Algèbre linéaire MA123

Alexis Bouthier

Table des matières

Chapitre 1

Théorie des groupes

1. Généralités sur les groupes

1.1. Groupes. Partant d'un ensemble, il s'agit de l'enrichir avec des structures supplémentaires, telles que des opérations.

Définition 1.1.1. Soit un ensemble E, une loi de composition interne (LCI) sur E est une fonction $* : E \times E \to E$. Cette loi est généralement notée entre deux éléments.

Exemple 1.1.2. Pour $(x, y) \in \mathbb{R}^2$, $(x, y) \mapsto x + y$ est une loi de composition interne. Si E est un ensemble non-vide et $\mathcal{P}(E)$ l'ensemble de ses parties, alors $(A, B) \mapsto A \cap B$ est une LCI sur $\mathcal{P}(E)$.

Définition 1.1.3. Soit $*$ une LCI sur E. On dit que $(E, *)$ est un monoïde si :

1. $\forall\ (x, y, z) \in E^3, (x * y) * z = x * (y * z)$ (Associativité).
2. $\exists\ e \in E, \forall\ x \in E, e * x = x * e = x$ (Existence d'un élément neutre).

Si pour toute paire $(x, y) \in E^2$, on a $x * y = y * x$, on dit que E est un monoïde commutatif ou abélien.

Remarque 1.1.4. L'utilité de l'associativité est qu'elle permet d'écrire $x * y * z$ sans se préoccuper du parenthésage. Toutes les lois de composition interne ne sont pas nécessairement associatives. La soustraction sur $\mathbb{R}$ est un exemple de loi non associative. $4 - (3 - 2) = 3 \neq (4 - 3) - 2 = -1$.

Exemple 1.1.5. $(\mathbb{N}, +)$ ou $(\mathbb{N}, \times)$ sont des monoïdes abéliens, $(M_n(\mathbb{R}), \times)$ est un monoïde non-commutatif.

Définition 1.1.6. Soit $*$ une LCI sur E. On dit que $(E, *)$ est un groupe si c'est un monoïde et qu'il vérifie :

$$\forall\ x \in E, \exists\ y \in E, xy = yx = e \text{(Existence d'un inverse)}.$$

C'est un groupe abélien si de plus $(E, *)$ est un monoïde abélien.

Exemple 1.1.7. $(\mathbb{Z}, +)$ est un groupe abélien, $(GL_n(\mathbb{R}), \times)$ est un groupe non-commutatif.

Lemme 1.1.8. *Soit $(E, *)$ un ensemble avec une LCI, si elle admet un élément neutre, alors il est unique. De plus, si $(E, *)$ est un groupe, alors il y a unicité de l'inverse.*

Démonstration. En effet, si e et e' sont deux éléments neutres, on a $e * e' = e$ et $e * e' = e'$. Pour la deuxième assertion, soit $x \in E$, supposons qu'il admette deux inverses $y, y' \in E$. On a alors $y = y(xy') = y'$. □

Ainsi, si $(E, *)$ est un groupe, pour tout $x \in E$, il résulte du lemme que l'on peut définir x^{-1}, l'inverse de x. On note immédiatement que pour toute paire $(x, y) \in E^2$:

$$(x * y)^{-1} = y^{-1} * x^{-1}$$

Dans la suite, on note la LCI de manière multiplicative, sauf mention explicite et l'élément neutre 1. Pour $n \in \mathbb{N}^*$, si l'on multiplie n fois x, on note x^n. Attention, en général :

$$(xy)^n \neq x^n y^n.$$

C'est vrai seulement si la loi est commutative (pensez aux matrices). En effet, on a :

$$x^2y^2 = xxyy \text{ et } (xy)^2 = xyxy.$$

1.2. Sous-groupes. On se donne dans la suite un groupe $(G, .)$.

Définition 1.2.1. Une partie non-vide H de G est un sous- groupe si :

$$\forall\ (x, y) \in H^2, xy^{-1} \in H.$$

Remarques.

1.2.2. On remarque que comme H est non-vide, on a automatiquement $1 \in H$. En effet, il suffit de choisir $x \in H$ et par hypothèse, on a $1 = x.x^{-1} \in H$.

1.2.3. Dans les applications, pour montrer que quelque chose est un groupe, il est souvent plus commode de montrer que c'est un sous-groupe d'un groupe de « référence ».

Exemple 1.2.4. $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$, $\mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

1.3. Morphismes de groupes. Soient deux groupes $(A, .)$ et $(B, .)$.

Un morphisme de groupes est une fonction entre groupes $f : A \to B$ telle que :

$$f(1_A) = 1_B, f(xy) = f(x)f(y).$$

Remarque 1.3.1. On a automatiquement $f(x)f(x^{-1}) = f(xx^{-1}) = 1$ soit $f(x^{-1}) = f(x)^{-1}$.

Exemple 1.3.2. $z \mapsto |z|$ de $(\mathbb{C}^*, .) \to (\mathbb{R}^*, .)$ ou $x \mapsto e^x$ de $(\mathbb{R}, +)$ sur $(\mathbb{R}^*, .)$ sont des morphismes de groupes.

Vocabulaire usuel sur les morphismes :

Définition 1.3.3. Soit $f : G \to H$, un morphisme de groupes. On dit que :

1. f est un *endomorphisme* si $G = H$.
2. f est un *isomorphisme* si c'est un morphisme de groupes bijectif.
3. f est un *automorphisme* si c'est un endomorphisme bijectif.

Exemples.

1.3.4. $x \mapsto x^2$ est un endomorphisme de groupes de $(\mathbb{R}^*, \times)$.

1.3.5. $x \mapsto e^x$ est une bijection de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$. On dit que ces groupes sont isomorphes.

aut-int

Exemple 1.3.6. Pour un groupe G et $x \in G$, $\phi_x : G \to G$ donné par $y \mapsto xyx^{-1}$ est un automorphisme de G. On appelle un tel automorphisme, un automorphisme intérieur. Si $x = 1$, on obtient l'automorphisme identité Id_G donné par $y \mapsto y$.

Exemple 1.3.7. Soit G un groupe, alors l'ensemble $\mathrm{Aut}(G)$ des automorphismes de G avec la composition des applications comme LCI est un groupe.

Démonstration. La loi de composition est clairement associative et pour tout $\sigma \in \mathrm{Aut}(G)$, on a $\mathrm{Id}_G \circ \sigma = \sigma \circ \mathrm{Id}_G = \sigma$. De plus comme σ est bijective, soit σ^{-1} son inverse, alors on a bien $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}$. Il suffit donc de vérifier que σ^{-1} est aussi un morphisme de groupes. On a $\sigma(1) = 1$ donc $\sigma^{-1}(1) = 1$. Soit $(x, y) \in G^2$, alors $\sigma(\sigma^{-1}(x)\sigma^{-1}(y)) = \sigma(\sigma^{-1}(x))\sigma(\sigma^{-1}(y)) = xy = \sigma(\sigma^{-1}(xy))$, soit $\sigma^{-1}(x)\sigma^{-1}(y) = \sigma^{-1}(xy)$ par injectivité de σ. □

1.4. Image et noyau d'un morphisme. Soit $\phi : G \to H$ un morphisme de groupes.

Lemme 1.4.1. *Soient $G' \subset G$, $H' \subset H$ des sous-groupes, alors $\phi(G')$ et $\phi^{-1}(H')$ sont aussi des sous-groupes.*

Démonstration. $1_G \in G'$ comme G' est un sous-groupe et $\phi(1_G) = 1_H \in \phi(G')$. De plus, $\phi(x)\phi(y)^{-1} = \phi(xy^{-1})$ et $xy^{-1} \in G'$ donc $\phi(G')$ est un sous-groupe. On a l'équivalence :

$$x \in \phi^{-1}(H') \iff \phi(x) \in H'.$$

Comme $\phi(1_G) = 1_H \in H'$, $1_G \in \phi^{-1}(H')$. Si $x, y \in \phi^{-1}(H')$, alors $\phi(x)\phi(y)^{-1} \in H'$. Or $\phi(x)\phi(y)^{-1} = \phi(xy^{-1})$, donc on obtient $xy^{-1} \in \phi^{-1}(H')$, ce qui conclut. □

Définition 1.4.2. (i) On définit l'image de ϕ, notée $\mathrm{Im}\,\phi$ par le sous-groupe $\phi(G) \subset H$. On a $\mathrm{Im}\,\phi = H$ si et seulement si ϕ est surjective.

(ii) On définit le noyau de ϕ, noté $\mathrm{Ker}\,\phi$, par le sous-groupe $\phi^{-1}(\{e\}) \subset G$.

Exemple 1.4.3.

$\phi : (\mathbb{C}, +) \to (\mathbb{R}, +)$, donné par $z \mapsto \mathrm{Re}(z)$ est surjectif, donc $\mathrm{Im}\,\phi = \mathbb{R}$. De plus, $\mathrm{Ker}\,\phi = i\mathbb{R}$.

$\phi : (\mathbb{R}, +) \to (\mathbb{U}, \times)$, donné par $x \mapsto e^{ix}$ est surjectif de noyau $2\pi\mathbb{Z}$.

Proposition 1.4.6. *Soit $\phi : G \to H$ un morphisme de groupes. Alors, ϕ est injectif si et seulement si* $\mathrm{Ker}\,\phi = \{1\}$.

Démonstration. Sens direct : soit $x \in G$ tel que $\phi(x) = 1$ alors $\phi(x) = \phi(1)$ et $x = 1$.

Sens réciproque : Si pour $(x, x') \in G^2$, on a $\phi(x) = \phi(x')$, alors $\phi(x)\phi(x')^{-1} = 1$, d'où $\phi(xx'^{-1}) = 1$. Comme $\mathrm{Ker}\,\phi = \{1\}$, on obtient $xx'^{-1} = 1$ et $x = x'$. □

Proposition 1.4.7. *Soit $\phi : G \to H$ un morphisme de groupes finis de même cardinal, alors on a l'équivalence :*

$$\phi \ \textit{ injective} \iff \phi \ \textit{ surjective} \iff \phi \ \textit{ bijective.}$$

Démonstration. On montre (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (1). Si ϕ est injective, $\mathrm{card}(G) = \mathrm{card}(\phi(G)) = \mathrm{card}(H)$ donc $\phi(G) = H$ et ϕ est surjective. Si ϕ est surjective, alors $\phi(G) = H$ et si ϕ n'est pas injective, on aurait $\mathrm{card}(H) = \mathrm{card}\,\phi(G) < \mathrm{card}\,G$, donc ϕ est injective donc bijective. La dernière assertion est triviale. □

fin **Lemme 1.4.8.** *Soit G un groupe fini, alors pour tout $x \in G$, il existe $n \in \mathbb{N}^*$, $x^n = 1$.*

Démonstration. En effet si tel n'est pas le cas alors on obtiendrait un morphisme de groupes injectif :

$$\mathbb{Z} \to G$$

donné par $k \mapsto x^k$. Or, G est fini, contradiction. □

Définition 1.4.9. Soit un groupe G, et $x \in G$, on appelle alors l'ordre de x le plus petit entier $d \in \mathbb{N}^*$ tel que $x^d = 1$.

2. Action de groupes

2.1. Définitions.

Définition 2.1.1. Soit un groupe G, on dit que G agit sur une ensemble X si on a une application :

$$G \times X \to X$$

$(g, x) \mapsto g.x$, où $g.(g'.x) = (gg').x$ et $1.x = x$.

En particulier, une action de groupe est équivalente à la donnée d'un morphisme de groupes :

$$\tau : G \to \Sigma(X),$$

donné par $g \mapsto (x \mapsto g.x)$, où $\Sigma(X)$ est le groupe des bijections de X dans X avec la composition des fonctions comme loi de groupe.

Remarque 2.1.2. L'inverse de $(x \mapsto g.x)$ est $(x \mapsto g^{-1}.x)$.

Exemple 2.1.3. (i) G agit sur lui-même par translation à gauche :

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

(ii) G agit sur lui-même par translation à droite :

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

(iii) G agit sur lui-même par conjugaison :

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

Définition 2.1.4. (i) Soit $x \in X$, on appelle stabilisateur de x le sous-ensemble :

$$G_x := \{g \in G \mid g.x = x\}.$$

(ii) On appelle orbite de x le sous-ensemble :

$$O_x := \{g.x, g \in G\}.$$

Lemme 2.1.5. *Pour tout $x \in X$, G_x est un sous-groupe de G.*

Démonstration. $1 \in G_x$.

Si $g, g' \in G$, alors $(gg').x = g.(g'.x) = g.x = x$ et $gg' \in G_x$.

Si $g \in G_x$, alors $x = 1.x = (g^{-1}g).x = g^{-1}.(g.x) = g^{-1}.x$, donc $g^{-1} \in G_x$. □

Dans le cas où G agit sur lui-même par conjugaison, pour tout $x \in G$, le stabilisateur s'appelle le *centralisateur* (ou commutateur) de x, noté $C_G(x)$. Il consiste en :

$$C_G(x) = \{g \in G, gx = xg\}.$$

Les orbites sont appelées les *classes de conjugaison.*

Définition 2.1.6. Soit G qui agit sur X. On dit que :

(i) l'action est transitive s'il n'y a qu'une seule orbite.

(ii) l'action est fidèle si le morphisme $G \to \Sigma(X)$ est injectif.

(iii) L'action est libre si les stabilisateurs sont triviaux.

2.2. Exemples.

Exemple 2.2.1. (Le groupe symétrique) Soit $n \in \mathbb{N}^*$, si $X = \{1, \dots, n\}$, on note $S_n = \Sigma(X)$, c'est le groupe symétrique à n éléments. S_n agit sur $[\![1, n]\!]$ par :

$$\begin{array}{ccc} S_n \times [\![1,n]\!] \to & [\![1,n]\!] \\ (\sigma, x) \mapsto & \sigma(x) \end{array}.$$

Le stabilisateur de 1 consiste en :

$$H := \{\sigma \in S_n \mid \sigma(1) = 1\}$$

et H est isomorphe à S_{n-1} par l'application :

$$\sigma \mapsto \sigma_{|[\![2,n]\!]}.$$

Comme pour tout $k \in [\![1, n]\!]$, il existe $\sigma \in S_n$ tel que $\sigma(1) = k$, l'orbite de 1 est $[\![1, n]\!]$. Ainsi l'action est transitive. Elle est aussi fidèle puisque si $\sigma(x) = x$ pour tout $x \in [\![1, n]\!]$, $\sigma = \mathrm{Id}$.

Exemple 2.2.2. (matrices conjuguées) Soit un corps k, considérons :

$$DZ_n(k) := \{A \in M_n(k) \mid \text{A est diagonisable}\}.$$

Le groupe $GL_n(k)$ agit par conjugaison sur $DZ_n(k)$ par :

$$P.A = PAP^{-1}$$

Soit $D_n(k)$ l'ensemble des matrices diagonales à coefficients dans k. Alors tout élément $A \in DZ_n(k)$ est conjugué à une matrice diagonale $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n) \in D_n(k)$. En particulier, l'ensemble des orbites est infini.

Si pour tout $i, j, \lambda_i \neq \lambda_j$ le stabiliseur D consiste en $D_n \cap GL_n(k)$.

Exemple 2.2.3. (Classes d'équivalence). Soit un corps k, $G = GL_n(k) \times GL_n(k)$, alors G agit sur $M_n(k)$ par :

$$(P, Q).A = PAQ^{-1}.$$

On appelle les orbites les classes d'équivalence. Par le théorème du rang, toute matrice $A \in M_n(k)$ est semblable à une matrice J_r pour $0 \leqslant r \leqslant n$, avec :

$$J_r = \mathrm{diag}(I_r, 0, \dots, 0).$$

En particulier, l'ensemble des orbites est fini, égal à $n + 1$.

Exemple 2.2.4. Soit un $\mathbb{K}$-espace vectoriel V, alors $GL(V)$ agit sur V, par $u.x = u(x)$ pour $u \in GL(V), x \in V$.

L'exemple précédent motive la définition suivante :

Définition 2.2.5. Soit un groupe G, alors une représentation de G à coefficients dans $\mathbb{K}$ est la donnée d'une paire (ρ, V) où V est un $\mathbb{K}$-espace vectoriel et $\rho : G \to GL(V)$ un morphisme de groupes. Une représentation de dimension un, i.e. si $\dim V = 1$, est appelée un caractère et consiste donc en un morphisme de groupes $\rho : G \to \mathbb{K}^\times$.

Remarques.

2.2.6. L'étude des représentations d'un groupe permet de pouvoir étudier un groupe abstrait en termes d'algèbre linéaire.

2.2.7. Si (ρ, V) est une représentation de V, on a une action naturelle de G sur V par :

$$g.x = \rho(g)(x), g \in G, x \in V.$$

Réciproquement si G agit sur un espace vectoriel V tel que pour tout $g \in G$, $\rho_g : x \mapsto g.x$ est une application linéaire, alors V est une représentation de G et $\rho : g \mapsto \rho_g$ est le morphisme associé.

Exemples.

2.2.8. Pour tout entier $n \in \mathbb{N}^*$, et $i \in [\![1, n]\!]$, soit $\Lambda^i V^\vee$ l'espace vectoriel des i-formes multilinéaires alternées de V, alors $\Lambda^i V^\vee$ est une représentation de $GL(V)$ via l'action :

$$u.f(x_1, \ldots, x_i) = f(u(x_1), \ldots, u(x_i)), (x_1, \ldots, x_i) \in V^i, f \in \Lambda^i V^\vee, u \in GL(V).$$

2.2.9. On a une action de $GL_n(\mathbb{K})$ sur $M_n(\mathbb{K})$, vu comme $\mathbb{K}$-espace vectoriel, par $M \mapsto AMA^{-1}$ qui est un automorphisme linéaire, on en déduit donc un morphisme $\mathrm{Ad} : GL_n(\mathbb{K}) \to GL(M_n(\mathbb{K}))$. On appelle cette représentation, la représentation adjointe.

2.3. Applications.

Théorème 2.3.1 (Cayley)**.** *Soit un groupe fini G de cardinal n, alors il existe un plongement*[1] *$G \to S_n$.*

Démonstration. Le groupe G agit sur lui-même par multiplication à gauche. On voit G comme un ensemble à n éléments. On obtient ainsi un morphisme :

$$\tau : G \to S_n,$$

donné par $g \mapsto i_g : y \mapsto gy$. Montrons l'injectivité de τ. Soit $g \in \mathrm{Ker}\,\tau$, alors $i_g = \mathrm{Id}$, mais $i_g(1) = g = 1$ donc l'injectivité suit. □

Proposition 2.3.2. *Tout groupe fini G de cardinal n peut-être plongé dans $GL_n(\mathbb{F}_p)$ pour tout premier p.*

1. i.e un morphisme de groupes injectif.

DÉMONSTRATION. Par le théorème de Cayley, on a déjà plongé G dans S_n. Donc il suffit de plonger S_n dans $GL_n(\mathbb{F}_p)$. On définit l'application $\phi : S_n \to GL_n(\mathbb{F}_p)$ qui envoie :

$$\sigma \mapsto A_\sigma,$$

avec $A_\sigma.e_i = e_{\sigma(i)}$ pour $(e_1, \ldots, e_n)$ la base canonique. Montrons l'injectivité de ϕ ; si $A_\sigma = \mathrm{Id}$ alors pour tout $i \in [\![1, n]\!]$, on a :

$$\sigma(i) = i,$$

donc $\sigma = \mathrm{Id}$ et ϕ est injective. □

glnfp **Proposition 2.3.3.** *Soit p premier, on a :*

$$a_n := \mathrm{card}(GL_n(\mathbb{F}_p)) = \prod_{i=0}^{n-1}(p^n - p^i) = p^{\frac{n(n-1)}{2}} \prod_{i=0}^{n-1}(p^k - 1).$$

DÉMONSTRATION. Construisons une matrice A typique de $GL_n(\mathbb{F}_p)$. Ses colonnes doivent former un système libre. Pour la colonne C_1, on a n coordonnées, la seule condition est que la colonne doit être non-nulle, donc on a $p^n - 1$ possibilités.

Pour C_2, la seconde colonne ne doit pas être colinéaire à C_1, i.e. pas de la forme λC_1 avec $\lambda \in \mathbb{F}_p$, on a donc $p^n - p$ possibilités.

Si on a construit $C_1, \ldots, C_{i-1}$, pour construire C_i on a un choix de vecteurs qui n'appartiennent pas à $\mathrm{Vect}(C_1, \ldots, C_{i-1})$. Cet espace vectoriel a p^i éléments donc, il y a $p^n - p^i$ choix pour C_i. On trouve alors :

$$\mathrm{card}(GL_n(\mathbb{F}_p)) = \prod_{i=0}^{n-1}(p^n - p^i) = p^{\frac{n(n-1)}{2}} \prod_{i=0}^{n-1}(p^k - 1).$$

□

2.4. Formule des classes.

Proposition 2.4.1. *L'ensemble des orbites $\{O_x, x \in E\}$ forme une partition de E. Si G est un groupe fini, on a :*

$$\mathrm{card}(O_x) = \frac{\mathrm{card}\, G}{\mathrm{card}\, G_x}.$$

DÉMONSTRATION. Sur E, on définit la relation d'équivalence $\mathcal{R}$ par :

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

Montrons que c'est une relation d'équivalence ; $x = 1.x$ donc $x\mathcal{R}x$ et $\mathcal{R}$ est réflexive.

