Université de Rennes

Groupes symétrique, linéaire, et orthogonal
générateurs et simplicités

Table des matières

I. Introduction, simplicité

Définition 1. *Un groupe G est simple s'il est non trivial et si tout sous-groupe normal $N \triangleleft G$ est soit trivial soit égal à G.*

Pourquoi cette notion est importante ? De même que les nombres premiers sont "les atomes" de l'arithmétique, les groupes simples peuvent être vus comme les atomes de la théorie des groupes.

Par exemple, si on s'intéresse aux groups finis, si un groupe n'est pas simple, il a un sous-groupe normal $N \triangleleft G$, et on peut essayer de le décrire en terme des groupes N et G/N, qui sont de cardinal inférieur.

Ca n'est pas si facile en réalité de décrire G a partir de N et G/N, mais c'est un bon début. Un exemple qui montre que c'est quand même compliqué : Si G et G' sont deux groupes de cardinal p^n (pour un certain nombre premier p), alors ils auront les mêmes "atomes" (qui seront tous isomorphes à $\mathbb{Z}/p\mathbb{Z}$), mais G et G' peuvent être très différents.

Cette vision "atomique" des groupes simples colle bien avec le théorème de Jordan-Hölder.

Soit G un groupe fini. Si G n'est pas simple, il a un sous-groupe normal N. Si N et G/N sont simples, on imagine que se sont les "atomes" composant G, on les appelle facteurs de Jordan-Hölder de G. Si N ou G/N n'est pas simple, on recommence en cherchant les facteurs de Jordan-Hölder de G.

Définition 2 (Définition des facteurs de Jordan-Hölderd'un groupe G.)**.** *Soit G un groupe fini non trivial. Si G est simple, on dit que la suite à 1 élément (G) est la suite de facteurs de Jordan-Hölder de G.*

Si G n'est pas simple, et si N est un sous-groupe normal non trivial de G, avec $N \neq G$, et si $(Q_1, \dots, Q_k)$ est une suite de facteurs de Jordan-Hölder de N et $(Q'_1, \dots, Q'_l)$ est une suite de facteurs de Jordan-Hölder de G/N, alors on dit que $(Q_1, \dots, Q_k, Q'_1, \dots, Q'_l)$ est une suite de facteurs de Jordan-Hölder de G.

Remarque 3. La def ci-dessus est en général présentée différemment (avec des filtrations de G), mais est équivalente.

Théorème 4. *Soit G un groupe fini non trivial. Alors la suite de facteurs de Jordan-Hölder de G est unique à permutation et isomorphisme près.*

Plus précisément, si $(Q_1, \dots, Q_k)$ et $(Q'_1, \dots, Q'_{k'})$ sont deux suites de facteurs de Jordan-Hölder de G, alors $k = k'$, et il existe une permutation σ de $\{1, \dots, k\}$ tq $Q_i \simeq Q'_i$.

Il y a un théorème fameux de classification des groupes finis simples,s dont la preuve est notoirement longue et compliquée. Elle s'étale sur des dizaines de milliers de pages publiées entre les années 1950 et 2000. Ce théorème donne une liste complète des groupes finis simples : il y a

- les $\mathbb{Z}/p\mathbb{Z}$ avec p premier
- les A_n avec $n \geq 5$
- les $PSL_n(K)$ avec K corps fini (avec 2 exceptions : $PSL_2(F_2)$ et $PSL_2(F_3)$), et plus généralement, les groupes *de type Lie* (qui contiennent, entre autres, des groupes simples associés [1] aux groupes orthogonaux et symplectiques)
- 26 groupes sporadiques qui n'entrent dans aucune liste.

A l'agreg, les théorèmes suivants sont classiques

Théorème 5. *Les groupes suivants sont simples*

- *A_n pour $n \geq 5$*
- *$PSL_n(K)$ pour tout $n \geq 2$ et tout corps K sauf $PSL_n(F_2)$ et $PSL_n(F_3)$*
- *$SO_3(\mathbb{R})$, et $PSO_n(\mathbb{R})$ pour $n \geq 5$.*

Par contre, $PSO_4(\mathbb{R})$ n'est pas simple.

Excellente référence : [Per95].

On va utiliser un critère d'Iwasawa qui s'applique de manière assez uniforme dans les diverses situations. Toutes les preuves que je connais commencent par comprendre le groupe dérivé, et cette approche n'y fait pas exception.

II. Groupe linéaire

Référence : [Per95], [Gro01]

1. il ne suffit parfois pas de se restreindre au determinant 1 et de quotienter par les homothéties

II.1 Définitions et énoncé

Commençons par énoncer précisément le 1er objectif.

Définition 6. *$PGL_n(K)$ est le quotient de $GL_n(K)$ par le sous-groupe de ses homothéties $K^*.I_n$.*

$PSL_n(K)$ est le quotient de $SL_n(K)$ par le sous-groupe de ses homothéties $SL_n(K) \cap K^*I_n = \mu_n(K).I_n$, où $\mu_n(K)$ est l'ensemble des racines n-ièmes de l'unité (le n est le même n que dans PSL_n).

Remarque 7. Le cas $K = \mathbb{F}_2$ est assez particulier. Dans ce cas, $K^* = \{1\}$, donc $GL_n(F_2) = SL_n(F_2) = PGL_n(F_2) = PSL_n(F_2)$. Pour $n = 2$, ces quatre groupes sont isomorphes à S_3 (par exemple, parce que l'action de $GL_2(F_2)$ sur $F_2^2 \setminus \{0\}$ (qui a 3 points) est fidèle, ce qui donne un morphisme injectif vers S_3 qui est surjectif pour des raisons de cardinalité ou parce que l'action et transitive et contient une transposition, donc contient les transpositions.

Le but est sera de montrer le théorème suivant.

Théorème 8. *Pour tout corps K et tout $n \geq 2$, $PSL_n(K)$ est simple sauf pour $PSL_2(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_3)$.*

II.2 Pourquoi "S" et pourquoi "P" ?

Pourquoi les "S" et "P" de PSL_n et pas simplement GL_n ?

$GL_n(K)$ n'est pas simple pour $n \geq 2$ a cause du déterminant $\det : GL_n(K) \to K^*$. Le déterminant est un morphisme de groupes, et son noyau est un sous-groupe normal (propre si K^* non trivial, ie si $\#K \geq 3$). Il est donc naturel de se restreindre à $SL_n(K)$. D'où le "S" (qui au passage signifie "spécial"...).

Pouquoi "P" dans PSL_n ? Les homothéties de $GL_n(K)$ commutent avec tous les éléments de $GL_n(K)$. En particulier, elles forment un sous-groupe normal (et même central !). Dans $SL_n(K)$, les seules homothéties sont les λI_n avec $\lambda^n = 1$, mais elles forment là aussi un sous-groupe normal car central. Donc on n'aura pas de simplicité si ce groupe est non trivial, d'où le quotient par les homothéties et le P de PGL_n et PSL_n.

Au passage, le P signifie "projectif". Le groupe $PGL_n(K)$ est le groupe linéaire projectif, et le groupe $PGL_n(K)$ est le groupe linéaire spécial projectif,

II.3 Action projective

$PGL_n(K)$ est un groupe qui agit naturellement sur $\mathbb{P}^{n-1}(K) = \mathbb{P}(K^n)$ puisque clairement, chaque homothétie agit comme l'identité, donc l'action de $GL_n(K)$ (définie par un morphisme de $GL_n(K) \to Bij(\mathbb{P}^{n-1}K)$) passe au quotient en une action de $PGL_n(K)$.

Lemme 9. *Si $g \in GL_n(K)$ préserve chaque droite vectorielle, alors g est une homothétie.*
De manière équivalence, l'action de $PGL_n(K)$ sur $\mathbb{P}^{n-1}(K)$ est fidèle.

Preuve. C'est vrai trivialement si $n = 1$. Supposons $n \geq 2$. Dans la base canonique, g est une matrice diagonale, disons $diag(\lambda_1, \ldots, \lambda_n)$. Le vecteur $v = e_1 + \cdots + e_n$ est envoyé sur $gv = \lambda_1 e_1 + \ldots \lambda_n e_n$. Puisque gv proportionnel à v, tous les λ_i sont egaux, et g est une homothétie. □

On a en fait le résultat un peu plus précis en termes de repère projectif.

Définition 10. *Un repère projectif de $\mathbb{P}^{n-1}(K)$ est la donnée d'une famille de $n+1$ points $([v_0], \ldots, [v_n])$ tels que $(v_1, \ldots, v_n)$ est une base de K^n et v_0 a toutes ses coordonnées non nulles dans cette base.*

De manière équivalente (version plus symétrique) : $([v_0], \ldots, [v_n])$ est une base projective si tout sous-ensemble de cardinal n de la famille $(v_0, \ldots, v_n)$ est une base de K^n.

De manière encore équivalente, dans la famille $([v_0], \ldots, [v_n])$, aucun sous-ensemble de cardinal n n'est contenu dans un sous-espace de codimension 1 de $\mathbb{P}^{n-1}(K)$.

Exercice. *Montrer l'équivalence des définitions.*

Lemme 11. *Si $([v_0], \dots, [v_n])$ et $([v'_0], \dots, [v'_n])$ sont deux repères projectifs, il existe un unique élément $g \in PGL_n(K)$ qui envoie l'un sur l'autre.*

Preuve. Existence : il existe $g \in GL_n$ qui envoie la base $\mathcal{B} = (v_1, \dots, v_n)$ sur $\mathcal{B}' = (v'_1, \dots, v'_n)$ puisque ce sont 2 bases. On peut donc supposer $\mathcal{B} = \mathcal{B}'$. Les deux vecteurs v_0 et v'_0 ont toutes leur coordonnées non nulles dans la base $(v_1, \dots v_n)$ (si la ieme coordonnee est nulle, si on enleve v_i a la famille $(v_0, \dots v_n)$, on obtient une famille non génératrice puisque contenue dans l'hyperplan $x_i = 0$). Puisque toutes les coordonnées sont non nulles, il existe une matrice diagonale qui envoie v_0 sur v'_0. Cette matrice préserve $([v_1], \dots [v_n]) = ([v'_1], \dots [v'_n])$ et envoie donc $([v_0], \dots, [v_n])$ sur $([v'_0], \dots, [v'_n])$.

L'argument de la preuve du lemme 9 permet de démontrer l'unicité : si g preserve $[v_1], \dots, [v_n]$, c'est une matrice diagonale dans cette base, et si elle préserve $[v_0]$, elle doit être l'identité. □

Proposition 12. *K^*I_n est le centre de $GL_n(K)$, et $\mu_n.I_n$ est le centre de $SL_n(K)$.*

Remarque 13. Du coup, certains auteurs definissent $PGL_n(K)$ et $PSL_n(K)$ comme le quotient de $GL_n(K)$ et $SL_n(K)$ par leur centre.

Preuve. Clairement, K^*I_n est contenu dans le centre de $GL_n(K)$.

Pour la réciproque, on montre que tout élément $g \in GL_n(K)$ qui commute avec tous les éléments de $SL_n(K)$ préserve toute les droites vectorielles (et est donc un homothétie). Ca montre les 2 affirmations.

Soit d une droite vectorielle, et soit $h \in SL_n(K)$ tq $\mathrm{Fix}(h) = d$: ca existe, on peut prendre v_1 vecteur directeur de d, compléter en une base et prendre pour h un bloc de jordan unipotent (ie $e_i \mapsto e_i + e_{i-1}$ pour $i \geq 2$), et la dimension du sous-espace fixe est 1 puisque rang $h - id = n - 1$. Si g est central, g commute avec h, donc preserve d et ce pour tout d. Donc g est une homothétie.

□

II.4 Transvections

Rappels sur les transvections.

Définition 14. *Une transvection $g \in GL_n(K)$ est une application linéaire qui s'écrit dans une certaine base sous la forme $T = \begin{bmatrix} I_{n-2} & & \\ & 1 & 1 \\ & 0 & 1 \end{bmatrix}$.*

Autrement dit, il existe une base $v_1, \dots, v_n$ de K^n tq $g : v_i \mapsto v_i$ pour $i \leq n-1$ et $g : v_n \mapsto v_n + v_{n-1}$.

Lemme 15 ([Per95])**.** *Les énoncés suivants sont équivalents :*

(a) g est une transvection

(b) g est l'identité sur un hyperplan mais n'est pas diagonalisable

(c) g est de la forme $x \mapsto x + l(x)\vec{v}$ pour une certaine forme linéaire l et un certain vecteur non nul $\vec{v} \in \ker l$.

