Université de Rennes

*Groupes symétrique, linéaire et orthogonal : générateurs et simplicité*

## Généralités sur le groupe dérivé

**Définition.** *Si $G$ est un groupe, son groupe dérivé $D(G)$ est le sous-groupe de $G$ engendré par les commutateurs $[g,h] = ghg^{-1}h^{-1}$.*

**Exercice 1.** Definitions équivalentes du groupe dérivé

**1.** Montrer que $D(G)$ est le plus petit noyau d'un morphisme de $G$ vers un groupe abélien. Autrement dit, $G/D(G)$ est abélien, et pour tout $\varphi : G \to A$ avec $A$ abélien, $\ker \varphi \supset D(G)$.
**2.** Sachant que $D(GL_n(K)) = SL_n(K)$ (sauf pour le cas exceptionnel $GL_2(F_2)$), montrer tout morphisme $\varphi : GL_n(K) \to A$ vers un groupe abélien $A$ s'écrit $\varphi = \psi \circ \det$ pour un certain morphisme $\psi : K^* \to A$.

**Exercice 2.** Groupe dérivé et carrés [Per95, exo 3.4 page 155].

Si $G$ est un groupe, on note $G^2$ le sous-groupe (distingué) engendré par l'ensemble $\{g^2 | g \in G\}$.
**1.** Montrer que pour tout groupe $G$, $D(G) \subset G^2$
**2.** Montrer que si $G$ est engendré par des involutions alors $D(G) = G^2$.
**3.** Montrer que si $G$ est engendré par des involutions qui sont toutes conjuguées, alors $G/D(G)$ est trivial ou isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
**4.** Appliquer ces résultats pour déterminer le groupe dérivé de $S_n$, $O(n)$.
**5.** Appliquer ces résultats pour déterminer le groupe dérivé de $A_n$ ($n \geq 5$), et $SO(n)$ ($n \geq 3$) en remarquant que les 3-cycles et les renversements sont des carrés.

## Groupe symétrique et alterné

**Exercice 3.** Quand un ensemble de transpositions est-il générateur ?

Le but de l'exercice est de caractériser les ensembles de transpositions qui engendrent $S_n$ en termes de connexité d'un graphe.
**1.** Montrer que $S_n$ est engendré par l'ensemble de ses transpositions
**2.** Montrer que $S_n$ est engendré par les transpositions de la forme $(1,i)$ pour $i \geq 2$.

Soit $T$ un sous-ensemble de l'ensemble des transpositions de $S_n$. On associe à $T$ le graphe $\Gamma$ dont l'ensemble des sommets est $[\![1,n]\!]$ et où on met une arête entre $i$ et $j$ pour chaque transposition $(ij)$ appartenant à $T$. On pourra dessiner le graphe $\Gamma$ pour quelques ensembles $T$ particuliers, par exemple si $T = \{(i, i+1) | i < n\}$ ou $T = \{(1,i) | i > 1\}$.
**3.** Montrer que si $\Gamma$ n'est pas connexe, alors $T$ n'engendre pas $S_n$ (on pourra montrer que si $K \subset [\![1,n]\!]$ est l'ensemble des sommets d'une composante connexe de $\Gamma$, alors $K$ est invariant par $\langle T \rangle$).
**4.** Montrer que si $\Gamma$ est connexe, alors $\langle T \rangle = S_n$. On pourra montrer que toutes les transpositions $(1,i)$ sont dans $\langle T \rangle$ et utiliser la question 2.

**Exercice 4.** Quand un ensemble de 3-cycles est-il générateur ?

Le but de l'exercice est de caractériser les ensembles de 3-cycles qui engendrent $A_n$ en termes de connexité d'un graphe. Le cas $n = 1, 2$ est spécial ($A_n = \{1\}$ dans ce cas), et on suppose dans la suite $n \geq 3$.
**1.** Montrer que pour $n \geq 3$, $\langle A_n, (n-1, n, n+1) \rangle = A_{n+1}$
**2.** Montrer que pour $n \geq 3$, $\langle A_n, (n, n+1, n+2) \rangle = A_{n+2}$.

**3.** Soit $n \geq 3$ et $T$ un sous-ensemble des 3-cycles de $A_n$. Soit $\Gamma$ le graphe dont l'ensemble des sommets est $[\![1, n]\!]$ et tel que pour chaque cycle $(abc) \in T$, on met les 3 arêtes $ab, bc, ac$. Montrer que $\Gamma$ est connexe ssi $\langle T \rangle = A_n$.

