'actions

#### II.1.1 Action par translation

**Définition 17 : Action par translation (à gauche) [Berhuy, p.170] :**

L'action  $\cdot : \begin{array}{l} G \times G \longrightarrow G \\ (g, x) \longmapsto g \cdot x = gx \end{array}$  est appelée **translation (à gauche)**.

**Théorème 18 : Théorème de Lagrange [Berhuy, p.148] :**

Soit  $H$  un sous-groupe de  $G$ .

On a  $\text{Card}(G) = \text{Card}(G/H) \text{Card}(H)$ .

En particulier, l'ordre de tout sous-groupe de  $G$  divise le cardinal de  $G$  et il en est de même pour l'ordre de tout élément de  $G$ .

#### II.1.2 Action par conjugaison

**Définition 19 : Action par conjugaison [Berhuy, p.171] :**

On considère  $H$  un sous-groupe distingué de  $G$ .

L'action  $\cdot : \begin{array}{l} G \times H \longrightarrow H \\ (g, x) \longmapsto g \cdot x = gxg^{-1} \end{array}$  est appelée **action par conjugaison**.

**Proposition 20 : [Berhuy, p.181]**

Si  $G$  est un  $p$ -groupe non trivial, alors  $Z(G)$  est non trivial.

**Proposition 21 : [Berhuy, p.194]**

Soit  $p$  un nombre premier.

Si  $G$  est d'ordre  $p^2$ , alors  $G \cong \mathbb{Z}/p^2\mathbb{Z}$  ou  $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

**II.1.3 Action par translation des classes**

**Définition 22 : Action par translation des classes [Berhuy, p.171] :**

On considère  $H$  un sous-groupe quelconque de  $G$ .

L'action  $\cdot : \left| \begin{array}{ccc} G \times G/H & \longrightarrow & G/H \\ (g, g') & \longmapsto & g \cdot g' = \overline{gg'} \end{array} \right.$  est appelée **translation des classes**.

**Lemme 23 : [Perrin, p.30]**

Soit  $H$  un sous-groupe d'indice  $n$  de  $\mathfrak{S}_n$ .

$H$  est isomorphe à  $\mathfrak{S}_{n-1}$ .

**Proposition 24 : [Perrin, p.106]**

On a  $\text{GL}_2(\mathbb{F}_2) = \text{SL}_2(\mathbb{F}_2) = \text{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$ .

**Théorème 25 : [Perrin, p.106]**

On a les isomorphismes suivants :

\*  $\text{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$  et  $\text{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$ .    \*  $\text{PGL}_2(\mathbb{F}_4) = \text{PSL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$ .

\*  $\text{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$  et  $\text{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$ .

**II.2 Le cas particulier des  $p$ -groupes**

Dans toute cette sous-partie, on suppose que  $G$  est de cardinal fini noté  $n$  et  $p$  un nombre premier.

**Définition 26 :  $p$ -sous-groupe de  $G$  [Berhuy, p.311] :**

On appelle  **$p$ -sous-groupe de  $G$**  tout sous-groupe de  $G$  de cardinal une puissance de  $p$ .

Désormais, on écrit  $\text{Card}(G) = n = p^m q$  où  $p \nmid q$  et  $m \in \mathbb{N}^*$ .

**Définition 27 :  $p$ -sous-groupe de Sylow de  $G$  [Berhuy, p.311] :**

On appelle  **$p$ -sous-groupe de Sylow de  $G$**  (ou plus simplement  $p$ -Sylow) tout sous-groupe de  $G$  d'ordre  $p^m$ .

**Exemple 28 :**

\*  $\mathbb{Z}/6\mathbb{Z}$  contient un 2-Sylow et un 3-Sylow (respectivement  $\mathbb{Z}/2\mathbb{Z}$  et  $\mathbb{Z}/3\mathbb{Z}$ ).

\*  $\mathbb{Z}/56\mathbb{Z}$  contient un 2-Sylow et un 7-Sylow (respectivement  $\mathbb{Z}/8\mathbb{Z}$  et  $\mathbb{Z}/7\mathbb{Z}$ ).

**Théorème 29 : Théorème de Sylow [Berhuy, p.313] :**

\* Il existe des  $p$ -sous-groupes de Sylow de  $G$  et tout  $p$ -sous-groupe de  $G$  est contenu dans un  $p$ -Sylow.

\* Le conjugué d'un  $p$ -Sylow est un  $p$ -Sylow et tous les  $p$ -Sylow de  $G$  sont conjugués entre eux.