Il y a encore d'autres caractérisations (voir [Per95]).

En particulier, si g s'écrit dans une certaine base sous la forme $\begin{bmatrix} I_{n-2} & & \\ & 1 & \lambda \\ & 0 & 1 \end{bmatrix}$, alors c'est une transvection d'après (2). De même, les matrices élémentaires de transvection sont des transvections.

Théorème 16. *Soit K un corps et $n \geq 2$.*

(a) *$SL_n(K)$ est engendré par ses transvections.*

(b) *Toutes les transvections sont conjuguées dans $GL_n(K)$.*

(c) *Si $n \geq 3$, toutes les transvections sont conjuguées dans $SL_n(K)$. Si $n = 2$, toute transvection est conjuguée dans $SL_2(K)$ à une matrice de la forme $\begin{bmatrix} 1 & \lambda \\ & 1 \end{bmatrix}$ avec $\lambda \neq 0$.*

Preuve. (a) L'élimination de Gauss montre qu'on peut transformer une matrice inversible en matrice triangulaire supérieure via des opérations élémentaires du type transvection : si on a besoin d'un échange de ligne, on peut le remplacer par une opération $L_i \leftarrow L_i + L_j$; ou alors, on peut utiliser la relation

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}$$

pour remplacer un echange de ligne par des opérations de transvection.

On peut ensuite arriver a une matrice diagonale en faisant encore des opérations élémentaires de transvection. On voit finalement que $\begin{bmatrix} \lambda & \\ & \frac{1}{\lambda} \end{bmatrix}$ est un produit de matrices élémentaires de transvection ([2]), ce qui permet d'arriver à l'identité. Conclusion $SL_n(K)$ est engendré par ses matrices élémentaires de transvections, donc par ses transvections.

(b) Les transvections sont toutes conjuguées dans GL_n par définition.

(c) Pour la conjugaison dans SL_n : si $g = PTP^{-1}$ avec P de déterminant λ, soit $D_\lambda = \begin{bmatrix} I_{n-1} & & \\ & \lambda & \\ & & \frac{1}{\lambda} \end{bmatrix} = \begin{bmatrix} I_{n-3} & & \\ & \lambda & \\ & & \frac{1}{\lambda} I_2 \end{bmatrix}$ (de déterminant $\frac{1}{\lambda}$). La matrice $P' = P.D_\lambda$ est de déterminant 1, et D_λ commute avec T puisque le dernier bloc 2×2 de D_λ est $\frac{1}{\lambda} I_2$. Donc $g = P'TP'^{-1}$.

Pour $n = 2$: si $g = PTP^{-1}$ avec P de déterminant λ, soit $D_\lambda = \begin{bmatrix} 1 & \\ & \frac{1}{\lambda} \end{bmatrix}$ (de déterminant $\frac{1}{\lambda}$), et $P' = PD_\lambda \in SL_n(K)$. Alors, $g = P'D_\lambda^{-1}TD_\lambda P'^{-1}$ est donc conjuguée dans SL_n à $D_\lambda^{-1}TD_\lambda = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}$.

□

II.5 Groupe dérivé

Définition 17. *Si G est un groupe, son groupe dérivé $D(G)$ est le sous-groupe engendré par tous les commutateurs $[g, h] = ghg^{-1}h^{-1}$. Le quotient $G/D(G)$ est "le plus gros quotient abélien" de G et s'appelle l'abélianisé de G.*

Un groupe G est parfait si son abélianisé est trivial, autrement dit si $D(G) = G$.

Théorème 18. *Soit K un corps et $n \geq 2$.*

(a) *$D(GL_n(K)) = SL_n(K)$ sauf dans le cas de $GL_2(F_2) \simeq S_3$.*

(b) *$SL_n(K)$ et $PSL_n(K)$ sont parfaits, sauf pour $SL_2(F_2)$, $SL_2(F_3)$, et $PSL_2(F_2)$, $PSL_2(F_3)$.*

Remarque 19. $SL_2(F_2) \simeq S_3$ n'est pas parfait puisque son groupe dérivé est isomorphe à A_3.

---

2. Indication : partir de la matrice $\begin{bmatrix} \lambda & \\ & \frac{1}{\lambda} \end{bmatrix}$ et lui appliquer des opérations élémentaires de transvection sur les lignes et colonnes pour arriver a l'identité : $\begin{bmatrix} \lambda & \\ & \lambda^{-1} \end{bmatrix}$. $C_2 = C_2 + C_1$: $\begin{bmatrix} \lambda & \lambda \\ & \lambda^{-1} \end{bmatrix}$. $L_2 = L_2 + L_1/\lambda$: $\begin{bmatrix} \lambda & \lambda \\ 1 & \lambda + 1\lambda^{-1} \end{bmatrix}$. $L_1 = L_1 + (1 - \lambda)L_2$: $\begin{bmatrix} 1 & \lambda^{-1} \\ 1 & 1 + \lambda^{-1} \end{bmatrix}$. $L_2 = L_2 - L_1$: $\begin{bmatrix} 1 & \lambda^{-1} \\ 0 & 1 \end{bmatrix}$: transvection.

Montrons que $PSL_2(F_3) = A_4$, et qu'il est donc d'abélianisé non trivial. Du coup $SL_2(F_3)$ est aussi d'abélianisé non trivial. $GL_2(F_3)$ est de cardinal $8 \times 6 = 48$, donc $PGL_2(F_3)$ est de cardinal 24. $SL_2(F_3)$ est un groupe de cardinal 24 et $PSL_2(F_3)$ est de cardinal 12. C'est un sous-groupe d'indice 2 de $PGL_2(F_3)$. Comme $PGL_2(F_3)$ agit fidèlement sur la droite projective qui à 4 éléments, $PGL_2(F_3)$ est isomorphe à un sous-groupe de S_4, et puisqu'on a égalité des cardinaux, $PGL_2(F_3) \simeq S_4$. Comme le seul sous-groupe d'indice 2 de S_4 est A_4, $PSL_2(F_3)$ est isomorphe à A_4. Il n'est donc pas parfait (son groupe dérivé est le groupe de Klein).

$GL_2(F_2) = SL_2(F_2)$ $= PGL_2(F_2) = PSL_2(F_2)$ $\simeq S_3$	$PGL_2(F_3)$ $\simeq S_4$	$PSL_2(F_3)$ $\simeq A_4$

TABLE 1 – Isomorphismes des exceptions. Notons que $SL_2(F_3)$ n'est pas isomorphe à S_4 même s'il a le même cardinal puisque $SL_2(F_3)$ a un centre non trivial $\pm I_2$.

Preuve. (a) On a que $D(GL_n(K)) \subset SL_n(K)$ puisque $SL_n(K)$ est le noyau du déterminant, qui est à valeurs dans un groupe abélien. L'autre inclusion découle de (b) puisque (b) montre que tout élément de $SL_n(K)$ est même un produit de comutateur d'éléments de $SL_n(K)$.

(b) ([Gro01]) Notons que si $SL_n(K)$ est parfait alors $PSL_n(K)$ aussi : si $PSL_n(K)$ avait un quotient abélien non trivial alors $SL_n(K)$ aussi. Il suffit donc de montrer la perfection de $SL_n(K)$.

Considérons d'abord le cas $n \geq 3$. On sait que $SL_n(K)$ est engendré par ses transvections, et qu'elles sont toutes conjuguées. Il suffit donc de voir qu'une transvection est un commutateur.

On prend $\tau : e_1 \mapsto e_1 + e_2$ qui fixe les autres e_i, $\sigma : e_2 \mapsto e_2 + e_3$ qui fixe les autres e_i. On a que $\tau^{-1} : e_1 \mapsto e_1 - e_2$ et $\sigma^{-1} : e_2 \mapsto e_2 - e_3$. Tous les e_i, $i \geq 3$ sont fixes. Le commutateur $\tau\sigma\tau^{-1}\sigma^{-1}$ fait :

$$e_1 \mapsto e_1 \mapsto e_1 - e_2 \mapsto e_1 - (e_2 + e_3) \mapsto e_1 + e_3$$

et

$$e_2 \mapsto e_2 - e_3 \mapsto e_2 - e_3 \mapsto e_2 \mapsto e_2$$

On a donc bien une transvection. Conclusion : $SL_n(K)$ est parfait pour $n \geq 3$.

Cas $n = 2$. Dans ce cas, on suppose $\#K > 3$, donc il existe $\lambda \in K \setminus \{0, \pm 1\}$. Pour $b \in K$, calculons le commutateur

$$\begin{bmatrix} \lambda & \\ & \lambda^{-1} \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \lambda^{-1} & \\ & \lambda \end{bmatrix} \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b(\lambda^2 - 1) \\ 0 & 1 \end{bmatrix}$$

Comme $\lambda^2 - 1 \neq 0$, en faisant varier b on obtient toutes les matrices $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$. Comme toutes les transvections sont conjuguées dans SL_2 à une matrice de la forme $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, on obtient que toute transvection est un commutateur dans $SL_2(K)$ des que $\#K > 2$. □

II.6 Enoncé du critère de simplicité d'Iwasawa pour les actions 2-transitives

Ref : [CG17, I. Exo C10] ou [Gro01, Thm 0.5]

Définition 20 (Action k-transitive)**.** *Soit $G \curvearrowright X$ une action de groupe sur un ensemble.*

On dit que cette action est transitive si pour tout $x \in X$, $G.x = X$ (il n'y a qu'une orbite).

On dit qu'elle est 2-transitive si $\#X \geq 2$ et si pour toutes paires ordonnées $(x, y), (x', y') \in X \times X$, avec $x \neq y$ et $x' \neq y'$ il existe $g \in G$ tel que $gx = x'$ et $gy = y'$. Autrement dit, l'action est 2-transitive si l'action naturelle de G sur $X \times X$ privé de la diagonale est transitive.

Plus généralement on dit que $G \curvearrowright X$ est k-transitive si $\#X \geq k$ et G agit transitivement sur les k-uplets d'éléments distincts de X.

Exemple : l'action de S_n sur $\{1, \ldots, n\}$ est k-transitive pour tout $k \leq n$.

L'action de $GL_2(K)$ sur la droite projective $\mathbb{P}^1(K)$ est 3-transitive [3]. Mais l'action $GL_n(K) \curvearrowright \mathbb{P}^{n-1}(K)$ n'est pas 3-transitive pour $n \geq 3$ ([4]) : parce qu'on ne peut pas envoyer 3 points alignés sur 3 points non alignés ! On verra qu'elle est quand même 2-transitive.

Théorème 21 (Critère de simplicité d'Iwasawa)**.** *Soit $G \curvearrowright X$ une action sur un ensemble, et soit $x_0 \in X$. On suppose :*

(a) G est parfait

(b) l'action $G \curvearrowright X$ est fidèle et 2-transitive

(c) G_{x_0} contient un sous-groupe abélien [5] $A_{x_0} \triangleleft G_{x_0}$ distingué dans G_{x_0} et tel que ses G-conjugués engendrent G : $\langle A_{x_0}^g | g \in G \rangle = G$

Alors G est simple.

On le prouvera plus tard (dans une version un peu plus générale).

Appliquons le ici.

II.7 2-transitivité de l'action projective

Lemme 22. *Les actions de $PGL_n(K)$ et de $PSL_n(K)$ sur $\mathbb{P}^{n-1}(K)$ sont 2-transitive.*

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

Preuve du lemme. 2-transitivité : soient $[v_1] \neq [v_2] \in \mathbb{P}^{n-1}(K)$. v_1 et v_2 sont non colinéaires puisque $[v_1] \neq [v_2]$. On peut donc les compléter en une base $\mathcal{B} = v_1, \ldots, v_n$ de K^n, Si on se donne une autre paire $[v_1'] \neq [v_2'] \in \mathbb{P}^{n-1}(K)$, on complète aussi en une base $\mathcal{B}' = (v_1', v_2', \ldots v_n')$. Il existe g qui envoie $\mathcal{B}$ sur $\mathcal{B}'$, ce qui montre que l'action de $PGL_n(K)$ est 2-transitive. Pour voir que l'action de $PSL_n(K)$ est 2-transitive, il suffit voir qu'on peut prendre g de déterminant 1. Quitte a changer v_1' en $\lambda v_1'$ (ce qui ne change pas $[v_1']$), on change le déterminant de g en le multipliant par λ, donc on peut choisir λ pour obtenir un g de déterminant 1. □

II.8 Preuve de la simplicité de $PSL_n(K)$

Preuve de la simplicité de $PSL_n(K)$ via Iwasawa. On a vu que $PSL_n(K)$ était parfait et que l'action sur $\mathbb{P}^{n-1}(K)$ était fidèle et 2-transitive, donc primitive.