Si $x\mathcal{R}y$ alors $y = g.x$ d'où $g^{-1}.y = x$, donc $y\mathcal{R}x$ et $\mathcal{R}$ est symétrique.

Enfin, si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $y = g.x$ et $z = g'.y$ donc $z = g'.(g.x) = (g'g).x$ et $\mathcal{R}$ est transitive. Comme les orbites sont des classes d'équivalence, par la théorie générale, les classes d'équivalence forment une partition.

Maintenant, on a une surjection $\phi : G \to O_x$ donnée par $g \mapsto g.x$. Si $\phi(g) = y$ alors

$$\operatorname{card}(\phi^{-1}(y)) = G_x,$$

puisque si $\phi(g) = \phi(g') = y$ alors, $y = g.x = g'.x$ donc $g'^{-1}g.x = x$ et $g'^{-1}g \in G_x$. On en déduit donc :

$$\operatorname{card}(O_x) = \frac{\operatorname{card} G}{\operatorname{card} G_x}.$$

□

Remarques.

2.4.2. Si E est un ensemble fini, on a alors un nombre fini d'orbites $O_1, \ldots, O_r$ et on déduit :

$$\operatorname{card}(E) = \sum_{i=1}^{r} \operatorname{card}(O_i).$$

2.4.3. $GL_n(\mathbb{R})$ agit sur $\mathbb{R}^n$. Soit le vecteur $e_1 = (1, 0, \ldots, 0) \in \mathbb{R}^n$, alors l'orbite de e_1 est $\mathbb{R}^n - \{0\}$ et le stabilisateur est isomorphe à $GL_{n-1}(\mathbb{R}) \times \mathbb{R}^{n-1}$.

On va tirer plusieurs applications de la formule des classes.

pcentre

Exemple 2.4.4. Soit G un p-groupe (i.e. de cardinal égal à la puissance d'un premier p) alors le centre $Z(G)$ est non-trivial.

Démonstration. G agit par conjugaison sur lui-même et par la formule des classes :

$$\operatorname{card}(G) = \operatorname{card}(Z(G)) + \sum_{i=1}^{d} \operatorname{card}(O_i).$$

où tout élément de $Z(G)$ consiste en une orbite avec un seul élément et avec $\operatorname{card}(O_i) \geqslant 2$. Ainsi, $\operatorname{card}(O_i)$ est divisible par p car l'orbite est non-triviale et G est un p-groupe, on déduit alors :

$$\operatorname{card}(G) = \operatorname{card}(Z(G)) = 0 \ [p].$$

Or, $1 \in Z(G)$, donc on a $\operatorname{card}(Z(G)) \geqslant p$, ce qui conclut. □

Théorème 2.4.5 (Lagrange)**.** *Soit un groupe fini G et un sous-groupe $H \subset G$, alors :*

$$\operatorname{card}(H) | \operatorname{card}(G).$$

Démonstration. On considère la relation d'équivalence :

$$x\mathcal{R}y \iff xy^{-1} \in H.$$

Soit G/H l'ensemble des classes d'équivalence, notons $(G : H)$ son cardinal. Pour $a \in G$ l'ensemble des classes d'équivalence forment une partition de G :

$$aH := \{g \in G, \exists h \in H, g = a.h\}$$

On en déduit donc que :

$$G = \bigcup_{\bar{a} \in G/H} aH$$

Maintenant, toutes ces classes sont de cardinal $\mathrm{card}(H)$ et l'on déduit :

$$\mathrm{card}(G) = (G : H)\,\mathrm{card}\,H.$$

□

Cela justifie donc la définition suivante :

Définition 2.4.6. Soit G un groupe fini, $H \subset G$, on définit l'indice de H dans G, comme le cardinal de G/H.

Proposition 2.4.7. *Soit un groupe fini G, soit $x \in G$ d'ordre r alors $r | \mathrm{card}(G)$. En particulier, on a :*

$$\forall\ x \in G, x^{\mathrm{card}(G)} = 1.$$

Démonstration. Soit $H := \{x^k, k \in \mathbb{Z}\} \subset G$, c'est un sous-groupe de cardinal r et on applique le théorème de Lagrange. □

Exemple 2.4.8. Si l'on prend $G = (\mathbb{Z}/p\mathbb{Z})^\times$, le corollaire donne $x^{p-1} = 1\ [p]$ et on retrouve le petit théorème de Fermat.

3. Groupes quotients

3.1. Groupes distingués. En général, si H est un sous-groupe, G/H n'est plus nécessairement un groupe, nous allons voir sous quelles hypothèses cela reste le cas.

Définition 3.1.1. Un sous-groupe $H \subset G$ est normal ou distingué si :

$$\forall x \in G, xHx^{-1} \subset H.$$

On note $H \lhd G$.

Remarques.

3.1.2. Si G est abélien, tout sous-groupe est distingué.

3.1.3. Si G est fini et $H \subset G$ distingué, on a même égalité, $xHx^{-1} = H$ pour des raisons de cardinal.

tri-mor **Proposition 3.1.4.** *Soit $\phi : G \to H$ un morphisme de groupes, alors* $\mathrm{Ker}\,\phi$ *est normal.*

Démonstration. Soit $x \in \operatorname{Ker}\phi$ et $g \in G$ alors

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = 1.$$

□

On a d'autres exemples de groupes distingués :

Lemme 3.1.5. *Le centre de G, $Z(G) := \{x \in G \mid yx = xy\} \subset G$ est distingué dans G. Le groupe dérivé $D(G) := \left\langle [x,y] := xyx^{-1}y^{-1}, x, y \in G \right\rangle \subset G$ est distingué.*

Démonstration. Pour $Z(G)$, c'est évident puisque la conjugaison agit trivialement sur $Z(G)$. Si $z \in G$ alors on a :

$$z[x,y]z^{-1} = [zxz^{-1}, zyz^{-1}] \in D(G),$$

donc $D(G)$ est distingué. □

scent **Exemple 3.1.6.** Si $n \geqslant 3$, on a $Z(S_n) = \{1\}$.

Démonstration. Soit $\sigma \in Z(S_n)$ avec $n \geqslant 3$, si $\sigma \neq \mathrm{Id}$ soit i tel que $j = \sigma(i) \neq i$ et on choisit $k \neq \{j, \sigma(i)\}$, ce qui est possible comme $n \geqslant 3$. Soit $\tau = (ijk)$, on a alors $\tau\sigma\tau^{-1} = \sigma$. Or, on a $\tau\sigma\tau^{-1}(\sigma(i)) = \tau\sigma(i) = k \neq \sigma(i)$, contradiction. □

Proposition 3.1.7. *Soit un corps k avec* $\operatorname{card}(k) \geqslant 3$*, alors $D(GL_n(k)) = \mathrm{SL}_n(k) = \{M \in GL_n(k), \det(M) = 1\}$.*

Démonstration. Tout d'abord, on a une inclusion immédiate $D(GL_n(k)) \subset \mathrm{SL}_n(k)$ puisque tout commutateur est de déterminant un. Comme $SL_n(k)$ est engendré par les transvections, il suffit donc d'écrire toute transvection comme un commutateur. On considère alors pour $\lambda \in k$ et $i, j \in [\![1, n]\!]$ avec $i \neq j$, la matrice de transvection $\tau_{ij}(\lambda) = I_n + (\lambda)E_{ij}$. Pour $\mu \in k$, on considère la matrice diagonale $d_i(\mu) = I_n + (\mu - 1)E_{ii}$, c'est la matrice diagonale avec que des 1 sauf en la place i où l'on place μ. On a alors la relation pour toute paire $\mu, \rho \in k$:

$$d_i(\mu)\tau_{ij}(\rho)d_i(\mu)\tau_i^{-1}(\rho) = \tau_{ij}((1 - \mu^{\operatorname{sign}(j-i)})\rho.$$

En particulier, en choisissant $\mu \neq 0, 1$, ce qui est possible comme $\operatorname{card}(k) \geqslant 3$ et en prenant $\rho = \frac{\lambda}{(1-\mu^{\operatorname{sign}(j-i)}}$, on obtient que $\tau_{ij}(\lambda)$ est un commutateur et $D(GL_n(k)) = \mathrm{SL}_n(k)$. □

Définition 3.1.8. Soit H un sous-groupe de G, On définit le normalisateur de H dans G, $N_G(H) := \{g \in G \mid gHg^{-1} \subset H\}$. Alors, $N_G(H)$ est un sous-groupe et on a $H \lhd N_G(H)$.

3.2. Groupes simples.

Définition 3.2.1. Un groupe G est simple s'il n'admet pas de sous-groupes normaux autres que $\{1\}$ et lui-même.

Remarque 3.2.2. Cette notion est analogue pour les groupes à celle de nombre premier, les diviseurs sont remplacés par les groupes distingués.

Lemme 3.2.3. *Un groupe simple est soit commutatif soit avec un centre trivial. Un groupe simple vérifie $D(G) = G$ ou est commutatif.*

Démonstration. On a $Z(G) \lhd G$ donc cela force $Z(G) = G$ ou $Z(G) = \{1\}$. De même pour $D(G)$, si $D(G) = \{1\}$, alors G est abélien, comme tout commutateur est trivial, i.e. $xyx^{-1}y^{-1} = 1$. □

Lemme 3.2.4. *Le seul groupe commutatif simple est $\mathbb{Z}/p\mathbb{Z}$, avec p premier.*

Démonstration. Si H est un sous-groupe alors son cardinal divise p, donc c'est p ou 1 et $\mathbb{Z}/p\mathbb{Z}$ est simple. Montrons que c'est le seul cas. Soit H un groupe simple commutatif d'ordre n. S'il admet un élément $x \in H$ d'ordre $2 \leqslant d \leqslant n-1$, alors $\langle x \rangle \lhd H$ et H ne peut être simple. Donc x est d'ordre n et $H \simeq \mathbb{Z}/n\mathbb{Z}$. Mais à nouveau, si n n'est pas premier, alors tout diviseur d de n engendre un sous-groupe distingué strict, i.e $\left\langle x^{\frac{n}{d}} \right\rangle$. □

Un des premiers exemples non-commutatifs de groupes simples est le suivant

asimp **Théorème 3.2.5.** *(Admis) Pour $n \neq 4$, A_n est simple.*

Remarques.

3.2.6. Les outils pour montrer cet énoncé sont largement au niveau de ce cours, mais cela nécessite d'établir un certain nombre de propriétés supplémentaires sur les groupes symétriques qui relèvent plus d'un cours de théorie des groupes que d'algèbre linéaire. Comme cela fait faire une trop grande digression, nous l'admettons et montrons en revanche les corollaires que nous pouvons en tirer.

3.2.7. Si $n = 4$, A_4 n'est pas simple, car $D(A_4)$ est un sous-groupe distingué d'ordre 4, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, engendré par les bitranspositions. On appelle $V_4 = D(A_4)$ le groupe de Klein.

dist1 **Corollaire 3.2.8.** *Si $n \neq 4$, A_n est le seul sous-groupe distingué propre non-trivial de S_n.*

Démonstration. Si $n \leqslant 2$, c'est clair, supposons donc $n \geqslant 3$. Soit $H \subset S_n$ un sous-groupe distingué, alors $H \cap A_n \lhd A_n$, donc $H \cap A_n = \{1\}$ ou $A_n \subset H$. Si $A_n \subset H$, alors

$H = A_n$ ou S_n. Si $H \cap A_n = \{1\}$, alors la signature ϵ induit un isomorphisme entre H et $\epsilon(H)$ d'où $\mathrm{card}(H) \leqslant 2$. Si $\mathrm{card}(H) = 2$, soit $\sigma \in H$ l'élément non-trivial, alors pour tout $\tau \in S_n$, comme $\tau\sigma\tau^{-1} \neq Id$, cela force $\tau\sigma\tau^{-1} = \sigma$ donc σ est central, or $Z(S_n) = \{1\}$, contradiction et $H = \{1\}$. □

index **Proposition 3.2.9.** *Si $n \neq 4$, soit $H \subset S_n$ un sous-groupe d'indice n, alors $H \simeq S_{n-1}$.*

Démonstration. Pour $n \leqslant 3$, c'est clair. Supposons $n \geqslant 5$, posons $G = S_n$, alors G agit par translation à gauche sur G/H et on a un morphisme $\phi : G \to \mathrm{Bij}(G/H) \simeq S_n$. Montrons qu'il est injectif. On a $\mathrm{Ker}\,\phi = \bigcap_{a \in G} aHa^{-1}$ et comme $\mathrm{Ker}\,\phi \lhd S_n$, le corollaire dist1 3.2.8 montre que $\mathrm{Ker}\,\phi = \{1\}$ puisque $(n-1)! < \frac{n!}{2}$. Pour une raison de cardinal, ϕ est un isomorphisme et H s'identifie au stabilisateur de $\bar{1} = H \in G/H$ dans S_n, c'est donc un groupe isomorphe à S_{n-1}. □

3.3. Construction de quotients.

Théorème 3.3.1. *Soit $H \subset G$ un sous-groupe normal, alors G/H, l'ensemble des classes à gauche, admet une structure de groupe.*

Lemme 3.3.2. *Même hypothèse que dans le théorème, si $x = x' \mod H$ et $y = y' \mod H$ alors $xy = x'y' \mod H$.*

Démonstration. On a $x = x'h$ et $y = y'h'$ alors

$$xy = x'hy'h' = x'y'(y'^{-1}hy')h'$$

et $y'^{-1}hy' \in H$ comme H est normal. □

Passons à la preuve du théorème :

Démonstration. On définit le produit

$$xH.yH = xy.H \tag{3.3.2.1}$$ {d-mult}

qui est bien défini par le lemme précédent. On vérifie alors aisément que G/H est un groupe. □

Corollaire 3.3.3. *L'application canonique*

$$G \to G/H$$

est un morphisme de groupes de noyau H.

On a donc une suite exacte :

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{p} G/H \longrightarrow 1$$

Par suite exacte, on entend que $\operatorname{Im} i = \operatorname{Ker} p$, i est injective et p surjective.

Proposition 3.3.4 (Propriété universelle des groupes quotients)**.** *Soit $\phi : G \to H$ et $N \lhd G$, alors si $N \subset \operatorname{Ker} \phi$ il existe un unique morphisme $\bar{\phi} : G/N \to H$, tel que :*

$$\bar{\phi} \circ p = \phi$$

avec $p : G \to G/N$.

Démonstration. Comme $\phi(N) = \{1\}$ on définit $\bar{\phi} : G/N \to H$ par $\phi(xN) = \phi(x)$. Montrons que c'est bien défini. Soit $x' \in G$ tel que $xN = x'N$, alors $x = x'n$ avec $n \in N$ et donc $\phi(x) = \phi(x')\phi(n) = \phi(x')$, donc l'application est bien définie. On vérifie alors immédiatement que $\bar{\phi}$ est un morphisme de groupes comme ϕ est un morphisme de groupes et en vertu de la multiplication dans G/N donnée par le lemme (d-mult 3.3.2.1). □

Une appplication de la propriété universelle est la suivante :

ab1 **Proposition 3.3.5.** *Soit $G^{ab} := G/D(G)$, alors c'est un groupe abélien et pour tout morphisme $\phi : G \to H$ tel que H est abélien, il existe un unique morphisme $\bar{\phi} : G^{ab} \to H$ tel que $\bar{\phi} \circ p = \phi$ avec $p : G \to G^{ab}$.*

Démonstration. On a $D(G) \lhd G$, donc le quotient est un groupe. Pour tout $x, y \in G$, on a :

$$xy = yx \mod (D(G))$$

comme $D(G)$ est engendré par les commutateurs. Comme H est abélien, on a

$$\phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = 1.$$

et $D(G) \subset \operatorname{Ker}(\phi)$ Ainsi par propriété universelle du quotient, on obtient un morphisme de groupes

$$\bar{\phi} : G^{ab} \to H.$$

□

3.4. Théorème d'isomorphisme de Noether.

Théorème 3.4.1. *Soit un morphisme de groupes $\phi : G \to H$, alors on a un isomorphisme :*

$$G/\operatorname{Ker} \phi \cong \operatorname{Im} \phi.$$

En particulier, si G est fini, $|G| = |\operatorname{Ker} \phi||\operatorname{Im} \phi|$.

DÉMONSTRATION. Comme $\mathrm{Ker}(\phi)$ est normal, on peut considérer le groupe quotient $G/\operatorname{Ker}\phi$. L'application $\phi : G \to H$ se factorise par définition par $\operatorname{Im}\phi$. On peut donc supposer que $H = \operatorname{Im}\phi$. L'application $G \to H$ se factorise en $\overline{\phi} : G/\operatorname{Ker}\phi \to H$ et $\overline{\phi}$ est surjective comme ϕ l'est. Montrons l'injectivité, si $\overline{\phi}(x) = \overline{\phi}(x')$ alors $xx'^{-1} \in \operatorname{Ker}\phi$, donc l'injectivité suit. □

Proposition 3.4.2. *L'action de G sur lui-même par conjugaison induit un morphisme*

$$\Phi : G \to \mathrm{Aut}(G),$$

avec $\operatorname{Ker}\Phi = Z(G)$*. On obtient ainsi par passage au quotient une injection :*

$$G/Z(G) \to \mathrm{Aut}(G),$$

et on appelle $\mathrm{Int}(G)$ *l'image de* Φ*. On appelle ce groupe, le groupe des automorphismes intérieurs et* $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$*. On appelle le quotient* $\mathrm{Out}(G) = \mathrm{Aut}(G)/\operatorname{Int}(G)$ *le groupe des automorphismes extérieurs.*

DÉMONSTRATION. La première partie de l'assertion vient de la propriété universelle des groupes quotients. Il suffit donc de voir que $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$. Or si $\sigma \in \mathrm{Aut}(G)$ et $x \in G$ alors $\sigma \circ \phi_x \circ \sigma^{-1} = \phi_{\sigma(x)} \in \mathrm{Int}(G)$ avec ϕ_x l'automorphisme intérieur associé à x. □

4. Groupes résolubles et nilpotents

4.1. Groupes résolubles. Soit un groupe G, pour tout $i \in \mathbb{N}$, on définit la suite de groupes $(D^i(G))_{i\in\mathbb{N}}$ par $D^0(G) = G$, $i \geqslant 1$, $D^i(G) = D(D^{i-1}(G)) \subset D^{i-1}(G)$.

Définition 4.1.1. Soit un groupe G, on dit qu'il est résoluble s'il existe $n \in \mathbb{N}$ tel que $D^n(G) = \{1\}$. On appelle alors classe de résolubilité, le plus petit entier $n \in \mathbb{N}$ tel que $D^n(G) = \{1\}$, noté $\mathrm{cl}(G)$.

Remarque 4.1.2. Ainsi $\mathrm{cl}(G) = 0$ équivaut à $G = \{1\}$ et $\mathrm{cl}(G) = 1$ à G abélien.

d0 **Lemme 4.1.3.** *Soit $H \subset G$ un sous-groupe, alors les propriétés suivantes sont équivalentes :*

(i) $D(G) \subset H$,

(ii) $H \lhd G$ *et* G/H *abélien.*

DÉMONSTRATION. Montrons le sens direct. Soit $H^{ab} = \pi(H) \subset G/D(G) = G^{ab}$, alors comme $D(G) \subset H$, on a $H = \pi^{-1}(H^{ab})$. Ainsi, pour $x \in G$, comme $D(G) \lhd G$, on a $D(G) \subset xHx^{-1}$ et donc $\pi(xHx^{-1}) = H^{ab}$ et $xHx^{-1} \subset H$, donc H est normal et G/H abélien d'après 3.3.5. Réciproquement, on a $H = \operatorname{Ker}(G \to G/H)$ et comme G/H abélien, par propriété universelle, on a $D(G) \subset H$. □

sol1 **Proposition 4.1.6.** *Soit un groupe G et $n \in \mathbb{N}^*$, les assertions suivantes sont équivalentes :*

(i) *G est de classe inférieure ou égale à n.*

(ii) *Il existe une suite :*
$$G = G_0 \supset \cdots \supset G_n = \{1\}$$
de sous-groupes normaux de G telle que G_i/G_{i+1} est abélien.

(iii) *Il existe une suite :*
$$G = G_0 \supset \cdots \supset G_n = \{1\}$$
de sous-groupes de G tels que G_{i-1} soit normal dans G_i et G_i/G_{i-1} abélien pour $1 \leqslant i \leqslant n$.

(iv) *Il existe un sous-groupe abélien A normal dans G tel que G/A soit résoluble et de classe inférieure ou égale à $n-1$.*

DÉMONSTRATION. $(i) \Longrightarrow (ii)$ Posons $G_i = D^i(G)$ pour $i \in \mathbb{N}$, comme $D(G)$ est stable par tout automorphisme de G, $D^i(G) \lhd G$ et la suite vérifie (ii).

$(ii) \Longrightarrow (iii)$ est clair.

$(iii) \Longrightarrow (i)$. Par récurrence sur k et 4.1.3, on voit que $D^k(G) \subset G_k$ d'où $D^n(G) = \{1\}$.

$(i) \Longrightarrow (iv)$ On prend $A = D^{n-1}(G)$.

$(iv) \Longrightarrow (i)$ D'après $(i) \Longrightarrow (ii)$ appliquée à G/A et à $n-1$, il existe une suite de sous-groupes normaux de G telle que la suite des quotients :
$$G/A \supset A_1/A \supset \cdots \supset A_{n-1}/A = \{1\},$$
vérifie (ii). Alors la suite :
$$G \supset A = A_1 \supset \cdots \supset A_{n-1} = A \supset \{1\}$$
vérifie (ii) et l'implication $(ii) \Longrightarrow (i)$ appliquée à G et n donne le résultat. □

Remarques.