En particulier, si  $S$  est un  $p$ -Sylow de  $G$ , alors  $S$  est distingué dans  $G$  si, et seulement si,  $S$  est l'unique  $p$ -Sylow de  $G$ .

\* Si  $n_p$  désigne le nombre de  $p$ -Sylow de  $G$ , alors  $n_p \equiv 1 [p]$  et  $n_p | q$ .

**Exemple 30 : [Berhuy, p.315 + 328]**

Tout groupe d'ordre 63 ou 255 n'est pas simple.

**Corollaire 31 :**

Tout groupe d'ordre  $pq$  avec  $p < q$  qui sont deux nombres premiers n'est pas simple.

**Corollaire 32 : [Berhuy, p.315]**

Tout groupe d'ordre 33 cyclique.

**Théorème 33 : Théorème de Cauchy [Berhuy, p.179] :**

$G$  possède au moins un élément d'ordre  $p$ .

**Proposition 34 : [Berhuy, p. 310]**

Soit  $p$  un nombre premier supérieur ou égal à 3.

Si  $G$  est d'ordre  $2p$ , alors  $G$  est isomorphe à  $\mathbb{Z}/2p\mathbb{Z}$  ou à  $D_{2p}$ .

**III Application des actions de groupes en algèbre linéaire**

Dans toute cette partie, on considère un corps  $\mathbb{K}$  commutatif quelconque.

**III.1 Action par translation : pivot de Gauss**

**Définition 35 : Action de translation à gauche [Rombaldi, p.184] :**

L'application  $\Psi : \left| \begin{array}{ccc} \text{GL}_n(\mathbb{K}) \times \mathcal{M}_{n,m}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,m}(\mathbb{K}) \\ (P, A) & \longmapsto & PA \end{array} \right.$  définit une action de  $\text{GL}_n(\mathbb{K})$  sur  $\mathcal{M}_{n,m}(\mathbb{K})$  appelée **action par translation à gauche**.

**Proposition 36 : [Rombaldi, p.184]**

Deux matrices sont dans la même orbite pour l'action de translation à gauche si, et seulement si, elles ont le même noyau.

**Définition 37 : Action de translation à droite [Rombaldi, p.184] :**

L'application  $\Psi : \begin{cases} \text{GL}_n(\mathbb{K}) \times \mathcal{M}_{n,m}(\mathbb{K}) & \longrightarrow \mathcal{M}_{n,m}(\mathbb{K}) \\ (P, A) & \longmapsto AP^{-1} \end{cases}$  définit une action de  $\text{GL}_n(\mathbb{K})$  sur  $\mathcal{M}_{n,m}(\mathbb{K})$  appelée **action par translation à droite**.

**Proposition 38 : [Rombaldi, p.184]**

Deux matrices sont dans la même orbite pour l'action de translation à droite si, et seulement si, elles ont la même image.

**Remarque 39 : [Rombaldi, p.185]**

Le noyau et l'image sont respectivement des invariants totaux pour l'action de translation à gauche/ à droite.

**Théorème 40 : [Rombaldi, p.191]**

Soit  $A \in \mathcal{M}_{n,m}(\mathbb{K})$ .  
Il existe une matrice  $P \in \text{GL}_n(\mathbb{K})$  produit de matrices de permutation et de transvection telle que la matrice  $PA$  soit échelonnée en ligne.  
Cette matrice  $PA$  est donc dans l'orbite de  $A$  pour l'action de translation à gauche

**Théorème 41 : [Rombaldi, p.192]**

Une opération élémentaire sur les lignes d'un système linéaire  $AX = b$  le transforme en un système équivalent.

**Remarque 42 :**

C'est ces deux derniers théorèmes qui justifient que la méthode du pivot de Gauss fonctionne bien pour toute matrice  $A \in \mathcal{M}_{n,m}(\mathbb{K})$ .

### III.2 Action de Steinitz

**Définition 43 : Action par équivalence (de Steinitz) [Rombaldi, p.195] :**

L'application  $\Psi : \begin{cases} (\text{GL}_n(\mathbb{K}) \times \text{GL}_m(\mathbb{K})) \times \mathcal{M}_{n,m}(\mathbb{K}) & \longrightarrow \mathcal{M}_{n,m}(\mathbb{K}) \\ ((P, Q), A) & \longmapsto PAQ^{-1} \end{cases}$  définit une action de  $\text{GL}_n(\mathbb{K}) \times \text{GL}_m(\mathbb{K})$  sur  $\mathcal{M}_{n,m}(\mathbb{K})$  appelée **action par équivalence**.