Il reste a voir pour $x_0 \in \mathbb{P}^{n-1}(K)$, son stabilisateur $\mathrm{Stab}(x_0)$ contient un sous-groupe abélien distingué $A_{x_0} \triangleleft \mathrm{Stab}(x_0)$ dont les conjugués dans $PSL_n(K)$ engendrent $PSL_n(K)$.

Prenons $x_0 = [e_1]$. On regarde son stabilisateur dans $SL_n(K)$ plutôt que dans $PSL_n(K)$. C'est la préimage de G_{x_0} dans $SL_n(K)$, on le note $\tilde{G}_{x_0}$. $\tilde{G}_{x_0}$ est l'ensemble des matrices g tq $ge_1 = \lambda e_1$, donc de la forme $g = \begin{bmatrix} \lambda & * \\ 0 & M \end{bmatrix}$ avec $M \in GL_{n-1}(K)$ vérifiant $\lambda \det(M) = 1$. L'application qui à $g \in \tilde{G}_{x_0}$ associe $(\lambda, M) \in K^* \times GL_{n-1}(K)$ est un morphisme de groupes dont le noyau $\tilde{A}_{x_0}$ est l'ensemble des matrices de la forme $\begin{bmatrix} 1 & * \\ 0 & I_{n-1} \end{bmatrix}$.

3. parce que 3 points distincts de $\mathbb{P}^1(K)$ forment une base projective

4. même si $K = \mathbb{F}_2$, les droites projectives sont de cardinal 3, il y a des triplets de points alignés d'autres non

5. Résoluble suffit

$\tilde{A}_{x_0} \lhd \tilde{G}_{x_0}$ est un sous-groupe distingué, abélien, isomorphe à K^{n-1}. Ses éléments on triviaux sont des transvections : en effet, pour $g \in \tilde{A}_{x_0}$, $g - id$ est de rang 1, donc a un noyau de dimension $n-1$, donc g fixe un hyperplan. Si g n'est pas l'identité, g n'est pas diagonalisable (toutes ses vap sont 1), et c'est donc une transvection.

Si $n \geq 3$, $\{\tilde{A}_{x_0}^g | g \in PSL_n(K)\}$ contient toutes les transvections puisqu'elles sont conjuguées dans $SL_n(K)$. Comme les transvections engendrent $SL_n(K)$, donc $\langle A_{x_0}^g | g \in PSL_n(K)\rangle = SL_n(K)$.

Si $n = 2$, puisque $\tilde{A}_{x_0}$ contient tous les $\begin{bmatrix} 1 & \lambda \\ & 1 \end{bmatrix}$, il contient un conjugué de toutes les transvections, donc $\{\tilde{A}_{x_0}^g\}$ contient toutes les transvections, donc engendre $SL_n(K)$.

On passe maintenant dans $PSL_n(K)$: soit A_{x_0} l'image de $\tilde{A}_{x_0}$ par $\pi : SL_n(K) \to PSL_n(K)$. C'est un groupe abélien. Puisque $\pi(\tilde{G}_{x_0}) = G_{x_0}$, A_{x_0} est distingué dans G_{x_0}. Puisque les conjugués de $\tilde{A}_{x_0}$ dans $SL_n(K)$ engendrent $SL_n(K)$, les conjugués de A_{x_0} dans $PSL_n(K)$ engendrent $PSL_n(K)$ vu que π est surjective. Le critère de simplicité d'Iwasawa s'applique donc. □

III. Critère de simplicité d'Iwasawa

III.1 Actions primitives

Définition 23 (Relation d'équivalence invariante)**.** *Une relation d'équivalence $\sim$ sur X est G-invariante si pour tout $x, y \in X$ et tout $g \in G$, on a*

$$x \sim y \Rightarrow gx \sim gy$$

Autrement dit, tout élément de G envoie une classe d'équivalence sur une (autre) classe d'équivalence. Dans ce cas G agit sur le quotient $X/\sim$.

Définition 24. *Une relation d'équivalence $\sim$ sur X est* triviale *si $\sim$ est soit la relation d'égalité, soit la relation grossière :*

- *(relation d'égalité) $\forall x, y$, $x \sim y$ ssi $x = y$ (autrement dit, $(X/\sim) \simeq X$)*
- *(relation grossière) $\forall x, y$, $x \sim y$ (autrement dit $(X/\sim) = \{*\}$)*

Définition 25 (Action primitive)**.** *On dit qu'une action $G \curvearrowright X$ est* primitive *si elle est transitive, et si toute relation d'équivalence G-invariante est triviale.*

Lemme 26. *Si $G \curvearrowright X$ est 2-transitive, alors elle est primitive.*

Preuve : exo. Soit $\sim$ une relation d'équivalence invariante sur X. Si $\sim$ n'est pas la relation grossière, il existe x, y avec $x \not\sim y$. Si $\sim$ n'est pas la relation d'égalité, il existe $x' \neq y'$ avec $x' \sim y'$. Par 2-transitivité, il existe g tq $gx = x'$, $gy = y'$, et $\sim$ n'est pas invariante. □

Exemple : l'action de S_n sur $\{1, \ldots, n\}$ est 2-transitive donc primitive.

L'action de $O_n(\mathbb{R})$ sur la sphère unité S^{n-1} de $\mathbb{R}^n$ est transitive, mais pas primitive. En effet, la relation d'antipodie (définie par $x \sim y$ si $x = \pm y$) est une relation d'équivalence invariante.

De même, l'action de $GL_n(K)$ sur $K^n \setminus 0$ est transitive mais n'est pas primitive (sauf pour $K = \mathbb{Z}/2\mathbb{Z}$) puisque la relation de proportionnalité [6] est une relation d'équivalence invariante (mais pour $K = \mathbb{Z}/2\mathbb{Z}$, c'est la relation d'égalité...).

Par contre, pour $n \geq 2$, l'action de $GL_n(K)$ sur l'espace projectif $\mathbb{P}^{n-1}K$ est 2-transitive donc primitive.

L'action du groupe des rotations $SO_2(\mathbb{R})$ sur S^1 est transitive, mais elle n'est pas primitive : la relation d'antipodie est une relation d'équivalence invariante non triviale. Pour la même raison, l'action de $SO_n(\mathbb{R})$ sur S^{n-1} n'est pas primitive. Par contre, on verra pour $n \geq 3$, $SO_n(\mathbb{R})$ sur $P^{n-1}(\mathbb{R})$ est primitive (mais pas pour $n = 2$, voyez vous pourquoi ?).

6. définie par $v \sim w$ si il existe $\lambda \in K^*$ tq $w = \lambda v$

Lorsqu'on a une action transitive $G \curvearrowright X$, si on fixe $x_0 \in X$, il y a une bijection équivariante $G/G_{x_0} \to X$: l'application orbitale $g \mapsto gx_0$ passe au quotient en une bijection $G/G_{x_0} \to X$ (la surjectivité vient du fait que $G \curvearrowright X$ est transitive).

Définition 27. *Sous-groupe maximal : soit G un groupe et H un sous-groupe de G. On dit que H est un sous-groupe maximal de G si $H \subsetneq G$ et si les seuls sous-groupes de G contenant H sont H et G.*

Exercice (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 surjective G-équivariante $f : X \twoheadrightarrow Y$, alors soit Y est réduit à un point, soit f est bijective.

(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

III.2 Le théorème d'Iwasawa

Ref : [CG17, I. Exo C10] ou [Gro01, Thm 0.5]

Théorème 28 (Critère de simplicité d'Iwasawa)**.** *Soit $G \curvearrowright X$ une action d'un groupe G non-trivial sur un ensemble X, et soit $x_0 \in X$. On suppose :*

(a) G est parfait (ie $G = D(G)$, ie tout quotient abélien de G est trivial).

(b) l'action $G \curvearrowright X$ est fidèle et primitive

(c) G_{x_0} contient un sous-groupe abélien[7] $A_{x_0} \lhd G_{x_0}$ distingué dans G_{x_0} et tel que ses G-conjugués engendrent G : $\langle A_{x_0}^g | g \in G \rangle = G$

Alors G est simple.

Preuve. Commençons par la remarque suivante : a tout $x \in X$, on peut associer de manière canonique un sous-groupe $A_x \lhd G_x$ de la façon suivante : on choisit $g \in G$ tq $gx_0 = x$, et on définit $A_x := gA_{x_0}g^{-1}$. Comme A_{x_0} est distingué dans G_{x_0}, on vérifie que ça ne dépend pas du choix de g : si g' est un autre élément tq $g'x_0 = x$, alors $g^{-1}g'x_0 = x_0$ donc $g^{-1}g' \in G_{x_0}$ normalise A_{x_0} donc $g^{-1}g'A_{x_0}g'^{-1}g = A_{x_0}$, et $g'A_{x_0}g'^{-1} = gA_{x_0}g^{-1}$. L'hypothese 3 dit que le groupe engendré par l'ensemble des groupes A_x est G tout entier.

Soit maintenant $N \lhd G$ un sous-groupe normal non trivial. La relation "être dans la même N-orbite" est une relation d'équivalence qui est G-invariante (parce que N est normal) :

$$x \sim y \text{ ssi } x \in Ny \text{ ssi } gx \in gNy \text{ ssi } gx \in Ngy \text{ ssi } gx \sim gy.$$

C'est donc la relation triviale ou grossière.

Si c'est la relation triviale, alors $Nx = \{x\}$ pour tout x donc N est dans le noyau de l'action et l'action n'est pas fidèle, contradiction. Donc c'est la relation grossière, autrement dit N agit transitivement sur X.

Considérons maintenant l'application quotient $\pi : G \to G/N$. On sait que $G = \langle A_x | x \in X \rangle = \langle A_{hx_0} | h \in N \rangle = \langle A_{x_0}^h | h \in N \rangle$. Mais tous les groupes $A_{x_0}^h$ ont la même image par π (puisque $h \in \ker \pi$), donc $\pi(G) = \pi(A_{x_0})$, donc $\pi(G)$ est abélien. Comme G est parfait, $\pi(G)$ est trivial, ie $N = G$.

□

7. Résoluble suffit

III.3 Simplicité de A_5

III.4 Simplicité de A_5 par Iwasawa

Pour éviter la confusion entre le groupe A_{x_0} du lemme d'Iwasawa et le groupe alterné $\mathbb{A}_n$, je note $\mathbb{A}_n$ le groupe alterné.

Théorème 29. *$\mathbb{A}_5$ est simple.*

Lemme 30. *Pour $n \geq 5$, A_n est parfait, et est engendré par ses doubles transpositions.*

Preuve : exo. Commençons par vérifier que $\mathbb{A}_n$ est parfait pour $n \geq 5$: $\mathbb{A}_n$ est engendré par les 3-cycles, il suffit donc de voir qu'un 3-cycle est un commutateur : d'abord dans S_3 :

$$[(12),(13)] = (12) \circ (13) \circ (12) \circ (13) = (123)$$

puis dans $\mathbb{A}_5$: c'est un commutateur de doubles transpositions obtenues en composant avec (45)

$$(12)(45) \circ (13)(45) \circ (12)(45) \circ (13)(45) = (123) \circ (45)^4 = (123)$$

puisque (45) commute avec les permutations de support dans $\{1,2,3\}$. Comme tous les 3-cycles sont conjugués dans S_n, donc dans $\mathbb{A}_n$ si $n \geq 5$, tous les 3-cycles sont des commutateurs, et $\mathbb{A}_n$ est parfait pour $n \geq 5$.

Cet argument montre en même temps que tout 3-cycle est produit de double transpositions, et donc que $\mathbb{A}_n$ est engendré par ses doubles transpositions pour $n \geq 5$. □

Preuve de la simplicité de A_5. $\mathbb{A}_5$ agit sur $[\![1,5]\!]$, et vérifions que le critère d'Iwasawa s'applique. Il y a 2 ingrédients a voir : $\mathbb{A}_5$ est parfait et est engendré par ses doubles transpositions (c'est vrai pour tout $n \geq 5$).

Vérifions que le critère d'Iwasawa s'applique.