4.1.11. Un groupe simple non-abélien n'est pas résoluble.

4.1.12. Les groupes symétriques S_n sont résolubles si et seulement si $n \leqslant 4$. En effet, si $n \geqslant 5$, $D(S_n) = {A_n}^2$ qui est simple. Si $n \leqslant 3$ c'est clair et si $n = 4$, on a la suite $S_4 \supset A_4 \supset V_4 = (\mathbb{Z}/2\mathbb{Z})^2 \supset \{1\}$.

commt **Définition 4.1.13.** Soit un groupe G, A, B deux sous-groupes de G, on note (A, B) le sous-groupe engendré par les commutateurs $xyx^{-1}y^{-1}$ avec $x \in A$, $y \in B$.

Remarque 4.1.14. On note en particulier que par définition $(G, G) = D(G)$.

Pour ce cours, l'exemple fondamental de groupe résoluble est le suivant :

2. pour montrer l'égalité, remarquer que $D(S_n) \lhd A_n$ et comme S_n non-abélien, $D(S_n) = A_n$ par simplicité. On peut aussi le montrer pour tout $n \in \mathbb{N}$ de manière élémentaire : on a clairement que $D(S_n) \subset A_n$ et on montre que les 3-cycles sont conjugués et engendrent A_n et qu'il existe un 3-cycle dans $D(S_n)$.

4.2. Sous-groupe fixant un drapeau. Soit un corps commutatif $\mathbb{K}$, V un $\mathbb{K}$-espace vectoriel, on se donne une suite décroissantes de sous-espaces vectoriels de V :

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = \{0\}$$

tels que $\mathrm{codim}(V_i) = i$. Une telle suite est appelée un *drapeau complet*, on note $(V_\bullet) = (V_i)_{0 \leqslant i \leqslant n}$. Soit

$$B(V) = \{u \in GL(V) \mid u(V_i) = V_i, 0 \leqslant i \leqslant n\}.$$

Le théorème est le suivant :

sol2 **Théorème 4.2.1.** *Le groupe $B(V)$ est résoluble.*

Démonstration. On définit la suite de sous-groupes $(B_i)_{0 \leqslant i \leqslant n}$ de $B(V)$ par :

$$B_i = \{s \in B(V) \mid (s - \mathrm{Id}_V)V_j \subset V_{i+j}, 0 \leqslant j \leqslant n - i\}. \qquad (4.2.1.1)$$ {bor1}

En particulier, on a $B_0 = B(V)$. Montrons un lemme :

bcomm **Lemme 4.2.2.** *Pour tout $0 \leqslant j \leqslant n$ et $0 \leqslant k \leqslant n$ avec $j + k \leqslant n$, on a $(B_j, B_k) \subset B_{j+k}$.*

Démonstration. Soient $s \in B_j$, $t \in B_k$ et $x \in V_i$, il existe $v_{i+k} \in V_{i+k}$ tel que :

$$t(x) = x + v_{i+k},$$

soit :

$$st(x) = s(x) + s(v_{i+k}) = x + w_{i+j} + v_{i+k} + t_{i+j+k},$$

avec $w_{i+j} \in V_{i+j}$ et $t_{i+j+k} \in V_{i+j+k}$. De même, on a :

$$ts(x) = t(x + w_{i+j}) = x + v_{i+k} + w_{i+j} + t'_{i+j+k},$$

avec $t'_{i+j+k} \in V_{i+j+k}$. Ainsi, on obtient :

$$st(x) = ts(x) \mod V_{i+j+k}$$

ou encore comme $s(V_{i+j+k)} = V_{i+j+k}$ et pareillement pour t :

$$s^{-1}t^{-1}st(x) = x \mod V_{i+j+k},$$

d'où le résultat. □

On peut maintenant terminer la preuve. On a :

- Pour $0 \leqslant i \leqslant n$, $(B_0, B_i) \subset B_i$, donc les B_i sont normaux dans $B_0 = B(V)$.
- Pour $1 \leqslant i \leqslant n$, $D(B_i) = (B_i, B_i) \subset B_{2i} \subset B_{i+1}$, donc les quotients B_i/B_{i+1} sont abéliens $1 \leqslant i \leqslant n$.
- Enfin B_0/B_1 s'identifie au groupe des matrices diagonales.

Donc la suite $(B_i)_{0 \leqslant i \leqslant n}$ vérifie (ii) de sol1 4.1.6 et $B(V)$ est résoluble. □

Exemple 4.2.3. Si $V = \mathbb{K}^n$, $(e_1, \ldots, e_n)$ la base canonique, alors pour $0 \leqslant i \leqslant n$, on pose $V_{n-i} = Vect(e_1, \ldots, e_i)$ avec la convention $V_n = \{0\}$. Alors $B(V)$ consiste en les matrices triangulaires supérieures inversibles.

Notons $\mathrm{Drap}(V)$ l'ensemble des drapeaux de V, on fait agir $GL(V)$ sur $\mathrm{Drap}(V)$ par

$$g.(V_\bullet) = (g.V_\bullet).$$

Si $W_\bullet$ et $W'_\bullet$ sont deux drapeaux, en choisissant des bases pour les V_i et les W_j, on voit qu'il existe $g \in GL(V)$ tel que $g.W_\bullet = W'_\bullet$. Ainsi $GL(V)$ agit transitivement sur les drapeaux et par définition $B(V)$ est le stabilisateur de $V_\bullet$. On en déduit donc que :

$$GL(V)/B(V) \cong \mathrm{Drap}(V). \tag{4.2.3.1}$$

{bij-drap}

Ainsi, cela justifie que l'on appelle le quotient $GL(V)/B(V)$ la variété de drapeaux de $GL(V)$ (bien que dans ce cours on n'ira pas jusqu'à la munir d'une structure de variété).

4.3. Groupes nilpotents. Soit un groupe G, on appelle suite centrale descendante de G, la suite $(C^nG)_{n\geqslant 1}$ de sous-groupes de G définie par récurrence par :

$$C^1(G) = G, C^{n+1}(G) = (G, C^nG), n \geqslant 1.$$

Définition 4.3.1. Un groupe G est dit nilpotent s'il existe $n \in \mathbb{N}$ tel que $C^{n+1}G = \{1\}$. La classe de nilpotence de G est alors le plus petit tel entier n.

Remarques.

4.3.2. Un groupe est abélien si et seulement si il est nilpotent de classe $\leqslant 1$.

4.3.3. Un produit fini de groupes nilpotents est nilpotent de classe de nilpotence le maximum des classes des groupes.

Lemme 4.3.4. *Tout groupe nilpotent est résoluble.*

Démonstration. Montrons par récurrence sur $i \in \mathbb{N}^*$ que $D^i(G) \subset C^i(G)$. Si $i = 1$ c'est clair, et pour $i \geqslant 2$:

$$D^{i+1}G = (D^iG, D^iG) \subset (C^iG, C^iG) \subset (G, C^iG) = C^{i+1}G,$$

où la première inclusion s'obtient par hypothèse de récurrence. □

nilp2

Proposition 4.3.5. *Un groupe G est nilpotent si et seulement si, il existe une suite décroissante :*

$$G_1 = G \supset \cdots \supset G_{n+1} = \{1\},$$

avec $(G, G_i) \subset G_{i+1}$ pour tout $1 \leqslant i \leqslant n$, ce qui est équivalent à la condition $G_i/G_{i+1} \subset Z(G/G_{i+1})$. En particulier, un sous-groupe (resp. un groupe quotient) d'un groupe nilpotent est nilpotent. Enfin, le centre d'un groupe nilpotent est non-trivial.

nilfor

Remarque 4.3.6. Une condition plus forte serait $(G_j, G_i) \subset G_{i+j}$.

DÉMONSTRATION. Si une telle filtration existe, alors $C^k G \subset G_k$ pour $k \geqslant 1$ donc G nilpotent. Réciproquement, si G nilpotent, on prend $G_k = C^k G$. Les assertions sur le passage au quotient et au sous-groupe se déduisent alors de la caractérisation à l'aide des filtrations. Enfin, si G est nilpotent de classe n, alors $C^{n+1}(G) = \{1\}$, donc $C^n(G) \neq \{1\}$ est dans le centre de G comme souhaité. □

Reprenons l'exemple de $B(V)$ de 4.2.1. Pour $1 \leqslant i \leqslant n$, on a :

$$B_i = \{s \in B(V) \mid (s - \mathrm{Id}_V)V_j \subset V_{i+j}, 0 \leqslant j \leqslant n - i\}.$$

nilp3 **Proposition 4.3.7.** *Pour tout $1 \leqslant i \leqslant n$, B_i est nilpotent. En particulier, si $U_n \subset GL_n(\mathbb{K})$ est le sous-groupe des matrices triangulaires supérieures unipotentes, il est nilpotent.*

Remarque 4.3.8. Pour rappel, une matrice $M \in M_n(\mathbb{K})$ est unipotente, si $M - I_n$ est nilpotente.

DÉMONSTRATION. Comme un sous-groupe d'un groupe nilpotent est nilpotent, il suffit de le vérifier pour B_1. Alors, d'après 4.2.2, la suite des $(B_i)_{1 \leqslant i \leqslant n}$ vérifie 4.3.6. Enfin, U_n correspond au groupe B_1 pour le drapeau standard de $\mathbb{K}^n$. □

kolch **Théorème 4.3.9** (Kolchin)**.** *Soit $\mathbb{K}$ un corps algébriquement clos, V un $\mathbb{K}$-espace vectoriel de dimension finie. Soit un groupe $G \subset GL(V)$ un sous-groupe où tous les éléments sont unipotents, alors il existe un drapeau complet $(V_\bullet)$ de V tel que G soit contenu dans le groupe B_1 correspondant (cf. ci-dessus). En particulier, G est nilpotent.*

Remarques.

4.3.9. On peut voir cet énoncé comme un exemple de cotrigonalisation dans le cas non-commutatif. Dans le cas abélien, il est bien connu.

4.3.9. Dans la suite, un sous-groupe $G \subset GL_n(\mathbb{C})$ constitué de matrices unipotentes est dit unipotent.

Le théorème se déduit de la proposition suivante :

fix **Proposition 4.3.10.** *Soit un sous-groupe G unipotent de $GL_n(\mathbb{K})$, avec $\mathbb{K}$ algébriquement clos, alors il existe $x \in V$ non-nul tel que pour tout $g \in G$, $g.x = x$.*

Voyons comment le théorème 4.3.9 se déduit de la proposition :

DÉMONSTRATION. On procède par récurrence sur la dimension. Si $n = 1$, c'est clair. Si $n \geqslant 2$, on considère L la droite engendrée par x tel que dans 4.3.10 et l'hypothèse de récurrence appliquée à V/L, fournit un drapeau complet de V/L stable par G, d'où aussitôt un drapeau complet de V stable par G et il est clair que G est contenu dans le sous-groupe B_1 correspondant. □

Il s'agit donc maintenant de montrer la proposition fix 4.3.10. On commence par faire la définition suivante :

Définition 4.3.11. Soit un $\mathbb{K}$-espace vectoriel E, soit un sous-espace vectoriel $\mathcal{A} \subset \mathcal{L}(E)$, on dit que c'est une sous-algèbre si elle est stable par composition. On dit que $\mathcal{A}$ est irréductible si les seuls sous-espaces vectoriels de E stables par $\mathcal{A}$ sont $\{0\}$ ou E.

L'énoncé fondamental pour montrer fix 4.3.10 est le théorème de Burnside :

burn **Théorème 4.3.12** (Burnside)**.** *[admis] Soient un corps $\mathbb{K}$ algébriquement clos, un $\mathbb{K}$-espace vectoriel E de dimension finie, et une sous-algèbre irréductible $\mathcal{A} \subset \mathcal{L}(E)$, alors $\mathcal{A} = \mathcal{L}(E)$.*

La proposition fix 4.3.10 est une application immédiate de Burnside :

Démonstration. On procède par récurrence sur la dimension. Si $n = 1$ c'est clair, supposons donc $n \geqslant 2$. S'il existe un sous-espace vectoriel strict et non-nul $V \subset \mathbb{K}^n$ qui est G-stable, alors on a le résultat par hypothèse de récurrence. On suppose donc que les seuls sous-espaces G-stables de $\mathbb{K}^n$ sont $\{0\}$ et $\mathbb{K}^n$. Notons $\mathcal{G} = \mathrm{Vect}(G) \subset M_n(\mathbb{K})$, comme G est un groupe, par linéarité, on a bien que $\mathcal{G}$ est stable par produit, donc c'est une sous-algèbre et par hypothèse, elle est irréductible, donc $\mathcal{G} = M_n(\mathbb{K})$. Soit $x \in G$, on écrit alors $x = I_n + N$ avec N nilpotente. Comme toutes les matrices sont unipotentes, on a pour tout $g \in G$, $\mathrm{Tr}(g) = n$. On trouve alors :

$$\forall\ g' \in G, \mathrm{tr}(ng') = \mathrm{Tr}((x - I_n)g') = \mathrm{Tr}(xg') - \mathrm{Tr}(g') = 0,$$

et donc comme $\mathcal{G} = M_n(\mathbb{K})$, par linéarité, on trouve que :

$$\forall\ M \in M_n(\mathbb{K}), \mathrm{Tr}(NM) = 0,$$

soit $N = 0$. Ainsi, $G = \{1\}$, contradiction. □

4.4. Exponentielle matricielle. Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, on munit $M_n(\mathbb{K})$ de la norme :

$$\|M\|_1 = \max_{1 \leqslant i \leqslant n} \sum_{j=1}^{n} |a_{ij}|.$$

Lemme 4.4.1. *La norme $\|\|_1$ est sous-multiplicative, i.e, on a :*

$$\forall\ A, B \in M_n(\mathbb{K}), \|AB\|_1 \leqslant \|A\|_1 \|B\|_1 .$$

Démonstration. En effet, on a :

$$\sum_{j=1}^{n} |(AB)_{ij}| \leqslant \sum_{j=1}^{n} \sum_{k=1}^{n} |a_{ik} b_{kj}| = \sum_{k=1}^{n} |a_{ik}| \sum_{j=1}^{n} |b_{kj}| \leqslant (\sum_{k=1}^{n} |a_{ik}|).\|B\|_1 \leqslant \|A\|_1 \|B\|_1 ,$$

soit en passant au max :

$$\|AB\|_1 \leqslant \|A\|_1 \|B\|_1 .$$

□

Pour $A \in M_n(\mathbb{C})$, on considère alors la série $\sum \frac{A^k}{k!}$; par sous-multiplicativité de $\|.\|_1$, on a :

$$\forall\ n \in \mathbb{N}, \sum_{k=0}^{n} \left\| \frac{A^k}{k!} \right\|_1 \leqslant \sum_{k=0}^{n} \frac{\|A\|_1^k}{k!},$$

et donc la série est normalement convergente, donc convergente. On définit ainsi :

$$\exp(A) = \sum_{k=0}^{+\infty} \frac{A^k}{k!}.$$

On remarque que l'on a $\exp(0) = I_n$. De plus, on remarque que si :

$$M = \begin{pmatrix} \lambda_1 & \cdots & \cdots & * \\ 0 & \lambda_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix} \in \mathcal{T}_n(\mathbb{K}),$$

alors pour tout $n \in \mathbb{N}$, on a :

$$\sum_{k=0}^{n} \frac{M^k}{k!} = \begin{pmatrix} \sum\limits_{k=0}^{n} \frac{\lambda_1^k}{k!} & \cdots & \cdots & * \\ 0 & \sum\limits_{k=0}^{n} \frac{\lambda_2^k}{k!} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sum\limits_{k=0}^{n} \frac{\lambda_n^k}{k!} \end{pmatrix} \in \mathcal{T}_n(\mathbb{K}),$$

donc en passant à la limite, on a :

$$\exp(M) = \begin{pmatrix} e^{\lambda_1} & \cdots & \cdots & * \\ 0 & e^{\lambda_2} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{\lambda_n} \end{pmatrix} \in \mathcal{T}_n(\mathbb{K}) \qquad (4.4.1.1) \quad \boxed{\texttt{\{exp-tri\}}}$$

exp-prop

Lemme 4.4.2. *On a les propriétés suivantes :*

(i) *Pour $A, B \in M_n(\mathbb{K})$ qui commutent,* $\exp(A)\exp(B) = \exp(A+B)$. *En particulier,* $\exp(A) \in GL_n(\mathbb{K})$, *d'inverse* $\exp(-A)$.

(ii) *Pour tout $P \in GL_n(\mathbb{K})$ et $A \in M_n(\mathbb{K})$,* $P\exp(A)P^{-1} = \exp(PAP^{-1})$.

(iii) *Pour tout $M \in M_n(\mathbb{K})$, on a* $\det(\exp(M)) = \exp(\mathrm{Tr}(M))$.

(iv) *Pour tout $M \in M_n(\mathbb{K})$,* $\exp(M)$ *est un polynôme en M.*

DÉMONSTRATION. (i) Soient $A, B \in M_n(\mathbb{K})$ qui commutent, en particulier, on peut appliquer le binôme de Newton, calculons le produit des séries absolument convergentes :

$$\exp(A).\exp(B) = (\sum_{i=0}^{+\infty} \frac{A^i}{i!})(\sum_{j=0}^{+\infty} \frac{B^j}{j!}) = \sum_{n=0}^{\infty}(\sum_{p+q=n} \frac{A^p B^q}{p!q!}) \tag{4.4.3.1}$$

$$= \sum_{n=0}^{\infty} \frac{1}{n!}(\sum_{p+q=n} \frac{n!}{p!q!} A^p B^q) = \sum_{n=0}^{+\infty} \frac{1}{n!}(\sum_{p=0}^{n} \binom{n}{p} A^p B^{n-p}) = \sum_{n=0}^{+\infty} \frac{1}{n!}(A+B)^n \tag{4.4.3.2}$$

$$= \exp(A+B). \tag{4.4.3.3}$$

Ainsi, en prenant $B = -A$ et comme $\exp(0) = I_n$, on obtient que $\exp(A)\exp(-A) = I_n$ d'où l'assertion.

(ii) Fixons $d \in \mathbb{N}$, on a :

$$P(\sum_{k=0}^{d} \frac{A^k}{k!})P^{-1} = \sum_{k=0}^{d} \frac{(PAP^{-1})^k}{k!},$$

il suffit alors de passer à la limite sur d.

(iii) Comme $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, on peut trigonaliser M dans $M_n(\mathbb{C})$, de telle sorte que $M = PTP^{-1}$ avec T triangulaire supérieure. Comme le déterminant et la trace sont invariants par conjugaison et extension de corps, on se ramène donc au cas triangulaire supérieur.

Maintenant, si $(\lambda_1, \ldots, \lambda_n)$ sont les valeurs propres de T, d'après (4.4.1.1), on trouve :

$$\det(\exp(T)) = \prod_{i=1}^{n} e^{\lambda_i} = e^{\sum_{i=1}^{n} \lambda_i} = e^{\mathrm{tr}(T)}.$$

(iv) Les sommes partielles $S_n(M)$ sont dans le sous-espace vectoriel $\mathbb{C}[M] \subset M_n(\mathbb{C})$ qui est fermé, donc $\exp(M) \in \mathbb{C}[M]$. □

On obtient ainsi une application continue $\exp : M_n(\mathbb{C}) \to GL_n(\mathbb{C})$. On va voir qu'elle est bijective sur certains morceaux de $GL_n(\mathbb{C})$.

Notons $\mathrm{Nilp}_n(\mathbb{C}) \subset T_n(\mathbb{C})$, l'espace vectoriel des matrices nilpotentes triangulaires supérieures. Si $M \in \mathrm{Nilp}_n(\mathbb{C})$, alors $M^n = 0$ et on a $\exp(M) = I_n + \sum_{k=0}^{n-1} \frac{M^k}{k!}$. En particulier, on a $\exp(M) \in U_n$.

exp-unip

Théorème 4.4.4. *Soit $U \subset GL_n(\mathbb{C})$ un sous groupe unipotent, alors $\exp : \mathfrak{n} = \exp^{-1}(U) \to U$ est un homéomorphisme et il existe $g \in GL_n(\mathbb{C})$ tel que $g\mathfrak{n}g^{-1} \subset \mathrm{Nilp}_n$. En particulier, on a un homéomorphisme $\exp : \mathrm{Nilp}_n \to U_n$, d'inverse $\ln : U_n \to \mathrm{Nilp}_n$.*

Démonstration. D'après le théorème de Kolchin, il existe $g \in GL_n(\mathbb{C})$ tel que $gUg^{-1} \subset U_n$, en vertu de exp-prop 4.4.2(ii), on est donc ramené à montrer que exp : $\mathrm{Nilp}_n \to U_n$ est un homéomorphisme. Pour ce faire, on définit $\ln : U_n \to \mathrm{Nilp}$ par :

$$\ln(M) = \sum_{d=1}^{\infty} (-1)^{d-1} \frac{(M - I_n)^d}{d}, M \in U_n.$$

Comme $M \in U_n$, alors $M - I_n$ est nilpotente, de telle sorte que la somme est en fait finie. Montrons que $\exp \circ \ln = Id_{\mathrm{Nilp}_n}$ et $\ln \circ \exp = Id_{\mathrm{Nilp}_n}$. Considérons les polynômes $P(X) = \sum_{k=1}^{n-1} \frac{X^k}{k!}$ et $Q(X) = \sum_{k=0}^{n-1} \frac{(-1)^{k-1} X^k}{k} \in \mathbb{C}[X]$. Il s'agit de voir que $P(Q(N)) = N$ pour $N \in \mathrm{Nilp}_n$. Pour la calculer, on a seulement besoin de tronquer $P \circ Q$ à l'ordre $n-1$. Or on a $e^x - 1 = P(x) + o(x^n)$ et $\ln(1+x) = Q(x) + o(x^{n-1})$, en particulier $P \circ Q$ tronqué à l'ordre $n-1$ est précisément le développement limité à l'ordre $n-1$ de $e^{\ln(1+x)} - 1 = x$, c'est-à-dire X. Ainsi $P(Q(N)) = N$, c'est pareil dans l'autre sens et exp est un homéomorphisme. □

ln-nilp **Remarque 4.4.5.** La preuve ci-dessus donne également que si $U \in U_n$, alors $\ln(U) \in \mathrm{Nilp}_n$ est un polynôme en U. Cela se déduit par le lemme argument que exp-prop 4.4.2.(iv).

