Christophe Mourougane

THÉORIE DES GROUPES ET GÉOMÉTRIE

Christophe Mourougane
Cours de l'Université de Rennes 1 (2008–2009).
Url : `http://perso.univ-rennes.fr/christophe.mourougane/`

Version du 24 avril 2009

THÉORIE DES GROUPES ET GÉOMÉTRIE

Christophe Mourougane

TABLE DES MATIÈRES

INTRODUCTION

Version du 24 avril 2009

CHAPITRE 1

GROUPES ET ACTIONS DE GROUPES

1.1. Définitions et formules des classes

Définition. — *Une* action d'un groupe $(G, *)$ sur un ensemble E *est la donnée équivalente ou bien d'une application* $\Phi : G \times E \to E$, $(g, x) \mapsto \Phi(g, x) =: g \cdot x$, *qui vérifie*

– $\forall x \in E, e_G \cdot x = x$.

– $\forall (g, g') \in G^2, g \cdot (g' \cdot x) = (g * g') \cdot x$.

ou bien d'un morphisme de groupes $\varphi : G \to \mathfrak{S}(E)$ *de* G *dans le groupe symétrique des bijections de l'ensemble* E.

L'équivalence consiste à poser $\Phi(g, x) = g \cdot x = \varphi(g)(x)$. Soit x un point de E. Le sous-ensemble $\mathcal{O}(x) := \{y \in E / \exists g \in G, g \cdot y = x\}$ des éléments de E obtenus par l'action sur x est appelé *l'orbite de* x. La relation binaire sur l'ensemble E définie par

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

est une relation d'équivalence. Par conséquent, deux orbites sont soit égales soit disjointes. Les orbites forment une partition de l'ensemble E. L'ensemble des orbites est noté E/G. Ainsi,

Lemme **(Première formule des classes)**. — *Soit* G *un groupe agissant sur un ensemble fini* E.

$$\sum_{\mathcal{O}_i \in E/G} \operatorname{card} \mathcal{O}_i = \operatorname{card} E.$$

Le sous-groupe $Stab(x) := \{g \in G, g \cdot x = x\}$ de G des éléments de G qui fixent x est appelé *le stabilisateur de* x. Deux éléments x et $y = g \cdot x$ de la même orbite ont des stabilisateurs conjugués ($Stab(y) = gStab(x)g^{-1}$)). L'application $f_x : G \to E$, $g \mapsto g \cdot x$ a pour image l'orbite de x. Deux éléments g et h de G ont la même image par f_x si et seulement si ils sont dans la même classe à gauche modulo $Stab(x)$ (i.e. $h^{-1}g \in Stab(x)$). Par conséquent, f_x réalise une bijection entre l'ensemble $G/Stab(x)$ des classes à gauche de G modulo $Stab(x)$ et l'orbite $\mathcal{O}(x)$ de x.

Lemme **(Seconde formule des classes)**. — *Soit* G *un groupe fini agissant sur un ensemble fini* E. *Pour tout* $x \in E$,

$$\operatorname{card} \mathcal{O}(x) \operatorname{card} Stab(x) = \operatorname{card} G.$$

Lemme **(Lemme de Burnside)**. — *Soit* G *un groupe fini agissant sur un ensemble fini* E. *Alors le nombre* N *d'orbites se calcule par*

$$N = \frac{1}{\operatorname{card} G} \sum_{g \in G} \operatorname{card} Fix(\varphi(g)) = \frac{1}{\operatorname{card} G} \sum_{x \in E} \operatorname{card} Stab(x).$$

En particulier, le nombre d'orbites est le nombre moyen de points fixes des éléments de G.

Démonstration. — Puisque,

$$\{(g, x) \in G \times E, g \cdot x = x\} = \{(g, x), g \in G, x \in Fix(g)\} = \{(g, x), x \in E, g \in Stab(x)\}$$

les deux sommes sont égales. Comme les orbites forment une partition,

$$\sum_{x \in E} \operatorname{card} Stab(x) = \sum_{\mathcal{O}_i \in E/G} \sum_{x \in \mathcal{O}_i} \operatorname{card} Stab(x).$$

Tous les éléments d'une même orbite ont des stabilisateurs conjugués donc équipotents. Donc, pour un point a de $\mathcal{O}_i$, $\sum_{x\in\mathcal{O}_i} \operatorname{card} Stab(x) = \operatorname{card}\mathcal{O}(a) \operatorname{card} Stab(a) = \operatorname{card} G$. Ainsi, $\sum_{x\in E} \operatorname{card} Stab(x) = \operatorname{card}(E/G) \operatorname{card} G$. □

L'existence d'une action d'un groupe G sur un ensemble E donne des renseignements aussi bien sur l'ensemble que sur le groupe, d'autant plus quand l'action satisfait des conditions supplémentaires.

Définition. — *Une action d'un groupe G sur un ensemble E est dite*
- transitive *s'il n'y a qu'une orbite i.e. si* $\forall(x,y)\in E^2, \exists g\in G, y = g\cdot x$.
- simplement transitive *si* $\forall(x,y)\in E^2, \exists! g\in G, y = g\cdot x$.
- fidèle *si le seul élément de G qui fixe tous les éléments de E est l'identité. i.e. si φ est injective.*
- sans points fixes *si aucun élément $\varphi(g)$ autre que $\varphi(e_G) = \mathrm{Id}_E$ n'a de point fixe. i.e. les stabilisateurs G_x sont tous réduits à $\{e_G\}$.*

1.2. Exemples

1.2.1. Actions par translation. — Tout groupe agit sur lui-même par translation à gauche $G\times G\to G, (g,x)\mapsto g\cdot x = gx$. Comme l'action est fidèle, l'application φ associée réalise le groupe G comme isomorphe à un sous-groupe du groupe $\mathfrak{S}(E)$. En particulier, tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$ (Théorème de Cayley).

Tout sous-groupe H d'un groupe G agit par translation à gauche sur les ensembles quotients G/S où S est un sous-groupe de G. Le stabilisateur de la classe à gauche gS est $H\cap gSg^{-1}$. Un point fixe gS est tel que $H\subset gSg^{-1}$, le sous-groupe agissant H est inclus dans le conjugué correspondant au point fixe.

1.2.2. Actions par conjugaison. — Tout groupe agit sur lui-même par automorphismes intérieurs. $G\times G\to G, (g,x)\mapsto g\cdot x = gxg^{-1}$. Les orbites sont appelées classes de conjuguaison. En particulier, si G est le groupe linéaire $GL(n,K)$ les classes de conjuguaison regroupent les matrices semblables. Le noyau de φ, $N(\varphi) = \{g\in G, \forall x\in G, gx = xg\}$ est par définition le *centre* $cent(G)$ du groupe G. C'est un sous-groupe distingué et même caractéristique, c'est à dire stable par tout automorphisme de G. Le centre d'un groupe abélien est le groupe lui-même. En particulier, on obtient un injection de $G/cent(G)$ dans $Aut(G)$ dont l'image est constituée des automorphismes intérieurs.

Le groupe $GL(n,K)\times GL(n,K)$ agit sur $M(n,K)$ par $(A,B)\cdot M = AMB^{-1}$. Les orbites regroupent les matrices de même rang.

Tout groupe agit sur l'ensemble de ses sous-groupes par conjugaison $G\times Sous-groupe(G)\to Sous-groupe(G), (g,H)\mapsto gHg^{-1}$. Le stabilisateur G_H d'un sous-groupe H est appelé normalisateur de H, $N_G(H) := \{g\in G, gHg^{-1} = H\}$. Le sous-groupe H est distingué dans son normalisateur.

1.2.3. Représentations linéaires. — Un exemple important d'action est fourni par les représentations linéaires $\varphi : G\to GL(n,K)$. La représentation de permutation $\varphi : \mathfrak{S}_n\to$

$GL(n,K)$, $\varphi(\sigma) = (\delta_{i,\sigma(j)})$ autrement dit $\varphi(\sigma)(e_j) = e_{\sigma(j)}$ est fidèle et permet de réaliser via le théorème de Cayley, tout groupe fini comme (isomorphe à) un sous-groupe de matrices.

Exercice. — *Les isométries d'un tétraèdre régulier induisent par restrictions aux sommets des permutations de $\mathfrak{S}_4$. Montrer que cette correspondance est bijective. Expliciter la représentation de $\mathfrak{S}_4$ dans le groupe des isométries d'un tétraèdre régulier. (voir Rauch, page 40). Quelle est l'image des transpositions, des 3-cycles, des $(2,2)$-cycles, et des 4-cycles ?*

Plus généralement, à toute action d'un groupe G sur un ensemble fini E, on peut associer une représentation linéaire dont l'espace vectoriel associé est $V := \oplus_{x\in E}\mathbb{C}e_x$ et l'action $\varphi(g) \,:\, e_x \mapsto e_{g\cdot x}$ échange les vecteurs de base e_x. La matrice de $\varphi(g)$ dans la base e_x est une matrice de permutation orthogonale, avec $e := \sum_{x\in E} e_x$ comme vecteur propre. L'orthogonal de e est donc aussi l'espace vectoriel d'une représentation de G.

1.3. Théorèmes de Sylow

Définition. — – *Un groupe d'ordre une puissance d'un nombre premier p est appelé un p-groupe.*
– *Soit G un groupe d'ordre $p^\alpha q$ où p est un nombre premier, α un entier naturel et q un entier premier avec p. Un groupe d'ordre p^α est appelé p-sous-groupe de Sylow de G.*

Théorème. — *Soit G un groupe d'ordre $p^\alpha q$ où p est un nombre premier et q un entier premier avec p. Alors*

1. *Il existe un sous-groupe de G d'ordre p^α.*
2. *Tout sous-groupe de G d'ordre p^β avec $1 \leq \beta \leq \alpha$ est inclus dans un p-Sylow de G.*
3. *Le groupe G opère par conjuguaison transitivement sur ses p-Sylow.*
4. *Le nombre n_p de p-Sylow de G est congru à 1 modulo p et divise q.*

Démonstration. — 1. ***Lemme***. — *Soit G un groupe d'ordre $n = p^\alpha q$ où p est un nombre premier et q un entier premier avec p. Soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe un conjugué aSa^{-1} de S tel que $H \cap aSa^{-1}$ soit un p-Sylow de H.*

Démonstration. — On fait opérer le groupe H sur l'ensemble G/S. Le stabilisateur de aS est $aSa^{-1} \cap H$, qui est un p-sous-groupe de H. Reste à trouver un a tel que l'indice de $aSa^{-1} \cap H$ dans H soit premier à p. Mais par la seconde formule des classes, cet indice est le cardinal de l'orbite de $aS \in G/S$ par H. Si tous ces indices étaient divisibles par p, par la première formule des classes, le cardinal q de G/S le serait aussi. □

Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $GL(n,\mathbb{F}_p)$. Ce dernier groupe est d'ordre $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{n(n-1)/2}q$. L'ensemble des matrices triangulaires supérieures de diagonale identité est un p-sous-groupe de Sylow. En appliquant le lemme à $G \subset GL(n,\mathbb{F}_p)$, on obtient (1).

2. Soit H un p-sous-groupe de G et S un p-Sylow. Il existe un p-Sylow de H de la forme $aSa^{-1}\cap H$. Comme H est un p-groupe, $H = aSa^{-1}\cap H$. Donc , H est inclus dans aSa^{-1} qui est un p-Sylow de G.

3. Si H est de plus un p-Sylow, il existe a tel que $aSs^{-1} \cap H = H$, donc par cardinalité, $H = aSa^{-1}$ et H est un conjugué de S.
4. On fait agir un p-Sylow S par conjuguaison sur l'ensemble X des p-Sylow de G.

$$\operatorname{card} X = \operatorname{card} Fix(X) + \sum_{\substack{\mathcal{O}_i \in X/S, \\ \operatorname{card} \mathcal{O}_i \neq 1}} \operatorname{card} \mathcal{O}_i = \operatorname{card} Fix(X) \pmod p$$

par la seconde formule des classes, car S est un p-groupe.

Soit T un p-Sylow de G stable par tous les éléments de S (i.e. normalisé par S). Soit N le sous-groupe de G engendré par S et T. Les groupes S et T sont deux p-Sylow de N et comme T est distingué dans N, $S = T$. Donc, $Fix(X) = \{S\}$.

Les p-Sylow forment une orbite sous l'action par conjugaison de G sur ses sous-groupes. Par conséquent, n_p divise $\operatorname{card} G = n$. Comme $n_p = 1 \pmod p$ est premier avec p, il divise q.

□

Exercice. — *Montrer que le centre d'un p-groupe n'est pas réduit à un singleton.*

1.4. Groupes dérivés et résolubilité

La notion suivante permet de déterminer si un groupe G est construit par une suite d'extensions de groupes abéliens.

Le groupe dérivé $D(G)$ d'un groupe G est le groupe engendré par les commutateurs $aba^{-1}b^{-1}$ de G. C'est un sous-groupe distingué et même caractéristique, car si φ est un automorphisme de G, $\varphi(aba^{-1}b^{-1})$ est un commutateur, le commutateur de $\varphi(a)$ et $\varphi(b)$. Le groupe dérivé d'un groupe abélien est le groupe $\{e_G\}$. Le groupe $G/D(G)$ est abélien. Si $f : G \to A$ est un morphisme de groupes de G vers un groupe abélien A, alors $D(G) \subset N(f)$ et le morphisme f se factorise donc par la projection canonique $G \to G/D(G)$.

Par récurrence, on définit les groupes dérivés supérieurs par $D^{(k+1)}(G) := D(D^{(k)}(G))$.

Définition. — *Un groupe G est dit* résoluble *si l'un de ses groupes dérivés supérieurs est réduit à l'élément neutre.*

Exercice. — *Montrer qu'un groupe G tel que $G/centre(G)$ est cyclique est en fait abélien.*

Exercice. — *Montrer qu'un groupe G d'ordre p^2 (p est un nombre premier) est abélien.*

Proposition. — *Soit H un sous-groupe distingué d'un groupe G. Pour que G soit résoluble, il faut et il suffit que H et G/H le soient.*

Démonstration. — Comme H est un sous-groupe de G, les groupes dérivés supérieurs $D^{(k)}(H)$ sont des sous-groupes de $D^{(k)}(G)$. L'image de $D^{(k)}(G)$ par la surjection canonique $G \to G/H$ (qui est un morphisme de groupe car H est distingué) est engendrée par l'image des commutateurs de G c'est à dire les commutateurs de G/H ; c'est donc $D^{(k)}(G/H)$. Par conséquent, si G est résoluble, H et G/H le sont aussi. Pour la réciproque, supposons pour commencer que H est résoluble et G/H abélien. On en déduit que le groupe dérivé $D(G)$ est inclus dans H. Il est donc résoluble, ainsi que G. Plus généralement maintenant si G/H est résoluble, soit k tel que $D^{(k)}(G/H) = \{e\}$. Le groupe $D^{(k-1)}(G)/H \cap D^{(k-1)}(G)$ est

le sous-groupe de G/H engendré par les images dans G/H des commuteurs d'ordre $k-1$ d'éléments de G. C'est donc $D^{(k-1)}(G/H)$ qui est abélien. On en déduit que

$$D^{(k)}(G) = D(D^{(k-1)}(G)) \subset H \cap D^{(k-1)}(G) \subset H$$

et donc que G est résoluble. □

Exercice. — *Montrer que tout p-groupe est résoluble.*

Les groupes d'ordre pq (avec $p < q$ deux nombres premiers distincts) sont résolubles. En effet, le nombre de q-sylow diviseur de p, congru à 1 modulo q, vaut 1. Ce q-Sylow est donc distingué et d'ordre premier (donc cyclique abélien) et le quotient du groupe par ce q-Sylow est aussi abélien.