- $\mathbb{A}_5$ est parfait
- l'action est 2-transitive donc primitive, et fidèle
- Le stabilisateur de $x_0 = 5$ est isomorphe à $\mathbb{A}_4$, il a un sous-groupe distingué abélien A qui est son groupe de Klein des doubles transpositions. De plus comme $\mathbb{A}_5$ est engendré par ses doubles transpositions, les conjugués de A engendrent $\mathbb{A}_5$.

Conclusion : le lemme d'Iwasawa s'applique et $\mathbb{A}_5$ est simple. □

IV. Groupe orthogonal

Ref : [Per95].

IV.1 Simplicité de $PSO_n(\mathbb{R})$ pour $n \geq 3$ impair par Iwasawa

Pour n pair, $SO_n(\mathbb{R})$ contient l'homothétie $-id$, et n'est donc pas simple. On considère donc $PSO_n(\mathbb{R})$ le quotient de $SO_n(\mathbb{R})$ par les homothéties qu'il contient, c'est à dire $PSO_n(\mathbb{R}) = SO_n(\mathbb{R})$ si n est impair, et $PSO_n(\mathbb{R}) = SO_n(\mathbb{R})/\{\pm Id\}$ si n pair.

Théorème 31. *$SO_3(\mathbb{R})$ est simple, et pour tout $n \geq 5$, $PSO_n(\mathbb{R})$ est simple.*

Le but de cette section est de montrer que $SO_3(\mathbb{R})$ est simple en appliquant Iwasawa. Quasiment la même preuve donne la simplicité de $SO_n(\mathbb{R})$ pour n impair.

Commençons par voir qu'il est parfait.

Proposition 32. *$SO_3(\mathbb{R})$ est engendré par ses renversements et est parfait.*

Plus généralement, on a

Proposition 33. *(a) Pour tout n, $O_n(\mathbb{R})$ est engendré par ses réflexions, et le groupe dérivé de $O_n(\mathbb{R})$ est $SO_n(\mathbb{R})$.*

(b) *Pour $n \geq 3$, $SO_n(\mathbb{R})$ est engendré par ses renversements et est parfait (pour $n = 2$, $SO_2(\mathbb{R})$ est abélien et n'est donc pas parfait, il n'est pas non plus engendré par son unique renversement qui est $-id$).*

On admet pour l'instant la proposition (voir les compléments) et on en déduit la simplicité via Iwasawa.

Quelle action utiliser ? L'action de $SO_3(\mathbb{R})$ sur la sphere unité S^2 n'est pas 2-transitive (parce que $SO_3(\mathbb{R})$ préserve la distance, donc ne peut pas envoyer une paire de points à distance d sur une paire de points à distance $d' \neq d$.

Elle n'est pas non plus primitive : il y a une relation d'équivalence invariante : la relation d'antipodie définie par $x \sim y$ si $x = \pm y$.

Du coup, on va plutôt utiliser l'action de $SO_3(\mathbb{R})$ sur $P^3(\mathbb{R})$ auquel on peut aussi penser comme au quotient de la sphère par la relation d'antipodie, ou encore comme à l'ensemble des paires de points antipodaux sur la sphère.

Cette action n'est toujours pas 2-transitive (la distance entre 2 paires de points est un invariant), mais elle est primitive.

Proposition 34. *L'action de $SO_3(\mathbb{R})$ sur $P^2(\mathbb{R})$ est primitive.*

Plus généralement, pour tout $n \geq 3$, l'action de $SO_n(\mathbb{R})$ sur $P^{n-1}(\mathbb{R})$ est primitive.

Preuve. On fait la preuve dans le cas $n = 3$, voir les notes de bas de page pour $n \geq 3$ quelconque.

Soit $\sim_{P^2}$ une relation d'équivalence invariante sur $P^2(\mathbb{R})$. Sa préimage $\sim = \sim_{S^2}$ dans S^2 (définie par $x \sim_{S^2} y$ si $\pi(x) \sim_{P^2} \pi(y)$) est une relation d'équivalence tq $x \sim -x$. Si $\sim_{P_2}$ n'est pas la relation d'égalité, c'est qu'il existe $a, b \in S^2$ tq $a \sim b$ mais $a \neq \pm b$. C'est notre point de départ et on veut montrer que $\sim$ est la relation grossière ce qui signifie que $\sim_{P^2}$ etait la relation grossière. [8]

Regardons l'orbite de a sous l'action du stabilisateur de b : $C = \{ga | g \in G_b\}$. Pour tout $g \in G_b$, le point $a' = ga \in C$, vérifie $a' \sim b$ puisque g envoie la paire (b, a) sur (b, a') et que $\sim$ est G-invariante. [9]

Le groupe G_b est l'ensemble de toutes les rotations d'axe (Ob) et C est donc un cercle passant par a et orthogonal a la droite (Ob). Ce cercle n'est pas réduit à un point car a n'est pas sur l'axe (Ob). Puisque pour tout $a' \in C$, $a \sim a'$, si on fait tourner C par des rotations d'axe (Oa) on obtient des points dans la classe d'équivalence de a. [10]

Affirmation : $\bigcup_{r \in G_a} r(C)$ contient un voisinage de a dans S. [11]

L'affirmation implique en particulier donc qu'on a tout un voisinage de a qui est équivalent à a.

Pour démontrer l'affirmation considérons a' un point dans $C \setminus \{a\}$, et soit $\eta = d(a, a')$. On a les 2 points suivants : [12]

(a) par le thm des valeurs intermédiaires, pour tout $d \in [0, \eta]$, C contient des points à distance exactement d de a

(b) deux points $v, v' \in S$ a même distance de a sont images l'un de l'autre par un élément de G_a

Ces deux points sont clairs géométriquement. [13] Les deux points démontrent ensemble l'affirmation : en effet, pour tout point c de S tq $d(c, a) \leq \eta$, (1) il existe $c' \in C$ tq $d(a, c) = d(a, c')$, et (2) que c et c' sont dans la meme orbite sous G_a donc $c \in \bigcup_{r \in G_a} r(C)$.

8. Jusque là, ça marche exactement pareil en toute dimension : en prenant pour S la sphère unité de $\mathbb{R}^n$

9. ça marche encore exactement pareil en toute dimension

10. Pour $n \geq 3$, on peut prendre un sous-espace de dimension 3 contenant a, b (qui sont non colinéaires), disons $V = Vect(a, b, c)$, et prendre C l'orbite par le groupe les rotations de V d'axe b, étendues par l'identité sur $V^\perp$. C'est un cercle dans le plan passant par a parallele a $(V + \mathbb{R}b)^\perp$.

11. L'énoncé de l'affirmation est inchangé en dimension n, mais le groupe G_a est isomorphe à $SO_{n-1}(\mathbb{R})$

12. L'énoncé des 2 points ne change pas en dimension n, sauf que G_a est plus compliqué en dimension n.

13. en dimension 3

Details pour le premier point : on a $a' = r_{\theta_0}(a)$ où r_θ est la rotation[14] d'angle θ autour de l'axe (Ob) ; on applique le théorème des valeurs intermédiaires à la fonction $\theta \in [0, \theta_0] \mapsto d(a, r_\theta(a))$.

Details pour le deuxième point : on se place dans une BON $(e_1, e_2, a = e_3)$, on écrit $v = (x, y, z)$, $v = (x', y', z')$; puisque $x^2 + y^2 + z^2 = 1$, on a $d(a, v)^2 = x^2 + y^2 + (z-1)^2 = 1 - z^2 + (z-1)^2 = -2z + 2$. Donc $d(a, v) = d(a, v')$ implique qu'ils ont la meme cordonnée $z = z'$, ils sont donc dans le meme cercle d'axe (Oa) et sont donc dans la même orbite sous l'action du groupe de rotations d'axe (Oa).[15]

Utilisation de l'affirmation. On a montré que la classe de a contient un voisinage de a. Comme l'action de SO_3 est transitive, et que $\sim$ est invariante, la classe de n'importe quel point $x \in S^2$ contient un voisinage de x. Autrement dit, chaque classe d'équivalence $[x]$ est ouverte.

Le complémentaire de $[x]$ est aussi ouvert, puisque c'est une union de classes d'équivalences qui sont elles-mêmes ouvertes. Comme S^2 est connexe, il n'y a donc qu'une seule classe d'équivalence, ie $\sim$ est grossière.[16] □

Théorème 35. *$SO_3(\mathbb{R})$ est simple.*

Preuve. On utilise Iwasawa. $SO_3(\mathbb{R})$ est parfait. L'action sur $P^2(\mathbb{R})$ est primitive. Elle est fidèle parce que le noyau de l'action de $GL_3(\mathbb{R})$ sur $\mathbb{P}^2(\mathbb{R})$ est l'ensemble des homothéties, mais $SO_3(\mathbb{R})$ ne contient pas d'homothétie à part I_3 (puisque $-I_3$ est de déterminant -1).

Soit $x_0 \in S^2$ et $[x_0] \in \mathbb{P}^2(\mathbb{R})$ son image. $G_{[x_0]}$ est le stabilisateur d'une paire de points antipodaux $\{\pm x_0\}$ dans S^2. Soit $A_{[x_0]}$ le stabilisateur de x_0 : c'est le groupe des rotations d'axe (Ox_0), et c'est un sous-groupe normal d'indice 2 de $G_{[x_0]}$. Toute élément de $SO_3(\mathbb{R})$ est conjugué a un élément de A_{x_0} donc $\langle A_{x_0}^g | g \in SO_3(\mathbb{R})\rangle = SO_3(\mathbb{R})$.

Iwasawa s'applique ! □

Théorème 36. *Pour $n \geq 3$ impair, $SO_n(\mathbb{R})$ est simple.*

Preuve. On applique Iwasawa a l'action sur $\mathbb{P}^{n-1}(\mathbb{R})$: elle est primitive, et elle est fidèle pour la même raison qu'au-dessus. On sait aussi que $SO_n(\mathbb{R})$ est parfait pour tout $n \geq 3$ (pair ou impair).

Reste a comprendre le stabilisateur G_{x_0} d'un point $x_0 \in \mathbb{P}^{n-1}$. Si on prend une BON $e_1, \ldots, e_n$ avec $[e_n] = x_0$, G_{x_0} est l'ensemble des matrices $\begin{bmatrix} A & \\ & \varepsilon \end{bmatrix}$ avec $A \in O_{n-1}$, $\varepsilon \in \{\pm 1\}$, et $\varepsilon \det(A) = 1$. Puisque n est impair, G_{x_0} contient l'involution $J = \begin{bmatrix} -I_{n-1} & \\ & 1 \end{bmatrix}$, et le groupe $A_{x_0} = \langle J \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ est un sous-groupe abélien distingué de G_{x_0}.

Il reste à montrer que $\langle A_{x_0}^g | g \in SO_n(\mathbb{R})\rangle = SO_n(\mathbb{R})$. Notons que $\langle A_{x_0}^g | g \in SO_n(\mathbb{R})\rangle$ est un sous-groupe normal de $SO_n(\mathbb{R})$ par définition. Pour $n = 3$, J est un retournement, et on sait que tous les retournements sont conjugués et que $SO_3(\mathbb{R})$ est engendré par les retournements, donc $\langle A_{x_0}^g | g \in SO_3(\mathbb{R})\rangle = SO_3(\mathbb{R})$. Si n quelconque, $\langle A_{x_0}^g | g \in SO_n(\mathbb{R})\rangle$ contient $J' = \begin{bmatrix} 1 & \\ & -I_{n-1} \end{bmatrix}$, car J' est conjuguée à J dans $SO_3(\mathbb{R})$, et contient donc JJ' qui est un retournement. Comme tous les retournements sont conjugués, $\langle A_{x_0}^g | g \in SO_n(\mathbb{R})\rangle$ les contient tous, et puisque $SO_n(\mathbb{R})$ est engendré par les retournements, $\langle A_{x_0}^g | g \in SO_n(\mathbb{R})\rangle = SO_n(\mathbb{R})$.

Le théorème d'Iwasawa s'applique donc. □

IV.2 Passage de A_5 à A_n, et de SO_5 à SO_n

On va appliquer le théorème ci-dessous à A_n en prenant pour $\mathcal{F}$ les 3-cycles, et Z le groupe trivial. Il faudra la version avec $Z = \{\pm \mathrm{id}\} \subset SO_n$: ca sera le centre dans les 2 cas.