La preuve ci-dessus nous permet de pouvoir définir un logarithme sur un certain voisinage de l'identité :

logid **Proposition 4.4.6.** *Soit $M \in M_n(\mathbb{C})$ avec $\|M - I_n\|_1 < 1$, alors la série $\sum_{d \geqslant 1} (-1)^{d-1} \frac{(M-I_n)^d}{d}$ converge, soit $\ln(M)$ sa somme, on a l'identité :*

$$\exp(\ln(M)) = M.$$

Démonstration. Par sous-multiplicativité de $\|\|_1$, on a immédiatement que la série est normalement convergente, donc convergente. Il suffit de vérifier que l'on a bien $\exp(\ln(M)) = M$. Si $M = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ avec $|\lambda_i - 1| < 1$ pour tout i, alors $\exp(\ln(M)) = \mathrm{diag}(\exp(\ln \lambda_1), \ldots, \exp(\ln(\lambda_n)) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) = M$ [3]. De plus, on a $\ln(PAP^{-1}) = P \ln(A) P^{-1}$ [4], donc en utilisant exp-prop 4.4.2(ii), on en déduit l'égalité pour toute matrice diagonalisable dans $\mathbb{C}$. On utilise alors la densité des matrices diagonalisables. La fonction $A \to \ln(A)$ est bien continue sur la boule ouverte $B(I_n, 1)$ car la série est normalement convergente sur tout compact de $B(I_n, 1)$. De même la série $A \to \exp(A)$ est continue, car normalement convergente sur tout compact. Par composition $\exp \circ \ln$ est donc aussi continue sur $B(I_n, 1)$. Les deux membres sont continus en A, donc en prenant une suite de matrices diagonalisables $A_r \to A$, avec $\|A - I_n\| < 1$, le cas des matrices diagonalisables donne que :

$$A_r = \exp(\ln(A_r)) \overset{r \to +\infty}{\to} \exp(\ln(A)),$$

et donc par unicité de la limite $\exp(\ln(A)) = A$. □

3. C'est standard dans $\mathbb{R}$, dans $\mathbb{C}$, on utilise la $\mathbb{C}$-dérivabilité de chacune des fonctions, à l'aide du théorème de séries entières, le fait que les dérivées sont les mêmes et que les fonctions ont même valeur en 1.

4. clair sur les sommes partielles et on passe à la limite.

Une autre utilité de l'exponentielle est qu'elle va nous permettre de linéariser la structure de groupe. On a besoin d'un lemme préliminaire :

stab-exp **Lemme 4.4.7.** *Soient $X, Y \in M_n(\mathbb{C})$, alors :*

$$\lim_{n\mapsto+\infty}(\exp(\frac{X}{n})\exp(\frac{Y}{n}))^n = \exp(X+Y).$$

On a également :

$$\lim_{n\mapsto+\infty}(\exp(\frac{X}{n})\exp(\frac{Y}{n})\exp(\frac{-X}{n})\exp(\frac{-Y}{n}))^{n^2} = \exp(XY-YX).$$

Démonstration. Comme $\exp(\frac{X}{n}) = \mathrm{Id} + \frac{X}{n} + O(\frac{1}{n^2})$, soit :

$$\exp(\frac{X}{n})\exp(\frac{Y}{n}) = \mathrm{Id} + \frac{X+Y}{n} + O(\frac{1}{n^2}).$$

Pour n assez grand, cette quantité est assez proche de l'identité de telle sorte que :

$$n\ln(\exp(\frac{X}{n})\exp(\frac{Y}{n})) = X + Y + O(\frac{1}{n}),$$

Il suffit maintenant d'appliquer l'exponentielle et d'utiliser logid 4.4.6. Pour la deuxième identité, elle se démontre de la même manière à l'aide du développement limité :

$$\exp(\frac{X}{n})\exp(\frac{Y}{n})\exp(\frac{-X}{n})\exp(\frac{-Y}{n}) = I_n + \frac{X^2+2XY+Y^2}{n^2} - \frac{(X+Y)^2}{n^2} + O(\frac{1}{n^3}) \tag{4.4.7.1}$$

$$= I_n + \frac{XY-YX}{n^2} + O(\frac{1}{n^3}). \tag{4.4.7.2}$$

□

Ce lemme nous permet de faire la proposition/définition suivante :

Proposition 4.4.8. *Soit un sous-groupe fermé $G \subset GL_n(\mathbb{C})$, on définit l'algèbre de Lie $\mathfrak{g} = \mathrm{Lie}(G)$ de G par $\mathfrak{g} = \{M \in M_n(\mathbb{C}), \forall\ t \in \mathbb{R}, \exp(tM) \in G\}$. C'est un sous-espace vectoriel de $M_n(\mathbb{C})$ stable par le crochet de Lie $(X,Y) \mapsto [X,Y] = XY - YX$.*

Démonstration. Immédiat avec le lemme stab-exp 4.4.7 et comme G est fermé. □

On a donc les exemples suivants :

lie-exa **Exemple 4.4.9.** (i) On a bien sûr $\mathrm{Lie}(GL_n(\mathbb{C})) = M_n(\mathbb{C})$, on la note souvent $\mathfrak{gl}_n$.

(ii) $\mathrm{Lie}(T_n) = D_n$, pour $T_n \subset GL_n(\mathbb{C})$, le tore diagonal, i.e. le sous-groupe des matrices diagonales inversibles et D_n l'espace vectoriel des matrices diagonales. En effet si $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, alors $e^D = (e^{\lambda_1}, \ldots, e^{\lambda_n})$ et $\exp : \mathbb{C} \to \mathbb{C}^\times$ est surjective. Ainsi, $\exp : \mathrm{Lie}(T_n) \to T_n$ est surjective.

(iii) On a vu que $\mathrm{Lie}(U_n) = \mathrm{Nilp}_n$ et que $\exp : \mathrm{Nilp}_n \to U_n$ est un homéomorphisme.

Il résulte donc du deuxième exemple que l'exponentielle n'est pas injective dans $M_n(\mathbb{C})$ puisque $\exp : \mathbb{C} \to \mathbb{C}^\times$ ne l'est pas. L'exponentielle n'est pas plus injective dans $M_n(\mathbb{R})$ pour $n \geqslant 2$. En effet, si on prend :

$$M = \begin{pmatrix} 0 & -2\pi \\ 2\pi & 0 \end{pmatrix},$$

elle est est semblable dans $M_2(\mathbb{C})$ à $\begin{pmatrix} 2i\pi & 0 \\ 0 & -2i\pi \end{pmatrix}$ dont l'exponentielle vaut I_n.

Théorème 4.4.10. *L'exponentielle* $\exp : \mathfrak{gl}_n(\mathbb{C}) \to GL_n(\mathbb{C})$ *est surjective.*

Démonstration. Soit $M \in M_n(\mathbb{C})$, si $M = D + N$ est la décomposition de Dunford de M en diagonalisable et nilpotent qui commutent, alors on a d'après 4.4.2(i) :

$$\exp(M) = \exp(D)\exp(N) = \exp(D) + \exp(D)(\exp(N) - I_n). \tag{4.4.10.1}$$

{dun-exp}

Les deux termes commutent clairement, $\exp(D)$ est bien diagonalisable et comme $\exp(N)$ est unipotente d'après (4.4.1.1), $(\exp(N) - I_n)$ est bien nilpotente et le reste en multiplicant par $\exp(D)$ comme elles commutent. On obtient donc que (4.4.10.1) est la décomposition de Dunford de $\exp(M)$.

Considérons maintenant $M' \in GL_n(\mathbb{C})$, soit $M' = D' + N'$, sa décomposition de Dunford. En vertu de (4.4.10.1), on cherche N nilpotente et D diagonalisable qui commutent telles que :

$$\exp(D) = D', \exp(D)(\exp(N) - I_n) = N'$$

D'après 4.4.4, il existe une unique matrice N nilpotente telle que $\exp(N) = I_n + (D')^{-1}N'$ et d'après 4.4.9, on peut trouver D diagonalisable telle que $\exp(D) = D'$. La difficulté est de faire en sorte que D et N commutent. Tout d'abord, d'après 4.4.5, N est un polynôme en N', il suffit donc de choisir D qui soit un polynôme en D'. Si $D' = \mathrm{diag}(d'_1, \ldots, d'_n)$, il suffit de prendre D telle que $d_i = d_j$ à chaque fois que $d'_i = d'_j$ et on a alors $D = Q(D')$ où Q est un polynôme d'interpolation de Lagrange [5] qui envoie les d'_i distincts sur les d_i. On obtient alors que pour un tel choix, D et N commutent et on obtient :

$$\exp(D + N) = M',$$

comme souhaité. □

5. On rappelle que si on a $(x_0, \ldots, x_n) \in \mathbb{K}^n$ distincts et $(y_0, \ldots, y_n) \in \mathbb{K}^n$, alors il existe un unique polynôme P de degré n tel que $P(x_i) = y_i$

Remarque 4.4.11. On peut montrer qu'en général si $G \subset GL_n(\mathbb{C})$ est un sous-groupe fermé $\exp(\mathrm{Lie}(G))$ engendre G, mais l'exponentielle n'est pas toujours surjective.

Chapitre 2

Étude de GL_n et SL_n

1. La simplicité de $PSL_n(\mathbb{K})$

1.1. Rappels sur les transvections. Soient un corps $\mathbb{K}$ et E un $\mathbb{K}$-espace vectoriel de dimension finie.

transv **Proposition 1.1.1.** *Soit $H = \mathrm{Ker}(f)$ un hyperplan de E, avec $f \in E^\vee$. Soit $u \in GL(E)$ tel que $u_{|H} = \mathrm{Id}_H$ et $u \neq \mathrm{Id}_E$. Les assertions suivantes sont équivalentes :*

(i) *On a $\det(u) = 1$.*

(ii) *u n'est pas diagonalisable.*

(iii) *On a $D = \mathrm{Im}(u - \mathrm{Id}) \subset H$.*

(iv) *Il existe $a \in H$, $a \neq 0$ tel que l'on ait :*

$$\forall\ x \in E, u(x) = x + f(x)a.$$

(v) *Dans une base convenable, la matrice de u s'écrit :*

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ & & \ddots & 1 \\ 0 & & \cdots & 1 \end{pmatrix}$$

On dit alors que u est la transvection d'hyperplan H et de droite $D = (a)$.

Démonstration. (i) $\Longrightarrow$ (ii) est clair, car sinon on aurait $u = \mathrm{Id}$, ainsi que (v) $\Longrightarrow$ (i). (ii) $\Longrightarrow$ (iii) également, car par le théorème du rang $\dim(\mathrm{Im}(u - \mathrm{Id})) = 1$, donc si $\mathrm{Im}(u - \mathrm{Id}) \not\subset H$, alors ils sont en somme directe et u diagonalisable.

(iii) $\Longrightarrow$ (iv) Soit $x_0 \in E$ tel que $f(x_0) = 1$, l'élément $a = u(x_0) - x_0 \in \mathrm{Im}(u - \mathrm{Id}) \subset H$ par hypothèse. Comme $x_0 \notin H$, $a \neq 0$ et on a donc pour tout $x \in E$:

$$u(x) = x + f(x)a.$$

(iv) $\Longrightarrow$ (v). On construit une base $e_1, \ldots, e_n$ de E en partant de $e_{n-1} = a$ que l'on complète en une base $e_1, \ldots, e_{n-1}$ de H et on prend enfin $e_n \notin H$ tel que $f(e_n) = 1$. □

Remarque 1.1.7. (i) On prendra garde au fait que la donnée de H et D ne détermine pas la transvection, il suffit de penser à la matrice $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$.

(ii) On rappelle le résultat que $SL(E)$ est engendré par les transvections et $GL(E)$ par les transvections et dilatations.

Dans la suite pour $f \in E^\vee$ avec $f \neq 0$ et $a \in \mathrm{Ker}(f) - \{0\}$, on note $\tau(f, a)$ la transvection donnée par la formule :

$$\tau(f, a)(x) = x + f(x)a.$$

tconj **Proposition 1.1.8** (Comportement par conjugaison)**.** *Soit τ une transvection d'hyperplan H et de droite D, $u \in GL(E)$, alors $u\tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$. Précisément si $\tau = \tau(f, a)$ alors $u\tau u^{-1} = \tau(f \circ u^{-1}, u(a))$*

Démonstration. Pour $x \in E$, on a $\tau u^{-1}(x) = u^{-1}(x) + f(u^{-1}(x))a$, d'où $u\tau u^{-1}(x) = x + f(u^{-1}(x))u(a)$, d'où le résultat. On notera que si $H = \mathrm{Ker}\, f$, alors $u(H) = \mathrm{Ker}(f \circ u^{-1})$. □

1.2. Centre de $GL_n(\mathbb{K})$.

centre **Proposition 1.2.1.** *Pour tout $n \in \mathbb{N}^*$, on a $Z(GL(E)) = \{\lambda Id_E, \lambda \in \mathbb{K}^\times\} \cong \mathbb{K}^\times$. De plus, on a $Z(SL(E)) = \{\lambda\, \mathrm{Id}_E, \lambda \in \mathbb{K}, \lambda^n = 1\} = \mu_n(\mathbb{K})$.*

Démonstration. Quitte à choisir une base, on peut supposer que $E = \mathbb{K}^n$. Soit $u \in Z(GL_n(\mathbb{K}))$ ou $Z(SL_n(\mathbb{K}))$, alors u commute avec toutes les transvections qui sont dans $SL_n(\mathbb{K})$, en particulier d'après tconj 1.1.8, on obtient que u stabilise toutes les droites vectorielles. En particulier, la base canonique de $\mathbb{K}^n$ est une base de vecteurs propres et u diagonalisable. Maintenant, pour toute matrice de permutation $A_\sigma \in GL_n(\mathbb{K})$, on doit avoir $A_\sigma D A_\sigma^{-1} = D$, ainsi si $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, on a :

$$A_\sigma D A_\sigma^{-1} = \mathrm{diag}(\lambda_{\sigma(1)}, \ldots, \sigma(\lambda_{\sigma(n)}))$$

ce qui force que pour tout $i \neq j$, $\lambda_i = \lambda_j$ et $u = \lambda I_n$. Enfin, si $u \in SL_n(\mathbb{K})$, on a $\det(u) = 1$, soit $\lambda^n = 1$. □

Remarque 1.2.2. On prendra garde au fait que l'on n'a pas nécessairement $\mathrm{card}(\mu_n(\mathbb{K})) = n$. En effet, si se place sur $\mathbb{F}_p$, on a $X^p - 1 = (X - 1)^p$ $[p]$ et $\mu_p(\mathbb{F}_p) = \{1\}$.

vect **Corollaire 1.2.3.** *Soit $u \in GL(E)$ qui stabilise toute droite vectorielle, alors u est une homothétie.*

Démonstration. En effet, dans ce cas, il commute avec toutes les transvections et dilatations qui engendrent $GL(E)$ donc c'est une homothétie. □

1.3. Espaces projectifs.

Définition 1.3.1. Le quotient de $GL(E)$ par son centre est appelé le groupe projectif linéaire noté $PGL(E)$. De même le quotient de $SL(E)$ par son centre est noté $PSL(E)$. On note $PGL_n(\mathbb{K})$ et $PSL_n(\mathbb{K})$ les groupes matriciels correspondants.

Soit h_λ l'homothétie $x \mapsto \lambda x$, on a $\det h_\lambda = \lambda^n$ de telle sorte que l'on a une suite exacte :

$$1 \to PSL(E) \to PGL(E) \to \mathbb{K}^\times/\mathbb{K}^{\times n} \to 1,$$

avec $\mathbb{K}^{\times n} = \{\lambda \in \mathbb{K}^\times, \exists \mu \in \mathbb{K}, \lambda = \mu^n\}$. En particulier, si $\mathbb{K}$ est algébriquement clos, on a $PSL(E) = PGL(E)$.

Notons $\mathbb{P}(E)$ l'ensemble des droites vectorielles de E, on l'appelle l'espace projectif. On a une application surjective :

$$\phi : E - \{0\} \to \mathbb{P}(E)$$

donnée par $x \mapsto \langle x \rangle$ et pour une droite $L \in \mathbb{P}(E)$, si on choisit un vecteur $x \in L$, non-nul, on a $\phi^{-1}(L) = \{\lambda x, \lambda \in \mathbb{K}^\times\}$. Ainsi l'action libre de $\mathbb{K}^\times$ sur $E - \{0\}$ induit une bijection par passage au quotient :

$$(E - \{0\})/\mathbb{K}^\times \cong \mathbb{P}(E). \tag{1.3.1.1}$$

{proj}

Le groupe $GL(E)$ agit sur les droites de $\mathbb{P}(E)$ et d'après 1.2.3 si $g \in GL(E)$ stabilise toute droite vectorielle, alors g est une homothétie. On en déduit le corollaire suivant :

fid

Corollaire 1.3.2. *Le groupe $PGL(E)$ agit fidèlement sur $\mathbb{P}(E)$. De plus, si $\mathbb{K}$ est un corps fini de cardinal q, on a* $\mathrm{card}(\mathbb{P}(E)) = \frac{q^n-1}{q-1}$ *avec* $n = \dim(E)$. *En particulier, si* $\dim(E) = 2$, *on trouve* $\mathrm{card}(\mathbb{P}(E)) = q + 1$.

Remarque 1.3.3. Cela justifie donc la terminologie de groupe projectif linéaire.

Démonstration. Il ne nous reste qu'à montrer l'assertion sur le cardinal, or on a $\mathrm{card}(E) = q^n$ et comme $\mathbb{K}^\times$ agit fidèlement, il résulte de (1.3.1.1) que l'on a :

$$\mathrm{card}(\mathbb{P}(E)) = \frac{q^n - 1}{q - 1}.$$

□

Si $E = \mathbb{K}^{n+1}$, on note $\mathbb{P}^n_{\mathbb{K}} = \mathbb{P}(\mathbb{K}^{n+1})$ et pour $n = 1$, on appelle $\mathbb{P}^1_{\mathbb{K}}$, la droite projective ; cela vient du fait que la donnée d'un élément $L \in \mathbb{P}^1(\mathbb{K})$ correspond, via (1.3.1.1) à une classe d'équivalence de paires $(x, y) \in \mathbb{K}^2 - \{0\}$. Ainsi, si $y \neq 0$, on a :

$$[x, y] \sim [\frac{x}{y}, 1]$$

et si $y = 0$, comme $(x, y) \neq (0, 0)$, on a $x \neq 0$, on déduit que $[x, 0] \sim [1, 0]$. On note alors $\infty = [1, 0]$. On a donc obtenu la description suivante :

proj2 **Proposition 1.3.4.** *Soit $\widehat{\mathbb{K}} = \mathbb{K} \cup \{\infty\}$, alors on a une bijection entre $\mathbb{P}^1_K \to \widehat{\mathbb{K}}$ donnée par $[x, y] \mapsto \frac{x}{y}$ si $y \neq 0$ et $[x, 0] \mapsto \infty$.*

1.4. Classes de conjugaison de transvections.

conj **Théorème 1.4.1.** *Dans $GL(E)$, toutes les transvections sont conjuguées. Si $n = \dim(E) \geqslant 3$, elles sont aussi conjuguées dans $SL(E)$.*

DÉMONSTRATION. Pour la première assertion, c'est clair d'après transv 1.1.1.(v). Pour la deuxième, si $n \geqslant 3$, soient u, v deux transvections et $w \in GL(E)$ tel que $u = wvw^{-1}$. Si $\lambda = \det(w)$, il suffit de trouver $s \in GL(E)$ tel que $\det(s) = \lambda^{-1}$ et $svs^{-1} = v$. En effet, on aura alors $sw \in SL(E)$ et $(sw)v(sw)^{-1} = u$. Pour ceci, on se place dans une base où la matrice de v est donnée par :

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ & & \ddots & 1 \\ 0 & & \cdots & 1 \end{pmatrix}$$

et on prend $s = \mathrm{diag}[1, \ldots, 1, \lambda, \frac{1}{\lambda}, \frac{1}{\lambda}]$, ce qui est possible comme $n \geqslant 3$. □

Pour $n = 2$, la proposition est fausse, on a le résultat suivant :

conj2 **Proposition 1.4.2.** (i) *Dans $SL_2(\mathbb{K})$, toute transvection est conjuguée à $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, avec $\lambda \in \mathbb{K}^\times$.*

(ii) *Soient $\lambda, \mu \in \mathbb{K}^\times$, alors $s = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $t = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjuguées dans $SL_2(\mathbb{K})$ si et seulement si $\frac{\lambda}{\mu}$ est un carré dans $\mathbb{K}$.*

DÉMONSTRATION. (i) Soient u une transvection, e_1, e_2 une base de E, $\mathbb{K}\epsilon_1$ l'hyperplan de u et $\epsilon_2 \notin \mathbb{K}\epsilon_1$, dans la base $(\alpha\epsilon_1, \epsilon_2)$, u a la matrice voulue et pour α convenable, on a $\det(\alpha\epsilon_1, \epsilon_2)/\det(e_1, e_2) = 1$, donc le changement de base est dans $SL_2(\mathbb{K})$.