**Proposition 44 : [Rombaldi, p.195]**

Les orbites pour l'action par équivalence sont les matrices de rang  $r$  pour tout  $r \in \llbracket 0; \min(n, m) \rrbracket$ .

**Théorème 45 : [Rombaldi, p.198]**

Deux matrices de  $\mathcal{M}_{n,m}(\mathbb{K})$  qui se déduisent l'une de l'autre par une suite finie d'opérations élémentaires sont de même rang (donc dans la même orbite).

**Théorème 46 : [Rombaldi, p.198]**

Soit  $A \in \mathcal{M}_{n,m}(\mathbb{K})$  de rang  $r \geq 1$ .  
Il existe deux matrices inversibles  $P \in \text{GL}_n(\mathbb{K})$  et  $Q \in \text{GL}_m(\mathbb{K})$ , produits de matrices élémentaires, telles que  $PAQ^{-1} = J_r$ .

### III.3 Action par conjugaison

**Définition 47 : Action par conjugaison [Rombaldi, p.199] :**

L'application  $\Psi : \begin{cases} \text{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) & \longrightarrow \mathcal{M}_n(\mathbb{K}) \\ (P, A) & \longmapsto PAP^{-1} \end{cases}$  définit une action de  $\text{GL}_n(\mathbb{K})$  sur  $\mathcal{M}_n(\mathbb{K})$  appelée **action par conjugaison**.

**Définition 48 : Matrices semblables [Rombaldi, p.199] :**

Deux matrices dans la même orbite pour l'action de conjugaison sont appelées **matrices semblables**.

**Remarque 49 : [Rombaldi, p.199]**

Deux matrices semblables sont équivalentes mais la réciproque est fausse !

**Proposition 50 : [Rombaldi, p.199]**

Deux matrices semblables ont le même rang/déterminant/polynôme caractéristique/polynôme minimal/trace.

**Remarque 51 : [Rombaldi, p.199]**

Les éléments cités dans la proposition précédente sont des invariants mais pas totaux : il faut plus pour que la réciproque soit vraie !

**Proposition 52 : [Rombaldi, p.199]**

Les propriétés de diagonalisabilité et de trigonalisabilité sont des propriétés de classe pour la relation de conjugaison.

### III.4 Dénombrément des endomorphismes nilpotents sur un corps fini

Dans toute cette sous-partie, on considère  $\mathbb{K}$  un corps commutatif quelconque,  $E$  un  $\mathbb{K}$ -espace vectoriel de dimension finie  $n > 0$  et  $u \in \mathcal{L}(E)$ .

**Lemme 53 : [Caldero (2), p.74]**

Les suites  $(\text{Ker}(u^k))_{k \in \mathbb{N}}$  et  $(\text{Im}(u^k))_{k \in \mathbb{N}}$  sont respectivement croissante et décroissante au sens de l'inclusion.

De plus, ces deux suites sont stationnaires à partir d'un certain rang  $n_0 \in \mathbb{N}$ .

**Lemme 54 : Lemme de Fitting [Caldero (2), p.74] :**

Avec les notations du lemme précédent, on a  $E = \text{Ker}(u^{n_0}) \oplus \text{Im}(u^{n_0})$ .  
De plus,  $u$  induit un endomorphisme nilpotent sur  $\text{Ker}(u^{n_0})$  et un automorphisme sur  $\text{Im}(u^{n_0})$ .

**Définition 55 : Décomposition de Fitting [Caldero (2), p.74] :**

La donnée de  $((F, G), v, w)$  où  $F = \text{Ker}(u^{n_0})$ ,  $G = \text{Im}(u^{n_0})$ ,  $v = u|_F$  et  $w = u|_G$  avec  $E = F \oplus G$ ,  $v$  nilpotent et  $w$  un automorphisme est appelée **décomposition de Fitting**.

**Développement 1 : [cf. CALDERO (2)]**

**Théorème 56 : [Caldero (2), p.74]**

Si  $\mathbb{K}$  est un corps fini commutatif de cardinal  $q$ , alors il y a  $n_d = q^{d(d-1)}$  matrices nilpotentes de taille  $d \times d$  à coefficients dans  $\mathbb{K}$ .

## IV Applications à d'autres domaines

### IV.1 En algèbre commutative

**Théorème 57 : Théorème de Wedderburn [Perrin, p.82] :**

Tout corps fini est commutatif.

### IV.2 En géométrie

Dans toute cette sous-partie, on fixe un espace affine euclidien  $\mathcal{E}$  de dimension 3.