À titre culturel, on peut retenir que

Théorème **(Théorème de Burnside)**. — *Soit p et q deux nombres premiers distincts et α et β deux entiers naturels. Tout groupe d'ordre $p^\alpha q^\beta$ est résoluble.*

1.5. Simplicité

On cherche à déterminer quand un groupe peut être obtenu par produit semi-direct à partir de groupes plus petits. Les briques élémentaires sont les groupes simples.

Définition. — *Un groupe G est dit* simple *s'il n'a pas de sous-groupes distingués propres.*

Noter que le centre et le sous-groupe dérivé d'un groupe sont des sous-groupes distingués (même caractéristiques). Le groupe dérivé d'un groupe simple est soit $\{Id\}$ et il est alors abélien, soit lui-même. Un groupe simple n'est donc résoluble que s'il est abélien.

Les morphismes d'un groupe simple vers un groupe quelconque sont constants ou injectifs. Parmi les groupes $\mathbb{Z}/n\mathbb{Z}$, seuls ceux pour n premiers sont simples. Un groupe qui admet un unique p-groupe de Sylow (unique donc distingué) propre n'est pas simple. C'est le cas des groupes d'ordre pq(avec $p < q$ deux nombres premiers distincts), par exemple $\mathfrak{S}_3$..

CHAPITRE 2

GROUPES SYMÉTRIQUES ET ALTERNÉS

2.1. Groupe symétrique

Théorème. — – *Toute permutation de $\mathfrak{S}_n$ peut s'écrire comme produit d'au plus $n-1$ transpositions.*

– *Toute permutation se décompose en produit de cycles à support disjoints. Cette décomposition est unique à l'ordre près des cycles.*

Démonstration. — – La démonstration se fait par récurrence sur n. Soit $\sigma \in \mathfrak{S}_n$. Si σ admet un point fixe a elle s'identifie à une permutation de $\{1, 2, \cdots, n\} - \{a\}$. Sinon, $\tau_{1,\sigma(1)} \circ \sigma$ admet 1 comme point fixe.

– On fait agir le groupe $< \sigma >$ engendré par une permutation σ sur $\{1, 2, \cdots, n\}$. On choisit un élément a_i dans chaque orbite. Alors,

$$\sigma = (a_1, \sigma(a_1), \cdots \sigma^{l_1-1}(a_1)) \circ (a_2, \sigma(a_2), \cdots \sigma^{l_2-1}(a_2)) \circ \cdots$$

L'unicité résulte du fait que dans toute écriture de σ en produit de cycles à support disjoint, les supports des cycles sont les orbites de l'action considérée.

□

En particulier, comme si les supports sont disjoints, les groupes engendrés par chacun des cycles ne s'intersectent qu'en l'identité, l'ordre d'une permutation est le $ppcm$ des ordres des cycles à support disjoint qui la compose.

Proposition **(Formules de conjugaison)**. — – *Soit $(i_1, i_2, \cdots, i_r)$ un cycle de longueur r et σ une permutation de $\mathfrak{S}_n$. Alors,*

$$\sigma \circ (i_1, i_2, \cdots, i_r) \circ \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \cdots, \sigma(i_r)).$$

– *Soit $c = c_N \circ c_{N-1} \circ \cdots \circ c_1$ une composée dans $\mathfrak{S}_n$ et σ une permutation de $\mathfrak{S}_n$. Alors,*

$$\sigma \circ c \circ \sigma^{-1} = (\sigma \circ c_N \circ \sigma^{-1}) \circ (\sigma \circ c_{N-1} \circ \sigma^{-1}) \circ \cdots \circ (\sigma \circ c_1 \circ \sigma^{-1}).$$

Corollaire. — *Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions $(1, i)$ $(2 \leq i \leq n)$ ou par les transpositions $(i, i+1)$, $1 \leq i \leq n-1$ ou encore par la transposition $(1, 2)$ et le cycle $(1, 2, \cdots, n)$.*

Démonstration. — On utilise les égalités $(1, 2, \cdots k) = (1, 2)(2, 3) \cdots (k-1, k)$, les relations de conjugaison et en particulier $(i, j) = (1, i)(1, j)(1, i)$. □

Définition. — *Le profil d'une permutation est la structure d'une de ses décompositions en produit de cycles à support disjoint. On la notera*

$$l_1^{n_1} \circ l_2^{n_2} \circ \cdots \circ {}_d^{n_d} = \underbrace{(\overbrace{\cdot\cdot}^{l_1})(\cdot\cdot)\cdots(\cdot\cdot)}_{n_1 \text{ fois}} \underbrace{(\overbrace{\cdot\cdot\cdot}^{l_2})(\cdot\cdot\cdot)\cdots(\cdot\cdot\cdot)}_{n_2 \text{ fois}} \cdots \underbrace{(\overbrace{\cdot\cdot\cdot\cdot\cdot}^{l_d})(\cdot\cdot\cdot\cdot\cdot)\cdots(\cdot\cdot\cdot\cdot\cdot)}_{n_d \text{ fois}}.$$

Théorème. — – *Deux permutations sont conjuguées dans $\mathfrak{S}_n$ si et seulement si elles ont le même profil de décomposition en produits de cycles à support disjoint.*

– *Un sous-groupe distingué de $\mathfrak{S}_n$ contient aucune ou toutes les permutations avec le même profil en produit de cycles à supports disjoints.*

– *Soit H un sous-groupe de $\mathfrak{S}_n$ qui, s'il contient une permutation, contient toutes les permutations avec le même profil. Alors H est distingué.*

Démonstration. — C'est aussi une conséquence des formules de conjugaison. □

***Proposition* (Théorème de Cauchy).** — *Dans $\mathfrak{S}_n$, le nombre d'éléments de profil $l_1^{n_1} \circ l_2^{n_2} \circ \cdots \circ l_d^{n_d}$ (le cardinal de la classe de conjugaison correspondante) est*

$$\frac{n!}{l_1^{n_1} l_2^{n_2} \cdots l_d^{n_d} n_1! n_2! \cdots n_d!}.$$

Démonstration. — Le groupe $\mathfrak{S}_n$ agit par conjugaison sur cette classe de conjugaison. L'action est transitive et le stabilisateur d'une telle permutation $\sigma = c_{1,1} \circ c_{1,2} \cdots \circ c_{1,n_1} \circ \cdots \circ c_{d,1} \circ \cdots c_{d,n_d}$ est le produit semi-direct

$$(< c_{1,1} > \times < c_{1,2} > \times \cdots < c_{d,n_d} >) \rtimes (\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2} \times \cdots \times \mathfrak{S}_{n_d}).$$

Ici, le produit $< c_{1,1} > \times < c_{1,2} > \times \cdots < c_{d,n_d} >$ des groupes engendrés par les cycles est un sous-groupe distingué de $stab(\sigma)$. On choisit une écriture des cycles $c_{k,i} = (a_{k,i,1}, a_{k,i,2} \cdots a_{k,i,l_k})$. Le groupe $\mathfrak{S}_{n_k}$ provient du groupe des permutations des premiers éléments $a_{k,i,1}$ ($1 \leq i \leq n_k$) dont l'action est prolongée sur les éléments suivants par la permutation σ. Le produit $\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2} \times \cdots \times \mathfrak{S}_{n_d}$ agit à travers l'application

$$\begin{array}{rcl} \mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_d} & \to & Aut(< c_{1,1} > \times \cdots < c_{d,n_d} >) \\ (\sigma_1, \cdots, \sigma_{n_d}) & \mapsto & \left\{ \begin{array}{ccc} < c_{1,1} > \times \cdots \times < c_{d,n_d} > & \to & < c_{1,1} > \times \cdots \times < c_{d,n_d} > \\ c_{1,1}^{p_{1,1}} c_{1,2}^{p_{1,2}} \cdots c_{1,n_1}^{p_{1,n_1}} \cdots c_{d,n_d}^{p_{d,n_d}} & \mapsto & c_{1,1}^{p_{1,\sigma_1(1)}} c_{1,2}^{p_{1,\sigma_1(2)}} \cdots c_{1,n_1}^{p_{1,\sigma_1(n_1)}} \cdots c_{d,n_d}^{p_{d,\sigma_d(n_d)}} \end{array} \right. \end{array}$$

Pour montrer que le produit $(< c_{1,1} > \times < c_{1,2} > \times \cdots < c_{d,n_d} >) \rtimes (\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2} \times \cdots \times \mathfrak{S}_{n_d})$ engendre le stabilisateur de σ il suffit de remarquer qu'un élément du stabilisateur (qui commute donc avec σ) qui fixe les premiers éléments $a_{k,i,1}$ ($1 \leq k \leq d$, $1 \leq i \leq n_k$) est nécessairement l'identité. □

Exercice 2.1.1. — Décrire les profils possibles et le nombre d'éléments dans les classes de conjuguaison pour $\mathfrak{S}_4$.

2.2. Groupe alterné

2.2.1. Définition. —

Théorème. — *L'application signature ε de $\mathfrak{S}_n \to \{-1, 1\}$ est définie pour $\sigma \in \mathfrak{S}_n$, par $\varepsilon(\sigma) = (-1)^{n-r}$ où r désigne le nombre de cycles figurant dans la décomposition de σ, y compris les cycles réduits à un point. C'est un morphisme de groupes (à valeurs dans un groupe abélien).*

Démonstration. — L'argument important est la comparaison des cycles de σ et ceux de $\sigma\tau$ où $\tau = (ij)$. Si i et j sont dans un même cycle de σ, $\sigma\tau$ a un cycle de plus que σ. Sinon, $\sigma\tau$ a un cycle de moins que σ. Par conséquent, $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Comme les transpositions engendrent le groupe symétrique, ε est un morphisme de groupes. □

On vérifie que

$$\varepsilon(\sigma) := \Pi_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Définition. — *Le groupe alterné $\mathfrak{A}_n$ est par définition le noyau du morphisme signature.*

Par exemple, $\mathfrak{A}_2 = \{\mathrm{Id}\}$, $\mathfrak{A}_3 = \{\mathrm{Id},\ (123),\ (132)\}$ et le groupe alterné $\mathfrak{A}_4$ est d'ordre 12. Il contient les cycles d'ordre 3 et les produits de 2 cycles d'ordre 2 de supports disjoints :

$\mathfrak{A}_4 = \{\mathrm{Id},\ (234),\ (243),\ (134),\ (143),\ (124),\ (142),\ (123),\ (132),\ (12)(34),\ (13)(42),\ (14)(23)\}$.

2.2.2. Générateurs. —

***Théorème* (Générateurs du groupe alterné).** —

– *Pour $n \geq 3$, le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles.*

– *Les 3-cycles sont conjugués dans $\mathfrak{S}_n$ et si $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

Démonstration. — – Il suffit de remarquer que

$$(i,j)(j,k) = (i,j,k) \text{ et } (i,j)(k,l) = (i,j)(j,k)(j,k)(k,l) = (i,j,k)(j,k,l)$$

et donc que tout produit d'un nombre pair de transpositions est un produit de 3-cycles.

– Il résulte de la formule de conjugaison, que tous les 3-cycles sont conjugués dans $\mathfrak{S}_n$. En conjuguant si nécessaire par une transposition dont le support ne rencontre pas le support du 3-cycle ($n \geq 5$), on montre que tous les trois cycles sont conjugués dans $\mathfrak{A}_n$.

□

2.3. Groupe dérivé et résolubilité

Le groupe dérivé de $\mathfrak{S}_3$ est (inclus dans) le sous-groupe alterné cyclique (engendré par un 3-cycle) donc abélien. Par conséquent, $\mathfrak{S}_3$ est résoluble.

L'ensemble $\mathfrak{D}_4$ des permutations de profil $(2,2)$ dans $\mathfrak{A}_4$ est un sous-groupe d'ordre 4 commutatif (isomorphe au groupe de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$) et distingué. Le quotient $\mathfrak{A}_4/\mathfrak{D}_4$ est un groupe d'ordre 3 donc cyclique. Par conséquent, $\mathfrak{A}_4$ est résoluble. Comme le groupe dérivé de $\mathfrak{S}_4$ est inclus dans $\mathfrak{A}_4$, $\mathfrak{S}_4$ est résoluble.

***Proposition*.** — – *Pour $n \geq 2$, le groupe dérivé $D(\mathfrak{S}_n)$ est $\mathfrak{A}_n$.*

– *Pour $n \geq 5$, le groupe dérivé $D(\mathfrak{A}_n)$ est $\mathfrak{A}_n$.*

Démonstration. — Soit $n \geq 5$. Comme $D(\mathfrak{A}_n) \subset D(\mathfrak{S}_n) \subset \mathfrak{A}_n$, et comme $\mathfrak{A}_n$ est engendré par les 3-cycles, il suffit de montrer que tout 3-cycle est un commutateur. Soit c un 3-cycle. Comme c^2 qui est un 3-cycle est conjugué dans $\mathfrak{A}_n$ ($n \geq 5$) avec c, il existe $\sigma \in \mathfrak{A}_n$ tel que $c^2 = \sigma c \sigma^{-1}$. Par conséquent, $c = c^{-1}\sigma c \sigma^{-1}$ est un commutateur. □

Comme corollaire, on obtient le

***Théorème*.** — *Si $n \geq 5$, le groupe $\mathfrak{A}_n$ n'est pas résoluble.*

2.4. Centre et simplicité

***Proposition*.** — – *Pour $n \geq 3$, le centre du groupe $\mathfrak{S}_n$ est réduit à $\{\mathrm{Id}\}$.*

– *Si $n \geq 4$, $cent(\mathfrak{A}_n) = \{\mathrm{Id}\}$.*

Démonstration. — – Soit $\sigma \in Cent(\mathfrak{S}_n)$. Puisque $\sigma(ij)\sigma^{-1} = (\sigma(i), \sigma(j))$, si $\sigma(j) \neq j$, $\sigma(j) = i$. Par conséquent, σ a au plus un point non fixe. Donc, σ est l'identité. La démonstration n'utilise que la commutation avec les transpositions.

– Soit $\sigma \in Cent(\mathfrak{A}_n)$. Si $\sigma \neq \mathrm{Id}$, soit a et $b \neq a$ tels que $\sigma(a) = b$. Soit $c \neq d$ deux autres éléments de $\{1, \cdots n\}$. Puisque $\sigma(a,c,d)\sigma^{-1} = (\sigma(a), \sigma(c), \sigma(d)) = (b, \sigma(c), \sigma(d))$ contient b dans son support, elle n'est pas égale à (a,c,d). Ceci contredit le fait que σ et (a,c,d) commutent. Donc, σ est l'identité.

□

Le groupe $\mathfrak{A}_3$ est cyclique d'ordre premier donc simple.

Le centre de $\mathfrak{A}_4$ est trivial. Mais $\mathfrak{A}_4$ contient l'ensemble $\mathfrak{D}_4$ des permutations de profil $(2,2)$ comme sous-groupe distingué. Par conséquent $\mathfrak{A}_4$ n'est pas simple.

Théorème. — *Si $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.*

Démonstration. — Soit H un sous-groupe distingué de $\mathfrak{A}_n$. S'il contient un 3-cycle, il contient toute la classe de conjuguaison, donc tous les 3-cycles. Comme ces derniers engendrent $\mathfrak{A}_n$, il suffit de montrer que H contient un 3-cycle.