(ii) On écrit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{K})$ qui conjugue s et t, soit $gs = tg$. On trouve alors :

$$gs = \begin{pmatrix} a & \lambda a + b \\ c & \lambda c + d \end{pmatrix} = tg = \begin{pmatrix} a + \mu c & b + \mu d \\ c & d \end{pmatrix},$$

soit $c = 0$ et $\lambda a = \mu d$ avec $d = \frac{1}{a}$ car $\det(g) = 1$, donc $\frac{\lambda}{\mu}$ est un carré. Réciproquement, si $\frac{\lambda}{\mu} = \delta^2 \in \mathbb{K}^\times$, on prend $a = \frac{1}{\delta}$, $c = 0$, b quelconque et g convient pour passer de s à t. □

Remarque 1.4.5. Les classes de conjugaison des transvections dans $SL_2(\mathbb{K})$ dépendent donc fortement du corps de base. En effet, si $\mathbb{K}$ est algébriquement clos, alors elles sont toutes conjuguées. En revanche, si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{F}_p$, on a deux classes de conjugaison, une infinité si $\mathbb{K} = \mathbb{Q}$.

1.5. L'énoncé de simplicité.

Le théorème fondamental est le suivant :

simpl **Théorème 1.5.1.** *Le groupe $PSL_n(\mathbb{K})$ est simple sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$.*

Remarque 1.5.2. L'idée de la preuve est d'utiliser le fait que les transvections engendrent $SL(E)$ et que dans un certain nombre de cas favorables, elles sont toutes conjuguées. En particulier, si on arrive à montrer qu'un sous-groupe distingué H contient une transvection, elle les contiendra toutes. Il faut évidemment diviser par le centre, parce que cela fournit de manière évidente un sous-groupe distingué non-trivial, mais en dehors de celui-ci, il n'y en a pas d'autres.

Démonstration. Soit E un $\mathbb{K}$-espace vectoriel de dimension n, notons $\overline{N} \subset PSL(E)$ un sous-groupe distingué non-trivial. Par image réciproque, on dispose donc d'un sous-groupe distingué $N \lhd SL(E)$ tel que N contient strictement le centre Z de $SL(E)$. On veut montrer que $N = SL(E)$, on distingue deux cas.

Premier cas : $n \geqslant 3$. D'après conj 1.4.1, toutes les transvections sont conjuguées et elles engendrent $SL(E)$, il suffit de montrer que l'une d'elles est dans N. Soit $\sigma \in N$ non-trivial. On fabrique de nouveaux éléments de N comme commutateurs :

$$\text{Si } \tau \in SL(E), \text{alors } \tau = \sigma(\tau\sigma^{-1}\tau^{-1}) \in N.$$

Si τ est une transvection d'hyperplan H, $\sigma\tau\sigma^{-1}$ est une transvection d'hyperplan $\sigma(H)$ donc $\rho = (\sigma\tau\sigma^{-1})\tau^{-1}$ est produit de deux transvections et est même une transvection si $\rho(H) = H$ et $\rho \neq \mathrm{Id}$. Il suffit donc de chercher un élément qui laisse globalement invariant un hyperplan. Soit $\sigma \in N$, $\sigma \notin Z$, comme σ n'est pas une homothétie, il existe $a \in E$ tel que $b = \sigma(a)$ ne soit pas colinéaire à a. Soit τ une transvection de droite $\langle a \rangle$ et posons $\rho = \sigma\tau\sigma^{-1}\tau^{-1}$. Soit H un hyperplan de E contenant $\mathrm{Vect}(a, b)$, il en existe comme $n \geqslant 3$. On a les trois propriétés suivantes :

— $\rho \in N$, $\rho \neq \mathrm{Id}$.

— $\forall\ x \in E, \rho(x) - x \in H$.

— $\rho(H) = H$

En effet, pour le premier point, on a clairement $\rho \in N$ et si $\rho = \mathrm{Id}$, alors $\tau = \sigma\tau\sigma^{-1}$, mais ces transvections sont respectivement de droites (a) et (b) et on a $(a) \neq (b)$. Pour le deuxième point, on remarque d'après transv 1.1.1.(iv) que l'on a $\rho(x) - x \in \mathrm{Vect}(a, b) \subset H$ et le troisième point en résulte aussitôt.

Deux cas sont possibles :

(i) Il existe une transposition u d'hyperplan H qui ne commute pas à ρ.
Alors si on pose $v = \rho u \rho^{-1} u^{-1}$, on a $v \in N$, $v \neq \mathrm{Id}$ et v produit des transvections u^{-1}, d'hyperplan H et $\rho u \rho^{-1}$ d'hyperplan $\rho(H) = H$, donc v est une transvection non-triviale de N.

(ii) Sinon, si ρ commute à toutes les transvections d'hyperplan H, soit $f \in E^\vee$ une équation de H et $u = \tau(f, c)$, avec $c \in H$, comme $\rho u = u\rho$, pour tout $x \in E$, on a :

$$\rho(x) + f(x)\rho(c) = \rho(x) + f(\rho(x))c.$$

Soit $x \notin H$ comme $\rho(x) - x \in H$, on a $f(\rho(x)) = f(x) \neq 0$ d'où $\rho(c) = c$, mais comme ceci vaut pour tout $c \in H$, on a $\rho_{|H} = \mathrm{Id}$ et comme ρ est de déterminant un, ρ est déjà une transvection.

Ainsi, dans les deux cas, N contient une transvection non-triviale, donc $N = SL(E)$ si $n \geqslant 3$.

Deuxième cas : $n = 2$. Dans cette situation, deux arguments ne marchent plus, les transvections ne sont plus toutes conjuguées en général et on a utilisé $n \geqslant 3$ dans la construction d'un élément de N qui fixe un hyperplan. En notant que si $n = 2$, l'existence d'un hyperplan stable revient à l'existence d'un vecteur propre non-nul, on en déduit que si k algébriquement clos, le même argument que ci-dessus s'étend en utilisant I.4.2. Dans le cas général, on va construire un élément $g \in N$ avec une valeur propre et suffisamment de transvections dans le groupe, à nouveau à l'aide de commutateurs.

Dans toute la suite, on suppose que $\mathrm{card}(\mathbb{K}) \geqslant 7$: On verra ensuite comment traiter le cas $\mathbb{K} = \mathbb{F}_5$ et que les cas $\mathbb{K} = \mathbb{F}_2, \mathbb{F}_3$ sont exceptionnels.

2simp **Lemme 1.5.5.** *Supposons* $\mathrm{card}(\mathbb{K}) \geqslant 7$*, soit* $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{K})$*, avec* $c \neq 0$*, alors il existe* $g \in SL_2(\mathbb{K})$ *tel que* $g^{-1}s^{-1}gs$ *admette une valeur propre* $\lambda \in \mathbb{K}$ *avec* $\lambda \neq 0, 1$.

Démonstration. On cherche g sous la forme $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{K})$. Soit $e_1 = (1, 0)$, on doit résoudre $g^{-1}s^{-1}gs(e_1) = \lambda e_1$, i.e. $gs(e_1) = \lambda sg(e_1)$, i.e. :

$$a\alpha + c\beta = \lambda(a\alpha + b\gamma) \qquad (1.5.5.1)$$ {1}

$$a\gamma + c\delta = \lambda(c\alpha + d\gamma). \qquad (1.5.5.2)$$ {2}

Soit $\lambda \in (\mathbb{K}^*)^2$ avec $\lambda \neq \pm 1$; un tel λ existe car $\mathrm{card}(\mathbb{K}) \geqslant 7$ donc $\mathrm{card}((\mathbb{K}^*)^2 \geqslant 3$. On prend alors $\gamma = 0$, $\delta = \sqrt{\lambda}$, $\alpha = \frac{1}{\delta}$ et (2) (I.5.5.2) est satisfaite puisque comme $c \neq 0$, on prend $\beta = \frac{(\lambda-1)a}{c\sqrt{\lambda}}$ et (1) (I.5.5.1) est satisfaite. □

3simp **Lemme 1.5.6.** *Si* $s \in SL_2(\mathbb{K})$ *a une valeur propre* $\lambda \in \mathbb{K}$*, avec* $\lambda \neq \pm 1$*, s est conjuguée dans* $SL_2(\mathbb{K})$ *à* $t = \mathrm{diag}(\lambda, \frac{1}{\lambda})$.

DÉMONSTRATION. Comme $s \in SL_2(\mathbb{K})$, les valeurs propres de s sont alors λ et $\frac{1}{\lambda}$ qui sont distinctes comme $\lambda \neq \pm 1$, ainsi s est diagonalisable, donc conjuguée dans $GL_2(\mathbb{K})$ à $t = \mathrm{diag}(\lambda, \frac{1}{\lambda})$. Soit $g \in GL_2(\mathbb{K})$ tel que $s = gtg^{-1}$ l'élément qui conjugue et $d = \det(g) \in \mathbb{K}^*$, alors $v = \mathrm{diag}(1, \frac{1}{d})$ commute à t, on a $gv \in SL_2(\mathbb{K})$ et $s = (gv)t(gv)^{-1}$. □

4simp **Lemme 1.5.7.** *Soit $\lambda \in \mathbb{K}^*$, avec $\lambda \neq \pm 1$ et $s = \mathrm{diag}(\lambda, \frac{1}{\lambda})$, soit $\mu \in \mathbb{K}^*$ et $t = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$. Alors il existe $g \in SL_2(\mathbb{K})$ tel que l'on ait $g^{-1}s^{-1}gs = t$.*

DÉMONSTRATION. On cherche g sous la forme $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{K})$ avec $gs = sgt$. On trouve alors :

$$gs = \begin{pmatrix} \lambda a & \frac{b}{\lambda} \\ \lambda c & \frac{d}{\lambda} \end{pmatrix} = sgt = \begin{pmatrix} a\lambda & \lambda\mu a + b\lambda \\ \frac{c}{\lambda} & \frac{c\mu}{\lambda} + \frac{d}{\lambda} \end{pmatrix}.$$

La relation $\lambda c = \frac{c}{\lambda}$ implique $c = 0$ car $\lambda^2 \neq 1$. Il reste $\frac{b}{\lambda} = \lambda(\mu a + b)$ et $ad = 1$. On prend alors $a = \frac{1}{\lambda} - \lambda$ de sorte que $a \neq 0$ et $b = \lambda\mu$. □

On peut maintenant terminer la preuve du théorème dans le cas $n = 2$: Soit $s \in N$, $s \neq \pm \mathrm{Id}$.

(i) Si s a une valeur propre $\lambda \in \mathbb{K}^*$, $\lambda \neq \pm 1$, alors d'après 3simp 1.5.6, s est conjugué dans $SL(E)$ à $s' = \mathrm{diag}(\lambda, \frac{1}{\lambda})$, donc $s' \in N$. Ainsi, pour tout $\mu \in \mathbb{K}^*$, d'après 4simp 1.5.7 il existe $g \in SL(E)$ tel que $t = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} = g^{-1}(s')^{-1}gs'$. On obtient ainsi $t \in N$ et d'après conj2 1.4.2, on a $N = SL(E)$.

(ii) Si $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $c \neq 0$ alors comme $\mathrm{card}(\mathbb{K}) \geqslant 7$ par hypothèse, d'après 2simp 1.5.5, il existe $g \in SL(E)$ tel que $g^{-1}s^{-1}gs$ ait une valeur propre $\lambda \neq \pm 1$. Comme $g^{-1}s^{-1}gs \in N$, on est ramené au cas précédent.

(iii) Avec les notations de (ii) si $c = 0$ et que l'on n'est pas dans le cas (i), alors $s = \begin{pmatrix} \epsilon & \mu \\ 0 & \epsilon \end{pmatrix}$ avec $\epsilon = \pm 1$ et $\mu \neq 0$ car s non diagonalisable. Soit alors $t = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL(E)$. On a alors que $tst^{-1} = \begin{pmatrix} \epsilon & \mu \\ -\mu & \epsilon \end{pmatrix} \in N$ et on est ramené au cas précédent.

□

Remarque 1.5.8. A strictement parler, la preuve ne sera complètement finie que lorsque l'on aura traité le cas où $\mathrm{card}(\mathbb{K}) = 4$ ou 5. C'est fait dans la section suivante.

1.6. Isomorphismes exceptionnels. On commence par rappeler les formules de cardinalité suivantes :

card **Proposition 1.6.1.** *Soit un corps fini $\mathbb{K}$ de cardinal q, $n \in \mathbb{N}^*$, on a les formules suivantes :*

(i) $\mathrm{card}(GL_n(\mathbb{K})) = \prod_{i=0}^{n-1}(q^n - q^i)$

(ii) $\mathrm{card}(SL_n(\mathbb{K})) = q^{n-1}\prod_{i=0}^{n-2}(q^n - q^i) = N$

(iii) $\mathrm{card}(PGL_n(\mathbb{K})) = \mathrm{card}(SL_n(\mathbb{K})) = N$

(iv) $\mathrm{card}(PSL_n(\mathbb{K})) = \frac{N}{d}$, *avec* $d = n \wedge (q-1)$.

DÉMONSTRATION. (i) a été vu dans glnfp 2.3.3. (ii) vient de la suite exacte :

$$1 \to SL_n(\mathbb{F}_p) \to GL_n(\mathbb{F}_p) \to \mathbb{F}_p^\times$$

et du fait que $\mathrm{card}(\mathbb{K}^*) = q-1$ et pareillement pour $PGL_n(\mathbb{K})$ puisque $|Z(GL_n(\mathbb{K}))| = q-1$. Enfin, le dernier point vient du lemme suivant root 1.6.2. □

root **Lemme 1.6.2.** *Avec les notations précédentes, on a $|\mu_n(\mathbb{K})| = n \wedge (q-1)$.*

DÉMONSTRATION. Par Bezout, il existe $r, s \in \mathbb{Z}$ tels que $d = r(q-1) + sn$. Soit $x \in \mathbb{K}^*$, si $x \in \mu_n(\mathbb{F}_p)$, comme $x^{q-1} = 1$, on a $x^d = 1$. Réciproquement, si $x^d = 1$, a fortiori comme $d|n$, $x^n = 1$. Ainsi, $\mu_n(\mathbb{K}) = \mu_d(\mathbb{K})$. Le polynôme $X^{q-1} - 1$ admet $q-1$ racines dans $\mathbb{K}$, donc $X^d - 1$ qui en est un diviseur en admet d et donc $\mu_n(\mathbb{K}) = d$. □

Théorème 1.6.3. *On a les isomorphismes suivants :*

(i) $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \cong S_3$.

(ii) $PGL_2(\mathbb{F}_3) \cong S_4$, $PSL_2(\mathbb{F}_3) \cong A_4$.

(iii) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \cong A_5$.

(iv) $PGL_2(\mathbb{F}_5) = PSL_2(\mathbb{F}_5) \cong A_5$.

Remarque 1.6.4. Pour rappel, on note $\mathbb{F}_q$ le corps à q éléments.

DÉMONSTRATION. (i) Comme $\mathbb{F}_2^\times = \{1\}$, on a $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2)$. De plus, $GL_2(\mathbb{F}_2)$ agit fidèlement sur $\mathbb{P}(\mathbb{F}_2^2)$ qui d'après fid 1.3.2 est de cardinal trois, on obtient donc un morphisme injectif $\phi : GL_2(\mathbb{F}_2) \to S_3$ qui est un isomorphisme pour des raisons de cardinal d'après card 1.6.1.

(ii) A nouveau $\mathrm{card}(\mathbb{P}(\mathbb{F}_3^2)) = 4$, donc on obtient une injection de $PGL_2(\mathbb{F}_3) \hookrightarrow S_4$ qui est un isomorphisme pour des raisons de cardinal. De la même manière, on a une injection de $PSL_2(\mathbb{F}_3) \hookrightarrow S_4$ et comme $PSL_2(\mathbb{F}_3)$ est d'indice deux, cela force $PSL_2(\mathbb{F}_3) \cong A_4$ d'après dist1 3.2.8.

(iii) On vérifie que les deux groupes sont de cardinal 60 et se plongent dans S_5 puisque $\mathrm{card}(\mathbb{P}^1_{\mathbb{F}_4}) = 5$. Comme ils sont d'indice deux, ils sont isomorphes à A_5 d'après 3.2.8.

(iv) Dans cette situation, on a un plongement injectif de $PGL_2(\mathbb{F}_5) \hookrightarrow S_6$, comme il est d'indice 6, d'après 3.2.9 on en déduit que $PGL_2(\mathbb{F}_5) \cong S_5$ et donc à nouveau $PSL_2(\mathbb{F}_5) \cong A_5$. □

Remarques.

1.6.5. L'énoncé précédent nous permet de compléter la preuve de 1.5.1 dans les cas où $\mathbb{K} = \mathbb{F}_4$ ou $\mathbb{F}_5$, puisque d'après 3.2.5, A_5 est simple.

1.6.6. Comme S_3 et A_4 ne sont pas simples, le théorème est bien en défaut si $n = 2$ et $\mathbb{K} = \mathbb{F}_2, \mathbb{F}_3$.

1.6.7. Le plongement de $PGL_2(\mathbb{F}_5)$ dans S_6 fournit un groupe isomorphe à S_5, mais non-trivial, i.e. qui n'est pas le stabilisateur d'un point. En effet, $PGL(E)$ agit transitivement sur $\mathbb{P}(E)$. L'existence d'un tel groupe permet de montrer que pour $n = 6$, on a $\mathrm{Aut}(S_n) \neq \mathrm{Int}(S_n)$. C'est d'ailleurs la seule valeur de n pour laquelle ça arrive.

On termine en listant les derniers isomorphismes exceptionnels :

Théorème 1.6.8. *On a les isomorphismes canoniques suivants :*

(i) $PSL_2(\mathbb{F}_7) \cong PSL_3(\mathbb{F}_2)$. *Il y a un unique groupe simple d'ordre 168.*

(ii) $PSL_2(\mathbb{F}_9) \cong A_6$.

(iii) $PSL_4(\mathbb{F}_2) \cong A_8$.

Remarque 1.6.9. En revanche, le groupe $PSL_3(\mathbb{F}_4)$ a même cardinal que A_8 égal à $20160 = \frac{8!}{2}$ mais ne lui est pas isomorphe. Cela fournit donc un exemple de deux groupes finis simples non-commutatifs de même cardinal, mais non-isomorphes.

2. Espaces topologiques

2.1. Topologie sur un ensemble.

Définition 2.1.1. Soit un ensemble E, une topologie sur E est la donnée d'un sous-ensemble $\tau \subset \mathcal{P}(E)$, dont les éléments sont appelés les ouverts, tel que :

(i) $\varnothing, E \in \tau$.

(ii) Pour tout famille $(U_i)_{i\in I}$ d'éléments de τ, on a $\bigcup U_i \in \tau$.

(iii) Pour tout famille finie $(U_i)_{i\in I}$ d'éléments de $\mathcal{U}$, on a $\bigcap U_i \in \tau$.

La donnée (E, τ) est alors appelée un espace topologique. Enfin, on appelle fermé le complémentaire d'un ouvert.

Exemples.

2.1.5. Il résulte de la définition qu'une intersection arbitraire de fermés est fermée.

2.1.6. $\mathbb{R}$ et $\mathbb{C}$ munis de la topologie usuelle sont des exemples d'espaces topologiques. Et par extension $\mathbb{R}^n$ ou $\mathbb{C}^n$ pour tout $n \in \mathbb{N}$.

2.1.7. Pour un ensemble E, si on prend $\tau = \mathcal{P}(E)$, on dit que E est muni de la topologie discrète. Dans ce contexte, tous les points sont des ouverts et des fermés.

2.1.8. Si (E, d) est un espace métrique, la topologie sur E est celle pour laquelle les ouverts sont des réunions de boules ouvertes. On a dans ce cas une caractérisation séquentielle des fermés :

$$F \text{ fermé} \iff \forall\ (x_n) \in F^{\mathbb{N}} \text{ convergente}, \lim x_n \in F.$$

2.1.9. Soit E un espace topologique $F \subset E$ un sous-ensemble, on appelle topologie induite la topologie donnée par $\tau \cap F$.