14. si $n \geq 3$, r_θ est la rotation d'angle θ autour de l'axe (Ob) dans V, et est l'identité sur $V^\perp$

15. Version en dimension n : on se place dans un espace W de dimension 3 contenant a, v, v', et on ne considère que des rotations de W étendues par l'identité sur $W^\perp$: le même argument fonctionne

16. l'argument est le meme en toute dimension : l'action de SO_n sur la sphère unité S est transitive, donc toutes les classes d'équivalences sont ouvertes, et on conclut par connexité de S.

Proposition 37. *Soit $G \curvearrowright X$ une action transitive (pas forcément primitive). Soit $x_0 \in X$ et supposons que G_{x_0} soit simple, et que le sous-groupe engendré par tous les conjugués de G_{x_0} est égal à G.*

On suppose aussi qu'il existe un ensemble $\mathcal{F} \subset G$ (et un sous-groupe distingué $Z \triangleleft G$) et formé d'éléments « ayant beaucoup de points fixes » au sens suivant : pour tout élément $g \in G \setminus Z$, il existe $f \in \mathcal{F}$ ne commutant pas avec g et tel que f et gfg^{-1} ont un point fixe commun.

Alors G/Z est simple.

Preuve. Soit $\bar{N} \triangleleft G/Z$ un sous-groupe normal non trivial, et N sa préimage dans G : c'est un sous-groupe normal de G tq $Z \subsetneq N$. Il suffit de montrer que $N = G$, ca impliquera $\bar{N} = G/Z$.

Soit $n \in N \setminus Z$, et soit $f \in \mathcal{F}$ ne commutant pas avec n et tq f et gfg^{-1} ont un point fixe commun. Le commutateur $[f, g] = f.gf^{-1}g^{-1}$ est non trivial, et a un point fixe $x \in X$. Il appartient à N parce que $[f, g] = fgf^{-1}.g^{-1}$.

Comme l'action sur X est transitive, G_x est conjugué à G_{x_0} donc simple. Comme $N \cap G_x$ est non-trivial (il contient $[f, g]$), on a donc $G_x \subset N$. Comme N est normal, il contient tous les conjugués de G_x, mais par hypothèse, ils engendrent G donc $N = G$. □

Corollaire 38. *Pour $n \geq 6$, A_{n-1} est simple $\Rightarrow$ A_n simple*

Preuve. Appliquer la proposition avec $X = [\![1, n]\!]$, et $\mathcal{F}$ les 3-cycles et $Z = \{1\}$. $G_{x_0} \simeq A_{n-1}$ est simple et contient un 3-cycle. Comme les 3-cycles engendrent A_n, les conjugués de G_{x_0} aussi. Pour la condition sur les points fixes :

Soit $g \in G \setminus 1$. Si on prend un 3-cycle $f = (abc)$ de support $S = \{a, b, c\}$ alors gfg^{-1} a pour support $g(S)$ Puisque $n \geq 6$, si $S \cup g(S)$ est de cardinal ≤ 5, on a donc que l'existence d'un point fixe commun. Etant donné g on veut donc choisir notre 3-cycle f tq $g(S) \neq S$ mais $g(S) \neq S$.

puisque $g \neq 1$, il existe a tq $g(a) \neq a$. On prend $b = g(a)$, et $c \neq a, b, g(b)$.

□

Corollaire 39. *Pour $n \geq 6$ pair, $SO_{n-1}(\mathbb{R})$ est simple $\Rightarrow$ $PSO_n(\mathbb{R})$ simple.*

Conclusion : pour $n \geq 3$ et tout $n \geq 5$, $PSO_n(\mathbb{R})$ est simple.

Preuve. Soit $n \geq 6$ pair. On applique la proposition avec $G = SO_n(\mathbb{R})$, $Z = \{\pm \mathrm{id}\}$, pour l'action sur $X = S$ la sphère unité de $\mathbb{R}^n$. Pour $x \in S$, $G_x \simeq SO_{n-1}(\mathbb{R})$ est bien simple puisque $n - 1$ est impair. G_x contient un renversement, le sous-groupe engendré par les conjugués de G_x est donc égal à $SO_n(\mathbb{R})$. On prend pour $\mathcal{F}$ la famille des renversements : un renversement a un espace de point fixe de codimension 2, l'intersection de de sous-espaces de codimension 2 est de codimension ≤ 4, donc de dimension $\geq 2 > 0$ puisque $n \geq 6$. Donc 2 renversements quelconques ont un point fixe commun non nul, donc un point fixe commun dans S. Il suffit donc de voir que si $g \notin Z$, il existe un renversement avec lequel il ne commute pas. Comme g n'est pas une homothétie, il existe v tq v, gv ne sont pas colinéaires. Si on prend f un renversement dont l'espace de points fixes plan contient v mais pas gv, alors g ne préserve pas $Fix(f)$ et donc f, g ne comuttent pas. □

IV.3 Complements sur le groupe orthogonal

Définition 40. *Une réflexion orthogonale est une symétrie orthogonale par rapport à un hyperplan*

Théorème 41. *$O(n)$ est engendré par les réflexions : toute isométrie est le produit d'au plus n réflexions.*

Pour démontrer le thm on utilise le lemme suivant

Lemme 42. *Pour toute paire de vecteurs unitaires $v \neq v' \in \mathbb{R}^n$, il existe une réflexion orthogonale σ qui échange v et v'.*

Preuve. En effet, la réflexion σ par rapport au plan médiateur de v et v' (ie par rapport à $(v'-v)^\perp$) convient. Matriciellement, si on voit $u = \frac{v'-v}{||v'-v||} \in \mathbb{R}^n$ comme une matrice colonne, c'est la matrice de Householder $\sigma = Id - 2^t uu$ ([17]). □

Preuve du thm. Soit M orthogonale. On montre qu'il existe des reflexions orthogonales $\sigma_1, \dots, \sigma_n$ tq $\sigma_1 \dots \sigma_n M = \mathrm{id}$. On le montre par recurrence sur n.

Si $Me_1 \neq e_1$, le lemme dit qu'il existe une réflexion orthogonale σ tq σM fixe e_1. Si $Me_1 = e_1$, c'est encore vrai avec $\sigma = \mathrm{id}$.

Comme $e_n^\perp$ est σM-invariant, $\sigma M = \begin{bmatrix} 1 & 0 \\ 0 & M' \end{bmatrix}$. Par recurrence, on peut trouver des σ_i (réflexions orthogonales ou l'identité) tq $\sigma_1 \dots \sigma_{n-1} M' = \mathrm{id}$. Les matrices $\tilde{\sigma}_i = \begin{bmatrix} 1 & 0 \\ 0 & \sigma_i \end{bmatrix}$ sont des réflexions orthogonales ou l'identité et on a $\tilde{\sigma}_1 \dots \tilde{\sigma}_{n-1} \sigma M = \mathrm{id}$. □

Théorème 43 (Variante, voir [Cia98] : decomposition QR via les matrices de Householder)**.** *toute matrice $M \in GL(n, \mathbb{R})$ s'écrit sous la forme QR avec R triangulaire supérieure a coef diagonaux positifs, et Q produit d'au plus n réflections (matrices de Householder)*

Preuve. le thm 41 implique le thm 39 : si $M \in O(n)$, R est aussi dans $O(n)$; R^{-1} est triangulaire supérieure à coef diagonaux positifs (c'est un groupe) mais puisque R orthogonale, $R^{-1} = R^t$, donc R^t est triangulaire supérieure. Donc R diagonale. Les coef sont > 0 et dans ± 1 donc $R = id$.

On démontre le point 2 du thm par récurrence sur n. On le démontre sous la forme : il existe $\sigma_1, \dots, \sigma_n \in O(n)$ avec σ_i une réflexion orthogonale ou l'identité tq $\sigma_1 \dots \sigma_n M$ soit triangulaire supérieure a coef diagonaux positifs.

Si $n = 1$: c'est facile : M est un réel, $\sigma_1 = \pm 1$, et $R = |M|$.

Cas général : soit $e_1' = Me_1/||Me_1||$. Si $e_1 \neq e_1'$, considérons σ une réflexion orthogonale tq $\sigma e_1' = e_1$; si $e_1' = e_1$ on prend $\sigma = id$. σM envoie e_1 sur $||e_1'||e_1$. La matrice σM est donc de la forme $\begin{bmatrix} ||e_1'|| & * \\ 0 & M' \end{bmatrix}$. Par recurrence, on peut écrire $\sigma_1 \dots \sigma_{n-1} M' = R'$ avec σ_i réflexion orthogonale ou l'identité et R' triangulaire supérieure a coef diagonaux positifs. Les matrices $\begin{bmatrix} 1 & 0 \\ 0 & \sigma_i \end{bmatrix}$ sont des réflexions orthogonales ou l'identité et $\sigma_1 \dots \sigma_{n-1} \sigma M = \begin{bmatrix} ||e_1'|| & * \\ 0 & R' \end{bmatrix}$ CQFD □

Application à la résolution de systèmes : pour résoudre $MX = b$, on détermine des σ_i tq $M = \sigma_1 \dots \sigma_k R$. $MX = b$ ssi $RX = \sigma_k \dots \sigma_1 b$. On calcule donc $b' = \sigma_k \dots \sigma_1 b$ puis on résoud le système triangulaire $RX = b'$.

Avantage : tous les systèmes intermédiaires ont le même conditionnement que le système initial. Autrement dit, les matrices $\sigma_1 \dots \sigma_k M = \sigma_i \dots \sigma_{k+1} R$ ont le même conditionnement que M (rappel : $cond(M) = |||M|||.|||M^{-1}|||$, et si on prend la norme d'opérateur associée à la norme euclidienne, multiplier à droite ou à gauche par une matrice orthogonale ne change pas son conditionnement). Ceci signifie en pratique que c'est une méthode très stable numériquement.

Générateurs de $SO(n)$

Définition 44. *Un renversement dans $SO_n(\mathbb{R})$ (ou demi-tour dans $SO(3)$) est une symétrie orthogonale par rapport à un sous-espace de codimension 2.*

De manière équivalente, c'est une transformation orthogonale ayant $n-2$ valeurs propres égales à 1 et 2 vap égales à -1.

Théorème 45. *Pour $n \geq 3$ $SO_n(\mathbb{R})$ est engendré par ses demi-tours.*

Remarque 46. C'est faux pour $n = 2$ puisqu'il n'y a qu'un renversement qui est $-id$.

17. Verifier que $\sigma v = v'$ et $\sigma^2 = \mathrm{id}$ à partir de la formule définissant σ

Preuve. Commençons par le cas $n = 3$. Soit $M \in SO_n(\mathbb{R})$. C'est un produit d'un nombre pair de réflexions $M = \sigma_1 \dots \sigma_k$. Les $-\sigma_i$ sont des renversements, et puisque k est pair, $M = (-\sigma_1) \dots (-\sigma_k)$.

Cas $n \geq 3$ quelconque. Soit $M \in SO_n(\mathbb{R})$. Comme c'est un produit d'un nombre pair de réflexions, il suffit donc de montrer que le produit de 2 réflexions est aussi un produit de deux renversements.

Soient σ_1, σ_2 deux réflexions par rapport à deux hyperplans H_1, H_2, et $M = \sigma_1\sigma_2$. Si $H_1 = H_2$, $\sigma_1 = \sigma_2$, et $\sigma_1\sigma_2 = \mathrm{id}$ donc rien à faire. On suppose donc $H_1 \neq H_2$. $V = H_1 \cap H_2$ est de codimension 2, et M est l'identité sur V. $V^\perp$ est un plan M-invariant, et c'est une rotation de ce plan. Soit $v \in V$ un vecteur non nul (existe parce que $n \geq 3$!) et $W = V^\perp \oplus \langle v \rangle$. On a donc W de dimension 3, et $\mathbb{R}^n = W \oplus W^\perp$ avec $M_{|W^\perp} = \mathrm{id}$. Soit J l'application qui est $-id$ sur W et id sur $W^\perp$. On a que σ_2 et $J \circ \sigma_i$ est un renversement. De plus, J commute avec σ_i. Du coup, on a $M = (J \circ \sigma_1) \circ (J \circ \sigma_2)$ et M est donc un produit de 2 renversements. □

Lemme 47. *Pour tout $k \leq n$, $O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$ agissent transitivement sur l'ensemble des sous-espaces de dimension k de $\mathbb{R}^n$.*

Preuve. Soient H_1, H_2 deux sev de dimension k. Considérons une BON de H_i, et complétons la en une BON $\mathcal{B}_i$ de $\mathbb{R}^n$. L'application linéaire u envoyant $\mathcal{B}_1$ sur $\mathcal{B}_2$ est donc dans $O_n(\mathbb{R})$ et envoie H_1 sur H_2. Si u n'est pas dans $SO_n(\mathbb{R})$, $det(u) = -1$. Si $\mathcal{B}_2'$ est obtenue en changeant le signe d'un des vecteurs de $\mathcal{B}_2$, l'application u' envoyant $\mathcal{B}_1$ sur $\mathcal{B}_2'$ est de déterminant $\det(u') = -\det(u) = 1$, et envoie toujours H_1 sur H_2. □

Corollaire 48. *Dans $O_n(\mathbb{R})$ toutes les réflexions sont conjuguées.*
Dans $SO_n(\mathbb{R})$, tous les renversements sont conjugués.