Soit $\sigma \in H$ une permutation différente de l'identité et de support de longueur minimale. Soit $\sigma = c_1 \circ c_2 \circ \cdots \circ c_r$ une décomposition en cycles à support disjoints avec $long(c_i)$ croissante. Montrons que σ est un 3-cycle. Si le support de σ est de longueur inférieure à 3, σ alterné est un 3-cycle. Sinon, puisque les 4-cycles sont impairs, soit le support de c_1 a au moins trois points $c_1 = (1,2,3,\cdots)$, soit $\sigma = (1,2) \circ (3,4,\cdots) \circ \cdots$. Dans le premier cas, le support de σ a au moins cinq points disons $1,2,3,4,5$. Soit $c = (3,4,5)$. Le commutateur $c\sigma^{-1}c^{-1}\sigma = (c\sigma^{-1}c^{-1})\sigma$ est dans le sous-groupe distingué H. Par ailleurs, $\sigma^{-1}c^{-1}\sigma = (\sigma^{-1}(5), \sigma^{-1}(4), \sigma^{-1}(3)) = (\sigma^{-1}(5), \sigma^{-1}(4), 2)$ n'est pas égal à c^{-1} car 2 n'est pas dans le support de c^{-1}. Le commutateur $c\sigma^{-1}c^{-1}\sigma$ n'est donc pas l'identité. Il n'agit pas en dehors du support de σ et admet 1 comme point fixe supplémentaire. Ceci contredit la minimalité de σ. Dans le second cas le même commutateur envoie 3 sur 5 et laisse invariants 1 (et 2). □

CHAPITRE 3

STRUCTURE DU GROUPE LINÉAIRE (ASPECTS ALGÉBRIQUES)

On va essayer de dégager des similitudes dans l'étude des groupes linéaires et symétriques (ou alternés).

3.1. Générateurs de $GL(E)$ et $SL(E)$

Dans toute cette partie k est un corps commutatif et E un k-espace vectoriel de dimension finie.

Les éléments les plus simples du groupe linéaire sont ceux qui admettent un hyperplan de points fixes.

Définition. — – *Le groupe général linéaire est l'ensemble des isomorphismes de E (endomorphismes de E bijectifs à inverse linéaire) muni de la loi de composition.*
– *Le groupe spécial linéaire $SL(E)$ est le noyau du morphisme déterminant (à valeurs dans un groupe abélien).*

Remarquer que les endomorphismes bijectifs sont des isomorphismes.

Deux espaces vectoriels de dimension finie sont isomorphes si et seulement si leur dimension sont les mêmes. En effet, le choix d'une base réalise un isomorphisme entre k^n et E. On notera donc $GL(n,k)$ le groupe $GL(n,k^n)$ isomorphe à tout groupe linéaire d'un k-espace vectoriel de dimension n.

Proposition. — *Soit $u \in GL(E)$ un isomorphisme de E qui admet un hyperplan $H = ker(u - \mathrm{Id})$ de points fixes. Alors,*
– *soit $\det u = \lambda \neq 1$, u est une dilatation de rapport λ et de droite $Im(u - Id) = Ker(u - \lambda Id)$ supplémentaire de H. L'endomorphisme u est diagonalisable : il existe une base de E dans laquelle u a pour matrice*

$$\begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & \ddots & & & \\ & & & & \ddots & & \\ & & & & & \ddots & \\ & & & & & & 1 \\ & & & & & & & \lambda \end{pmatrix}.$$

– *soit $\det u = 1$, u est une tranvection. Il existe une forme linéaire f définissant H et un vecteur a non nul de $Im(u - \mathrm{Id})$ tels que $u = \mathrm{Id} + f \cdot a$. Il existe une base de E composée d'une base de H de dernier vecteur a et d'un vecteur b hors de H tel que $f(b) = 1$, dans*

laquelle u a pour matrice

$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & \ddots & & & & \\ & & & & \ddots & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & 1 \\ & & & & & & & 1 \end{pmatrix}.$$

***Théorème* (Générateurs du groupe spécial linéaire).** —

- *Les transvections engendrent le groupe spécial linéaire $SL(E)$. Les transvections et les dilatations engendrent le groupe linéaire $GL(E)$.*
- *Les transvections sont conjuguées dans $GL(E)$ et si $\dim E \geq 3$ les transvections sont conjuguées dans $SL(E)$.*

Démonstration. — On commence par démontrer deux lemmes.

***Lemme*.** — *Soit E un espace vectoriel de dimension au moins 2. Soit x et y deux vecteurs non nuls de E. Il existe une transvection ou un produit de deux tranvections qui envoie x sur y.*

Démonstration. — On cherche u sous la forme $u = \mathrm{Id} + f \cdot (y - x)$, avec $f(x) = 1$ et $f(x - y) = 0$. Si x et y ne sont pas colinéaires alors $(x, x - y)$ est libre, et on peut trouver la forme linéaire f. Sinon, on passe par un vecteur intermédiaire z colinéaire ni à x, ni à y. □

***Lemme*.** — *Soit z un vecteur non nul de E et H et H' deux hyperplans qui ne contiennent pas x. Alors, il existe une transvection (ou l'identité) u telle que $u(z) = z$ et $u(H) = H'$.*

Démonstration. — Dans le cas où $H = H'$ on prend pour u, l'identité de E. Sinon, $H \cap H'$ est de codimension 2. On choisit l'hyperplan $h = vect(H \cap H', z)$. Comme $z \in h$ et $z \notin H$, $h \not\subset H$ et comme h est un hyperplan $H \not\subset h$. Soit donc $x \in H - h$ et de même $y \in H' - h$. Soit f une équation de h. Comme $f(x) \neq 0$ et $f(y) \neq 0$, on peut supposer $f(x) = f(y) = 1$ et donc $y - x \in h$. On a alors $H = vect(H \cap H', x)$ et $H' = vect(H \cap H', y)$. Comme $H \neq H'$, x et y ne sont pas colinéaires. La transvection $\mathrm{Id} + f(y - x)$ fixe h donc z et envoie x sur y donc H sur H'. □

La démonstration du théorème se fait par récurrence sur $\dim E$. Si $\dim E = 1$, $SL(E) = \{\mathrm{Id}\}$. On suppose que les tranvections engendrent le groupe spécial linéaire en dimension $n-1$ et on considère u dans $SL(E)$ où E est de dimension n. Soit x non nul dans E et τ une transvection ou un produit de deux transvections tel que $\tau \circ u(x) = x$. Soit H un hyperplan supplémentaire de $vect(x)$. Si $\tau \circ u$ est l'identité aussi sur H, $u = \tau^{-1}$ est un produit de transvections. Sinon, il existe une tranvection t telle que $t(x) = x$ et $t(\tau \circ u(H)) = H$. Par hypothèse de récurrence il existe un produit de tranvections τ_i de H telles que $t \circ \tau \circ u_{|H} = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$. En définissant les tranvections $\widetilde{\tau_i} := \tau \oplus \mathrm{Id}_{vect(x)}$ sur $E = H \oplus vect(x)$, on peut écrire $t \circ \tau \circ u$ comme $\widetilde{\tau_1} \circ \widetilde{\tau_2} \circ \cdots \circ \widetilde{\tau_k}$, et donc u comme produit de transvections.

Soit τ et t deux transvections. Les transvections sont conjuguées dans $GL(E)$ car elles ont même réduite de Jordan. Soit donc $u \in GL(E)$ telle que $u\tau u^{-1} = t$. Soit $\lambda = \det u$. Soit B une base de E où t a pour matrice

$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & \ddots & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & & & & & & 1 & 1 \\ & & & & & & & 1 \end{pmatrix}.$$

Soit d l'isomorphisme de E dont la matrice dans la base B est

$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & \ddots & & & & \\ & & & & 1 & & & \\ & & & & & \lambda & & \\ & & & & & & \lambda^{-1} & \\ & & & & & & & \lambda^{-1} \end{pmatrix}.$$

Ainsi du appartient à $SL(E)$ et comme t et d commutent, $du\tau(du)^{-1} = dtd^{-1} = t$. □

3.2. Groupe dérivé et résolubilité

Proposition. — *Pour $n \geq 3$ et k un corps de caractéristique différente de 2,*
- *le groupe dérivé $D(GL(n,k)) = SL(n,k)$ et*
- *le groupe dérivé $D(SL(n,k)) = SL(n,k)$.*

Démonstration. — Si τ est une transvection, τ^2 n'est pas égale à l'identité car $2 \neq 0$ dans le corps k. Comme les transvections sont toutes conjuguées dans $SL(n,k)$, il existe $g \in SL(n,k)$ tel que $\tau^2 = g\tau g^{-1}$, soit $\tau = \tau^{-1} g\tau g^{-1}$. Ainsi, nous avons montré que les groupes $D(SL(n,k))$ et donc $D(GL(n,k))$ contiennent toutes les transvections et par suite tout $SL(n,k)$. Les inclusions opposées résulte du fait que les commutateurs sont de déterminant 1 ou encore que $SL(n,k)$ est le noyau d'un morphisme de groupes de $GL(n,k)$ à valeurs dans un groupe abélien. □

Comme corollaire on obtient le

Théorème. — *Si $n \geq 3$ et si k un corps de caractéristique différente de 2, les groupes $GL(n,k)$ et $SL(n,k)$ ne sont pas résolubles.*

3.3. Centres de $GL(E)$ et $SL(E)$, simplicité de $PSL(E)$

Proposition. — *Le centre de $GL(E)$ est formé des homothéties. Le centre de $SL(E)$ est formé des homothéties de rapport racine* $\dim E$*-ième de l'unité.*

Démonstration. — Soit u dans $GL(E)$ qui commute à tout $SL(E)$. Soit D une droite de E et τ une transvection de droite D. La conjuguée $u\tau u^{-1}$ est une transvection de droite $u(D)$. Comme u commute à τ, $u(D) = D$. Ainsi, l'image par u de tout vecteur x est colinéaire à x. Soit x et y deux vecteurs de E. On peut écrire $u(x) = \lambda x$ et $u(y) = \mu y$. Si x et y sont deux vecteurs colinéaires, comme u est une homothétie sur la droite $vect(x)$, $\lambda = \mu$. Si x et y sont deux vecteurs non colinéaires et $u(x+y) = \lambda x + \mu y$ n'est colinéaire à $x+y$ que si $\lambda = \mu$ (par indépendance). Donc, u est une homothétie. La démonstration n'utilise que la commutation avec les transvections. □

On retiendra de la démonstration le

Lemme. — *Les éléments du centre de $GL(E)$ sont exactement les éléments qui conservent globalement les droites de E.*

On considère $P(E)$ l'espace projectif des droites de E. Le groupe $GL(E)$ agit sur $P(E)$. Son centre est exactement le noyau du morphisme $GL(E) \to \mathfrak{S}(P(E))$ associé à l'action. Par conséquent, le groupe quotient $PGL(E) := GL(E)/centre(GL(E))$ agit de manière fidèle sur $P(E)$. On l'appelle groupe projectif linéaire.

Le groupe $SL(E)$ qui a un centre non trivial n'est pas simple, mais

Théorème. — *Si $n \geq 3$, le groupe quotient $PSL(E) = SL(E)/cent(SL(E))$ est simple.*

$$1 \to SL(E) \to GL(E) \stackrel{\det}{\to} k^\star \to 1$$
$$1 \to cent(SL(E)) \to SL(E) \to PSL(E) \to 1$$

Démonstration. — Soit $\overline{N}$ un sous-groupe distingué de $PSL(E)$ non réduit à l'élément neutre. Son image réciproque N dans $SL(E)$ est un sous-groupe distingué contenant strictement le centre de $SL(E)$. Comme toutes les transvections sont conjuguées dans $SL(E)$ ($\dim E \geq 3$), et qu'elles engendrent $SL(E)$, il suffit de montrer que N contient une transvection pour montrer que $N = SL(E)$.

Soit $u \in N$ qui n'est pas une homothétie et $a \in E$ tel que a et $u(a)$ ne soit pas colinéaires. Soit t une transvection de droite $vect(a)$. Le commutateur $v = utu^{-1}t^{-1} = u(tu^{-1}t^{-1})$ est dans le groupe distingué N. Le conjugué utu^{-1} est une transvection de droite $vect(u(a)) \neq vect(a)$. Donc, $utu^{-1} \neq t$ et v n'est pas l'identité. La transvection t s'écrit

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

On en déduit que

$$\begin{aligned} t^{-1}(y) &= y - f(t^{-1}(y))a \\ utu^{-1}(x) &= x + f(u^{-1}(x))u(a) \\ v(y) &= utu^{-1}t^{-1}(y) = y - f(t^{-1}(y)a + f(u^{-1}(t^{-1}(y)))u(a). \end{aligned}$$

En particulier, v laisse globalement invariant tout hyperplan contenant a et $u(a)$.

Soit H un tel hyperplan. S'il existe une transvection τ d'hyperplan H qui ne commute pas à v, $v\tau v^{-1}\tau^{-1}$ produit de τ^{-1} transvection d'hyperplan H et de $v\tau v^{-1}$ transvection d'hyperplan $v(H) = H$, est une transvection non triviale dans N. Sinon, τ commute à toutes les transvections d'hyperplan H. Soit $c \in H$ et $\theta = \mathrm{Id} + F(x)c$ une transvection de droite $vect(c)$. La commutation de v avec θ montre que pour tout $x \in E$, $F(x)v(c) = F(v(x))c$ ce qui implique en choisissant x hors de H (et donc $F(v(x)) = F(x + v(x) - x) = F(x) \neq 0$ puisque $v(x) - x$ est dans H) que $v(c) = c$. Par conséquent $v \in N$ est une transvection non triviale d'hyperplan H. □

3.4. Groupes linéaires sur les corps finis

Dans tout ce paragraphe k désigne un corps fini de caractéristique p, de cardinal $q = p^\alpha$. On cherche dans ce chapitre à déconstruire les groupes finis en extension de groupes élémentaires.

3.4.1. Ordre des groupes linéaires sur les corps finis. — On note $\mathbb{F}_q$ "le" corps à $q = p^\alpha$ éléments où p est un nombre premier et α un entier naturel non nul.

Lemme. — *Les cardinaux des groupes sur $\mathbb{F}_q$ sont*
- $| \, GL(n, \mathbb{F}_q) \, | = (q^n - 1)(q^n - q) \cdot \cdots \cdot (q^n - q^{n-1})$
- $| \, SL(n, \mathbb{F}_q) \, | = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-2})q^{n-1}$
- $| \, PGL(n, \mathbb{F}_q) \, | = | \, SL(n, \mathbb{F}_q) \, |$
- $| \, PSL(n, \mathbb{F}_q) \, | = | \, SL(n, \mathbb{F}_q) \, | \, / \, \mathrm{pgcd}(n, q - 1)$.

Le nombre de racine $n$ième de l'unité dans $\mathbb{F}_q$ est $\mathrm{pgcd}(n, q - 1)$.

3.4.2. Isomorphismes exceptionnels. —

Proposition. — *On a les isomorphismes suivants*
- $GL(2, \mathbb{F}_2) = SL(2, \mathbb{F}_2) = PSL(2, \mathbb{F}_2) = PGL(2, \mathbb{F}_2) = \mathfrak{S}_3$
- $PGL(2, \mathbb{F}_3) = \mathfrak{S}_4$ *et* $PSL(2, \mathbb{F}_3) = \mathfrak{A}_4$.
- $PGL(2, \mathbb{F}_4) = PSL(2, \mathbb{F}_4) = \mathfrak{A}_5$.

Démonstration. — Le morphisme $SL(E) \to \mathfrak{S}(P(E))$ associé à l'action de $SL(E)$ sur les droites de E a pour noyau $centre(SL(E))$. Par conséquent, on obtient un morphisme injectif de groupes

$$PSL(E) \to \mathfrak{S}(P(E)).$$

Si E est de dimension 2, la droite projective $P(E)$ a $q + 1$ éléments, alors que $PSL(E)$ a $q(q^2 - 1)/2$ éléments si q est impair et $q(q^2 - 1)$ si q est pair.
- Si $k = \mathbb{F}_2$, $\mathbb{F}_2^\star = \{1\}$, les groupes sont tous de cardinal 6 le morphisme est une bijection.
- Si $k = \mathbb{F}_3$, $| \, PGL(2, \mathbb{F}_3) \, | = 24 = | \, \mathfrak{S}_4 \, |$, donc $PGL(2, \mathbb{F}_3) = \mathfrak{S}_4$ et le seul sous-groupe d'indice 2 de $\mathfrak{S}_4$ est $PSL(2, \mathbb{F}_3) = \mathfrak{A}_4$ (voir en TD).
- Si $k = \mathbb{F}_4$, $PSL(2, \mathbb{F}_4)$ de cardinal 60 est d'indice 2 dans $\mathfrak{S}_5$ donc distingué. Comme $\mathfrak{A}_5$ est simple, on connait la liste de ses sous-groupes distingués (voir en TD). On en déduit que $PSL(2, \mathbb{F}_4)$ est isomorphe à $\mathfrak{A}_5$.