Indication : Si $K \subset [\![1, n]\!]$, on note $A_K$ le sous-groupe des permutations paires a support dans $K$. On pourra montrer que si que si $K \subset [\![1, n]\!]$ est tq $A_K \subset \langle T \rangle$, avec $3 \leq \#K < n$, alors il existe $K' \supsetneq K$ tq $A_{K'} \subsetneq K$.

Rq : c'est faux si $n = 2$ : $A_2$ est trivial, et il n'y a pas de 3-cycle. Mais le graphe $\Gamma$ est toujours disconnexe, mais $T = \emptyset$ engendre.

**Exercice 5.**

On sait que pour $n \geq 5$, $A_n$ est simple.

En déduire que pour $n \geq 5$ les seuls sous-groupes distingués de $S_n$ sont $\{1\}$, $A_n$ et $S_n$.

Le théorème qui suit a une jolie preuve qui est expliquée en remarque 5.4(3) page 107 de [Per95].

**Théorème.** *$S_6$ possède un automorphisme qui n'est pas intérieur (on rappelle qu'un automorphisme intérieur d'un groupe $G$, est un automorphisme de $G$ de la forme $x \mapsto gxg^{-1}$ pour un certain $g \in G$ ; autrement dit, un automorphisme intérieur, c'est une conjugaison par un élément de $G$).*

C'est une exception car on démontre que pour tout $n \neq 6$, tout automorphisme de $S_n$ est intérieur.

**Exercice 6.**

On se propose de démontrer le théorème ci-dessus.
**1.** Montrer que l'action de $PGL_2(\mathbb{F}_5)$ sur la droite projective $D = \mathbb{P}^1(\mathbb{F}_5)$ est fidèle.
**2.** En déduire un isomorphisme entre $PGL_2(\mathbb{F}_5)$ et un sous-groupe $H \subset Sym(D)$ qu'on identifie à $S_6$. Montrer que $H$ ne fixe aucun point de $D$.
**3.** Calculer $\#H$ et en déduire le cardinal de l'ensemble $X = S_6/H$.
**4.** Montrer que l'action de $S_6$ sur $X$ est fidèle (on pourra utiliser la structure des sous-groupes normaux de $S_6$), et vérifier que $H$ à un point fixe dans $X$.
**5.** En identifiant $X$ avec $\{1, \ldots, 6\}$ on obtient un isomorphisme $\varphi$ de $S_6$ dans lui-même. Montrer que $\varphi$ n'est pas intérieur.

## Théorème de Jordan-Holder

Références : Rotman, an introduction to the theory of groups. Calais, éléments de théorie des groupes

**Définition 1.** *Soit $G$ un groupe. Une filtration[1] de $G$ est une suite de sous-groupes*

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$$

*tels que $G_i$ est distingué dans $G_{i+1}$ pour tout $i < n$ (on ne suppose pas $G_i$ distingué dans $G$). L'entier $n$ s'appelle la longueur de la filtration. Les $n$ quotients $Q_1 = G_1/G_0$, $G_2/G_1, \ldots$, $Q_n = G_n/G_{n-1}$ s'appellent les* facteurs *de la filtration.*

*Une filtration de Jordan-Hölder d'un groupe $G$ est une filtration de $G$ telle que pour tout $i < n$, le quotient $G_i/G_{i+1}$ est un groupe simple (non trivial[2]).*

On va énoncer qu'il y a unicité des facteurs des filtrations de Jordan-Holder à isomorphisme et permutation près : si $(Q_1, \ldots, Q_l)$, $(Q'_1, \ldots, Q'_{l'})$ sont deux suites de groupes, on note

$$(Q_1, \ldots, Q_l) \sim (Q'_1, \ldots, Q'_{l'})$$

si $l = l'$ et s'il existe une permutation $\sigma$ de $\{1, \ldots, l\}$ tq $Q_i \simeq Q'_{\sigma(i)}$.

1. on dit aussi *suite de composition* de $G$
2. On préfère en général adopter la convention que le groupe trivial n'est pas un groupe simple ce qui simplifie un certain nombre d'énoncés (comme le thm de Jordan-Hölder ci-dessous). C'est analogue à la convention que 1 n'est pas un nombre premier.