Proposition 49. *(a) Pour tout n, le groupe dérivé de $O_n(\mathbb{R})$ est $SO_n(\mathbb{R})$.*

(b) Pour $n \geq 3$, le groupe dérivé de $SO_n(\mathbb{R})$ est $SO_n(\mathbb{R})$ (pour $n = 2$, $SO_2(\mathbb{R})$ est abélien et son groupe dérivé est donc trivial).

Preuve. 1. Clairement, $O_n(\mathbb{R})' \subset SO_n(\mathbb{R})$ puisque SO_n est le noyau du déterminant, qui est un morphisme vers un groupe abélien.

Pour l'autre inclusion, si $\varphi : O_n(\mathbb{R}) \to A$ est un morphisme vers un groupe abélien, il faut voir que $\varphi(SO_n(\mathbb{R})) = \{1\}$. Puisque les réflexions sont conjuguées, toutes les réflexions ont la même image dans A (puisque A est abélien) : on note $a \in A$ tq $a = \varphi(\sigma)$ pour toute réflexion σ. Puisque σ est une involution, $\varphi(\sigma)$ est d'ordre 1 ou 2. Tout élément de $SO_n(\mathbb{R})$ est un produit d'un nombre pair de réflexions, donc son image par φ est une puissance paire de a. Donc $\varphi(SO_n(\mathbb{R})) = \{1\}$.

Autre preuve de la 2eme inclusion : On écrit $M = \sigma_1 \dots \sigma_{2k} \in SO_n(\mathbb{R})$ comme un produit d'un nombre pair de reflections. Il suffit donc de voir que le produit $\sigma_1\sigma_2$ de 2 réflexions est un commutateur. Puisque $\sigma_2 = \sigma_2^{-1}$ est conjugué à σ_1^{-1}, $\sigma_1\sigma_2 = \sigma_1 g \sigma_1^{-1} g^{-1} = [\sigma_1, g]$. CQFD.

2. Il suffit de voir qu'un renversement est un commutateur. Comme ils sont tous conjugues, il suffit de voir qu'un certain reversement est un commutateur. On chosit un BON et considère les 3 renversements suivants (qu'on compléte par Id sur $e_4, \dots e_n$) : $\sigma_1 = \begin{bmatrix} 1 & & \\ & -1 & \\ & & -1 \end{bmatrix}$, $\sigma_2 = \begin{bmatrix} -1 & & \\ & 1 & \\ & & -1 \end{bmatrix}$, $\sigma_3 = \begin{bmatrix} -1 & & \\ & -1 & \\ & & 1 \end{bmatrix}$ (ce sont les renversement par rapport aux 3 axes de coordonnées dans $\mathrm{Vect}(e_1, e_2, e_3)$). On a $\sigma_1 = \sigma_2\sigma_3$, et $\sigma_3 = \sigma_3^{-1} = g\sigma_2^{-1}g^{-1}$ pour un certain g donc $\sigma_1 = [\sigma_2, g]$. □

IV.4 Structure de $PSO_4(\mathbb{R})$

Théorème 50. *Pour $n = 4$, $PSO_4(\mathbb{R})$ n'est pas simple : $PSO_4(\mathbb{R}) \simeq S/\{\pm 1\} \times S/\{\pm 1\} \simeq SO_3(\mathbb{R}) \times SO_3(\mathbb{R})$. où S est le groupe des quaternions de norme 1.*

Remarque 51. Ce théorème utilise le lien entre S et $SO_3(\mathbb{R})$, c'est à dire l'isomorphisme $S/\{\pm 1\} \simeq SO_3(\mathbb{R})$. Il vaut mieux commencer par comprendre cet isomorphisme avant de comprendre la structure de $SO_4(\mathbb{R})$.

Idée de preuve. Voir Perrin chapitre VII : le fait que $(S/\{\pm 1\}) \simeq SO_3(\mathbb{R})$ est un fait indépendant qui se démontre en regardant l'action de S par conjugaison sur $\mathbb{H}$, qui préserve le sous-espace des quaternions imaginaires purs.

Le groupe S des quaternions de norme 1 agit par translation à gauche sur $\mathbb{H} \simeq \mathbb{R}^4$, ce qui donne une action par isométrie sur $\mathbb{R}^4$. Il agit aussi par translation à droite, et on met ces 2 opérations ensemble : On regarde l'action de $S \times S \curvearrowright \mathbb{H}$ donnée par $(s, s').h = shs'^{-1} = sh\bar{s}'$. C'est une action à gauche par isométries, ce qui donne donc un morphisme $\varphi : S \times S \to O_4(\mathbb{R})$. Par connexité de $S \times S$ et par continuité du morphisme , il a valeurs dans $SO_4(\mathbb{R})$.

On obtient en composant par l'application quotient un morphisme $\bar{\varphi} : S \times S \to PSO_4$.

On montre facilement que $\ker \bar{\varphi}$ (qui est la preimage de $\pm id$ par φ) est $\{\pm 1\} \times \{\pm 1\}$, Par le thm d'isomorphisme il reste à voir que φ est surjectif (ce qui implique $\bar{\varphi}$ surjectif).

Soit H_0 le sous-espace des quaternions imaginaires purs (orthogonal de 1). On montre que l'image de φ contient le groupe fixant $1_{\mathbb{H}}$, isomorphe à $SO(H_0)$: par exemple en montrant que si $s \in S$ est imaginaire pur, $h \mapsto shs^{-1}$ fixe $1_{\mathbb{H}}$ et agit sur H_0 comme le renversement d'axe $\mathbb{R}s$. Comme les renversements engendrent $SO(\mathbb{H}_0)$ l'image de φ contient tout le stabilisateur de $1_{\mathbb{H}}$. Mais si $g \in SO(\mathbb{H})$ est quelconque, $s = g(1_{\mathbb{H}})$ est un élément de S, et en appliquant la translation à gauche par s^{-1} (qui est dans l'image de φ), on obtient un élément qui fixe $1_{\mathbb{H}}$, donc dans l'image de φ. □

V. Simplicité de A_n par Iwasawa

La preuve par de la simplicité de A_n directement par Iwasawa n'est pas la plus simple. Il faut trouver une action primitive telle que les stab de points aient un sous-groupe abelien normal, ca ne s'applique pas a l'action sur $[\![1, n]\!]$ pour $n \geq 6$. On note $\mathcal{P}_k([\![1, n]\!])$ l'ensemble des parties à k éléments.

V.1 Actions sur les parties à k éléments

On note $\mathcal{P}_k([\![1, n]\!])$ l'ensemble des parties à k éléments.

Proposition 52. *Soit $k \in [\![1, n-1]\!]$. L'action $S_n \curvearrowright \mathcal{P}_k([\![1, n]\!])$ est primitive sauf si $n = 2k$.*

Si $n = 2k$, l'action n'est pas primitive : la relation $P \sim P'$ définie par $P = P'$ ou $P = P'^c$ est une relation d'équivalence invariante sur $\mathcal{P}_k([\![1, n]\!])$.

Remarque 53. L'action n'est pas 2-transitive si $2 \leq k \leq n-2$. En effet, on peut trouver deux parties $A \neq B \in \mathcal{P}_k([\![1, n]\!])$ tq $A \cap B = k - 1$, et deux autres parties $A' \neq B' \in \mathcal{P}_k([\![1, n]\!])$ tq $A' \cap B' = k - 2$. La paire (A, B) et la paire (A', B') ne sont donc pas dans la même orbite.

Preuve. Note : si $k = 1$, c'est l'action de S_n $[\![1, n]\!]$ dont on sait qu'elle est 2-transitive.

L'action est clairement transitive. On veut mq $H = Stab([\![1, k]\!])$ est maximal. Comme $Stab([\![1, k]\!]) = Stab([\![k + 1, n]\!]) \simeq S_k \times S_{n-k}$, quitte à changer k en $n - k$, ops $k < 2n$. Autrement dit, en notant $A = [\![1, k]\!]$ et $B = [\![k + 1, n]\!]$, on a $|B| > |A|$.

Partant de $\sigma \notin H$, il suffit d'exhiber une transposition $\tau \in \langle \sigma, H \rangle$ qui échange un point de A et un point de B : par conjugaison par des éléments de H, on obtient toutes les transpositions à cheval sur A et B, et comme H contient toutes les autres transpositions, on les a toutes.

Soit $\sigma \notin H = \mathrm{Stab}(B)$. Il existe donc $i \in B$ tq $\sigma(i) \in A$. Mais ca ne peut pas etre le cas pour tout i sinon $\sigma(B) \subset B$, contredit $|B| > |A|$. Donc il existe aussi $j \in B$ tq $\sigma(j) \in B$. La transposition $\tau = (i, j)$ est dans $\mathrm{Stab}(B) = H$, et en conjugant τ par σ, on obtient la transposition $\tau' = (\sigma(i), \sigma(j))$ désirée. □

Proposition 54. *Soit $n \geq 3$ et $k \leq n$. Si $n \neq 2k$, l'action $A_n \curvearrowright \mathcal{P}_k(\llbracket 1, n \rrbracket)$ est primitive.*

Remarque 55. Pour $n = 2$, A_2 est trivial...

Preuve. Comme au-dessus, quitte a changer k en $n - k$, on suppose $k < n/2$. Le cas $k = 1$ est clair, puisque l'action est 2-transitive. On suppose donc $k \geq 2$, donc $n \geq 5$. On se donne $H = \mathrm{Stab}(\llbracket 1, k \rrbracket)$ et $\sigma \notin H$, on veut Mq $\langle H, \sigma \rangle = A_n$.

Comme au-dessus $i, j \in B$ tq $\sigma(i) \in A$ et $\sigma(j) \in B$. Comme $|B| > 3$, il existe $k \in B \setminus \{i, j\}$. Le 3-cycle $(i, j, k) \in H$ mais son conjugué par σ et un un 3-cycle τ dont le support est a cheval sur A et B.

Quitte a re-echanger A et B (on ne suppose donc plus $|A| < |B|$), ops que le support de τ a 2 point dans A et 1 dans B. Par conjugaison par H, on trouve tous les 3-cycles ayant un tel support, et pour avoir tous les 3-cycles, on veut mq $\langle \sigma, H \rangle$ contient tous les 3-cycles dont le support a 1 point dans A et 2 dans B. Il suffit d'en produire un.

Soit $\tau_0 = (1, 2, n) \in \langle \sigma, H \rangle$, avec $1, 2 \in A$, $n \in B$. Puisque $\#B \geq 2$, on trouve aussi $\tau_1 = (2, 1, n-1) \in \langle \sigma, H \rangle$ en conjugant par $(12)(n-1, n)$, et donc en faisant le produit $\tau' = (12n)(21, n-1) = (1, n-1, n)$ convient : son support a un point dans A et deux dans B. □

V.2 Preuve de la simplicité de A_n directe par Iwasawa

Simplicité de A_n. On a vu que A_n est parfait.

Pour $n \geq 5$, $n \neq 6$: on fait agir A_n sur $X = \mathcal{P}_3(\llbracket 1, n \rrbracket)$. L'action est primitive puisque $n \neq 6$ (Proposition 54).

L'action est fidèle : supposons que σ préserve toutes les parties à 3 éléments. Pour tout $x \in \llbracket 1, n \rrbracket$, on peut trouver A, B de cardinal 3 tq $A \cap B = \{x\}$ (car $n \geq 5$), donc $\{\sigma(x)\} = \sigma(A) \cap \sigma(B) = A \cap B = \{x\}$. On conclut que $\sigma = \mathrm{id}$ et donc que l'action est fidèle.