□

3.4.3. Inversibles d'une sous-algèbre de matrices et sous-groupes de Sylow. —

Théorème. — *Soit $A \in M(n,k)$ et $P(A) \in GL(n,k) \cap k[A]$. Alors $P(A)^{-1}$ est un polynôme en A. En conséquence, l'ensemble $GL(n,k) \cap k[A]$ est un sous-groupe abélien de $GL(n,k)$.*

Démonstration. — La stabilité par produit est simple à montrer. Soit $B \in GL(n,k) \cap k[A]$ et $\mu \in k[X]$ son polynôme minimal de coefficient dominant 1. Son terme constant c_0 est non nul, car A est inversible. La relation $\mu(A) = 0$ donne une relation

$$A(-B^{d-1} - c_{d-1}B^{d-1} - \cdots - c_1)c_0^{-1} = \mathrm{Id}$$

qui explicite un inverse de B comme polynôme en B. □

Noter que l'ensemble $GL(n,k) \cap k[A]$ est donc l'ensemble des inversibles de l'algèbre $k[A]$.

Soit $A \in GL(n,k)$, P son polynôme minimal et $P = \Pi_{i=1}^{d} P_i^{m_i}$ son écriture en produit de polynômes irréductibles. Alors, l'algèbre $k[A]$ est isomorphe à $k[X]/(P)$ (par l'application naturelle de $k[X] \to k[A], Q \mapsto Q(A)$) donc par le théorème chinois, à $\Pi_{i=1}^{d} k[X]/(P_i^{m_i})$. Le groupe des inversibles $k[A]^\star$ est par conséquent isomorphe au groupe produit $\Pi_{i=1}^{d} ((k[X]/(P_i^{m_i}))^\star$. Si toutes les multiplicités m_i sont égales à 1, les anneaux $k[X]/P_i^{m_i}$ sont des corps et leur ensemble d'inversibles $k[X]/P_i^{m_i} - \{0\}$. Le groupe précédent est alors de cardinal $\Pi_{i=1}^{d} \left((\operatorname{card} k)^{\deg P_i} - 1\right) = \Pi_{i=1}^{d} \left(p^{\alpha \deg P_i} - 1\right)$. On peut donc chercher parmi ces groupes d'inversibles, des groupes de Sylow abéliens, en particulier ceux d'ordre p ou p^2 (p premier).

Par exemple, le groupe $GL_3(\mathbb{F}_2)$ est de cardinal $(2^3-1)\times(2^3-2)\times(2^3-2^2) = 2^3\times 3\times 7$. Un groupe de Sylow d'ordre 2^3 est donné par le sous-groupe des matrices triangulaires supérieures inversibles.

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

Si A est une matrice de $GL_3(\mathbb{F}_2)$ dont le polynôme minimal est irréductible de degré 3, alors $k[A]^\star$ fournit un sous-groupe de Sylow d'ordre $2^3 - 1 = 7$.On peut choisir par exemple

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

dont le polynôme minimal est $X^3 + X^2 + 1$ de degré 3 sans racines dans $\mathbb{F}_2$ est irréductible dans $\mathbb{F}_2$.

Si A est une matrice de $GL_3(\mathbb{F}_2)$ dont le polynôme minimal est produit d'un polynôme de degré 1 par un polynôme de degré 2, alors $k[A]^\star$ fournit un sous-groupe de Sylow d'ordre $2^2 - 1 = 3$. On peut choisir par exemple

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

dont le polynôme minimal est $(X-1)(X^2+X+1)$.

CHAPITRE 4

GÉOMÉTRIE PROJECTIVE

4.1. Espaces projectifs

4.1.1. Projection conique. — Soit H un hyperplan d'un espace affine E et O un point de E hors de H. On notera H_O l'hyperplan de E parallèle à H passant par O. En vectorialisant E en O, on obtient un hyperplan affine H d'un espace vectoriel E_{vect}.

La projection depuis O sur H est l'application

$$\begin{array}{rccc} p\ : & E - H_O & \to & H \\ & x & \mapsto & (Ox) \cap H. \end{array}$$

Cette application vérifie

$$p(x) = p(y) \iff (Ox) = (Oy).$$

Pour prolonger la prolonger, on considère H comme un sous-ensemble de l'ensemble $P(E_{vect})$ des droites vectorielles de E_{vect}. On obtient alors

$$\begin{array}{rccc} P\ : & E - \{O\} & \to & P(E_{vect}) \\ & x & \mapsto & (Ox). \end{array}$$

qui est l'application de passage au quotient modulo l'action de $k^\star$ par homothétie sur $E - \{0\}$.

4.1.2. Espaces projectifs. —

Définition. — *Soit V un espace vectoriel. L'espace projectif $P(V)$ est l'ensemble des droites vectorielles de V. Un sous-espace projectif de $P(V)$ est un sous-ensemble de la forme $P(W)$ où W est un sous-espace vectoriel de V.*

Si V est de dimension finie sur un corps k, la dimension de $P(V)$ est $\dim_k V - 1$. Cette définition est compatible avec le calcul de dimension de l'image et des fibres de l'application P précédente.

Proposition. — *Si W_1 et W_2 sont deux sous-espaces vectoriels d'un espace vectoriel V, $P(W_1) \cap P(W_2)$ est un sous-espace projectif de $P(V)$. Si W_1 et W_2 sont de dimension finie, $P(W_1) \cap P(W_2)$ est de dimension*

$$\dim P(W_1) \cap P(W_2) = \dim P(W_1) + \dim P(W_2) - \dim P(W_1 + W_2).$$

En particulier, si $\dim P(W_1) + \dim P(W_2) \geq \dim P(V)$, alors $P(W_1)$ et $P(W_2)$ s'intersectent. (C'est le cas de deux droites dans un plan.)

Démonstration. — Elle résulte de l'observation $P(W_1) \cap P(W_2) = P(W_1 \cap W_2)$ et de l'égalité

$$\dim(W_1 \cap W_2) = \dim W_1 + \dim W_2 - \dim(W_1 + W_2).$$

□

4.1.3. Applications projectives. — Soit V et V' deux espaces vectoriels et $f : V \to V'$ une application linéaire. Si d est une droite de V incluse dans le noyau de f, $f(d) = \{0\}$. Si d est une droite de V non incluse dans $kerf$, $f(d)$ est une droite de V'. Par conséquent, on obtient une application

$$\begin{array}{rccc} P(f) : & P(V) - P(kerf) & \to & P(V') \\ & d & \mapsto & f(d) \end{array}$$

Si f est un isomorphisme, on dit que $P(f)$ est une homographie.

Par exemple, si V de dimension au moins 3, se décompose en $V = \Pi \oplus D$ comme somme d'un hyperplan Π et d'une droite D, l'application projective associée à la projection vectorielle sur Π parallèlement à D est appelée perspective

$$P(V) - \{D\} \to P(\Pi).$$

Exercice 4.1.4. — Soit $F = P(f)$ une homographie d'une droite projective dans elle-même. À quoi correspondent en terme de f les points fixes de F ? Montrer que si F admet trois points fixes deux à deux distincts, F est l'identité.

Lemme. — *Toute application projective $P(f)$ préserve l'alignement.*

Démonstration. — Soit A, B, C trois points de $P(V) - P(kerf)$ alignés sur une droite projective $P(W)$ (W est un plan non totalement inclus dans $kerf$). Les images $P(f)(A), P(f)(B)$ et $P(f)(C)$ sont sur l'ensemble $P(f)(W) = P(f(W))$ qui est une droite si $W \cap kerf = \{0\}$ et un point si $W \cap kerf$ est une droite. □

4.1.5. Prolongement vectoriel canonique d'un espace affine. — On montre dans ce paragraphe que tout espace affine peut-être réalisé comme complémentaire d'un hyperplan dans un espace projectif.

Théorème. — *Soit E un espace affine. Alors, il existe un espace vectoriel $\hat{E}$ et une forme linéaire $h : \hat{E} \to k$ telle que*

- *$Kerh$ est isomorphe comme espace vectoriel à la direction $\overrightarrow{E}$*
- *$h^{-1}(1)$ est isomorphe comme espace affine de direction $kerh$ à l'espace affine E de direction $\overrightarrow{E}$.*

En particulier, les quantités $x + \overrightarrow{u}$ dans E peuvent se calculer dans $\hat{E}$.

On a alors la décomposition

$$P(\hat{E}) = E \cup P(\overrightarrow{E}).$$

On notera en particulier $P(k_{ev}) = \infty$ et $P^1 := P(\hat{k}) = k \cup \{\infty\}$.

4.1.6. Structure affine du complémentaire d'un hyperplan projectif. —

Théorème. — *Soit P un espace projectif de dimension n et H un hyperplan (projectif) de P. L'ensemble $\mathcal{T}$ composé de l'identité et des homographies de P qui laissent fixes tous les points de H et eux seulement est un groupe isomorphe au groupe additif $(k^n, +)$ qui agit de façon simplement transitive sur $P - H$. Le complémentaire $P - H$ est donc naturellement un espace affine de dimension n.*

On dit alors que H est l'hyperplan à l'infini.

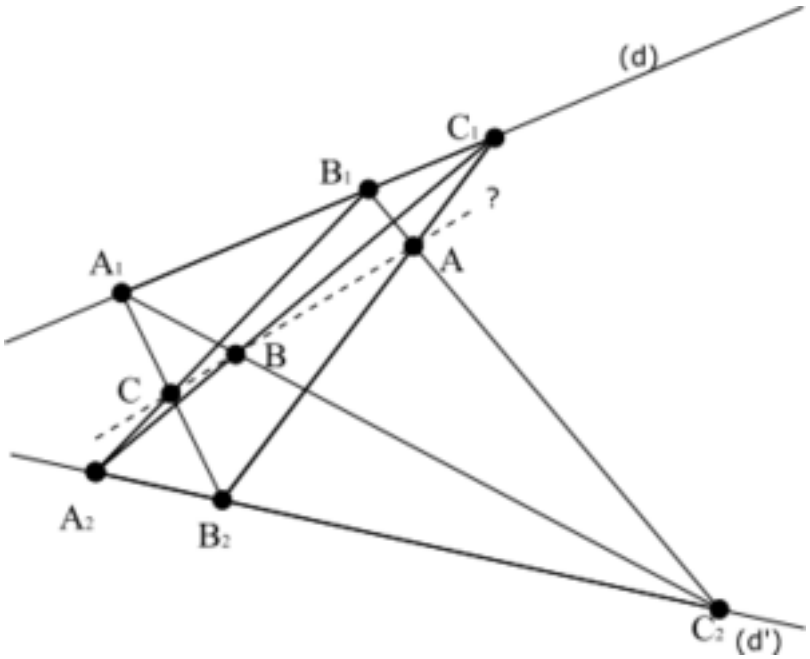
Démonstration. — On écrit $P = P(V)$, $H = P(h)$ et on fixe un supplémentaire kz de h dans V, $V = h \oplus kz$. Soit $T = P(t) \in \mathcal{T}$. Par hypothèse, puisque t fixe toutes les droites de h, il existe $a \in k$ tel que pour tout $x \in h$, $t(x) = ax$. De plus, $t(z)$ s'écrit $t(z) = x_0 + bz$, avec $x_0 \in h$ et $b \in k$.

$$t(x_0 + (b-a)z) = ax_0 + (b-a)x_0 + b(b-a)z = b(x_0 + (b-a)z).$$

Le point $x_0 + (b-a)z$ est donc sur h. Par conséquent, $a = b$. On peut même normaliser t, sans changer T, de sorte à avoir la formule $t(z) = x_t + z$ avec $x_y \in h$. La formule $x_{t\circ\tau} = x_t + x_\tau$ donne l'isomorphisme de groupes de $\mathcal{T}$ avec $(h, +)$. La simple transitivité résulte de la simple transitivité des translations de h sur $z + h$. □

4.1.7. Changement d'hyperplan à l'infini. — Soit E un espace affine. On le réalise comme complémentaire dans $P(\hat{E})$ de $P(\overrightarrow{E})$. On pourrait ensuite choisir sur $P(\hat{E})$ un autre hyperplan à l'infini que $P(\overrightarrow{E})$ et obtenir ainsi un autre espace affine E' dans lequel toute configuration de sous-espaces affines dans E est transformée en une nouvelle configuration.

***Théorème* (Théorème de Pappus).** — *Soit L et L' deux droites d'un plan projectif et A, B, C trois points sur L et A', B', C' trois points sur L'. Alors les points d'intersection $(AB') \cap (A'B)$, $(BC') \cap (B'C)$ et $(CA') \cap (C'A)$ sont alignés.*



Démonstration. — On choisit la droite joignant $(AB') \cap (A'B)$ et $(BC') \cap (B'C)$ comme droite à l'infini. La version affine du théorème de Pappus permet alors de conclure. □

Exercice 4.1.8. — Démontrer le théorème de Pappus affine : Soit d et d' deux droites d'un plan affine E. Soit A, B, C (resp. A', B', C') trois points sur d (resp. sur d'.) Si les droites (AB') et (BA') sont parallèles ainsi que les droites (BC') et (CB'), alors les droites (CA') et (AC') le sont aussi.

4.2. Théorème fondamental de la géométrie projective

Théorème. — *Soit $P(V)$ et $P(V')$ deux espaces projectifs de même dimension $n \geq 2$ sur deux corps k et k'. Si F est une bijection de P sur P' qui préserve l'alignement, alors il existe un automorphisme de corps s de k sur k', une application bijective g de V sur V' additive et s semi-linéaire (i.e. satisfaisant $g(\lambda x) = s(\lambda)g(x)$), tels que F provient par passage aux quotients de g.*

En particulier, toute bijection d'un espace projectif de dimension au moins 2 qui préserve l'alignement est composée d'un automorphisme de corps et d'une homographie.

Dans le cas où le corps k n'admet que l'identité comme automorphisme, on peut donc interpréter le groupe projectif $PGL(V) = GL(V)/centre(GL(V))$ comme le groupe des bijections de $P(V)$ qui préservent l'alignement, puisque le $centre(GL(V))$ est l'ensemble des éléments de $GL(V)$ qui fixent chaque droite de V.

4.3. Dualité projective

À tout sous-espace vectoriel F d'un espace vectoriel V, on peut associer un sous-espace F' de $V^\star$ défini par

$$F' := \{u \in V^\star, u_{|F} = 0\}.$$

On note que l'application de restriction $V^\star \to F^\star$ est surjective et a pour noyau F'. Par conséquent,

$$F^\star \simeq V^\star/F'.$$

Si V est de dimension finie, $\dim F + \dim F' = \dim V$. De plus, si $F \subset G$, alors $G' \subset F'$. En géométrie projective, cette correspondance permet de transformer des objets de $P(V)$ en objets de $P(V^\star)$ en conservant des relations d'incidence. Noter qu'un sous-espace projectif $P(F)$ de dimension d dans $P(V)$ de dimansion n donne le sous-espace projectif $P(F')$ de dimension $n - d - 1$ dans $P(V^\star)$. En particulier, dans un plan projectif, cette dualité échange droites et points.

Exercice 4.3.1. — Énoncer le théorème dual du théorème de Pappus.

4.4. Birapport

Dans un espace projectif P, le sous-espace projectif $< S >$ engendré par une partie S est le plus petit sous-espace projectif de P contenant S. C'est l'intersection de tous les sous-espaces projectifs de P contenant S.