Soit un ensemble E et $A \subset \mathcal{P}(E)$, il existe des topologies contenant A, la topologie discrète par exemple. De plus, on vérifie immédiatement qu'une intersection de topologies est une topologie, on définit alors la topologie τ_A *la plus fine contenant* A, comme :

$$\tau_A = \bigcap_{A \subset \tau} \tau.$$

On peut aussi appeler τ_A la *topologie engendrée* par A. De manière concrète, les éléments de τ_A sont de la forme :

$$\bigcup_{\alpha \in A} \Big(\bigcap_{\substack{i \in K_\alpha \\ K_\alpha \text{ fini}}} U_i \Big) \tag{2.1.9.1}$$

{engtop}

avec $U_i \in A$ auxquels on ajoute $\varnothing$ et E. L'ensemble de ces éléments est clairement stable par union et aussi par intersection finie, car les intersections finies commute aux unions arbitraires.

Définition 2.1.10. Soit E un espace toplogique, $A \subset E$ un sous-ensemble, alors comme E est fermé, A est contenu dans un fermé, on définit donc $\overline{A}$ l'adhérence de A, comme le plus petit fermé contenant A, il s'obtient comme :

$$A = \bigcap_{A \subset F} F.$$

Exemple 2.1.11. Dans $\mathbb{R}$ avec la topologie usuelle, si $D(0,1)$ est le disque ouvert de rayon un, alors $\overline{D(0,1)}$ est le disque fermé de rayon un. On a aussi par exemple $\overline{\mathbb{Q}} = \mathbb{R}$, puisque $\mathbb{Q}$ est dense dans $\mathbb{R}$.

2.2. Continuité.

Définition 2.2.1. Soit $f : X \to Y$ une application entre espaces topologiques, elle est dite continue si pour tout ouvert U de Y, on a $f^{-1}(U)$ qui est ouvert.

Remarque 2.2.2. On obtient immédiatement de la définition qu'une composée de fonctions continue est continue, en effet pour $f : X \to Y$ et $g : Y \to Z$ continues, si W est ouvert dans Z, on a $(g \circ f)^{-1}(W) = f^{-1}(g^{-1}(W))$.

Cela va nous permettre de définir de nouvelles topologies :

Définition 2.2.3. Soit X un ensemble, une famille d'applications $f_i : X \to X_i$, $i \in I$, dans des espaces topologiques X_i, alors on appelle topologie initiale, la topologie la plus fine qui rend les applications $f_i : X \to X_i$ continues. Autrement dit c'est la topologie engendrée par les $f_i^{-1}(U_i)$ pour U_i ouvert dans X_i.

On a la propriété universelle suivante, en conservant les notations précédentes :

init **Lemme 2.2.4.** *Soit un espace topologique Z, X muni de la topologie initiale, alors $g : Z \to X$ est continue si et seulement si pour tout $i \in I$ $f_i \circ g$ est continue.*

Démonstration. Le sens direct est clair, vu qu'une composée de fonctions continue est continue. Réciproquement, soit U un ouvert de X, alors il résulte de (engtop 2.1.9.1) qu'il écrit sous la forme :

$$\bigcup_{\alpha \in A} \Big(\bigcap_{\substack{k \in K_\alpha \subset I \\ K_\alpha \text{ fini}}} f_k^{-1}(U_k) \Big),$$

avec U_k ouvert dans X_k. Or, pour tout $i \in I$, $f_i \circ g$ est continue, le résultat suit. □

Une application de cette construction générale est la suivante :

Définition 2.2.5. Soit $(X_i, \tau_i)_{i \in I}$ une famille d'espaces topologiques, posons $X = \prod_{i \in I} X_i$, on appelle topologie produit sur X la topologie initiale définie par les projections $p_i : X \to X_i$ pour $i \in I$.

Il résulte donc de la définition que la topologie produit est engendré par les ensembles de la forme :

$$U_i \times \prod_{j \neq i} X_j, i \in I, U_i \in \tau_i,$$

et donc elle consiste en les unions arbitraires d'éléments de la forme :

$$\prod_{k=1}^{n} U_{i_k} \times \prod_{j \neq \{i_1, \ldots, i_n\}} X_j, i_1, \ldots, i_n \in I, \forall\ 1 \leqslant k \leqslant n, U_{i_k} \in \tau_{i_k},$$

car-prod **Remarque 2.2.6.** Ainsi si I est *fini*, un produit d'ouverts est bien ouvert. En revanche, si I est infini, un produit infini d'ouverts non-vides n'est pas ouvert si un nombre infini d'iceux sont différents des X_i.

On a une notion duale de la topologie initiale, la topologie finale :

Définition 2.2.7. Soit X un ensemble $(f_i : X_i \to X)_{i\in I}$ une famille d'applications avec X_i des espaces topologiques, alors on appelle topologie finale associée à $(f_i)_{i\in I}$, la topologie la plus fine qui rend les applications $f_i : X_i \to X$ continues. Autrement dit, un sous-ensemble U de X est ouvert si et seulement si $f_i^{-1}(U)$ est ouvert pour tout $i \in I$.

final **Remarque 2.2.8.** On a la propriété universelle analogue à celle de init 2.2.4, une application $g : X \to Z$ est continue si pour tout $i \in I$, $f_i \circ g : X_i \to X \to Z$ est continue.

2.3. Séparation et connexité.

Définition 2.3.1. Soit E un espace topologique, il est dit séparé (ou Hausdorff) si pour tout couple $(x, y) \in E^2$ il existe des ouverts U, V tels que $U \cap V = \varnothing$ et $x \in U, y \in V$.

sep1 **Remarques.**

2.3.2. Soit E un espace topologique séparé, alors pour tout $x \in E$, $\{x\}$ est fermé. En effet, si $U = X - \{x\}$, on a $U = \bigcup_{y\in U} U_y$ où U_y est un ouvert qui ne contient pas x.

2.3.3. Toute partie d'un espace séparé est séparée.

diag **Lemme 2.3.4.** *Si E est séparé, alors la diagonale $\Delta : E \to E \times E$ est fermée, i.e. l'image d'un fermé est fermée.*

Démonstration. Soit $F \subset E$ un fermé, U l'ouvert complémentaire, soit W le complémentaire de $\Delta(F)$. Soit $(x, y) \in W$ alors soit $x \neq y$ ou $y = x \in U$ Dans le premier cas, soit U_x, U_y des ouverts disjoints tels que $x \in U_x$ et $y \in U_y$, alors $(x, y) \in U_x \times U_y \subset W$ dans le second cas $\Delta(U) \subset U \times U \subset W$ et W est ouvert d'après car-prod 2.2.6. □

Exemple 2.3.5. (Une topologie non séparée). Soit $X = \mathbb{C}^n$. Soit $S \subset \mathbb{C}[X_1, \ldots, X_n]$ un sous-ensemble de polynômes, on définit :

$$V(S) = \{x = (x_1, \ldots, x_n) \in \mathbb{C}^n | \ \forall\ P \in S, P(x) = 0\}.$$

Un tel ensemble est appelé ensemble algébrique. On a $V(\{1\}) = \varnothing$ et $V(\{0\}) = \mathbb{C}^n$ et on vérifie immédiatement que :

$$\bigcap_{i\in I} V(S_i) = V(\bigcup_{i\in I} S_i).$$

Les ensembles algébriques définissent donc les fermés d'une topologie, *la topologie de Zariski*[1].

1. C'est la topologie fondamentale de la géométrie algébrique.

Les ouverts sont donc les complémentaires et on vérifie que tout ouvert non-vide U contient un ouvert $D(f) = \{(x_1, \ldots, x_n) | f(x_1, \ldots, x_n) \neq 0\}$ pour $f \neq 0 \in \mathbb{C}[X_1, \ldots, X_n]$. Si on considère alors deux ouverts non-vide $D(f)$ et $D(g)$, alors on a $D(f) \cap D(g) = D(fg)$ qui n'est jamais vide car $fg \neq 0$. Ainsi, tous les ouverts se rencontrent et la topologie n'est pas séparée.

Définition 2.3.6. Soit un espace topologique X, il est dit connexe s'il n'est pas réunion de deux ouverts disjoints.

Remarque 2.3.7. Soit $f : Y \to X$ continue entre espaces topologiques, si Y est connexe, alors $f(Y)$ est connexe.

gln-conn **Exemple 2.3.8.** $GL_n(\mathbb{C})$ est un ouvert connexe de $M_n(\mathbb{C})$.

Démonstration. Il est clairement ouvert car $GL_n(\mathbb{C}) = \det^{-1}(\mathbb{C}^*)$ et det est continu. Pour la connexité, soient A, B deux matrices inversibles, le complémentaire dans $\mathbb{C}$ de l'ensemble fini des zéros de $P(z) = \det(zA+(1-z)B)$ est connexe, son image par l'application $z \mapsto zA + (1-z)B$ est donc un connexe de $GL_n(\mathbb{C})$. □

3. Groupes topologiques

3.1. Définitions.

Définition 3.1.1. Soit un groupe G, muni d'une topologie τ. On dit que G est un groupe topologique si la multiplication $G \times G \to G$ est continue ainsi que l'inversion $\iota : G \to G$.

adh **Remarque 3.1.2.** Si G est un groupe topologique, alors l'adhérence d'un sous-groupe H est un sous-groupe. En effet, il suffit de montrer que pour tout $x, y \in \overline{H}$, $xy^{-1} \in \overline{H}$. Or $\phi : H \times H \to H$ donnée par $(x, y) \mapsto xy^{-1}$ est continue et on a $\phi^{-1}(\overline{H})$ qui est fermé et qui contient $H \times H$, donc en particulier $\overline{H} \times \overline{H} \subset \phi^{-1}(\overline{H})$ d'où $\phi(\overline{H} \times \overline{H}) \subset \overline{H}$.

int-id **Lemme 3.1.3.** *Soit G un groupe topologique, $H \subset G$ un sous-groupe, alors H est ouvert si et seulement si 1 admet un voisinage ouvert inclus dans H. Si H est ouvert, alors H est fermé.*

Démonstration. Soit V un voisinage de 1 inclus dans H, alors pour tout $x \in H$, xV est un voisinage ouvert de x, donc $H = \bigcup_{x \in H} xV$ et H est ouvert. De plus, on a $G \backslash H = \bigcup_{x \notin H} xH$, qui est donc également une réunion d'ouverts, donc H est fermé. □

Exemple 3.1.4. Le groupe $GL_n(\mathbb{C}) \subset M_n(\mathbb{C})$ avec la topologie induite est bien un groupe topologique. En effet, la multiplication est polynomiale sur les coefficients et l'inversion $g \mapsto g^{-1} = \frac{{}^t \mathrm{Com}(g)}{\det(g)}$ est également continue comme produit de fonctions continues.

der-top **Lemme 3.1.5.** *Soit G un groupe topologique connexe résoluble, alors $D(G)$ est connexe.*

DÉMONSTRATION. Soit S l'ensemble des commutateurs et $\Phi : G^2 \to G$ donnée par $(m,n) \mapsto mnm^{-1}n^{-1} \in S$. Le groupe G^2 est connexe et Φ continue donc $\Phi(G \times G) = S$ est connexe. Soit $m \geqslant 1$ et S_m l'ensemble des produits $s_1 \dots s_m$ avec $s_i \in S$. C'est l'image de S^m la multiplication $G^m \to G$, qui est donc connexe, comme S^m l'est et que le morphisme est continu. Or $D(G) = \{Id\} \cup (\bigcup_{m \geqslant 1} S_m)$ et comme $Id \in S_m$ pour tout $m \geqslant 1$, $D(G)$ est connexe. □

3.2. Actions de groupes topologiques. Soit un espace topologique E, G un groupe topologique qui agit sur E. On dit que G *agit continûment* si l'application $(g,x) \mapsto g.x$ est continue. En particulier, à g fixé l'application $f(g) : E \to E$ donnée par $x \mapsto g.x$ est un homéomorphisme d'inverse $f(g^{-1})$.

stab **Lemme 3.2.1.** *Supposons E séparé, alors pour tout x, les stabilisateurs $G_x \subset G$ sont fermés.*

DÉMONSTRATION. Comme E est séparé, d'après diag 2.3.4, Δ est fermée. Posons $\Gamma = \{(g,x) \in G \times E, gx = x\}$, on a $\Gamma = \psi^{-1}(\Delta)$ pour $\psi : G \times E \to E \times E$. donnée par $(g,x) \mapsto (g.x, x)$. Comme $(g,x) \mapsto g.x$ est continue et que les projections $G \times E \to E$ sont continues d'après la définition de la topologie produit, il résulte de init 2.2.4 que ψ est continue, donc H est fermé. Ainsi comme $\{x\}$ est fermé, $\Gamma_x = p^{-1}(\{x\}) \cap \Gamma$ est fermé comme intersection de fermés. Il suffit alors de remarquer que $G_x = i^{-1}(\Gamma_x)$ via $i : G \to G \times E$ donnée par $g \mapsto (g,x)$, qui est continue à nouveau par init 2.2.4. □

Définition 3.2.2. Soit H un sous-groupe d'un groupe topologique G, la topologie quotient sur G/H est la topologie finale associée $G \to G/H$, i.e. la plus fine qui rend la projection continue.

ouv **Remarque 3.2.3.** On a toujours que $\pi : G \to G/H$ est une application ouverte, i.e. envoie un ouvert sur un ouvert, en effet si U est ouvert dans G, alors $\pi^{-1}(\pi(U)) = G.U$ qui est une union d'ouverts donc ouvert.

Considérons un groupe topologique G muni d'une action continue sur un espace topologique séparé E, fixons $x \in E$, on peut alors munir G/G_x de la topologie quotient et l'orbite O_x de la topologie induite par celle de E. La flèche $\phi_x : g \mapsto g.x$, induit une bijection

$$\overline{\phi}_x : G/G_x \to O_x,$$

qui est continue par final 2.2.8 et comme $\phi_x : G \to O_x$ l'est. L'inconvénient est qu'en général, ϕ n'est pas nécessairement un homéomorphisme. Il faut rajouter des hypothèses pour que ce soit le cas. On rappelle la définition suivante :

Définition 3.2.4. (i) Soit un espace topologique E, il est dit compact s'il est séparé et quasi-compact, i.e. de tout recouvrement ouvert de $E = \bigcup U_\alpha$, on peut extraire un recouvrement fini. Si E est séparé, alors une partie $A \subset E$ est relativement compacte, si son adhérence $\overline{A}$ est compacte.

(ii) Soit un groupe topologique G, il est dit localement compact, s'il est séparé et si pour tout $x \in G$ et tout voisinage ouvert V_x, il admet un voisinage ouvert W_x relativement compact tel que $\overline{W_x} \subset V_x$. On appelle voisinage compact l'adhérence d'un voisinage ouvert relativement compact.

locf **Remarque 3.2.7.** On en déduit en particulier qu'un ouvert et un fermé d'un localement compact est localement compact et donc par extension également un localement fermé [2] d'un localement compact est localement compact.

homeo **Théorème 3.2.8.** *Soit G un groupe topologique localement compact, dénombrable à l'infini (i.e. réunion dénombrable de compacts), opérant continûment transitivement sur E localement compact, alors pour tout $x \in E$, la bijection $\overline{\phi}_x : G/G_x \to E$ est un homéomorphisme.*

sig-com **Remarque 3.2.9.** Il résulte de la définition de la compacité que dans un espace dénombrable à l'infini, de tout recouvrement ouvert, on peut extrainre un recouvrement dénombrable.

On aura besoin de la proposition suivante que l'on admettra :

baire **Proposition 3.2.10.** *Soit E un espace localement compact, alors il est de Baire, i.e. si $X = \bigcup_{n\in\mathbb{N}} F_n$ où les F_n sont fermés alors il existe $n_0 \in \mathbb{N}$ tel que F_{n_0} contienne un ouvert non-vide.*

Passons maintenant à la preuve du théorème.

Démonstration. Il suffit de montrer que $\overline{\phi}_x$ est ouverte et par définition de la topologie quotient, il s'agit de voir que $\phi_x : G \to E$ est ouverte. Soit U un ouvert de G, montrons que $U.x$ est ouvert dans E. Soit $g \in U$, il s'agit de construire un voisinage ouvert de gx dans $U.x$ ou ce qui revient au même un voisinage ouvert de x dans $g^{-1}U.x$, où $g^{-1}U$ est maintenant un voisinage ouvert de 1.

Soit W un voisinage compact symétrique de 1 tel que $W^2 \subset g^{-1}U$ [3]. Comme $G = \bigcup_{t\in G} t.W$ et que G est dénombrable à l'infini, d'après la remarque sig-com 3.2.9, il existe une famille dénombrable (g_n) tel que :

$$G = \bigcup_{n\in\mathbb{N}} g_n W.$$

2. i.e. l'intersection d'un ouvert avec un fermé.

3. L'application $\tau : g \mapsto g^2$ est continue et il suffit de prendre un voisinage compact symétrique de 1 inclus dans $\tau^{-1}(g^{-1}U)$ qui reste un voisinage ouvert de 1 et est aussi localement compact d'après locf 3.2.7

d'où $E = \bigcup_{n\in\mathbb{N}} g_n W.x$ comme le groupe opère transitivement. Les $g_n W.x$ sont compacts, donc fermés dans E. Comme E est localement compact, il est de Baire d'après 3.2.10, donc il existe n_0 tel que $g_{n_0} W.x$ contienne un ouvert non-vide, donc un élément $g_{n_0} wx$ admet un voisinage ouvert V et on a :

$$x \in w^{-1} g_{n_0}^{-1} V \subset w^{-1} g_{n_0}^{-1} (g_{n_0} W.x) = w^{-1} W.x \subset W^2.x \subset g^{-1} U.x,$$

ce qui conclut. □

homex **Exemples.**

3.2.11. Le groupe topologique $GL_n(\mathbb{K})$ avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ est localement compact, dénombrable à l'infini puisqu'il est ouvert dans $M_n(\mathbb{K})$. On a une action continue transitive de $GL_n(\mathbb{K})$ sur $\mathbb{K}^n - \{0\}$, également localement compact et le stabilisateur de $(1, 0, \ldots, 0)$ est $GL_{n-1}(\mathbb{K}) \times \mathbb{K}^{n-1}$, on en déduit donc un homéomorphisme :

$$GL_n(\mathbb{K})/(GL_{n-1}(\mathbb{K}) \times \mathbb{K}^{n-1}) \cong \mathbb{K}^n - \{0\}.$$

3.2.12. Soit $\mathcal{S}_n(\mathbb{R})^{++}$ l'ensemble des matrice symétriques définies positives. C'est un ouvert de $\mathbb{R}^{\frac{n(n+1)}{2}}$, donc localement compact qui admet une action transitive de $GL_n(\mathbb{R})$ par $P.M = PM^tP$ [4], $P \in GL_n(\mathbb{R})$, $M \in \mathcal{S}_n^{++}(\mathbb{R})$. Le stabilisateur de I_n s'identifie à $O_n(\mathbb{R})$, on obtient donc un homéomorphisme :

$$GL_n(\mathbb{R})/O_n(\mathbb{R}) \cong \mathcal{S}_n(\mathbb{R})^{++}.$$

i-comp **Lemme 3.2.13.** *Soit $f : X \to Y$ une application continue avec X compact et Y séparé, alors l'image d'un compact est compacte.*

Démonstration. Comme une partie d'un espace séparé est séparée, il suffit de montrer que l'image d'un quasi-compact K est quasi-compacte. On considère un recouvrement ouvert $f(X) = \bigcup_{i\in I} U_i$, on a donc $X = \bigcup_{i\in I} f^{-1}(U_i)$ dont on peut extraire un recouvrement fini $X = \bigcup_{i\in K} f^{-1}(U_i)$, avec K fini et on a alors $f(X) = \bigcup_{i\in K} U_i$. □

Pour pouvoir être en mesure de pouvoir appliquer 3.2.8, cela suppose donc de savoir si l'espace d'arrivée est localement compact. Typiquement, si X est un espace topologique localement compact sur lequel un groupe G satisfaisant les hypothèses de 3.2.8 agit continûment ; pour appliquer le théorème, on a besoin de savoir si les orbites sont elles aussi localement compactes. Malheureusement en général ce n'est pas le cas, il faudra donc le montrer à chaque fois au cas par cas.

4. Toute matrice définie positive M admet une racine carrée H aussi définie positive donc $M = H^2 = H^tH$.

3.3. Propriétés des groupes topologiques. On étudie quelques propriétés des groupes topologiques.

qu-op **Proposition 3.3.1.** *Soit G un groupe topologique, $H \subset G$ un sous-groupe fermé, alors G/H est séparé.*

DÉMONSTRATION. Soit $\Gamma = \{(x, hx) \in G \times G, h \in H\}$, alors Γ est fermé comme image réciproque de H, qui est fermé par l'application $(x, y) \mapsto xy^{-1}$. Si $\pi(x) \neq \pi(y)$, $(x, y) \notin \Gamma$ et et comme Γ est fermé, alors il existe des ouverts U, V contenant respectivement x et x tels que $U \times V$ ne rencontre par Γ. En particulier, $\pi(U)$ et $\pi(V)$ sont disjoints et comme π est ouverte d'après 3.2.3, cela conclut. □

prop-top **Proposition 3.3.2.** *On a les propriétés suivantes :*

(i) *Si G est connexe, il est engendré par tout voisinage ouvert de l'identité.*

(ii) *Si G/H est connexe et H connexe alors G est connexe.*

(iii) *Si G localement compact et H fermé, alors G/H est localement compact.*

(iv) *Soit H un sous-groupe localement compact, alors il est fermé.*

(v) *Si G est localement compact et connexe, il est dénombrable à l'infini.*

DÉMONSTRATION. (i) On applique 3.1.3 au groupe H engendré par un voisinage ouvert de 1. Il est donc ouvert fermé et non-vide et comme G connexe, on a $G = H$.