**Théorème 2** (Thèorème de Jordan-Hölder.). *Soit $G$ un groupe fini. Alors*

*(a) $G$ admet une filtration de Jordan-Hölder.*

*(b) toutes les filtrations de Jordan-Hölder de $G$ ont la même longueur et les facteurs de ces filtrations sont uniques à isomorphisme et permutation près : si $(G_i)_{i \leq l}$ et $(G'_i)_{i \leq l'}$ sont deux filtrations de Jordan-Hölder de $G$, alors $l = l'$ et $(G_1/G_0, \ldots, G_l/G_{l-1}) \sim (G'_1/G'_0, \ldots, G'_l/G'_{l-1})$.*

*Ces facteurs $G_i/G_{i-1}$ s'appellent les facteurs de Jordan-Hölder de $G$.*

### Exercice 7.

**1.** Montrer que tout groupe fini admet une filtration de Jordan-Hölder.
**2.** Donner un exemple de groupe infini n'ayant pas de filtration de Jordan-Hölder.
**3.** Donner un exemple de groupe infini ayant une filtration de Jordan-Hölder.
**4.** Montrer que $G$ est fini et si $Q_1, \ldots, Q_n$ sont des facteurs d'une filtration de $G$, alors $\#G = \prod_i \#G_i$
**5.** Donner les facteur de Jordan-Holder de $\mathbb{Z}/n\mathbb{Z}$.
**6.** Retrouver l'unicité de la décomposition en facteur premiers de $n$ à partir du théorème de Jordan-Hölder.

### Exercice 8.

Donner les facteur de Jordan-Holder de $S_n$ pour $n = 3, 4$ et $n \geq 5$.

### Exercice 9. Preuve du théorème de Jordan-Hölder.

Le but de l'exercice est de démontrer le théorème de Jordan-Hölder. On a déja vu la partie existence. Pour l'unicité, on raisonne par récurrence sur le cardinal de $G$. Soient

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_h = G \quad \text{et} \quad \{1\} = K_0 \lhd K_1 \lhd \ldots \lhd K_k = G$$

deux filtrations de Jordan-Hölder de $G$. On note $H = H_{h-1}$ et $K = K_{k-1}$.
**1.** Cas facile : montrer le théorème si $H = K$. On suppose donc dans la suite que $H \neq K$, et soit $L = H \cap K$.
**2.** (le point clé) : démontrer que $H/L \simeq G/K$, et que $K/L \simeq G/H$.
**3.** Soit

$$\{1\} = L_0 \lhd L_1 \lhd \ldots \lhd L_l = L$$

une filtration de Jordan-Hölder de $L$. En appliquant la question (1) à

$$\{1\} = L_0 \lhd L_1 \lhd \ldots \lhd L_{l-1} \lhd L \lhd H \lhd G \quad \text{et} \quad \{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_{h-1} \lhd H \lhd G$$

montrer que $l + 1 = h - 1$ et que

$$(L_1/L_0, \ldots, L/L_{l-1}, H/L, G/H) \sim (H_1/H_0, \ldots, H/H_{h-2}, G/H).$$

Montrer de même que

$$(L_1/L_0, \ldots, L/L_{l-1}, K/L, G/K) \sim (K_1/K_0, \ldots, K/K_{k-2}, G/K)$$

**4.** Conclure en utilisant la question 2.

## Groupe linéaire

Ref : [Per95].

### Exercice 10.

Soit $u \in GL(E)$ un automorphisme d'un espace vectoriel $E$ de dimension $n$. Soit $r \in [\![1, n-1]\!]$ et supposons que $u$ laisse invariant tous les sous-espaces vectoriels de dimension $r$ de $E$. Montrer que $u$ est une homothétie.

**Exercice 11.** Automorphisme extérieur de $GL_n(K)$ [CG17, exo C.8 p.32].

Soit $K$ un corps de caractéristique $\neq 2$. Il s'agit de montrer que l'automorphisme $\sigma$ de $GL_n(K)$ défini par $\sigma : g \mapsto {}^t g^{-1}$ n'est pas intérieur, c'est à dire qu'il n'existe pas de matrice $P \in GL_n(K)$ tq pour tout $g \in GL_n(K)$, ${}^t g^{-1} = PgP^{-1}$. On suppose donc que c'est le cas, et on veut aboutir à une contradiction.

**1.** Montrer que $\sigma$ est bien un automorphisme de groupes

**2.** Montrer que $P \in O_n(K)$ au sens où ${}^t P = P^{-1}$.

**3.** Montrer que $P$ appartient au centre de $O_n(K)$

**4.** Montrer que $P$ est diagonale utilisant que $P$ commute avec $g$ diagonale avec un coefficient diagonal égal à $-1$ et les autres égaux à 1.

**5.** Montrer que $P$ est une homothétie en utilisant que $P$ commute avec les matrices de transposition.

**6.** Conclure en observant que $\sigma$ n'est pas l'identité.

On sait que $PSL_n(K)$ est simple pour $n \geq 2$ et tout corps $K$, sauf pour les cas exceptionnels de $PSL_2(F_2) \simeq S_3$ et $PSL_2(F_3) \simeq A_4$. Montrons que ce n'est plus le cas si on remplace $K$ par un anneau.