Définition. — *Un repère projectif d'un espace projectif P de dimension n est la donnée de $n + 2$ points telle que chaque sous-ensemble de $n + 1$ points engendre P.*

Si $e_1, \cdots e_{n+1}$ est une base d'un espace vectoriel V, les droites $ke_1, \cdots, ke_{n+1}, k(e_1 + \cdots e_{n+1})$ forment un repère projectif de $P(V)$.

Lemme 4.4.1. — *Réciproquement chaque repère projectif* $\mathcal{R} = (d_1 = ku_1, \cdots, d_{n+1} = ku_{n+1} d_{n+2} = ku_{n+2})$ *provient par cette construction d'une unique base* $\mathcal{B}_\mathcal{R}$ *de* V *à multiplication près par une constante non nulle.*

Démonstration. — En effet, puisque $d_1, \cdots d_{n+1}$ engendrent tout $P(V)$, $u_1, \cdots u_{n+1}$ est une base de V. On écrit u_{n+2} dans cette base comme $u_{n+2} = \alpha_1 u_1 + \cdots \alpha_{n+1} u_{n+1}$.

Une base solution doit s'écrire $e_1 = \lambda_1 u_1, e_{n+1} = \lambda_{n+1} u_{n+1}$. La condition $d_{n+2} = k(e_1 + \cdots e_{n+1})$ soit $k(\alpha_1 u_1 + \cdots \alpha_{n+1} u_{n+1}) = k(\lambda_1 u_1 + \cdots + \lambda_{n+1} u_{n+1})$ requiert l'existence d'une constante c telle que $\lambda_i = c\alpha_i$, ce qui fixe la base à une constante près. □

Définition. — *Soit* $\mathcal{R} = (A_1, A_2, \cdots, A_{n+1}; A_{n+2})$ *un repère projectif de* $P(V)$. *Soit* d *une droite de* V *et* $[d]$ *le point de* $P(V)$ *correspondant. Les* coordonnées homogènes $[X_1 : X_2 : \cdots : X_{n+1}]$ *de* $[d]$ *sont les coordonnées cartésiennes* $(X_1, X_2, \cdots, X_{n+1})$ *d'un vecteur directeur* v *de* d *dans une base* $\mathcal{B}_\mathcal{R}$ *associée au repère* $\mathcal{R}$. *Elles sont bien définies à multiplication près par un scalaire non nul du corps* k.

Proposition. — *Si* $d_1, \cdots, d_{n+2}$ *et* $d'_1, \cdots, d'_{n+2}$ *sont deux repères projectifs d'un espace projectif* $P(V)$, *il existe une unique homographie* $h \in PGL(V)$ *telle que* $h(d_i) = d'_i$.

Démonstration. — Soit $e_1, \cdots, e_{n+1}$ et $e'_1, \cdots, e'_{n+1}$ deux bases de V associées aux repères précédents. Il existe un isomorphisme $\varphi \in GL(V)$ tel que $\varphi(e_i) = e'_i$ et donc $P(\varphi)(d_i) = d'_i$.

Si $F = P(f)$ est une homographie solution, comme $F(d_i) = d'_i$, il existe des constantes λ_i telle que $f(e_i) = \lambda_i e'_i$ pour $1 \leq i \leq n+1$ et pour $i = n+2$, $f(e_1 + \cdots e_{n+1}) = \lambda_{n+2}(e'_1 + \cdots e'_{n+1})$ soit $\lambda_1 e'_1 + \cdots + \lambda_{n+1} e'_{n+1} = \lambda_{n+2}(e'_1 + \cdots e'_{n+1})$. Ainsi $f = \lambda_{n+2}\varphi$ et donc $F = P(\varphi)$. □

Définition. — *Soit* A, B, C *trois points distincts d'une droite projective* L *et* D *un point de* L. *Soit* h *l'unique homographie de* L *sur* P^1 *telle que* $h(A) = \infty$, $h(B) = 0$ *et* $h(C) = 1$. *Le birapport du quadruplet* (A, B, C, D) *est*

$$[A, B, C, D] := h(D) \in P^1 = k \cup \{\infty\}.$$

Proposition. — – *Les homographies entre droites projectives préservent les birapports.*
- *Une bijection entre deux droites projectives qui préserve le birapport des quadruplets de points disctincts est une homographie.*

Démonstration. — – Soit g une homographie de L sur L'. Soit A, B, C trois points distincts de L et D un point de L. Soit h' l'unique homographie de L' sur P^1 telle que $h'(g(A)) = \infty$, $h'(g(B)) = 0$ et $h'(g(C)) = 1$. Alors, $h' \circ g$ permet de calculer le birapport de A, B, C, D qui est donc

$$[A, B, C, D] := (h' \circ g)(D) = h'(g(D)) = [g(A), g(B), g(C), g(D)].$$

– Soit g une bijection de P^1 sur P^1 qui conserve les birapports. Comme $0, 1, \infty$ forment un repère projectif de P^1, il existe une homographie h telle que $h(\infty) = g(\infty)$, $h(0) = g(0)$ et $h(1) = g(1)$. Soit D un point de P^1. La bijection $h^{-1} \circ g$ conserve les birapports et vérifie donc $[\infty, 0, 1, D] = [h^{-1} \circ g(\infty), h^{-1} \circ g(0), h^{-1} \circ g(1), h^{-1} \circ g(D)]$, soit $D = [\infty, 0, 1, h^{-1} \circ g(D)] = h^{-1} \circ g(D)$. Par conséquent, $h^{-1} \circ g = \mathrm{Id}$ et $g = h$ est une homographie.

Si maintenant g est une homographie entre deux droites L et L', il suffit de fixer deux homographies entre L et P^1, puis L' et P^1.

□

Exercice 4.4.1. — Montrer en utilisant les birapports qu'une homographie d'une droite projective qui a trois points fixes deux à deux distincts est l'identité.

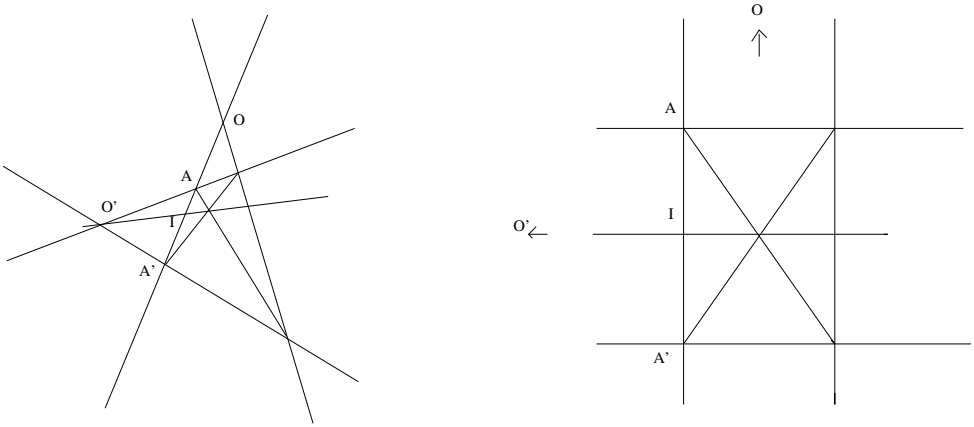
4.4.2. Expression du birapport en coordonnées. — Soit (e_1, e_2) une base de V. Si $v = Z_1e_1 + Z_2e_2$, on dit que $[Z_1 : Z_2]$ est un couple de coordonnées homogènes de la droite $vect(v)$ de $P(V)$. Soit $A[A_1 : A_2]$, $B[B_1 : B_2]$, $C[C_1 : C_2]$, $D[D_1 : D_2]$. L'application $h : P(V) \to P^1$,

$$[Z_1 : Z_2] \mapsto \frac{\frac{Z_1}{Z_2} - \frac{B_1}{B_2}\,\frac{C_1}{c_2} - \frac{A_1}{A_2}}{\frac{Z_1}{Z_2} - \frac{A_1}{A_2}\,\frac{C_1}{C_2} - \frac{B_1}{B_2}}$$

envoie A sur ∞, B sur 0 et C sur 1. Par conséquent,

$$[A, B, C, D] = \frac{\frac{D_1}{D_2} - \frac{B_1}{B_2}\,\frac{C_1}{c_2} - \frac{A_1}{A_2}}{\frac{D_1}{D_2} - \frac{A_1}{A_2}\,\frac{C_1}{C_2} - \frac{B_1}{B_2}} = \frac{\overline{BD}}{\overline{AD}}\frac{\overline{AC}}{\overline{BC}}.$$

En particulier, si le point $A = [1 : 0]$ (le point à l'infini $1/0$), on trouve $[A, B, C, D] = \dfrac{\overline{BD}}{\overline{BC}}$. Par exemple, si dans une carte affine O est à l'infini et I au milieu de $[AA']$, alors le birapport $[O, I, A, A'] = -1$: on dit alors que (O, I, A, A') forment une division harmonique.



Dans cette figure $[O, I, A, A'] = -1$.

4.5. Théorèmes classiques

Théorème **(Théorème de Thalès (version projective))**. — *Dans un espace projectif P, soit H_A, H_B, H_C, H_D quatre hyperplans contenant un même sous-espace Ω de codimension 2. Soit L et L' deux droites coupant H_A, H_B, H_C et H_D en quatre points distincts A, B, C, D respectivement A', B', C', D'. Alors les birapports $[A, B, C, D]$ et $[A', B', C', D']$ sont égaux. Ce birapport sera appelé birapport des quatre hyperplans H_A, H_B, H_C, H_D.*

Le théorème de Thalès (version affine) est obtenu en choisissant H_A comme hyperplan à l'infini.

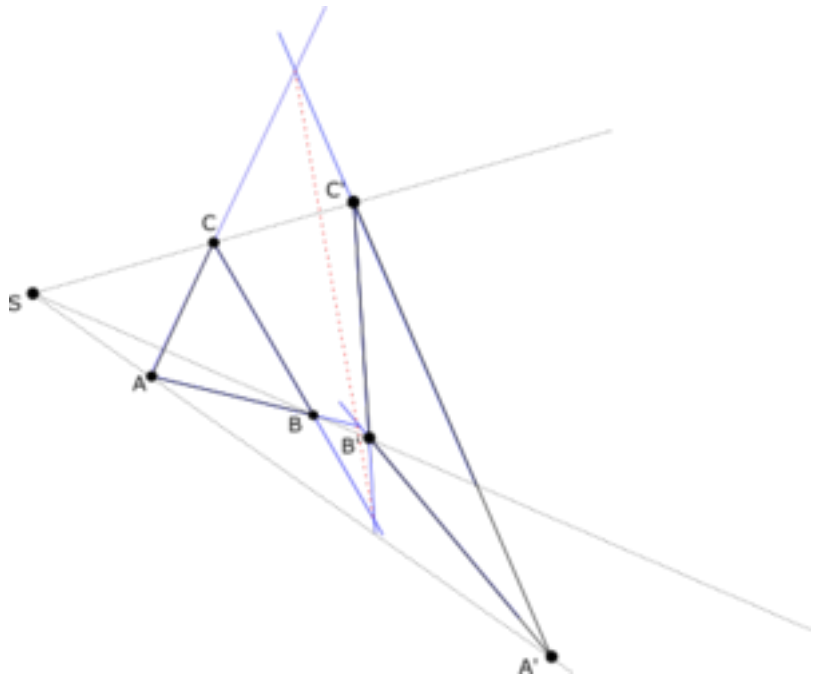
Démonstration. — Il suffit de considérer restriction à L de la projection depuis Ω sur L'. Comme c'est une homographie entre deux droites, elle conserve les birapports. □

4.5.1. Projections et théorème de Desargues. —

Proposition. — *Une homographie entre deux droites disctinctes d'un plan projectif est un projection si et seulement si elle fixe le point d'intersection de ces deux droites.*

Démonstration. — Les projections de l sur l' fixent $l \cap l'$. Réciproquement, soit h une homographie de l sur l' qui fixe $O := l \cap l'$. Soit A et B deux points distincts de $l - \{O\}$. En particulier $(Ah(A))$ et $(Bh(B))$ sont deux droites bien définies et distinctes. Soit $\Omega := (Ah(A)) \cap (Bh(B))$. Soit π la projection de l sur l' depuis Ω. Les homographies h et π coïncident sur le repère projectif (O, A, B) et sont donc égales. □

Théorème **(Théorème de Desargues)**. — *Soit ABC et $A'B'C'$ deux triangles ayant des sommets et des côtés distincts. Les points d'intersection $P = (AB) \cap (A'B')$, $Q = (BC) \cap (B'C')$ et $R = (CA) \cap (C'A')$ sont alignés si et seulement si les droites (AA'), (BB') et (CC') sont concourantes.*



Démonstration. — Si les droites (AA'), (BB') et (CC') sont concourantes, la composée de la projection de (AA') sur (BB') depuis $P = (AB) \cap (A'B')$ et de la projection de (BB') sur (CC') depuis $Q = (BC) \cap (B'C')$ est une projection qui envoie A en C et A' en C' et a donc pour centre $R = (CA) \cap (C'A')$. Le point d'intersection $(AA') \cap (PQ)$ et son image par cette composée sont sur (PQ). Donc, R appartient à la droite (PQ).

Pour la réciproque, on considère une dualité. □

4.5.2. Axe d'une homographie et théorème de Pappus. —

Lemme. — *Soit L L' et l trois droites disctinctes d'un plan projectif. Soit A un point de $L-l\cap L$ et A' un point de $L'-l\cap L'$. L'application de L sur L' qui a tout point M de L associe le point M' de L' tel que (AM') et $(A'M)$ se coupent sur l est une homographie de L sur L'.*

Démonstration. — L'application est la composée de la projection de L sur l depuis A' et de la projection de l sur L' depuis A. □

Théorème. — *Soit $h : L \to L'$ une homographie entre deux droites projectives distinctes d'un plan projectif. Alors, il existe une droite l (appelée axe de l'homographie) telle que pour tout couple (M, N) de points de L les droites $(Mh(N))$ et $(Nh(M))$ se coupent sur la droite l. Si h est une projection, la droite l passe par $L\cap L'$. Si h n'est pas une projection, la droite l joint les points $h(L\cap L')$ et $h^{-1}(L\cap L')$.*

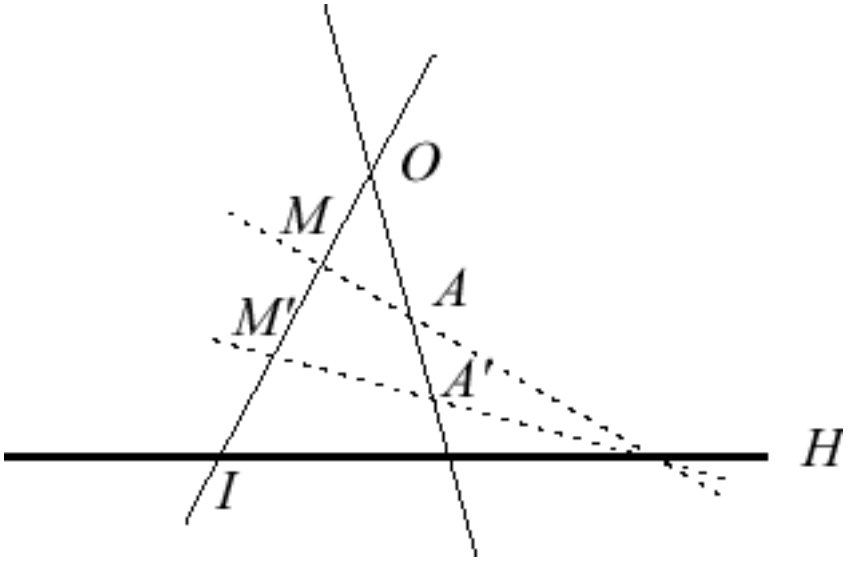
Démonstration. — Si h n'est pas une projection, les trois points $O = L\cap L'$, $P = h^{-1}(O)$ et $Q = h(O)$ sont deux à deux distincts. L'homographie construite comme au lemme précédent avec les points $A = M$ et $A' = h(M)$ et la droite (PQ) coïncide avec h en A, P et O. Elles sont donc égales. Pour tout point N de L les droites $(Mh(N)$, $(Nh(M)$ se coupent sur la droite (PQ).