(ii) Soit $f : G \to \{0, 1\}$ une application continue, comme H est connexe, xH l'est aussi pour tout $x \in H$, donc induit une application continue par passage au quotient $f : G/H \to \{0, 1\}$ qui est constante comme G/H est connexe, donc f aussi et G connexe.

(iii) D'après 3.3.1, G/H est séparé et comme $G \to G/H$ est continue ouverte, c'est clair d'après 3.2.13.

(iv) On a le lemme suivant :

Lemme 3.3.8. *Soit H un sous-groupe localement compact dense de G, alors $H = G$.*

DÉMONSTRATION. Soit V un voisinage de 1 tel que $V \cap H$ est compact, comme H est dense, $\overline{V \cap H} \supset \mathrm{Int}(V)$, mais $V \cap H$ est compact, donc $\mathrm{Int}(V) \subset V \cap H \subset H$ et e est intérieur à H, donc H est ouvert, donc fermé d'après 3.1.3 et $H = G$. □

Il suffit alors d'appliquer le lemme à $G = \overline{H}$ et en utilisant 3.1.2.

(v) Soit V un voisinage compact symétrique de l'identité ($V = V^{-1}$), alors V engendre G par (i) et $G = \bigcup V^n$ et chaque V^n est compact d'après 3.2.13. □

3.4. Applications.

3.4.1. *Sous-groupes bornés de $GL_n(\mathbb{C})$.*

Théorème 3.4.2. *Soit $G \subset GL_n(\mathbb{C})$ un sous-groupe borné, alors il est diagonalisable.*

Démonstration. Fixons une norme $\|.\|$ sur $\mathbb{C}^n$, on définit sur $M_n(\mathbb{C})$ la norme triple subordonnée :

$$\forall\ M \in M_n(\mathbb{C}), |||M||| = \sup_{X \neq 0} \frac{\|MX\|}{\|X\|}.$$

Soit λ une valeur propre de $M \in G$, alors en prenant X un vecteur propre non-nul, on a :

$$|||M||| \geqslant \frac{\|MX\|}{X} = |\lambda|.$$

Or, G est borné, donc $(\lambda^n)_{n\in\mathbb{N}}$ est borné si et seulement si $|\lambda| \leqslant 1$. Mais, comme $M^{-1} \in G$, on doit avoir aussi $(\lambda^{-n})_{n\in\mathbb{N}}$ borné et $|\lambda| = 1$. Pour montrer que M est diagonalisable, on utilise la décomposition de Dunford $M = D + N$ avec $DN = ND$, D diagonalisable et N nilpotente. Soit s l'indice de nilpotence de N, supposons $s \geqslant 2$, sinon $N = 0$. On a donc $\operatorname{Ker} N$ strictement inclus dans $\operatorname{Ker} N^2$, soit $X \in \operatorname{Ker} N^2 \setminus \operatorname{Ker} N$. Pour $p \geqslant s$, en utilisant la formule du binôme, on déduit :

$$M^p = (D+N)^p = D^p + pD^{p-1}N + \cdots + \binom{p}{s-1} D^{p-s+1}N^{s-1},$$

Ainsi, $M^pX = D^pX + pD^{p-1}NX$, il en découle que la suite (M^pX) n'est pas bornée une contradiction. □

De ce théorème, on retrouve par exemple que le groupe des matrices orthogonales $O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}), A^tA = I_n\}$ est diagonalisable dans $\mathbb{C}$. De même, pour le groupe des matrices unitaires :

$$U_n(\mathbb{C}) = \{U \in M_n(\mathbb{C}), U^t\overline{U} = I_n\}.$$

3.4.3. *Les espaces projectifs.* Soit $\mathbb{P}^n(\mathbb{K})$ l'ensemble des droites de $\mathbb{K}^{n+1}$, on a une action transitive de $GL_{n+1}(\mathbb{K})$ de stabilisateur un sous-groupe $P_{n+1}(\mathbb{K})$ qui s'écrit par blocs sous la forme :

$$\begin{pmatrix} \mathbb{K}^\times & \mathbb{K}^n \\ 0 & GL_n(\mathbb{K}) \end{pmatrix}$$

avec $B \in GL_n(\mathbb{K})$. On obtient alors une bijection ensembliste $GL_{n+1}(\mathbb{K})/P_{n+1}(\mathbb{K}) \cong \mathbb{P}^n(\mathbb{K})$, dont on se sert pour mettre une structure d'espace topologique localement compact sur $\mathbb{P}^n(\mathbb{K})$ d'après prop-top 3.3.2. De plus, notons que l'action de $GL_{n+1}(\mathbb{K})$ sur $\mathbb{P}^n(\mathbb{K})$ se relève en une action transitive continue de $GL_{n+1}(\mathbb{K})$ sur $\mathbb{K}^{n+1} - \{0\}$ et la projection

$$GL_{n+1}(\mathbb{K}) \to \mathbb{P}^n(\mathbb{K})$$

se factorise en :

$$GL_{n+1}(\mathbb{K}) \to \mathbb{K}^{n+1} - \{0\} \xrightarrow{\phi} \mathbb{P}^n(\mathbb{K})$$

On a alors le théorème suivant :

proj-comp **Théorème 3.4.4.** *L'application $\phi : \mathbb{K}^{n+1} - \{0\} \to \mathbb{P}^n(\mathbb{K})$ est continue surjective et l'espace projectif $\mathbb{P}^n(\mathbb{K})$ est compact.*

Remarque 3.4.5. Notez qu'ici $\mathbb{K}^{n+1} - \{0\}$ a une structure topologique naturelle, donc on a besoin de homeo 3.2.8 pour montrer la compatibilité avec la topologie quotient.

DÉMONSTRATION. D'après homex 3.2, la flèche $\pi : GL_{n+1}(\mathbb{K}) \to \mathbb{K}^{n+1} - \{0\}$ induit un homéomorphisme :

$$GL_{n+1}(\mathbb{K})/(GL_n(\mathbb{K}) \times \mathbb{K}^{n-1}) \cong \mathbb{K}^{n+1} - \{0\}.$$

Et de plus π est ouverte d'après ouv 3.2.3. Soit U un ouvert de $\mathbb{P}^n(\mathbb{K})$, par définition, $(\phi \circ \pi)^{-1}(U)$ est ouvert dans $GL_{n+1}(\mathbb{K})$, donc $\pi((\phi \circ \pi)^{-1}(U)) = \phi^{-1}(U)$ est aussi ouvert, donc ϕ est continue.

Pour la compacité, il suffit de construire une application continue surjective $Z \to \mathbb{P}^n(\mathbb{K})$ avec Z compact. On considère alors $\mathbb{S}^n = \{(z_0, \dots, z_n) \in \mathbb{K}^{n+1}, \sum_{i=0}^{n} |z_i|^2 = 1.\}$ C'est clairement un compact de $\mathbb{K}^{n+1}$ en tant que fermé borné, inclus dans $\mathbb{K}^{n+1} - \{0\}$. D'après précédemment, la composée $\mathbb{S}^n \to \mathbb{P}^n(\mathbb{K})$ est bien continue. Montrons qu'elle est surjective. Comme $\mathbb{P}^n(\mathbb{K}) \cong \mathbb{K}^{n+1} - \{0\}/\mathbb{K}^\times$ ensemblistement d'après proj (1.3.1.1), il suffit de voir que l'on a :

$$\mathbb{K}^\times.\mathbb{S}^n = \mathbb{K}^{n+1} - \{0\},$$

ce qui est clair car si $(z_0, \dots, z_n) \in \mathbb{K}^{n+1} - \{0\}$, alors $\lambda = \sqrt{|z_0|^2 + \cdots + |z_n|^2} \in \mathbb{K}^*$ et $(\frac{z_0}{\lambda}, \dots, \frac{z_n}{\lambda}) \in \mathbb{S}^n$. □

3.4.6. *Action par équivalence.* Soit $G = GL_n(\mathbb{K})$ avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On a une action de $G \times G$ sur $M_n(\mathbb{K})$ par $(P, Q).M = PMQ^{-1}$. Il est bien connu que les orbites sont les $\mathcal{O}_i = \{M \in M_n(\mathbb{C}), \mathrm{rg}(M) = i\}$ pour $0 \leqslant i \leqslant n$.

Proposition 3.4.7. *Les orbites $\mathcal{O}_i$ sont localement fermées pour tout $0 \leqslant i \leqslant n$ et on a :*

$$\overline{\mathcal{O}}_i = \bigcup_{j \leqslant i} \mathcal{O}_j. \tag{3.4.7.1}$$ {adh-rg}

Il y a une unique orbite fermée $\mathcal{O}_0$ et une seule orbite ouverte $\mathcal{O}_n = G$.

Remarque 3.4.8. Le fait que les orbites sont localement fermées implique qu'elles sont des ouverts denses de leur adhérence.

DÉMONSTRATION. En effet, on a la caractérisation : $M \in \mathcal{O}_i$ si et seulement si elle admet un mineur d'ordre i non-nul et si tous les mineurs d'ordre $i + 1$ sont nuls, la première condition est ouverte et la deuxième est fermée donc $\mathcal{O}_i$ est localement fermée dans $M_n(\mathbb{K})$.

Si $M \in \mathcal{O}_j$ avec $r < i$, elle s'écrit $M = PJ_rQ$ et la suite $M_n = P\tilde{J}_nQ$ avec :

$$\tilde{J}_n = \begin{pmatrix} I_r & & & & \\ & \frac{1}{n}I_{i-r} & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix},$$

est une suite d'éléments de $\mathcal{O}_i$ convergeant vers M, ce qu'on voulait. Les deux dernières assertions s'obtiennent immédiatement de (adh-rg 3.4.7.1). □

On en déduit donc que pour tout $1 \leqslant i \leqslant n$, on peut appliquer homeo 3.2.8, et on a un homéomorphisme :

$$G/G_{J_r} \cong \mathcal{O}_r.$$

On vérifie alors que le stabilisateur G_{J_r} s'identifie au produit :

$$G_{J_r} = \begin{pmatrix} GL_r(\mathbb{K}) & M_{r,n-r}(\mathbb{K}) \\ 0 & GL_{n-r}(\mathbb{K}) \end{pmatrix} \times \begin{pmatrix} GL_r(\mathbb{K}) & 0 \\ M_{n-r,r}(\mathbb{K}) & GL_{n-r}(\mathbb{K}) \end{pmatrix}$$

4. Étude de la variété de drapeaux

4.1. Sous-groupes de Borel. Soit un corps $\mathbb{K}$, soit $B_n \subset GL_n(\mathbb{K})$ le sous-groupe des matrices triangulaires supérieures inversibles, notons $U_n \subset B_n$ le sous-groupe des matrices unipotentes et $T_n \subset B_n$ le sous-groupe des matrices diagonales inversibles.

semidir **Lemme 4.1.1.** *On a $U_n \lhd B_n$ et une décomposition $B_n = T_nU_n = U_nT_n$.*

Démonstration. Soit $u \in U_n$ et $b \in B_n$, comme les coefficients diagonaux se multiplient, on a bien $bub^{-1} \in U_n$. De plus si $b \in B_n$, soit $d \in T_n$, la matrice diagonale qui a les mêmes coefficients diagonaux que ceux de B, alors $u = bd^{-1} \in U_n$ et on a bien $b = du$ et $B_n = T_nU_n$. Enfin, comme $U_n \lhd B_n$, on a $T_nU_n = U_nT_n$. □

On a vu dans sol2 4.2.1, que B_n était résoluble et si $\mathbb{K} = \mathbb{C}$, il est aussi clairement connexe vu qu'il est homéomorphe à $(\mathbb{C}^\times)^n \times \mathbb{C}^{\frac{n(n-1)}{2}}$. On montre maintenant une propriété générale des groupes connexes résolubles qui va nous permettre de se ramener au groupe B_n par cotrigonalisation.

bor-stab **Proposition 4.1.2.** *Soit G un sous-groupe connexe résoluble de $GL_n(\mathbb{C})$, alors il admet un sous-espace vectoriel G-stable strict et non-trivial $V \subset \mathbb{C}^n$.*

Remarque 4.1.3. On travaille sur les complexes pour avoir une notion de connexité. Si on voulait travailler sur un corps $\mathbb{K}$ arbitraire, on aurait besoin de la topologie de Zariski.

Démonstration. Notons m la classe de résolubilité de G. Si $m = 1$, alors G abélien et c'est le résultat bien connu de cotrigonalisabilité. Supposons $m \geqslant 2$. soit $H = D^{m-1}(G)$, alors H est abélien non-trivial. Soit P l'ensemble des vecteurs propres non-nuls simultanément pour tous les éléments de H. Comme H est abélien et que l'on est dans $GL_n(\mathbb{C})$, les éléments sont cotrigonalisables, donc on sait que P est non-vide. Soit $v \in P$ non-nul, pour un tel v notons $\chi_v(h)$ la valeur propre associée à $v$pour l'élément h. Comme $H \lhd G$, on en déduit que pour pour tout $g \in G$, $gv \in P$, avec $\chi_{gv}(h) = \chi_v(ghg^{-1})$ pour tout $h \in H$.

Pour h fixé l'image de $g \mapsto \chi_{gv}(h)$ est d'image finie car comprise dans l'ensemble des valeurs propres de h et elle est connexe car l'application est continue. C'est donc un singleton, ainsi $V = \mathrm{Vect}(g.v, g \in G)$ est un sous-espace propre pour tout $h \in H$. Par construction ce sous-espace est G-stable et non-nul. Montrons qu'il est strict. Si par l'absurde $V = \mathbb{K}^n$, alors tout élément de h de H est une homothétie de rapport λ_h. De plus comme $H \subset D(G)$ $(m \geqslant 2)$, tout élément de H est de déterminant un, donc on obtient que λ_h est une racine n-ième de l'unité. Donc l'ensemble des λ_h étant fini et devant être connexe comme H est connexe, on obtient que $H = \{1\}$, contradiction. □

Le théorème qui nous intéresse est le suivant :

bor2 **Théorème 4.1.4** (Lie-Kolchin)**.** *Soit B un sous-groupe connexe résoluble de $GL_n(\mathbb{C})$ alors il est simultanément trigonalisable.*

Démonstration. On procède par récurrence sur $n \in \mathbb{N}$. Si $n = 0$, il n'y a rien à montrer. Passons de n à $n + 1$. D'après bor-stab 4.1.2, il existe un sous-espace vectoriel strict et non-nul $H \subset \mathbb{K}^n$ stable par G. En complétant une base de H en une base de $\mathbb{K}^n$, on obtient que tout élément $g \in G$ se met sous la forme :

$$g = \begin{pmatrix} \phi_1(g) & \psi(g) \\ 0 & \phi_2(g) \end{pmatrix}$$

et les applications $\phi_1 : G \to GL_d(\mathbb{C})$ et $\phi_2 : G \to GL_{n-d}(\mathbb{C})$ sont des morphismes continus en tant que projections et sont des morphismes de groupes. Comme l'image d'un groupe résoluble par un morphisme de groupes est résoluble et que l'image d'un groupe connexe par un morphisme continu est aussi connexe, on peut appliquer l'hypothèse de récurrence pour conclure. □

Définition 4.1.5. On appelle sous-groupe de Borel de $GL_n(\mathbb{C})$ un sous-groupe connexe résoluble maximal pour l'inclusion.

Soit B_n le sous-groupe des matrices triangulaires supérieures inversibles. D'après sol2 4.2.1, il est résoluble et connexe car isomorphe à $(\mathbb{C}^\times)^n \times \mathbb{C}^{\frac{n(n-1)}{2}}$.

Dans la suite, soit $T_n \subset B_n$ le sous-groupe des matrices diagonales diagonales inversibles et notons $G = GL_n(\mathbb{C})$.

Weyl **Proposition 4.1.6.** *On a $N_G(T_n) = S_nT_n$ où l'on identifie S_n à un sous-groupe de G via les matrices de permutations. Ainsi, $N_G(T_n)/T_n \cong S_n$.*

Remarque 4.1.7. On appelle le quotient de $N_G(T)/T$ le groupe de Weyl de GL_n. Ce groupe de Weyl joue un rôle crucial et on le verra à nouveau apparaître lors de la décomposition de Bruhat.

DÉMONSTRATION. Soit $n \in N_G(T_n)$, alors on a nT_nn^{-1}. Pour $t = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ avec les λ_i deux à deux distincts, on obtient que $ntn^{-1} = \mathrm{diag}(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)})$ pour une certaine permutation $\sigma \in S_n$. En particulier, on déduit que $\sigma^{-1}ntn^{-1}\sigma = t$. Or comme t est diagonale à valeurs propres distinctes, on obtient que son centralisateur $C_G(t)$ s'identifie à T_n, donc $\sigma^{-1}n \in T$, d'où le résultat. □

W-bor **Proposition 4.1.8.** *On a $N_G(B_n) = B_n$. En particulier, le groupe B_n est un sous-groupe de Borel.*

DÉMONSTRATION. Soit $n \in N = N_G(B_n)$, alors $nT_nn^{-1} \subset B_n$, donc il existe $b \in B$ tel que $bn \in N_G(T_n)$. Ainsi, on a $N_G(B_n) \subset B.(N_G(T_n) \cap N)$. Il suffit de montrer que $N_G(T_n) \cap N \subset B$, soit donc $n \in N_G(T_n) \cap N$, d'après 4.1.6, on peut supposer que $n = \sigma \in S_n$. Si par l'absurde $\sigma \neq Id$, soit une paire (i, j) avec $i < j$ telle que $\sigma(i) > \sigma(j)$, on a alors que $\sigma(I_n + E_{ij})\sigma^{-1} = I_n + E_{\sigma(i)\sigma(j)}$ et $\sigma B\sigma^{-1} \not\subset B$, donc $\sigma = \mathrm{Id}$ et l'énoncé est montré.

Passons à la deuxième assertion, si B_n n'est pas maximal, soit alors $H \supset B_n$ connexe résoluble, alors d'après le théorème de Lie-Kolchin, il existe $g \in GL_n(\mathbb{C})$ tel que $gHg^{-1} \subset B_n$, d'où $gBg^{-1} \subset gHg^{-1} \subset B$ et $g \in N_{GL_n(\mathbb{C})}(B_n)$ et $g \in B$ d'après ci-dessus, donc $H = B_n$. □

Le théorème de Kolchin admet le corollaire suivant :

conj-bor **Corollaire 4.1.9.** *Tout sous-groupe de Borel de B de $GL_n(\mathbb{C})$ est conjugué au sous-groupe B_n.*

DÉMONSTRATION. Soit B un Borel, alors d'après le théorème de Lie-Kolchin, il existe $g \in GL_n(\mathbb{C})$ tel que $gBg^{-1} \subset B_n$. Or gBg^{-1} est à nouveau résoluble maximal et comme B_n est un Borel d'après 4.1.8, on en déduit que $gBg^{-1} = B_n$. □

top-bor **4.2. Structure topologique sur G/B.** On suppose $\mathbb{K} = \mathbb{C}$. Pour simplifier les notations, on note $G = GL_n(\mathbb{K})$ et $B \subset GL_n(\mathbb{K})$ le sous-groupe des matrices triangulaires supérieures inversibles. Dans ce cas $GL_n(\mathbb{K})$ est localement compact et B est un sous-groupe fermé. Il résulte alors de 3.3.2 que G/B est naturellement un espace topologique connexe, localement compact. On a également vu dans (4.2.3.1) que du point de vue ensembliste on a une bijection :

$$G/B \cong \mathrm{Drap}$$

On obtient donc sur Drap une structure d'espace topologique connexe localement compact et cela justifie que l'on appelle G/B la variété de drapeaux. On a le renforcement suivant :

dr-comp **Théorème 4.2.1.** *La variété de drapeaux est compacte.*

Démonstration. Soit $U(n) = \{g \in G, g^t\bar{g} = I_n\}$, c'est fermé borné de $\mathbb{C}^{n^2}$, donc il est compact. L'application composée $U_n \to GL_n \to G/B$ est donc continue, il suffit de montrer qu'elle est surjective, pour déduire que G/B est compacte d'après 3.2.13. Pour montrer que la flèche est surjective, cela se ramène à montrer que $U(n)$ agit transitivement sur les drapeaux de $\mathbb{C}^n$. Soit $V_\bullet$ un drapeau complet de $\mathbb{C}^n$. On utilise le procédé d'orthonormalisation de Gram-Schmidt. On part d'une base orthonormée de V_1 que l'on complète en une BON de V_2 et de proche, on construit une BON $(f_1, \ldots, f_n)$ de $\mathbb{C}^n$ telle que $(f_1, \ldots, f_i)$ est une base de V_i. La matrice de passage de la base canonique de $\mathbb{C}^n$ à la base $(f_1, \ldots, f_n)$ est une matrice unitaire qui envoie le drapeau standard sur le drapeau $V_\bullet$. □

4.3. Décomposition de Bruhat. Soit un corps $\mathbb{K}$. Notons T le sous-groupe des matrices diagonales inversibles et $U \subset B$ le sous-groupe des matrices unipotentes.

Théorème 4.3.1 (Décomposition de Bruhat)**.** *On a une décomposition :*

$$GL_n(\mathbb{K}) = \coprod_{w \in S_n} BwB,$$

où w est la matrice de permutation associée à $w \in S_n$.