**Proposition 58 :**

Soit  $\mathcal{P}$  un polyèdre convexe de  $\mathcal{E}$ .  
Si l'on note  $\mathcal{P}_s$  l'ensemble des sommets de  $\mathcal{P}$ , alors on a :  $\text{Isom}(\mathcal{P}) = \text{Isom}(\mathcal{P}_s)$  et  $\text{Isom}^+(\mathcal{P}) = \text{Isom}^+(\mathcal{P}_s)$ .

**Remarque 59 :**

\* Plus généralement, une isométrie d'un polyèdre convexe non aplati de l'espace préserve les sommets, les arêtes et les faces du polyèdre.  
\* Si  $\mathcal{P}$  est un polyèdre convexe non aplati de l'espace, on en déduit qu'il existe un morphisme de groupes injectif  $\lambda : \text{Isom}(\mathcal{P}) \rightarrow \text{Bij}(X)$ , avec  $X$  l'ensemble des sommets de  $\mathcal{P}$ .

**Théorème 60 : [Combes, p.147]**

L'ensemble des polyèdres réguliers de  $\mathcal{E}$  sont à similitude près le tétraèdre régulier, le cube, l'octaèdre régulier, le dodécaèdre régulier et l'icosaèdre régulier.

**Développement 2 : [cf. COMBES]**

**Théorème 61 : [Combes, p.175]**

On a  $\text{Isom}^+(\mathcal{C}) \cong \mathfrak{S}_4$  et  $\text{Isom}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ .

**Théorème 62 : [Caldero (3), p.222 + 227]**

\* On a  $\text{Isom}^+(\mathcal{T}) \cong \mathfrak{A}_4$  et  $\text{Isom}(\mathcal{T}) \cong \mathfrak{S}_4$ .  
\* On a  $\text{Isom}^+(\mathcal{O}) \cong \mathfrak{S}_4$  et  $\text{Isom}(\mathcal{O}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ .  
\* On a  $\text{Isom}^+(\mathcal{D}) \cong \text{Isom}^+(\mathcal{I}) \cong \mathfrak{A}_5$  et  $\text{Isom}(\mathcal{D}) \cong \text{Isom}(\mathcal{I}) \cong \mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$ .

**Théorème 63 : [Combes, p.171]**

Les sous-groupes finis de  $\text{Isom}^+(\mathcal{E})$  sont exactement à isomorphismes près :  
\* Le groupe cyclique  $\mathbb{Z}/n\mathbb{Z}$ . \* Le groupe diédral  $D_{2n}$ .  
\* Les groupes  $\mathfrak{A}_4$ ,  $\mathfrak{S}_4$  et  $\mathfrak{A}_5$ .

**Remarque 64 :**

\* Ce théorème s'applique aussi aux sous-groupes finis de  $\text{SO}_3(\mathbb{R})$  car on peut le considérer comme un sous-groupe de  $\text{Isom}^+(\mathcal{E})$ .  
\* Chacun des groupes ci-dessus est le groupe des déplacements d'un polyèdre de l'espace affine euclidien  $\mathcal{E}$  (respectivement le groupe des déplacements d'un polygone régulier à  $n$  côtés, le groupe des déplacements d'un "épaississement" d'un polygone régulier à  $n$  côtés et enfin le groupe des déplacements d'un tétraèdre régulier, d'un cube et d'un dodécaèdre régulier).

## Remarques sur le plan

- On peut également parler de topologie (actions continues, parties connexes ou bien parties compacts), de représentations avec des actions sur un espace vectoriel, de caractères ou de produit semi-direct.
- Il faut donner de nombreux exemples ainsi que des actions transitives et fidèles, parler de certaines propriétés de l'orbite (elles partitionnent l'ensemble et trouver des invariants totaux et un représentant simple peut parfois s'avérer utile) et savoir utiliser les actions de groupes pour trouver des sous-groupes d'un certain ordre (structure quotient +  $p$ -Sylow).

## Liste des développements possibles

- Classification des groupes d'ordre  $p^2$  et  $2p$ .
- Dénombrement des endomorphismes nilpotents sur un corps fini.
- Groupe des isométries du cube.

## Bibliographie

- Grégory Berhuy, *Algèbre : le grand combat*.
- Philippe Caldero, *Carnet de voyage en Analystan*.
- Daniel Perrin, *Cours d'algèbre*.
- Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.
- Philippe Caldero, *Carnet de voyage en Algèbrie*.
- François Combes, *Algèbre et géométrie*.
- Philippe Caldero, *Nouvelles histoires hédonistes de groupes et de géométries, tome 2*.