Si h est une projection de centre Ω, soit $O = L\cap L'$ et soit A et B deux points distincts de $L - L\cap L'$. Soit l la droite joignant $L\cap L'$ et $(Ah(B))\cap(Bh(A))$. Soit deux points M et N de L. En étudiant la figure affine obtenue en envoyant (ΩO) à l'infini, on montre l'alignement de O, $(Ah(B))\cap(Bh(A))$ et $(Mh(N)\cap(Nh(M)$, comme dans le théorème de Pappus. □

Ce théorème permet de construire explicitement l'image d'un point M quelconque de L par une homographie h connaissant l'image de trois points deux à deux distincts de L.

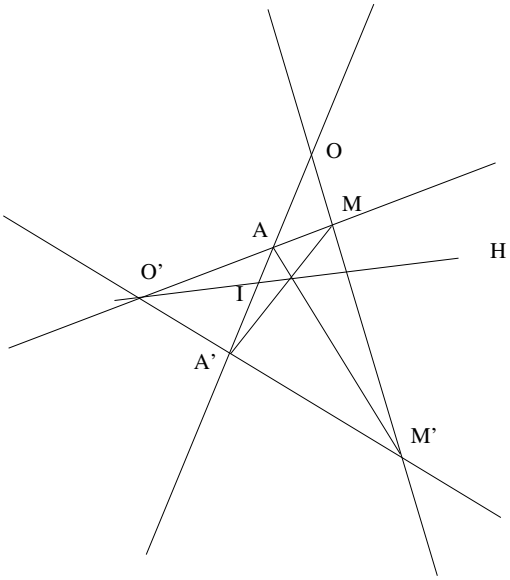
4.6. Générateur du groupe projectif $PGL(E)$

Définition. — *Une homologie d'un espace projectif $P(E)$ est une homographie qui admet un hyperplan H de points fixes et un autre point fixe O. Ce sont les projectivisations des dilatations.*



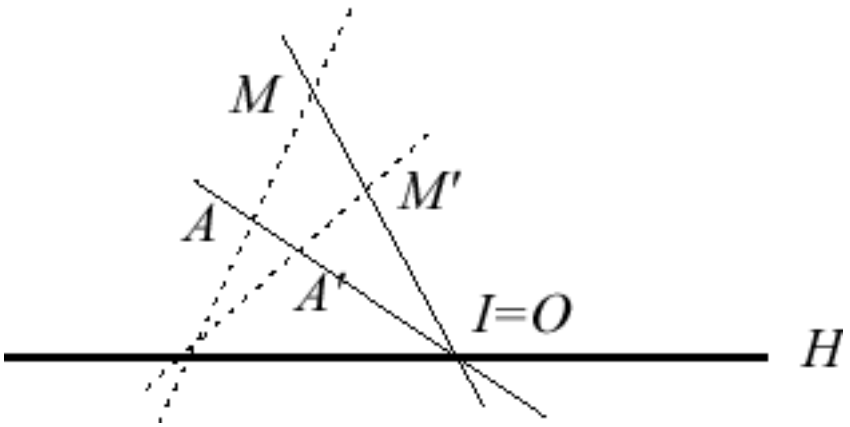
Si f est une dilatation et si $E = E_1 \oplus E_\lambda$ somme de l'hyperplan fixe $E_1 = vect(e_1, e_2, \cdots e_{n-1})$ et de la droite propre $E_\lambda = vect(e_n)$, toute droite d de E s'écrit $vect(x' + ae_n)$ avec $x' \in E_1$. La droite d, son image $vect(x' + \lambda ae_n)$ et la droite $vect(e_n)$ sont coplanaires. Tout point M de $P(E)$, son image M' par $P(f)$ et le point O (correspondant à la droite $vect(e_n)$) sont donc alignés. On en déduit donc la construction précédente de l'image d'un point quelconque M par $P(f)$ connaissant l'hyperplan de point fixe H, le point fixe O et l'image A' par $P(f)$ d'un point A.

Si $P(E)$ est un plan projectif, la droite d qui relie les points I de H et O est globalement fixe par la dilatation f et I et O sont des points fixes de la restriction $f_{|d}$ de f à d. Par conséquent, cette restriction est caractérisée par le birapport $[O, I, M, f_{|d}(M)]$. Par la construction, on vérifie que ce birapport ne dépend ni de M choisi sur d, ni de la droite d passant par O, puisque les droites (AM) $(A'M')$ et H sont concourantes en ω : c'est le birapport des droites (ωO), H, (ωA), $(\omega A')$. On l'appelle birapport de l'homologie f.



Le dessin représente une homologie de rapport -1, qui est donc une involution.

Définition. — *Une élation d'un espace projectif $P(E)$ est une homographie qui admet exactement un hyperplan H de points fixes. Ce sont les projectivisations de transvections.*



Comme conséquence des énoncés sur les générateurs du groupe $GL(E)$, on obtient

Théorème. — *Le groupe projectif $PGL(E)$ est engendré par les homologies et les élations.*

4.7. Le groupe circulaire

(Lire [**?**] V.7)

La droite projective complexe $P^1(\mathbb{C})$ est une complétion de $\mathbb{C}$ (donc de $\mathbb{R}^2$ par l'ajout d'un seul point. Elle est à distinguer de $P(\mathbb{R}^2)$.

Proposition. — *Pour que quatre points de $\mathbb{C}$ (dont les trois premiers sont deux à deux distincts) soient alignés ou cocycliques, il faut et il suffit que leur birapport soit réel ou ∞.*

Démonstration. — Si le quatrième point est l'un des précédents, le résultat est simple. Si les quatre points sont deux à deux distincts, le rapport $\dfrac{b-d}{a-d}\dfrac{a-c}{b-c}$ a pour argument une mesure de l'angle de vecteurs $(\overrightarrow{DB},\overrightarrow{DA}) - (\overrightarrow{CB},\overrightarrow{CA})$. Les points sont cocycliques ou alignés si et seulement si cette mesure est 0 ou π modulo 2π. □

Corollaire. — *Toute homographie de la droite projective complexe $P^1(\mathbb{C})$ transforme un cercle ou une droite en un cercle ou une droite.*

Définition. —
- *Le groupe de Moebius est le groupe des homographies de la droite projective complexe $P^1(\mathbb{C})$.*
- *Le groupe circulaire G est le sous-groupe des bijections de la droite projective complexe $P^1(\mathbb{C})$ engendré par les homographies et la symétrie $[X:Y] \mapsto [\overline{Y}:\overline{X}]$.*

Théorème. — *Le groupe G est le groupe des bijections de $P^1(\mathbb{C})$ qui préservent globalement l'ensemble des cercles-droites réels.*

Démonstration. — En notant que la symétrie $[X:Y] \mapsto [\overline{Y}:\overline{X}]$ transforme un cercle ou une droite en un cercle ou une droite, on montre que G est inclus dans le groupe des bijections de $P^1(\mathbb{C})$ qui préservent globalement l'ensemble des cercles-droites réels.

Réciproquement, soit φ une bijection de $P^1(\mathbb{C})$ qui préserve globalement l'ensemble des cercles-droites réels. Quitte à composer par une homographie, on peut supposer que $\varphi(\infty) = \infty$ et donc que φ transforme le droites en droites et les cercles en cercles. Par le théorème fondamental, φ est affine puisqu'elle conserve l'alignement. Puisque, φ préserve les cercles, on peut alors montrer qu'elle est sur $\mathbb{C}$ de la forme $z \mapsto az + b$ ou $z \mapsto a\overline{z} + b$, c'est à dire que c'est une similitude du plan euclidien. □

CHAPITRE 5

DÉCOMPOSITIONS DES MATRICES INVERSIBLES

5.1. Décomposition LU

Il n'est pas utile de préciser ici le corps de base.

Les opérations élémentaires sur les lignes se font par produit de matrices à gauche

$$\begin{pmatrix} 1 & & & & & & & 0 \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & 0 & \ddots & & & & \\ & & \vdots & & \ddots & & & \\ & & l_{ki} & \cdots & \cdots & 1 & & \\ & & \vdots & & & & \ddots & \\ 0 & & 0 & & & & & 1 \end{pmatrix} \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_i \\ \vdots \\ L_k \\ \vdots \\ L_n \end{pmatrix} = \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_i \\ \vdots \\ l_{ki}L_i + L_k \\ \vdots \\ L_n \end{pmatrix}$$

et sur les colonnes par produit à droite

$$\begin{pmatrix} C_1 & C_2 & \cdots & C_i & \cdots & C_k & \cdots & C_n \end{pmatrix} \begin{pmatrix} 1 & & & & & & & 0 \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & 0 & \ddots & & & & \\ & & \vdots & & \ddots & & & \\ & & l_{ki} & & & 1 & & \\ & & \vdots & & & & \ddots & \\ 0 & & 0 & & & & & 1 \end{pmatrix}$$
$$= \begin{pmatrix} C_1 & C_2 & \cdots & C_i + l_{ki}C_k & \cdots & C_k & \cdots & C_n \end{pmatrix}$$

On peut aussi noter l'action des matrices de permutation. Par la représentation linéaire du groupe $\mathfrak{S}_n$ sur l'espace vectoriel $\oplus_{i=1}^n ke_i$, la permutation σ est envoyée sur l'endomorphisme $\varphi(\sigma)$ tel que $\varphi(\sigma)(e_i) = e_{\sigma(i)}$. Par exemple, la matrice du cycle $(1, 2, 3)$ de $\mathfrak{S}_3$ est

$$M(\sigma) := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

La multiplication à gauche induit une action sur les lignes par σ^{-1}

$$M(\sigma) \begin{pmatrix} L_1 \\ L_2 \\ L_3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} L_1 \\ L_2 \\ L_3 \end{pmatrix} = \begin{pmatrix} L_3 \\ L_1 \\ L_2 \end{pmatrix} = \begin{pmatrix} L_{\sigma^{-1}(1)} \\ L_{\sigma^{-1}(2)} \\ L_{\sigma^{-1}(3)} \end{pmatrix}$$

La multiplication à droite induit une action sur les colonnes par σ

$$\begin{pmatrix} C_1 & C_2 & C_3 \end{pmatrix} M(\sigma) = \begin{pmatrix} C_1 & C_2 & C_3 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} C_2 & C_3 & C_1 \end{pmatrix} = \begin{pmatrix} C_{\sigma(1)} & C_{\sigma(2)} & C_{\sigma(3)} \end{pmatrix}$$

Soit A une matrice de taille $n \times n$. La factorisation LU, consiste, pour une matrice A, à déterminer une matrice triangulaire inférieure L à diagonale unité et une matrice triangulaire supérieure U telles que $A = LU$ avec

$$L = \begin{pmatrix} 1 & & & \\ l_{21} & 1 & & \\ \vdots & \vdots & \ddots & \\ l_{n1} & l_{n2} & \cdots & 1 \end{pmatrix} \text{ et } U = \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ & u_{22} & \cdots & u_{2n} \\ & & \ddots & u_{n-1,n} \\ & & & u_{nn} \end{pmatrix}$$

Théorème. — *– Si A admet une décomposition LU, alors celle-ci est unique.*

– *A admet une décomposition LU si, et seulement si, ses mineurs principaux sont non nuls (le mineur principal d'ordre i de A désigne le déterminant de la matrice obtenue à partir de A en extrayant les i premières lignes et colonnes).*

– *Si A est inversible, alors A peut s'écrire $A = LUP$, où P est une matrice de permutation.*

Démonstration. — – Sachant que l'inverse d'une matrice triangulaire inférieure est aussi une matrice triangulaire inférieure et que le produit de deux matrices triangulaires inférieures est encore une matrice triangulaire inférieure, si $A = LU = L'U'$, alors $(L')^{-1}L = U'U^{-1}$ est une matrice triangulaire inférieure à diagonale unité et aussi une matrice triangulaire supérieure. C'est donc l'identité.

– On définit $A^{(0)} := A$ et les itérations se font pour $i = 1, ..., n-1$ de la manière suivante, de façon à obtenir des i premières colonnes "triangulaires supérieures". L'algorithme repose sur l'égalité

$$\begin{pmatrix} 1 & & & & & & & 0 \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & 0 & \ddots & & & & \\ & & \vdots & & \ddots & & & \\ & & l_{ki} & \cdots & \cdots & 1 & & \\ & & \vdots & & & & \ddots & \\ 0 & & 0 & & & & & 1 \end{pmatrix} \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_i \\ \vdots \\ L_k \\ \vdots \\ L_n \end{pmatrix} = \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_i \\ \vdots \\ l_{ki}L_i + L_k \\ \vdots \\ L_n \end{pmatrix}.$$

Sur la i-ième colonne de $A^{(i-1)}$, on élimine les éléments sous la diagonale en ajoutant à la k-ième ligne de cette matrice, la i-ième ligne multipliée par

$$l_{k,i} := -\frac{a_{k,i}^{(n-1)}}{a_{i,i}^{(n-1)}}$$

pour $k = i+1, \ldots, n$. Noter que $a_{i,i}^{(n-1)}$ est le mineur principal de $A^{(i-1)}$ d'ordre i et donc aussi celui de A. Cette opération sur les lignes peut être faite en multipliant par la gauche

$A^{(n-1)}$ avec la matrice triangulaire inférieure

$$L_i = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & l_{i+1,i} & \ddots & \\ & & \vdots & & \ddots \\ 0 & & l_{n,i} & & 1 \end{pmatrix}.$$

soit $A^{(i)} := L_i A^{(i-1)}$. Après $n-1$ itérations, nous avons éliminé tous les éléments sous la diagonale, par conséquent, nous avons maintenant une matrice triangulaire supérieure $A^{(n-1)}$.

Nous obtenons la décomposition $L_{n-1} \dots L_1 A = A^{(n-1)}$. Notons U la matrice triangulaire supérieure $A^{(n-1)}$ et $L = L_1^{-1} \dots L_{n-1}^{-1}$ triangulaire inférieure. On obtient $A = LU$.

Puisque L est triangulaire inférieure et U triangulaire supérieure, la matrice carrée des i premières lignes et colonnes du produit LU se calcule comme le produit des matrices carrées des i premières lignes et colonnes de L et de U. Par conséquent, le mineur d'ordre i d'un tel produit est $u_1 u_2 \cdots u_i$. La condition est donc nécessaire.

– Au vu de l'algorithme, il est nécessaire que $a_{i,i}^{(i-1)} \neq 0$ à chaque itération. Si, au cours du calcul, ce cas de figure venait à se produire, il faut intervertir la i-ième ligne avec une autre d'indice plus grand pour pouvoir continuer (il est toujours possible de trouver un élément non nul sur la colonne qui pose problème car la matrice est inversible). Cette opération sur les colonnes peut être fait en multipliant $A^{(i-1)}$ à droite par une matrice de permutation. Au bout de $n-1$ itérations, on trouve $L_{n-1} \dots L_1 A P_1 \dots P_{n-1} = A^{(n-1)}$ triangulaire supérieure. C'est la raison pour laquelle la décomposition LU s'écrit généralement $A = LUP$.

□

5.1.1. Application à la résolution de système. — Pour la résolution de système linéaire de la forme $Ax = b$, le système devient

$$LUx = b \Leftrightarrow \begin{cases} Ly = b & (1), \\ Ux = y & (2). \end{cases}$$

On résout le système (1) pour trouver le vecteur y, puis le système (2) pour trouver le vecteur x. La résolution est facilitée par la forme triangulaire des matrices. Noter que $L_{n-1} \dots L_1 \,\mathrm{Id} = L^{-1}$, c'est à dire que L^{-1} s'obtient en appliquant les mêmes opérations sur les lignes à Id.