**Exercice 12.**

On définit $PSL_n(\mathbb{Z}) = SL_n(\mathbb{Z})/\{\pm I_n\}$ comme le quotient de $SL_n(\mathbb{Z})$ par les homothéties qu'il contient.

**1.** Montrer que pour $n \geq 2$, n'est pas simple. On pourra utiliser la réduction modulo $p$.

**2.** Généraliser pour tout anneau $A$ qui n'est pas un corps, où on définit $PSL_n(A) = SL_n(A)/(A^\times.I_n)$.

**Définition 3.** *Une transvection d'un espace vectoriel $V$ est un endomorphisme $u \neq Id$ tel qu'il existe une base dans laquelle $u$ s'écrit* $\begin{bmatrix} 1 & 0 & \dots & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & 1 & 0 & 0 \\ \vdots & & \ddots & 1 & 1 \\ 0 & \dots & \dots & 0 & 1 \end{bmatrix}$.

En particulier, $u$ est l'identité sur l'hyperplan engendré par les $n-1$ premiers vecteurs de la base. Par définition, les transvections sont toutes conjuguées.

**Exercice 13.** Voir [Per95, prop 2.2 p. 97]

Soit $u \in GL(E)$, $g \neq Id$, et $H \subset E$ un hyperplan tel que $u_{|H} = id$.

**1.** Montrer que les conditions suivantes sont équivalentes :

(a) $u$ est une transvection

(b) $\det(u) = 1$

(c) $u$ n'est pas diagonalisable

(d) $\mathrm{Im}(u - id) \subset H$

(e) l'endomorphisme induit $\bar{u} : E/H \to E/H$ est l'identité de $E/H$

(f) il existe une forme linéaire $f$ dont le noyau égal à $H$ et $a \in H \setminus \{0\}$ tel que $u(x) = x + f(x)a$.

**2.** Vérifier que si on remplace le 1 hors diagonale de la matrice ci-dessus par un $\lambda \neq 0$ quelconque, on obtient encore un transvection.

**Exercice 14.** Groupe dérivé de $PGL_n(K)$ et de $PSL_n(K)$ [Per95, Exo §3.1 p112]

On rappelle que $D(GL_n(K)) = SL_n(K)$ (sauf pour $GL_2(F_2)$) et $D(SL_n(K)) = SL_n(K)$ (sauf pour $SL_2(F_2)$ et $SL_2(F_3)$).

Déterminer $D(PGL_n(K))$ et $D(PSL_n(K))$.

## Actions transitives et primitives, critère d'Iwasawa

**Exercice 15.**

Montrer qu'une action 2-transitive est primitive.

**Exercice 16.**

Montrer que l'action de $PGL_2(K)$ sur $\mathbb{P}^1(K)$ est 3-transitive, mais que ce n'est pas le cas pour $n \geq 3$ et $\#K > 2$.

**Exercice 17.** Action primitive et sous-groupes maximaux

Soit $G \curvearrowright X$ une action transitive, avec $\#X \geq 2$.

Montrer que les énoncés suivants sont équivalents

(a) $G \curvearrowright X$ est primitive

(b) si $G \curvearrowright Y$ est une action telle qu'il existe une application $G$-équivariante $f : X \to Y$, alors $f$ est constante ou injective.

(c) Pour tout $x \in X$, $G_x$ est un sous-groupe maximal de $G$

(d) Il existe $x \in X$ tq $G_x$ est un sous-groupe maximal de $G$

**Exercice 18.**

**1.** Montrer que l'action de $SO_3(\mathbb{R})$ sur la sphere unité $S$ de $\mathbb{R}^3$ n'est pas primitive.
**2.** Montrer que l'action de $SO_3(\mathbb{R})$ sur l'espace projectif $P^2\mathbb{R}$ (qu'on peut identifier aux paires de points antipodaux de $S$) n'est pas 2-transitive. Montrer qu'elle est primitive.

**Théorème 4** (Exo I.C.14 p41 [CG17])**.** *Soit $G$ agissant sur un ensemble fini $X$ de manière 4-transitive. Supposons qu'il existe $x \in X$ tel que $G_x$ soit simple. Alors $G$ est simple.*

## Références


[CG17] Philippe Caldero and Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome 1*, volume 117 of *Math. Devenir.* Paris : Calvage et Mounet, 2nd edition edition, 2017.

[Per95] Daniel Perrin. *Cours d'algèbre.* CAPES-AGREG mathématiques. Ellipses, Paris, 1995.