Soit $x_0 = \llbracket 1, 3 \rrbracket$, et H son stabilisateur. Le sous-groupe $A_{x_0} \lhd H$ des permutations (paires) qui sont l'identité sur $\llbracket 4, n \rrbracket$ est un sous-groupe distingué de H, isomorphe à $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$. Le groupe N engendré par les conjugués de A_{x_0} contient un 3-cycle, donc tous les 3-cycles (tous les 3-cycles sont conjugués dans A_n), donc est égal à A_n.

Le critère d'Iwasawa s'applique donc et dit que A_n est simple pour $n \neq 6$.

Pour $n = 6$, on fait agir A_6 sur $\mathcal{P}_2(\llbracket 1, 6 \rrbracket)$. Elle est fidèle et primitive comme au-dessus. Pour $x_0 = \llbracket 5, 6 \rrbracket$, le stabilisateur H de $\llbracket 5, 6 \rrbracket$ a comme sous-groupe distingué A_{x_0} le groupe de Klein de $\llbracket 1, 4 \rrbracket$ (les trois doubles transpositions et l'identité). Le groupe engendré par les conjugués de A_{x_0} est un sous-groupe normal contenant toutes les doubles transpositions (elles sont toutes conjuguées dans A_n), et donc le 3-cycle $(12)(34) \circ (12)(45) = (345)$ □

Remarque 56. Pour $n = 5$, on aussi faire agir A_5 sur $X = \llbracket 1, 5 \rrbracket$. L'action est 2-transitive donc primitive. Elle est clairement fidèle.

Soit $x_0 = 1$ et $H = G_{x_0} \simeq A_4$. Le groupe de Klein $K \lhd H \simeq A_4$ des doubles transpositions est abélien normal. Soit N le groupe engendré par les conjugués de G_{x_0}. N est un sous-groupe normal de A_5. Il suffit de montrer qu'il contient un 3-cycle. Il contient toutes les doubles transpositions de A_5. Comme $(12)(34) \circ (12)(45) = (345)$, il contient un 3-cycle donc tous les 3-cycles CQFD.

V.3 Complements sur S_n et A_n

Théorème 57. *Il existe un unique morphisme $\varepsilon : S_n \to \{\pm 1\}$ qui envoie chaque transposition sur -1.*

Par définition, A_n est le noyau de ε.

Preuve. L'unicité découle du fait que les transpositions engendrent. L'existence n'est pas évidente.

Une preuve possible (voir [Lan02]) : On regarde l'action (à droite) de S_n sur les polynômes à n variables $\mathbb{Q}[X_1, \ldots, X_n]$: On note $P \circ \sigma$ l'action de σ sur P, qu'on voit comme

composition de P par l'automorphisme de $\mathbb{Q}[X_1, \ldots, X_n]$ qui envoie X_i sur $X_{\sigma(i)}$. On vérifie que l'action d'une transposition sur le polynôme $P = \prod_{i<j}(X_i - X_j)$ l'envoie sur son opposé. Une fois que c'est fait, en utilisant que S_n est engendré par ses transpositions, on obtient que le groupe S_n préserve donc l'ensemble $\pm P$, et on définit $\varepsilon(\sigma) \in \{\pm 1\}$ tq $P \circ \sigma = \varepsilon(\sigma) \times P$. □

Remarque 58. $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$. A_2 est le groupe trivial. $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$.

Théorème 59. *S_n est engendré par ses transpositions.*
A_n est engendré par ses 3-cycles.
Pour $n \neq 5$, A_n est aussi engendré par ses doubles transpositions.

Preuve. 1. Par rec sur n. OK pour $n = 1$ et 2. Soit $\sigma \in S_n$. Si $\sigma(n) = n$, OK par recurrence. Sinon soit $i = \sigma(n)$, et $(i, n) \circ \sigma$ fixe n.

2. Par rec sur n. OK pour $n = 1, 2$ (A_n est trivial !). OK aussi pour $n = 3 : A_3 = \mathbb{Z}/3\mathbb{Z}$. Soit $\sigma \in A_n$, $n \geq 3$. Si $\sigma(n) = n$, OK par recurrence. Sinon soit $i = \sigma(n)$, et $j \notin \{n, i\}$ (existe car $n \geq 3$). Alors $(j, i, n) \circ \sigma$ fixe n.

3. On commence par écrire un 3-cycle (ijk) comme produit de 2 transposition $(ijk) = (ij) \circ (jk)$. Comme $n \geq 5$, on peut trouver $l, m \notin \{i, j, k\}$, et on a le produit de 2 doubles transpositions $(ijk) = (ij)(lm) \circ (jk)(lm)$. □

Lemme 60. *Toutes les transpositions de S_n sont conjuguées.*
Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n (mais pas pour $n = 3$ ou $n = 4$).
Pour tout $n \geq 4$, doubles transpositions sont conjuguées dans A_n.

Définition 61. *Si G est un groupe, son groupe dérivé $D(G)$ est le sous-groupe de G engendré par les commutateurs $[g, h] = ghg^{-1}h^{-1}$.*

De manière équivalente, $D(G)$ est le plus petit noyau d'un morphisme de G vers un groupe abélien : $G/D(G)$ est abélien, et pour tout $\varphi : G \to A$ avec A abélien, $D(G) \subset \ker \varphi$.

Proposition 62 (Groupes dérivés)**.** *$D(S_n) = A_n$ pour tout n*
$D(A_n) = A_n$ pour $n \geq 5$.
Pour $n = 3$, $A_3 = \mathbb{Z}/3\mathbb{Z}$ et $D(A_3) = 1$. Pour $n = 4$, $D(A_4) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ est le groupe de Kleine, c'est à dire l'ensemble des doubles transpositions union l'identité (qui, seulement pour $n = 4$, forme un groupe[18] *!)*

Remarque 63. Pour $n = 4$, on a un morphisme de $S_4 \to S_3$ lié au faut qu'il y a dans $[\![1, 4]\!]$, il y 3 partitions en paires d'éléments[19], et S_4 agit naturellement sur ces partitions, ce qui donne un morphisme $S_4 \to S_3$. Lorsqu'on restreint à A_4, on obtient un morphisme $\rho : A_4 \to S_3$; les doubles transpositions sont dans le noyau de ce morphisme[20] et les 3 cycles non. Donc l'image des 3-cycles sont d'ordre 3, donc des 3-cycles de S_3, donc l'image de ρ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, sont noyau est le groupe de Kleine.

Preuve. $D(S_n) \subset A_n$ puisque A_n est le noyau du morphisme signature. Pour voir qu'on a égalité, il suffit de montrer que $S_n/D(S_n) \simeq \mathbb{Z}/2Z$. Les transpositions étant conjuguées, elles ont la même image dans $S_n/D(S_n)$. Cette image est un élément d'ordre 2 qui engendre $S_n/D(S_n)$ puisque S_n est engendré par ses tranpositions.

Pour $n \geq 5$, A_n est engendré par ses doubles transpositions qui sont conjuguées donc $A_n/D(A_n)$ est engendré par un seul élément d'ordre au plus 2, $A_n/D(A_n)$ est trivial ou $\mathbb{Z}/2\mathbb{Z}$. Mais A_n est aussi engendré par ses 3-cycles, deviennent triviaux dans $A_n/D(A_n)$ puisque leur image est d'ordre divisant 2 et 3. donc $A_n/D(A_n)$ est trivial. □

Théorème 64. *Pour $n \geq 5$, A_n est simple.*

1ere preuve [Per95, Th 8.1,p. 28]. On commence par A_5, on fera A_n par recurrence ensuite. On liste les 60 éléments de A_5 :

18. OK, pour $n \leq 3$ aussi vu qu'il n'y a pas de double transposition
19. $\{1, 2\} \cup \{3, 4\}$, $\{1, 3\} \cup \{2, 4\}$ et $\{1, 4\} \cup \{2, 3\}$ sont ces partitions
20. la double transposition (12)(34) fixe aussi les 3 partitions, y compris $\{1, 3\} \cup \{2, 4\}$ et $\{1, 4\} \cup \{2, 3\}$!

— id
— 3-cycles : il y en a 2 pour chaque support donc $\binom{5}{\times}3 = \binom{5}{\times}2 = \frac{5\times4}{2} \times 2 = 20$.
— 5-cycles : les 5-cycles sont tous conjugués dans S_5 (mais pas dans A_5), le centralisateur d'un 5-cycle est le groupe cyclique qu'il engendre, donc de cardinal 5, il y a donc $\frac{5!}{5} = 24$ 5-cycles. Il sont répartis en 2 classes de conj dans A_5
— les doubles transpositions : il y en a 3 par support, donc $5 \times 3 = 15$.

Un sous-groupe normal $N \triangleleft A_5$ qui contient un 3-cycle doit les contenir tous, et donc $N = A_5$ puisque les 3-cycles engendrent. Idem pour les doubles transposition. Donc N doit être formé de 5-cycles et l'identité. Les cardinaux possibles sont $1 + 12$ ou $1 + 24$, mais ca ne divise pas 60.

Ensuite on suppose A_{n-1} simple et $n \geq 6$, et on montre que A_n simple. Si $N \triangleleft A_n$, $N \cap A_{n-1}$ est un sous-groupe normal de A_{n-1} donc s'il est non trivial, $N \supset A_{n-1}$ donc contient un 3-cycle de A_n, donc les contient tous, donc $N = A_n$. Reste à voir $N \cap A_{n-1} \neq \{1\}$. En fait, il suffit de voir que N contient un élément ayant un point fixe.

Méthode : Si $N \triangleleft G$, le commutateur d'un élément $\nu \in N(^{21})$ avec n'importe quel élément $g \in G$ appartient à N : en effet, $[g, \nu] = g\nu g^{-1}\nu^{-1} = (g\nu g^{-1})\nu^{-1}$ est un produit de deux éléments de N. Le principe est que si g a beaucoup de points fixes, alors $[g, \nu] = g(\nu g^{-1}\nu^{-1})$ en aura beaucoup aussi. Par contre, il faut quand meme faire attention que $[g, \nu]$ ne soit pas l'identité pour que ça soit intéressant.

Soit $\nu \in N \setminus \{1\}$. On va prendre pour g un 3-cycle, de sorte que les supports de g et $\nu g^{-1}\nu^{-1}$ se chevauchent : on aura donc un support de cardinal ≤ 5 donc au moins un point fixe puisque $n \geq 6$.[22]

Si $\nu(1) = 1$, on n'a rien à faire (ν a déjà un point fixe), supposons donc que $i = \nu(1) \neq 1$. Soit $g = (1, i, j)$ un 3-cycle contenant $1, i$ (donc on veut $j \notin \{1, i\}$, on verra qu'on veut aussi $j \notin \{1, i, \nu(i)\}$, ce qui est toujours possible puisque $n \geq 6$). On a donc que $[g, \nu]$ a au moins un point fixe mais le risque est que ça soit l'identité, c'est à dire que g commute avec ν. Si c'est le cas, alors ν doit préserver le support $\{1, i, j\}$ de g, et $\nu_{|\{1,i,j\}}$ doit être un 3-cycle, ie $\nu_{|\{1,i,j\}} = (1, i, j)$. Si on a choisi $j \neq \nu(i)$, c'est bon. □

On va voir une autre preuve avec le critère d'Iwasawa, qui s'applique aussi à $PSL_n(K)$, et à $SO_3(\mathbb{R})$.

Corollaire 65. *Pour $n \geq 5$ les seuls sous-groupes distingués de S_n sont $\{1\}$, A_n et S_n.*

Preuve. Soit $N \triangleleft S_n$ non trivial. Si $N \cap A_n \neq 1$, alors par simplicité de A_n, $A_n \subset N \subset S_n$ donc N est égal à A_n ou S_n. Si $N \cap A_n = \{1\}$, alors $\#N \leq 2$ puisque A_n est d'indice 2, donc $N = \{1, \nu\} = \simeq \mathbb{Z}/2\mathbb{Z}$. Mais l'élément ν serait central dans S_n, ce qui est impossible : ν est un produit de transpositions à supports disjoints, soit (ij) une de ces transpositions. Si on choisit g tel que $g(i) = i$ et $g(j) \neq j$ (possible dès que $n \geq 3$), on voit que c'est impossible. □

Notons d'autres théorèmes de *rigidité* pour A_n et S_n.

Théorème 66. *Pour tout $n \neq 6$, tout automorphisme $\varphi : S_n \to S_n$ est intérieur : il existe $\tau \in S_n$ tel que pour tout $\sigma \in S_n$, $\varphi(\sigma) = \tau\sigma\tau^{-1}$.*

Schema de preuve, voir [Per95]. Partant de φ, il faut trouver une permutation τ qui fonctionne.