5.2. Décomposition de Bruhat (description par opérations élémentaires)

Théorème. — *Soit A une matrice dans $GL(n,k)$. Il existe une matrice triangulaire supérieure unipotente U, une matrice triangulaire supérieure V et une matrice de permutation T_σ telles que $A = UT_\sigma V$. La matrice T_σ est uniquement déterminée par la matrice A.*

Démonstration. — Soit A une matrice dans $GL(n,k)$. L'un des coefficients de sa première colonne est non nul. Soit i_1 maximal tel que $a_{i_1,1} \neq 0$. Pour tout i entre 1 et i_1 on effectue l'opération élémentaire

$$L_i \leftarrow L_i - \frac{a_{i,1}}{a_{i_1,1}} L_{i_1}$$

en multipliant à gauche par une matrice triangulaire supérieure unipotente. On effectue aussi les opérations élémentaires $C_1 \leftarrow C_1/a_{i_1,1}$ puis pour tout j entre 2 et n,

$$C_j \leftarrow C_j - a_{i_1 j} C_1$$

en multipliant à droite par des matrices triangulaires supérieures. À la fin de cette étape, on obtient une matrice

$$\begin{pmatrix} 0 & & & & & \\ 0 & & & & \star & \\ \vdots & & & & & \\ \vdots & & & & & \\ 1 & 0 & 0 & & & 0 \\ 0 & & & & & \\ \vdots & & & & \star & \\ 0 & & & & & \end{pmatrix}.$$

On recommence à partir de la deuxième colonne en remarquant que l'indice i_1 ne sera plus utilisé. Au bout de $n-1$ étapes, on obtient une matrice de permutation.

Pour montrer l'unicité, on utilise le lemme suivant □

Lemme. — *Si U et V sont deux matrices triangulaires supérieures inversibles et si T_s et T_σ sont deux matrices de permutations telles que $T_\sigma^{-1} U T_s = V$, alors $s = \sigma$.*

Démonstration. — Supposons $s \neq \sigma$. Soit i tel que $\sigma(i) > s(i)$. Le coefficient u_{ii} non nul de U est envoyé en position $(\sigma(i), i)$ en multipliant U à gauche par T_σ^{-1} puis en position $(\sigma(i), s(i))$ en multipliant à droite par T_s. Ceci contredit le fait que V est triangulaire supérieure. □

Exercice 5.2.1. — Décrire la décomposition de Bruhat d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $SL(2,k)$.

Si $c \neq 0$ (c'est le cas générique) on verifiera

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & ac^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & -c^{-1} \end{pmatrix}.$$

5.3. Drapeaux

5.3.1. Définition des drapeaux. — Soit E un espace vectoriel de dimension finie n sur un corps K. Un drapeau $d = (V_i)_{0 \leq i \leq l}$ est la donnée d'une famille croissante de sous-espaces vectoriels de E. Un drapeau $d = (V_i)_{0 \leq i \leq l}$ est complet si $l = n$ et si chaque V_i est de dimension i.

À chaque base $B = (e_\alpha)_{1\leq\alpha\leq n}$ de E on peut associer un drapeau complet $\delta(B)$, où chaque V_i est engendré par les i premiers vecteurs de base.

$$\begin{array}{rcl} \delta\ :\ \mathcal{B}ase & \to & \mathcal{D}rap \\ B = (e_\alpha)_{1\leq\alpha\leq n} & \mapsto & \delta(B) = (Vect(e_\alpha, \alpha \leq i))_{0\leq i\leq n} \end{array}$$

5.3.2. Sous-groupe conservant un drapeau. — Le groupe linéaire $GL(E)$ agit de façon fidèle et transitive sur l'ensemble $\mathcal{B}ase$ des bases de E par

$$g \cdot (e_\alpha)_{1\leq\alpha\leq n} = (g(e_\alpha))_{1\leq\alpha\leq n}.$$

Il agit aussi de façon transitive sur l'ensemble $\mathcal{D}rap$ des drapeaux complets de E par

$$g \cdot (V_i)_{0\leq i\leq n} = (g(V_i))_{0\leq i\leq n}$$

de façon compatible avec l'application δ

$$\forall B \in \mathcal{B}ase, \forall g \in GL(E), \delta(g \cdot B) = g \cdot \delta(B).$$

Le stabilisateur du drapeau complet standard d_0 est le sous-groupe $\mathcal{B}$ (de Borel) des matrices triangulaires supérieures inversibles. On obtient donc une bijection

$$\begin{array}{rcl} GL(n)/\mathcal{B} & \to & \mathcal{D}rap \\ A\mathcal{B} & \mapsto & Ad_0 = (A\varepsilon_\alpha)_{1\leq\alpha\leq n}. \end{array}$$

Après le choix d'une base $B_0 = (\varepsilon_\alpha)_{1\leq\alpha\leq n}$, le groupe linéaire $GL(E)$ des isomorphismes de E s'identifie au groupe linéaire $GL(n)$ des matrices inversibles $n \times n$. L'ensemble $\mathcal{B}ase$ des bases de E s'identifie alors à $GL(n)$ par l'action fidèle et transitive. En effet, l'application

$$\begin{array}{rcl} GL(n) & \to & \mathcal{B}ase \\ A & \mapsto & AB_0 = (A\varepsilon_\alpha)_{1\leq\alpha\leq n} \end{array}$$

est une bijection.

L'application δ s'identifie à un morphisme de groupes π :

$$\begin{array}{rcl} GL(n) & \to & \mathcal{B}ase \\ \pi\downarrow & & \downarrow\delta \\ GL(n)/\mathcal{B} & \to & \mathcal{D}rap \end{array}$$

On notera $\mathcal{U}$ le sous-groupe de $GL(n)$ des matrices triangulaires supérieures unipotentes (i.e. à diagonale identité). On notera $\mathcal{T}$ le sous-groupe de $GL(n)$ des matrices diagonales inversibles. On a

$$\mathcal{U} \subset \mathcal{B} \text{ et } \mathcal{T} \subset \mathcal{B} \text{ et } \mathcal{B} = \mathcal{T}\mathcal{U}.$$

Le sous-groupe $\mathcal{U}$ agit sur les bases sans changer les drapeaux associés. Le sous-groupe $\mathcal{T}$ agit sur les bases en multipliant chaque vecteur par une constante non nulle.

D'autre part, le groupe symétrique $\mathfrak{S}_n$ peut alors être réalisé comme sous-groupe du groupe linéaire $GL(n)$ par la représentation

$$\begin{array}{rcl} \mathfrak{S}_n & \to & GL(n) \\ s & \mapsto & A_s = (\delta_{j,s(i)})_{1\leq i,j\leq n} A_s e_i = e_{s(i)} \end{array}$$

qui est un morphisme injectif de groupes. Alors, il centralise le groupe $\mathcal{T}$

$$\forall s \in \mathfrak{S}_n, \quad \forall T \in \mathcal{T}, \quad A_s T A_s^{-1} = T.$$

On vérifie que le normalisateur $N_{GL(E)}(\mathcal{T})$

$$N_{GL(E)}(\mathcal{T}) := \{A \in GL(E), A\mathcal{T}A^{-1} \subset \mathcal{T}\}$$

de $\mathcal{T}$ dans $GL(E)$ est l'ensemble des matrices avec un unique coefficient non nul sur chaque ligne et chaque colonne (si n_{ij} est non nul, les autres coefficients de la ligne i et de la colonne j sont nuls.) On trouve

$$N_{GL(E)}(\mathcal{T})/\mathcal{T} \simeq \mathfrak{S}_n.$$

5.4. Décomposition de Bruhat (description abstraite)

Une base $B = (e_\alpha)_{1\leq\alpha\leq n}$ de E *définit le drapeau complet* V si $\delta(B) = V$. Une base $B = (e_\alpha)_{1\leq\alpha\leq n}$ de E est dite *adaptée* au drapeau complet $V = (V_i)_{0\leq i\leq n}$ si chaque V_i est engendré par i vecteurs de B. Ceci revient à dire qu'il existe une permutation s de $\mathfrak{S}_n$ telle que $s \cdot B = (e_{s(\alpha)})_{1\leq\alpha\leq n}$ définit le drapeau complet V.

Lemme. — *Soit V et W deux drapeaux. Il existe une base de E définissant V et adaptée à W. Autrement dit, il existe une base B de E et une permutation s de $\mathfrak{S}_n$ telles que $V = \delta(B)$ et $W = \delta(s \cdot B)$.*

Démonstration. — À $i \geq 1$ fixé, puisque $V_{i-1}+W_n = V_i+W_n$, il existe un plus petit $j =: s(i)$ tel que $V_i + W_j = V_{i-1} + W_j$. Maintenant

$$\begin{aligned} V_i &\subset V_i + W_j = V_{i-1} + W_j \\ V_i + W_{j+1} &\subset V_{i-1} + W_j + W_{j+1} = V_{i-1} + W_{j+1} \end{aligned}$$

et donc pour tout $k \geq s(j)$, $V_i + W_k = V_{i-1} + W_k$. Noter que pour $k < s(j)$, $\dim(V_i + W_k) = \dim(V_{i-1} + W_k) + 1$ car l'inclusion $V_{i-1} + W_k \subset V_i + W_k$ est stricte.

On cherche maintenant à $j = s(i)$ fixé le plus petit $l = \sigma(j)$ tel que $W_j + V_l = W_{j-1} + V_l$. Si $\sigma(j) \leq i - 1$, $W_j + V_{i-1} = W_{j-1} + V_{i-1}$

$$V_i + W_{j-1} = V_i + W_{j-1} + V_{i-1} = V_i + W_j + V_{i-1} = V_i + W_j = V_{i-1} + W_j = W_{j-1} + V_{i-1}$$

ce qui contredit la minimalité de j. Maintenant, l'inclusion $W_{j-1} + V_i \subset W_j + V_i$ et l'égalité

$$\dim(W_j + V_i) = \dim(W_j + V_{i-1}) = \dim(W_{j-1} + V_{i-1}) + 1 = \dim(W_{j-1} + V_i)$$

montre que $\sigma(j) = i$.

Par conséquent, $\sigma \circ s = Id$. Donc s est bijective.

La base cherchée vérifie pour tout i, $(e_1, \cdots, e_i)$ est une base de V_i et $e_i \in W_{s(i)}$. En particulier, $(e_{\sigma(1)}, \cdots, e_{\sigma(j)})$ est (une famille libre donc) une base de W_j. Elle est obtenue par récurrence. Le vecteur e_1 est choisi non nul dans V_1. Comme $V_1 \subset V_1+W_{s(1)} = V_0+W_{s(1)} = W_{s(1)}$, le vecteur e_1 appartient à $W_{s(1)}$. On suppose les e_k construits jusqu'au rang $i - 1$ et on note $j = s(i)$. Comme $V_i + W_j = V_{i-1} + W_j$, si x est un vecteur de V_i qui n'est pas dans V_{i-1} il s'écrit comme somme $y + z$ d'un vecteur y de V_{i-1} et z de W_j. Le vecteur $e_i := z$ est dans $V_i \cap W_j$ mais n'est pas dans V_i. Ainsi, $(e_1, \cdots e_{i-1}, e_i)$ est une base de V_i. □

Soit maintenant $A \in GL(n)$. Soit B_1 la base canonique de K^n et B_2 l'image de cette base par A. Autrement dit $A = Mat(a, B_1, B_1)$ et $\mathrm{Id} = Mat(a, B_1, B_2)$. On considère une base $B_2' = (e_k)$ définissant le même drapeau que la base B_2 et adaptée à la base B_1. On note $B_1' = (e_{s(j)})$ définissant le même drapeau que la base B_1. La matrice $U_2 = Mat(\mathrm{Id}, B_2, B_2')$ de passage de la base B_2' à la base B_2 est triangulaire supérieure unipotente (avec diagonale identité) pour une bonne normalisation de B_3. La matrice $U_1 = Mat(\mathrm{Id}, B_1', B_1)$ de passage de la base B_1 à la base B_1' (dont la j-ième colonne est formée des composantes du j-ième vecteur de B_1' par rapport à la base B_1) est triangulaire supérieure. La matrice $Mat(\mathrm{Id}, B_2', B_1')$ est la matrice $T_\sigma = (\delta_{i,\sigma(j)})$ de la permutation σ. On trouve

$$\begin{aligned} A &= Mat(a, B_1, B_1) = Mat(\mathrm{Id}, B_1', B_1) Mat(\mathrm{Id}, B_2', B_1') Mat(\mathrm{Id}, B_2, B_2') Mat(a, B_1, B_2) \\ &= U_1 T_\sigma U_2 \,\mathrm{Id} = U_1 T_\sigma U_2. \end{aligned}$$

On a ainsi démontré

Théorème. — *Toute matrice $A \in GL(n)$ s'écrit $A = UT_\sigma V$ avec U triangulaire supérieure unipotente, T_σ matrice de permutation et V triangulaire supérieure.*

Théorème **(Décomposition de Bruhat)**. —

$$GL(n) = \cup_{s \in \Sigma_n} \mathcal{U} T_s \mathcal{B}$$

et la réunion est disjointe.

Noter que avec s définie par $s(k) = n - k + 1$, la matrice $L := UT_s$ est triangulaire inférieure unipotente et on retrouve la décomposition LU.

CHAPITRE 6

FORMES BILINÉAIRES ET QUADRATIQUES

Dans tout ce chapitre, les espaces vectoriels considérés seront de dimension finie. Soit k un corps et σ un automorphisme de k. On notera souvent λ^σ au lieu de $\sigma(\lambda)$.

Comme exemple d'automorphismes de corps, on peut penser à l'identité, la conjugaison complexe, mais aussi par exemple sur $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, (a,b) \in \mathbb{Q}\}$, $\sigma(a + b\sqrt{2}) = (a + b\sqrt{2})^\sigma = a - b\sqrt{2}$, ou encore sur $\mathbb{F}_{p^\alpha}$, $(\lambda)^\sigma = \lambda^p$.

Noter que, puisqu'ils sont déterminés par l'image de 1, les seuls automorphismes de $\mathbb{Q}$ et $\mathbb{F}_p$ (p premier) sont les applications identités. Comme les éléments positifs de $\mathbb{R}$ sont les carrés, la relation d'ordre a une définition algébrique et tout automorphisme de $\mathbb{R}$ est croissant. Comme sa restriction à $\mathbb{Q}$ est l'identité, par la construction de $\mathbb{R}$ par coupures, on montre que le seul automorphisme de $\mathbb{R}$ est l'identité.

6.1. Définitions

Définition. — *Soit k un corps et σ un automorphisme de k. Soit E un k espace vectoriel. Une forme σ-sesquilinéaire est une application $f : E \times E \to k$ linéaire par rapport à la première variable (i.e. à y fixé, $x \mapsto f(x,y)$ est linéaire) et σ-linéaire par rapport à la seconde (i.e. à $f(x, \lambda y + y') = \lambda^\sigma f(x,y) + f(x,y')$).*

Écriture matricielle : On choisit une base $\mathcal{B} = (e_i)_{i=1,\cdots,n}$ de E. Soit $x = \sum_{i=1}^n x_i e_i$ et $y = \sum_{i=1}^n y_i e_i$ deux vecteurs de E représentés par des vecteurs colonnes X et Y. La valeur $f(x,y)$ se calcule par sesquilinéarité

$$f(x,y) = \sum_{i,j} x_i y_j^\sigma f(e_i, e_j) = \sum_{i,j} x_i a_{ij} y_j^\sigma = {}^t X A Y^\sigma$$

si $A = (a_{ij}) = (f(e_i, e_j))_{1 \le i,j \le n} =: Mat(f, \mathcal{B})$.