La preuve se fait en analysant l'algorithme du pivot de Gauss. Avant de commencer la preuve, rappelons que si $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ est une matrice de transvection et $M \in M_n(\mathbb{C})$, la multiplication à gauche de A par $T_{ij}(\lambda)$ revient à l'opération sur les lignes $L_i \mapsto L_i + \lambda L_j$ et la multiplication à droite revient à l'opération sur les colonnes $C_i \mapsto C_i + \lambda C_j$. Enfin, si $i < j$, $T_{ij}(\lambda) \in B$.

Rappelons également que si $D_i(\alpha) = I_n + (\alpha - 1)E_i i \in T$ est une matrice de dilatation, multiplier A à gauche (resp. à droite) par $D_i(\alpha)$ revient à multiplier la i-ème ligne (resp. colonne) par α.

Démonstration. Soit $A \in GL_n(\mathbb{C})$, d'après ce qui précède, si on fait agir B par multiplication à droite et à gauche, on peut ajouter à toute ligne une combinaison linéaire de lignes d'indices supérieurs et à toute colonne une combinaison linéaire de colonnes d'indices inférieurs. Comme A est inversible, $C_1 \neq 0$, soit i_1 le plus petit indice tel que $a_{i_1 1} \neq 0$. En multipliant par $T_{k i_1}(\lambda)$, on peut alors annuler tous les coefficients a_{k1} pour $k < i_1$ et quitte à utiliser une dilatation, on peut supposer que $a_{i_1 1} = 1$. Enfin, en opérant sur les colonnes, on peut faire en sorte que tous les coefficients sur la i_1-ème ligne soient nuls. Soit A_1 la matrice obtenue. Comme elle est inversible, sa seconde colonne n'est pas nulle. On réitère l'algorithme et on construit de la sorte une suite $i_1, \ldots, i_n$ injective d'entiers de 1 à n, et en notant σ la permutation qui envoie k sur i_k, on obtient que la matrice A_n est précisément

la matrice de permutation de σ. Comme on a multiplié A à gauche et à droite que par des éléments de B, on trouve $B_1AB_2 = A_\sigma$, avec $B_1, B_2 \in B$.

Il reste à prouver que les orbites sont indexées par S_n. Supposons qu'il existe $\sigma, \sigma' \in S_n$ et $b_1, b_2 \in B$ tels que $b\sigma = \sigma' b_2$, montrons que $\sigma = \sigma'$. On a $(\sigma)_{ij} = \delta_{i\sigma(j)}$ et pareillement pour σ' de telle sorte que $(b_1\sigma)_{ij} = (b_1)_{i\sigma(j)}$ et $(\sigma' b_2)_{ij} = (b_2)_{(\sigma')^{-1}(i),j}$.

Remarquons maintenant que si $i = \sigma(j)$, $(b_1)_{i\sigma(j)} \neq 0$ car b_1 inversible, donc $(b_2)_{(\sigma')^{-1}(i),j} \neq 0$ et on doit avoir $(\sigma')^{-1}(i) \leqslant j$ comme b_2 est triangulaire supérieure. Ainsi si $i = \sigma(1)$, $(\sigma')^{-1}(i) \leqslant 1$, donc $(\sigma')^{-1}(i) = 1$, donc $\sigma'(1) = \sigma(1)$. Si $i = \sigma(2)$, $(\sigma')^{-1}(2) \leqslant 2$ et $(\sigma')^{-1}(2) \neq 1$, donc $(\sigma')^{-1}(i) = 2$ et de proche en proche, on montre que $\sigma = \sigma'$. □

D'après Weyl 4.1.6, on a $S_n \subset N_G(T)$, donc :

$$\forall\ \sigma \in S_n, \sigma T \sigma^{-1} = T, \text{soit } \sigma T = T\sigma. \tag{4.3.1.1}$$ {normal}

De plus, d'après semidir 4.1.1, on peut écrire $B = UT = TU$, donc en utilisant (normal 4.3.1.1), on peut récrire la décomposition de Bruhat sous la forme :

$$GL_n(\mathbb{C}) = \coprod_{w \in S_n} UTwB = \coprod_{w \in S_n} UwB. \tag{4.3.1.2}$$ {eqbru}

On va en tirer le corollaire suivant :

ouv2 **Théorème 4.3.2.** *Soit $\mathbb{K} = \mathbb{C}$, soit $w_0 = \text{antidiag}(1, \ldots, 1)$, alors la double orbite $C(w_0) = Bw_0B$ est ouverte dense dans $GL_n(\mathbb{C})$. On l'appelle la grosse cellule ou la cellule ouverte.*

Démonstration. D'après (eqbru 4.3.1.2), on a $\mathcal{O}_{w_0} = Uw_0B$ et pour montrer l'énoncé, il suffit de montrer que $w_0\mathcal{O}_{w_0}$ est bien un ouvert dense. Comme on a immédiatement que $w_0Uw_0 = U^-$, le sous-groupe des matrices triangulaires inférieures unipotentes, il suffit de montrer la proposition suivante :

prop **Proposition 4.3.3.** *Soit $\phi : U^- \times B \to GL_n(\mathbb{C})$ donné par la multiplication, alors ϕ est un homéomorphisme sur son image qui consiste en les matrices dont tous les mineurs principaux sont non-nuls, qui est un ouvert dense de $Gl_n(\mathbb{C})$.*

Rappelons que le mineur principal d'ordre p d'une matrice M est le déterminant de la matrice extraite $(m_{ij})_{1 \leqslant i,j \leqslant p}$.

Démonstration. Décrivons l'image. Fixons $1 \leqslant p \leqslant n$ On écrit $m = ub$, et on écrit en blocs $u = \begin{pmatrix} S_p & 0 \\ A & S_{n-p} \end{pmatrix}$ et $b = \begin{pmatrix} T_p & C \\ 0 & T_{n-p} \end{pmatrix}$. Les matrices S_P et T_p sont inversibles et on a $m = \begin{pmatrix} S_pT_p & S_pC \\ AT_p & AC + S_{n-p}T_{n-p} \end{pmatrix}$ et le mineur principal est donc $\det(S_pT_p) \neq 0$. Réciproquement, montrons par récurrence que si M a tous ses mineurs principaux non-nuls,

alors $M = ub$ avec $u \in U^-$ et $b \in B$ de manière unique, avec u et b qui dépendent continûment de M. Si $n = 2$, les formules ci-dessus donnent :

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & \frac{det(m)}{a} \end{pmatrix}.$$

Si le résultat est vrai au rang $n-1$, cherchons à écrire :

$$m = \begin{pmatrix} M_1 & C \\ L & \alpha \end{pmatrix} = \begin{pmatrix} U_1 & 0 \\ L_1 & 1 \end{pmatrix} \begin{pmatrix} T_1 & C_1 \\ 0 & s_2 \end{pmatrix} = \begin{pmatrix} U_1T_1 & U_1C_1 \\ L_1T_1 & L_1C_1 + s_2 \end{pmatrix},$$

avec $U_1 \in GL_{n-1}(\mathbb{C})$ unipotente triangulaire inférieure et $T_1 \in GL_{n-1}(\mathbb{C})$ triangulaire supérieure. Par hypothèse de récurrence, on a existence et unicité de U_1 et T_1 et qui sont continus en les coefficients de M l'existence et l'unicité de $L_1 = LT_1^{-1}$ et de $s_2 = \alpha - L_1C_1$, ainsi que leur dépendance continue en résulte. On obtient donc que ϕ est continue, bijective sur son image et d'inverse continue, donc c'est bien un homéomorphisme sur son image. □

Pour conclure, la preuve du théorème, cela vient du fait immédiat que l'image de ϕ est bien un ouvert dense de $GL_n(\mathbb{C})$. □

Corollaire 4.3.4. *Le groupe $GL_n(\mathbb{C})$ contient un ouvert homéomorphe à $\mathbb{C}^{\frac{n(n-1)}{2}} \times ((\mathbb{C}^*)^n \times \mathbb{C}^{\frac{n(n-1)}{2}})$.*

Remarque 4.3.5. Ce corollaire nous permet d'obtenir une description d'un gros morceau de l'espace topologique de $GL_n(\mathbb{C})$.

Démonstration. En effet, on a $B \cong ((\mathbb{C}^*)^n \times \mathbb{C}^{\frac{n(n-1)}{2}})$ et $U^- \cong \mathbb{C}^{\frac{n(n-1)}{2}}$. □

4.4. Racines et groupe de Weyl. Afin de pouvoir décrire les orbites de Bruhat, on a besoin d'étudier d'un peu plus près le groupe unipotent U et la façon dont le tore diagonal T agit dessus. Soit $\mathbb{K}$ un corps. On fait agir le tore diagonal $T \subset GL_n(\mathbb{C})$ par conjugaison sur $M_n(\mathbb{C})$. On obtient alors une décomposition en sous-espaces stables.

$$M_n(\mathbb{C}) = \mathfrak{t} \oplus \mathfrak{n} \oplus \mathfrak{n}^-$$

où $\mathfrak{t} = \mathrm{Lie}(T)$, $\mathfrak{n} = \mathrm{Lie}(U)$ et $\mathfrak{n}^- = \mathrm{Lie}(U^-)$. On a en particulier, d'après exp-unip 4.4.4, que $\mathrm{Lie}(U) = \mathrm{Nilp}_n = \bigoplus_{i<j} \mathbb{K}E_{ij}$ et $\mathrm{Lie}(U^-) = \bigoplus_{i>j} \mathbb{K}E_{ij}$. De plus, pour tout $t \in T$ si $t = \mathrm{diag}(t_1, \ldots, t_n)$, on a pour $i < j$:

$$tE_{ij}t^{-1} = \frac{t_i}{t_j}E_{ij}$$

et si $i > j$, alors dans ce cas, $tE_{ij}t^{-1} = \frac{t_j}{t_i}E_{ij}$. On note alors $\alpha_{ij} : T \to \mathbb{C}^\times$ donnée par :

$$(t_1, \ldots, t_n) \mapsto \frac{t_i}{t_j}.$$

et $-\alpha_{ij} : T \to \mathbb{C}$ l'application $t \mapsto -\alpha_{ij}(t) = \frac{t_j}{t_i}$.

Définition 4.4.1. On appelle $R^+ = \{\alpha_{ij}, 1 \leqslant i < j \leqslant\}$ l'ensemble des *racines positives* et $R^- = \{-\alpha_{ij}, 1 \leqslant i < j \leqslant n\}$ l'ensemble des *racines négatives* et $R = R^+ \cup R^-$ l'ensemble des *racines.*

En notant $M_n(\mathbb{C}) = \mathfrak{g}$, on a donc une décomposition :

$$\mathfrak{g} = \mathfrak{t} \bigoplus_{\alpha \in R_+} \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$$

avec par définition $\mathfrak{g}_\alpha := \{M \in \mathfrak{g}, \forall\, t \in T, tMt^{-1} = \alpha(t)M\}$ et $\dim \mathfrak{g}_\alpha = 1$. On les appelle les *espaces de racines.* On va voir comme agit S_n sur ces espaces de racines. Pour $\sigma \in S_n$, on a :

$$\sigma E_{ij} \sigma^{-1} = E_{\sigma(i)\sigma(j)}.$$

On en déduit ainsi une action de S_n sur l'ensemble des racines. On va voir quel est le lien entre S_n et l'ensemble des racines.

Définition 4.4.2. Pour $w \in S_n$, on définit l'ensemble :

$$R(w) = \{\alpha \in R^+, w.\alpha \in R^-\}.$$

Rappelons que S_n est engendré par les transpositions et même par celles de la forme $(1i)$ pour $i \in [\![1, n]\!]$. En utilisant, la relation :

$$(1i) = (12)(23)\dots(i-1i)(i-2i-1)\dots(12),$$

on obtient aussi que S_n est engendré par $D = \{\tau_i := (ii+1), i \in [\![1, n]\!]\}$. L'ensemble D s'identifie alors au sous-ensemble $\Delta = \{\alpha_i := \alpha_{ii+1}, i \in [\![1, n]\!]\} \subset R^+$, que l'on appelle l'ensemble des *racines simples.* L'espace vectoriel engendré par les espaces de racines $\mathfrak{g}_\alpha$ pour $\alpha \in \Delta$ s'identifie à :

$$\begin{pmatrix} 0 & \alpha_1 & 0 & & 0 \\ 0 & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & 0 & \alpha_{n-1} \\ 0 & & \cdots & & 0 \end{pmatrix}$$

Dans la suite, pour $\alpha \in \Delta$, on note $s_\alpha \in D$ la transposition correspondante. Pour $\sigma \in S_n$, on définit la longueur $\ell(\sigma)$ de σ, comme le plus petit entier $h \geqslant 0$ tel que σ s'écrive comme un produit de h transpositions de D. Une décomposition réduite de σ est alors une suite $\mathbf{s} = (s_{i_1}, \dots, s_{i_h})$ telle que $\sigma = s_{i_1} \dots s_{i_h}$. On remarque que $\ell(\sigma) = \ell(\sigma^{-1})$.

permut **Lemme 4.4.3.** *Soit $\alpha \in \Delta$, alors s_α permute les éléments de $R^+ - \{\alpha\}$.*

Démonstration. Soit $i \in [\![1, n]\!]$, tel que $s_\alpha = (ii+1)$. Alors pour toute racine $\beta = (i, j) \neq \alpha$ avec $i < j$ et $j \geqslant i+2$, on $s_\alpha \beta = (\sigma(i)\sigma(j)) = (i+1, j) \in R_+$, comme souhaité. □

On tire en particulier de ce lemme que $R_\alpha = \{\alpha\}$ pour $\alpha \in \Delta$. En particulier, on a :

$$R(ws_\alpha) = s_\alpha.R(w) \cup \{\alpha\}, \text{si } w.\alpha \in R_+, \tag{4.4.3.1}$$ {simp1}

$$R(ws_\alpha) = s_\alpha(R(w) - \{\alpha\}) \text{si } w.\alpha \in -R^+. \tag{4.4.3.2}$$ {simp2}

La proposition suivante explique le lien entre $R(w)$ et la longueur $\ell(w)$ de w.

lgueur **Proposition 4.4.4.** *Soit $\boldsymbol{s} = (s_{i_1}, \ldots, s_{i_h})$ une décomposition réduite de $w \in S_n$ avec $s_{i_k} = s_{\alpha_{i_k}}$. On a :*

(i) $R(w) = \{\alpha_{i_h}, s_{i_h}\alpha_{i_{h-1}}, \ldots, s_{i_h} \ldots s_{i_2}\alpha_{i_1}\}$.

(ii) *On a* $\mathrm{card}(R(w)) = \ell(w)$.

Démonstration. (i) est vrai pour $h = 1$, d'après permut 4.4.3. Si $h > 1$, soit $w' = s_{i_1} \ldots s_{i_{h-1}}$. Par hypothèse de récurrence, on a $R(w') = \{\alpha_{i_{h-1}}, s_{i_h}\alpha_{i_{h-1}}, \ldots, s_{i_{h-1}} \ldots s_{i_2}\alpha_{i_1}\}$. L'énoncé se déduit alors de (simp1 4.4.3.1) si $w'\alpha_{i_h} \in R^+$. Si tel n'est pas le cas, on a $\alpha_{i_h} = s_{i_{h-1}} \ldots s_{i_{k+1}}\alpha_{i_k}$ pour un certain k, d'où :

$$s_{i_h} = s_{i_{h-1}} \ldots s_{i_k} s_{i_{k+1}} \ldots s_{i_{h-1}},$$

et $w = s_{i_1} \ldots s_{i_{k-1}} s_{i_{k+1}} \ldots s_{i_{h-1}}$, contredisant la minimalité de h. Cela montre (i).

(ii) se déduit maintenant de (i). □

4.5. Applications de la décomposition de Bruhat. Soit $\mathbb{K} = \mathbb{C}$, on a vu dans la section top-bor 4.2 que G/B admettait une structure de variété compacte. On a toujours une action à gauche de B sur G/B et la décomposition de Bruhat décrit les B-orbites, elles sont indexées par S_n, que l'on appelle le groupe de Weyl de GL_n. De plus, il résulte de eqbru 4.3.1.2 que les B-orbites de G/B sont aussi les U-orbites de G/B. On va se servir de ce fait pour obtenir une description topologique des strates. Tout d'abord, pour $w \in S_n$, si $\mathcal{O}_w$ est l'orbite de w dans G/B, décrivons le stabilisateur de w dans U. Soit $u \in U$ qui stabilise w, alors $w^{-1}uw \in B$ et comme il est unipotent, on a $wuw^{-1} \in U$ et le stabilisateur s'identifie à $U^w := U \cap wUw^{-1}$. On veut maintenant identifier U/U^w à l'orbite $\mathcal{O}_w$. Pour ce faire, on a besoin de montrer que celle-ci est localement fermée dans G/B. On commence par la proposition préliminaire suivante :

unip-pro **Proposition 4.5.1.** *Soit $U_w = U \cap wU^-w^{-1}$, l'application produit $U_w \times U^w \to U$ est un homéomorphisme. De plus, U_w est homéomorphe à $\mathbb{C}^{l(w)}$.*

Remarque 4.5.2. On va admettre la première partie car la preuve nécessite d'établir un certain nombre de propriétés supplémentaires sur les racines. Voyons comment on obtient la deuxième.

DÉMONSTRATION. Comme U_w est unipotent, d'après 4.4.4, $\exp : \mathrm{Lie}(U_w) \to U_w$ est un homéomorphisme. Or, on a :

$$\mathrm{Lie}(U_w) = \mathrm{Lie}(U) \cap w\,\mathrm{Lie}(U)^- w^{-1} = \bigoplus_{\alpha \in R_+, w^{-1}\alpha < 0} \mathfrak{g}_\alpha,$$

et d'après 4.4.4, $\dim(\mathrm{Lie}(U_w)) = \mathrm{card}(R(w^{-1})) = \ell(w^{-1}) = \ell(w)$. □

Lemme 4.5.3. *Pour tout $w \in W$, $\mathcal{O}_w \subset G/B$ est localement fermée.*

DÉMONSTRATION. Commençons par montrer que la double orbite $BwB \in G$ est localement fermée. On a vu que $BwB = UwB$ et de plus, d'après 4.5.1, on a :

$$Uwb = U_w wB,$$

où la décomposition dans le membre de droite est unique. Il suffit donc de montrer que $w^{-1}(U_w wB)$ est localement fermé. Or $w^{-1}U_w w = w^{-1}Uw \cap U^-$. Maintenant l'application continue :

$$w^{-1}U_w w \times B \to G$$

se factorise en :

$$w^{-1}U_w w \times B \to U^- \times B \to G.$$

La première application est l'inclusion d'un sous-groupe fermé et la deuxième est une immersion ouverte d'après 4.3.2, donc BwB est bien localement fermé. Pour obtenir l'assertion analogue dans G/B, si l'on note $\pi : G \to G/B$, on remarque que l'on a :

$$\pi^{-1}(\overline{\mathcal{O}}_w) = \overline{BwB}.$$

Ainsi comme d'après 3.2.3, π est ouverte, il en est de même de $\pi_{|\pi^{-1}(\overline{\mathcal{O}}_w)}$ et BwB étant localement fermée, elle est ouverte dans son adhérence donc $\mathcal{O}_w$ est localement fermée comme souhaité. □

Ainsi, comme $\mathcal{O}_w$ est localement fermé dans G/B qui est compacte, on obtient que l'orbite est localement compacte et on applique 3.2.8 pour obtenir un homéomorphisme :

$$U/(U \cap wUw^{-1}) \cong \mathcal{O}_w. \tag{4.5.3.1}$$ {orb-u}

On en déduit maintenant de manière immédiate :

strates **Théorème 4.5.4.** *Soit $w \in S_n$, alors on a $\mathcal{O}_w \cong \mathbb{C}^{l(w)}$.*

DÉMONSTRATION. Cela se déduit immédiatement de 4.5.1 et de (4.5.3.1). □

On s'intéresse maintenant à l'adhérence de ces orbites.

Proposition 4.5.5. *Pour tout $w \in S_n$, on a $\overline{\mathcal{O}_w} = \coprod_{w' \in A_w} \mathcal{O}_{w'}$. On dit alors que $w' \leqslant w$ si $O_{w'} \subset \overline{\mathcal{O}_w}$.*

Remarque 4.5.6. Cette description en orbites nous permet donc d'obtenir une relation d'ordre partiel sur les éléments de S_n.

DÉMONSTRATION. En effet par continuité, $\overline{\mathcal{O}_w}$ reste B-invariante et si pour $w' \in S_n$, on a $S'_w := \mathcal{O}_{w'} \cap \overline{\mathcal{O}_w} \neq \varnothing$, alors $B.S'_w = \mathcal{O}_{w'} \subset \overline{\mathcal{O}}_w$ et comme $G/B = \coprod_{w \in S_n} \mathcal{O}_w$, on conclut. □

On aimerait avoir une description concrète de cet ordre. Nous nous contenterons de donner le résultat sans démonstration : Soit $w \in S_n$, $\mathbf{s} = (s_{i_1}, \ldots, s_{i_h})$ une décomposition réduite. On note alors $W(\mathbf{s})$, l'ensemble des $x \in W$ qui s'obtiennent en supprimant certains facteurs du produit $s_{i_1} \ldots s_{i_h}$. On a alors :

$$\forall\ (x, w) \in S_n \times S_n, x \leqslant w \Longleftrightarrow x \in W(\mathbf{s}).$$

On obtient en particulier que l'ensemble $W(\mathbf{s})$ ne dépend pas du choix de la décomposition réduite pour w.