Une idée (qu'on ne va pas exactement suivre) serait de démontrer que si σ a un seul point fixe, alors $\varphi(\sigma)$ a un seul point fixe. Dans ce cas, τ devrait forcément envoyer le point fixe de σ sur celui de $\varphi(\sigma)$. Si le point fixe de $\varphi(\sigma)$ ne dépendait que du point fixe de σ et pas de σ elle même, on saurait comment construire τ.

Il se trouve que c'est plus facile de travailler avec les transpositions plutot qu'avec les permutations ayant un seul point fixe : on montre que le lemme suivant (vrai meme pour $n = 6$) :

21. la lettre n est prise !
22. Si $n \geq 7$, pour n'importe quel 3-cycle, on aura bien que $[g, \nu]$ a un point fixe. Attention quand meme à ce que g et ν ne commutent pas.

Lemme 67. *si φ envoie transposition sur transposition, alors φ est intérieur.*

Idee de preuve du lemme. Pour démontrer le lemme, on a que φ permet d'associer de manière naturelle à une paire d'éléments de $[\![1,n]\!]$ une autre paire d'éléments de $[\![1,n]\!]$. Pour construire τ on veut en déduire une façon d'associer à un élément de $[\![1,n]\!]$ un autre élément de $[\![1,n]\!]$. On utilise que deux transpositions commutent ssi leurs supports sont disjoints pour conclure. [23] □

Fin de la preuve du thm 66 en utilisant le lemme. Pour utiliser le lemme, on veut donc montrer que φ envoie transposition sur transposition. C'est automatique si $n \leq 3$ puisque ce sont les seuls éléments d'ordre 2.

Pour $n \geq 4$ le risque est que φ pourrait l'envoyer une transposition un produit de transpositions de supports disjoints. Comme $D(S_n) = A_n$, donc $\varphi(A_n) = A_n$, donc l'image d'une transposition doit etre un produit d'un nombre impair de transpositions, donc au moins 3, donc ça ne peut arriver que si $n \geq 6$.

On suppose donc $n \geq 7$, et on montre que le centralisateur d'une transposition n'est jamais isomorphe au centralisateur d'un produit de k transpositions à supports disjoints pour $k \neq 1$. La raison est que le centralisateur d'une transposition est isomorphe à $\mathbb{Z}/2 \times S_{n-2}$ alors que le centralisateur d'un produit de k transpositions possède un sous-groupe normal isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$, engendré par ces k transpositions. Mais $\mathbb{Z}/2 \times S_{n-2}$ n'a pas de tel sous-groupe normal parce que $n-2 \geq 5$, donc S_{n-2} n'a pas de sous-groupe normal abélien. □

Par contre, on a le joli théorème suivant :

Théorème 68. *S_6 possède un automorphisme qui n'est pas intérieur.*

La jolie preuve qui suit est expliquée en remarque 5.4(3) page 107 de [Per95].

Preuve. La preuve utilise l'action de $PGL_2(\mathbb{F}_5)$ sur la droite projective $D = \mathbb{P}^1(\mathbb{F}_5)$ qui a 6 éléments. On identifie donc $Sym(D)$ avec S_6 en choisissant une bijection de D avec $[\![1,6]\!]$. Cette action est fidèle : 3 points distincts de la droite projective forment un repère projectif, et tout élément de $PGL_2(\mathbb{F}_5)$ qui fixe ces 3 points est l'identité. L'image du morphisme $PGL_2(\mathbb{F}_5)$ dans $Sym(D) = S_6$ est un sous-groupe de $H \subset S_6$, isomorphe à $PGL_2(\mathbb{F}_5)$ puisque l'action est fidèle. Un calcul de cardinaux montre que $\#PGL_2(F_5) = 120 = \#S_5$, donc que H est d'indice 6 dans S_6. Ce sous-groupe H ne fixe aucun point dans $[\![1,6]\!]$ (puisque $PGL_2(\mathbb{F}_5)$ agit de manière transitive, voire 3-transitive sur la droite projective D).

On en déduit un automorphisme non intérieur de S_6 de la façon suivante (voir [Per95, Prop 8.10 p.33]. D'abord, on a une action de S_6 sur l'ensemble $X = S_6/H$, qui est de cardinal 6. En identifiant X avec $\{1,\dots,6\}$ ca donne donc un morphisme φ de S_6 dans lui-même. Mais H ne fixe aucun point dans $[\![1,6]\!]$ alors que H fixe un point dans X, donc $\varphi(H)$ fixe un point dans $[\![1,6]\!]$, ce qui empêche φ d'être intérieur. □

VI. Théoreme de Jordan-Holder

Référence : Rotman, an introduction to the theory of groups. Calais ?

Définition 69. *Soit G un groupe. Une filtration sous-normale de G est une suite de sous-groupes $1 = G_0 \lhd G_1 \lhd \dots \lhd G_n = G$ tels que G_i est distingué dans G_{i+1} pour tout $i < n$. L'entier n s'appelle la longueur de la filtration.*

Les n groupes G_1/G_0, G_2/G_1,..., G_n/G_{n-1} s'appellent les facteurs de la filtration.

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

23. à i_0 fixé, l'image des transpositions (i_0, j) sont $n-1$ transpositions dont aucune d'entre elles commutent. ca ne suffit pas a conclure, mais il suffit d'interdire que l'image de ces transposition contienne un triangle $(xy),(yz),(zx)$: la raison est que $(i_0a)(i_0b)(i_0c)$ est un 4-cycle alors que $(xy)(yz)(zx)$ est la transposition (zy).

Remarque 70. On ne suppose pas que G_i est distingué dans G.

Remarque 71. On rappelle que par convention, le groupe trivial n'est pas considéré comme un groupe simple. C'est analogue à la convention que 1 n'est pas un nombre premier, ce qui permet d'avoir l'unicité de la décomposition en nombres premiers. Le fait de ne pas considérer le groupe trivial comme un groupe simple permet de manière analogue d'avoir l'unicité dans le théorème de Jordan-Hölder.

Théorème 72 (Thèorème de Jordan-Hölder.)**.** *Soit G un groupe fini. Alors*

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

(b) toutes les filtrations de Jordan-Hölderde G ont la même longueur

(c) les classes d'isomorphisme des facteurs de la fitration sont uniques à permutation près : si 1 et G'_i sont deux filtrations de Jordan-Hölderde G, et si $Q_i = G_i/G_{i+1}$ et $Q'_i = G'_i/G'_{i+1}$ sont leurs quotients, alors il existe une permutation σ de $\{0, \dots, n-1\}$ tq $Q_i \simeq Q'_i$.

On appelle les Q_i les facteurs de Jordan-Hölder de G.

Remarque 73. Il n'y a pas unicité de la filtration de Jordan-Hölder elle-même, et il peut être nécessaire d'introduire une permutation : si $p \neq q$ sont deux nombres premiers, et $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, on peut prendre $G_1 = \mathbb{Z}/p\mathbb{Z} \times \{1\}$ ou $G_1 = \{1\} \times \mathbb{Z}/q\mathbb{Z}$, ça donne deux suites de Jordan-Hölder différentes avec quotients associés dans l'ordre inverse.

Remarque 74. Un groupe infini n'a pas en général de filtration de Jordan-Hölder : le groupe $\mathbb{Z}$ est un contrexemple : si le groupe $G = \mathbb{Z}$ avait une filtration de Jordan-Hölder $G = G_0 \supset \cdots \supset G_n = \{1\}$, chacun des quotients de la filtration serait abélien donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier, donc chacun des G_i serait d'indice fini dans le précédent, donc d'indice fini dans G, ce qui contredit que le groupe trivial est d'indice infini dans G.

Exercice. *Donner les facteur de Jordan-Holder de $\mathbb{Z}/n\mathbb{Z}$.*

Retrouver l'unicité de la décomposition en facteur premiers de n à partir du théorème de Jordan-Hölder.

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

Preuve. Existence : par récurrence sur le cardinal. Le cas $G = \{1\}$ est spécial : il a une filtration de Jordan-Hölder de longueur 0, et il n'en a pas d'autre... Si G est simple, il a une filtration de Jordan-Hölder de longueur 1 : $G_0 = G$, $G_1 = \{1\}$. Si G n'est pas simple, soit $N \subsetneq G$ un sous-groupe normal non-trivial. Par hypothèse de récurrence, N et G/N ont une filtration de Jordan-Hölder : $N = N_0 \supset N_1 \supset \cdots \supset N_p = \{1\}$ et $G/N = H_0 \supset H_1 \cdots \supset H_q = \{1\}$. En notant $\pi : G \to G/N$ l'application quotient, on obtient une filtration de Jordan-Hölder :

$$G = \pi^{-1}(H_0) \supset \cdots \supset \pi^{-1}(H_1) = N_0 \supset N_1 \cdots \supset N_p.$$

Pour l'unicité, on raisonne aussi par récurrence sur le cardinal de G. On se donne

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_h = G$$

et

$$\{1\} = K_0 \lhd K_1 \lhd \ldots \lhd K_k = G$$

deux filtrations de Jordan-Hölder de G. On note $H = H_{h-1}$ et $K = K_{k-1}$, qui sont de cardinal inférieur au cardinal de G.

Si $H = K$, alors on a deux filtrations de Jordan-Hölder de ce groupe : $H_0 \lhd \ldots \lhd H_{h-1} = H$ et $K_0 \lhd \ldots \lhd K_{k-1} = K$ donc par récurrence, $h = k$ et ces deux filtrations ont les mêmes facteurs donc les filtrations initiales aussi.

On suppose donc $H \neq K$, et soit $L = H \cap K$. Remarquons d'abord que $H/L \simeq G/K$. En effet, considérons l'application quotient $\pi : G \to G/K$. Le groupe $\pi(H)$ est non-trivial, et c'est un sous-groupe normal de G/K (car $H \lhd G$ et π surjectif) donc $\pi(H) = G/K$.

On applique le théorème d'isomorphisme à $\pi_{|H} : H \to \pi(H) = G/K$, et comme $\ker \pi_{|H} = H \cap K$, on obtient $H/(H \cap K) \simeq \pi(H) = G/K$, c'est à dire $H/L \simeq G/K$. Par symétrie de l'argument, on a aussi $K/L \simeq G/K$.

On a une première filtration de Jordan-Hölder de H :

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_{h-1} = H$$

dont les facteurs sont

$$H_1/H_0, \ldots, H/H_{h-2}.$$

Soit

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

une filtration de Jordan-Hölder de L, et utilisons la pour construire une deuxième filtration de H :

$$1 = L_0 \lhd L_1 \lhd \ldots \lhd L_{l-1} \lhd L \lhd H$$

est une filtration de Jordan-Hölder de H dont les facteurs sont

$$L_1/L_0, \ldots, L_l/L_{l-1}, H/L.$$

Par hypothèse de récurrence (puisque $\#H < \#G$), on a

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

où $\sim$ signifie qu'on a isomorphisme entre les groupes quitte à réordonner. En ajoutant G/H à la fin de chacune des deux listes, on obtient

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

De même, la filtration de L donne une deuxième filtration de K

$$1 = L_0 \lhd L_1 \lhd \ldots \lhd L_{l-1} \lhd L \lhd K$$

et en appliquant l'hypothèse de récurrence à K, on a

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

et en ajoutant G/K, on obtient

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

Puisque $G/H \simeq K/L$ et $H/L \simeq G/K$, on a équivalence entre les membres de gauche de $(*)$ et $(**)$:

$$(L_1/L_0, \ldots, L/L_{l-1}, H/L, G/H) \sim (L_1/L_0, \ldots, L/L_{l-1}, K/L, G/K)$$

et on conclut donc que

$$(H_1/H_0, \ldots, H/H_{h-2}, G/H) \sim (K_1/K_0, \ldots, K/K_{k-2}, G/K).$$

□

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.

[Cia98] P.G. Ciarlet. *Introduction à l'analyse numérique matricielle et à l'optimisation*. Collection Mathématiques appliquées pour la maîtrise. Dunod, 1998.

[Gro01] Larry C. Grove. *Classical groups and geometric algebra*, volume 39 of *Grad. Stud. Math.* Providence, RI : American Mathematical Society (AMS), 2001.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Grad. Texts Math.* Springer, New York, NY, 3rd revised ed. edition, 2002.

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