Dans une autre base $\mathcal{B}' = (e'_i)_{i=1,\cdots,n}$ de E, avec la matrice $P := Mat(\mathrm{Id}, \mathcal{B}', \mathcal{B})$ de passage de la base $\mathcal{B}$ à la base $\mathcal{B}'$ $X = PX'$, $Y = PY'$ on obtient

$$Mat(f, \mathcal{B}') = {}^t P Mat(f, \mathcal{B}) P^\sigma.$$

Définition. — *Deux formes sesquilinéaires f sur un espace E et f' sur un espace E' sont dites équivalentes s'il existe $u \in GL(E, E')$ telle que*

$$\forall (x,y) \in E^2, f(x,y) = f'(u(x), u(y)).$$

Autrement dit, deux formes sesquilinéaires f sur un espace E et f' sur un espace E' sont équivalentes si et seulement si il existe deux bases $\mathcal{B}$ de E et $\mathcal{B}'$ de E' telles que $Mat(f, \mathcal{B}) = Mat(f', \mathcal{B}')$.

En terme matriciel, dans le cas où $E = E'$, après le choix d'une base $\mathcal{B}$ de E, deux formes sont équivalentes s'il existe une matrice P inversible telle que

$$Mat(f, \mathcal{B}) = {}^t P Mat(f', \mathcal{B})) P^\sigma.$$

6.1.1. Discriminant, noyaux et forme non-dégénérée. — Le sous-groupe $\{\lambda\lambda^\sigma, \lambda \in k^\star\}$ de $k^\star$ est appelé sous-groupe des normes. Avec les notations précédentes, noter que $\det Mat(f, \mathcal{B})$ diffère de $\det Mat(f, \mathcal{B})$ par $\det {}^t P \det P^\sigma = \det P \det P^\sigma$ qui est un élément du sous-groupe des normes.

Définition. — *Le discriminant $\Delta(f)$ de la forme f est l'image de* $\det Mat(f, \mathcal{B})$ *dans le quotient* $\{0\} \cup k^\star/\{\lambda\lambda^\sigma, \lambda \in k^\star\}$.

Définition. — *Le noyau à gauche d'une forme sesquilinéaire $f : E \times E \to k$ est le sous-espace vectoriel de E*

$$Ker_g(f) := \{x \in E, \forall y \in E, f(x, y) = 0\}.$$

En écriture matricielle, $Ker_g(f) := \{x \in E, {}^tXA = 0\} = \{x \in E, {}^tAX = 0\}$ et $Ker_d(f) := \{y \in E, AY^\sigma = 0\} = \{y \in E, A^\sigma Y = 0\}$. Comme le rang des matrices se calcule par non-annulation de mineurs et commme σ est un isomorphisme de corps, $\mathrm{rang}({}^tA) = \mathrm{rang}(A) = \mathrm{rang}(A^\sigma)$. On obtient par le théorème du rang,

$$\dim Ker_g(f) = \dim Ker_d(f) = \dim E - \mathrm{rang}\, A.$$

Définition. — *Une forme sesquilinéaire $f : E \times E \to k$ est dite non-dégénérée si $Ker_g(f) = \{0\}$ ou bien de façon équivalente $\Delta(f) \neq 0$. On dit aussi alors que (E, f) est un espace non-singulier.*

Exercice 6.1.2. — Soit f une forme sesquilinéaire sur un espace vectoriel E. Définir une forme sesquilinéaire naturelle non-dégénérée sur l'espace vectoriel quotient $E/Ker(f)$.

6.2. Formes réflexives et orthogonalité

6.2.1. Définitions. —

Définition. — *Une forme sesquilinéaire $f : E \times E \to k$ est dite*
- *réflexive si l'annulation $f(x, y) = 0$ implique $f(y, x) = 0$.*
- *(ici $\sigma = \mathrm{Id}$ et $car(k) \neq 2$) symétrique si $\forall (x, y) \in E, f(x, y) = f(y, x)$.*
- *(ici $\sigma = \mathrm{Id}$) anti-symétrique si $\forall (x, y) \in E, f(x, y) = f(y, x)$.*
- *(ici $\sigma \neq \mathrm{Id}$) à symétrie hermitienne si $\forall (x, y) \in E$, $f(y, x) = f(x, y)^\sigma$.*

Si f est non nulle à symétrie hermitienne, σ est une involution. Toutes les trois propriétés de symétrie précédentes impliquent la réflexivité. Réciproquement,

Proposition. — *Soit $f : E \times E \to k$ une forme σ-sesquilinéaire, non-dégénérée et réflexive sur un espace vecoriel E de dimension au moins 2. Alors*
- *l'automorphisme σ est une involution (i.e. $\sigma^2 = \mathrm{Id}$.)*
- *si $\sigma = \mathrm{Id}$, f est symétrique ou anti-symétrique.*
- *si $\sigma \neq \mathrm{Id}$, il existe un scalaire $\alpha \in k^\star$ tel que αf soit hermitienne.*

Exemple 6.2.1. — La forme $f(x, y) = (x_1y_2 - x_2y_1) + (x_3y_4 - x_4y_3)$ est une forme bilinéaire anti-symétrique.

6.2.2. Orthogonalité. — Soit E un espace vectoriel muni d'une forme sesquilinéaire f réflexive. Deux vecteurs x et y de E sont dits *orthogonaux* (relativement à f) si $f(x,y) = 0$. Puisque f est supposée réflexive, la relation d'orthogonalité associée est symétrique. Deux sous-espaces V et W de E sont dits orthogonaux si leurs vecteurs le sont (i.e. $\forall x \in V, y \in W, f(x,y) = 0$). L'*orthogonal* $P^\perp$ d'une partie P de E est le sous-espace vectoriel de E des vecteurs orthogonaux à tous les vecteurs de P. Le *noyau* (on dit aussi radical) de f (ou de E si la donnée de f est naturelle dans le contexte) est $Ker(f) = Ker_g(f) = Ker_d(f) = E^\perp$.

Un vecteur de E est dit *isotrope* s'il est orthogonal à lui-même. L'ensemble $C(f)$ des vecteurs isotropes forme un cône (i.e. $\forall x \in C(f), \lambda \in k, \lambda x \in C(f)$) appelé cône isotrope de f. Un sous-espace W est dit *isotrope* si $Ker(f_{|W\times W}) = W \cap W^\perp \neq \{0\}$. Dire que W est isotrope revient à dire que $f_{|W\times W}$ est dégénérée. Un sous-espace W est dit *totalement isotrope* s'il est orthogonal à lui-même. Dire que W est totalement isotrope revient à dire que $f_{|W\times W}$ est nulle. L'indice d'une forme sesquilinéaire réflexive est

$$\nu(f) = \max\{\dim V, V \text{ sous-espace vectoriel totalement isotrope de } E\}.$$

Une forme sesquilinéaire $f : E \times E \to k$ est dite *alternée* si tout vecteur de E est isotrope.

Lemme. — *– Si $car(k) \neq 2$ et si f est anti-symétrique, alors f est alternée.*
– Si f est alternée non-nulle, alors $\sigma = \mathrm{Id}$ et f est anti-symétrique. En particulier, toute forme symétrique ou hermitienne non nulle admet un vecteur non isotrope.

Démonstration. — – Si $car(k) \neq 2$ et si f est anti-symétrique, $f(x,x) = -f(x,x)$ et $2f(x,x) = 0$ soit $f(x,x) = 0$.
– En développant $f(x+y, x+y) = 0$, on trouve $f(x,y) = -f(y,x)$. Soit x, y tels que $f(y,x) \neq 0$.

$$\begin{aligned} f(\lambda x, y) &= \lambda f(x,y) = -\lambda f(y,x) \\ &= -f(y, \lambda x) = -\lambda^\sigma f(y,x). \end{aligned}$$

□

Théorème. — *Soit (E,f) un espace muni d'une forme sesquilinéaire, réflexive non-dégénérée et V un sous-espace de E. Alors,*
– $\dim V + \dim V^\perp = \dim E$.
– $(V^\perp)^\perp = V$.
– $Ker(V, f_{|V}) = ker(V^\perp, f_{|V^\perp}) = V \cap V^\perp$.
– *Si $(V, f_{|V})$ est non-singulier alors $E = V \oplus^\perp V^\perp$.*
– *Si $V \oplus^\perp W = E$ alors $W = U^\perp$ et V et W sont non singuliers.*

Démonstration. — – On notera n la dimension de E et p celle de V. L'application naturelle

$$\begin{array}{rccc} f_V : & E & \to & V^\star \\ & y & \mapsto & f(\cdot, y) \end{array}$$

est semi-linéaire et se factorise par $E/V^\perp$ en une application injective $E/V^\perp \to V^\star$. Donc, $n \leq \dim V^\star + \dim V^\perp = p + \dim V^\perp$.

Considérons maintenant l'application

$$\begin{array}{rccc} f_E: & E & \to & E^\star \\ & y & \mapsto & f(\cdot, y) \end{array}.$$

Elle est semi-linéaire et bijective, puisque E est non-singulier. Soit $e_1 \cdots e_p$ une base de V complétée par $e_{p+1} \cdots e_n$ en une base de E. Soit $e_1^\star, \cdots, e_n^\star$ la base duale. L'image de $V^\perp$ est contenue dans l'espace des formes linéaires nulles sur V. Les formes linéaires $u = \sum_{i=1}^n u_i e_i^\star$ nulles sur V sont telles que pour $1 \leq i \leq p$, $u(e_i) = u_i = 0$; elles forment donc un espace de dimension $n - p$. Donc, $\dim V^\perp = \dim f(V^\perp) \leq n - p$.

- Il résulte des définitions que $V \subset (V^\perp)^\perp$ et il résulte de l'égalité précédente que cette inclusion est en fait une égalité.
- résulte des définitions et du point précédent.
- Dans ce cas $V \cap V^\perp = \{0\}$ et la somme $V + V^\perp$ est orthogonale directe.
- $W \subset V^\perp$ et $\dim W = \dim E - \dim V = \dim V^\perp$.

□

Corollaire. — *L'indice d'une forme sesquilinéaire, réflexive non-dégénérée est inférieure à (la partie entière de)* $\dim E/2$.

Démonstration. — Il suffit de remarquer que pour tout sous-espace totalement isotrope V, $V \subset V^\perp$ et $2 \dim V \leq \dim V + \dim V^\perp = \dim E$. □

6.3. Espace irréductible et décomposition

Cas de dimension 2 :

Lemme. — *Soit (E, f) un espace de dimension 2 muni d'une forme symétrique ou anti-symétrique non dégénérée. Soit x un vecteur isotrope non nul de E. Alors, il existe un vecteur isotrope y tel que $f(x, y) = 1$.*

Démonstration. — On choisit un vecteur z non colinéaire à x et on cherche y sous la forme $y = \alpha x + \beta z$. Notons que $f(x, z)$ est non nul car E n'est pas singulier. Dans le cas anti-symétrique, comme tout vecteur est isotrope, il suffit d'assurer que $f(x, y) = f(x, \beta z) = \beta f(x, z) = 1$. On dit dans ce cas que (x, y) est une paire symplectique. Dans le cas symétrique, il faut de plus choisir α tel que $f(y, y) = 0$ soit comme $\beta \neq 0$, $2\alpha f(x, z) + \beta f(z, z) = 0$. Ce choix est possible car le corps n'est pas de caractéristique 2 et $f(x, z)$ est non nul. On dit dans ce cas que (x, y) est une paire hyperbolique. □

Exercice. — *Montrer que toute forme symétrique sur un espace réel non-dégénérée d'indice 1 en dimension 3 est à un scalaire près, équivalente à la forme de Lorentz (dont la forme quadratique associée est) $x^2 + y^2 - z^2$.*

Définition. — *Un espace (E, f) est dit réductible s'il peut s'écrire $E = E_1 \oplus^\perp E_2$ où E_1 et E_2 sont deux sous-espaces stricts de E muni de la restriction de f. Sinon, il est dit irréductible.*

Comme on a toujours, si V est un supplémentaire de $E^\perp$, la décomposition $E = E^\perp \oplus^\perp V$, un espace irréductible est soit totalement isotrope (i.e. $f = 0$), soit non-singulier. Dans le cas irréductible isotrope, il est de dimension 1. Dans le cas irréductible symétrique ou hermitien (plus généralement si $\sigma \neq \mathrm{Id}$), E admet un vecteur non isotrope x. Noter alors que $vect(x)$ est non-singulier. Mais alors comme E est irréductible et $E = \mathrm{vect}(x) \oplus^\perp x^\perp$, on a $x^\perp = \{0\}$. Donc, E est de dimension 1. Dans le cas irréductible anti-symétrique, soit x un vecteur non nul de E et, puisque E est non-singulier, soit y tel que $f(x, y) = 1$. Alors, $vect(x, y)$ est non-singulier et puisque $vect(x, y) \oplus^\perp vect(x, y)^\perp = E$, $vect(x, y)^\perp = \{0\}$ et $E = vect(x, y)$.

Théorème. — – *Un espace avec une forme symétrique ou hermitienne est de la forme* $E = vect(x_1) \oplus^\perp vect(x_2) \oplus^\perp \cdots \oplus^\perp vect(x_n)$. *En d'autres termes,* E *admet une base orthogonale.*

– *Un espace avec une forme anti-symétrique est une somme orthogonale de plans symplectiques (non-singuliers) et de droites isotropes.*

Démonstration. — La démonstration se fait par récurrence en utilisant le fait que si $(V, f_{|V})$ est non-singulier alors $E = V \oplus^\perp V^\perp$. □

Corollaire **(Classification des formes alternées)**. — *Deux formes alternées sur des espaces de même dimension sont équivalentes si et seulement si elles ont même rang.*

6.4. Classification des formes bilinéaires symétriques

Deux formes bilineaires symétriques équivalentes ont même rang, même indice, même discriminant (dans $\{0\} \cup k^\star/(k^\star)^2$). Le théorème de décomposition précédent, permet de classifier les formes bilinéaires symétriques à équivalence près.

6.4.1. Sur les corps algébriquement clos. —

Théorème. — *Soit* $n \in \mathbb{N}$. *Sur les corps algébriquement clos, toutes les formes bilinéaires symétriques de même rang sur des espaces de dimension* n *sont équivalentes.*

Démonstration. — Si f n'est pas dégénérée, dans une décomposition

$$E = vect(x_1) \oplus^\perp vect(x_2) \oplus^\perp \cdots \oplus^\perp vect(x_n),$$

les vecteurs x_i ne sont pas isotropes. Puisque k est algébriquement clos, il existe des scalaires λ_i tels que $\lambda_i^2 = f(x_i, x_i)^{-1}$. Ainsi, la base $\lambda_i e_i$ est orthonormée et la matrice de f dans cette base est l'identité. Dans le cas général, le nombre de vecteurs isotropes dans une décomposition $E = vect(x_1) \oplus^\perp vect(x_2) \oplus^\perp \cdots \oplus^\perp vect(x_n)$ est $n - \operatorname{rang} f$. On peut alors trouver une base

dans laquelle la matrice de f est

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

□

Exercice. — *Montrer que l'indice d'une forme bilinéaire symétrique non-dégénérée sur un espace vectoriel de dimension n sur un corps algébriquement clos est la partie entière de $n/2$.*

6.4.2. Sur $\mathbb{R}$. —

Théorème. — *Soit f une forme bilinéaire symétrique sur un espace vectoriel réel. Il existe une base dans laquelle la forme quadratique associée est*

$$q(x) = \sum_{i=1}^{p} x_i^2 - \sum_{j=1}^{q} x_j^2.$$

On peut trouver une base dans laquelle la matrice de f est

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & -1 & & & \\ & & & & & \ddots & & \\ & & & & & & -1 & \\ & & & & & & & 0 \\ & & & & & & & & \ddots \\ & & & & & & & & & 0 \end{pmatrix}.$$

Sur $\mathbb{R}$, les formes bilinéaires symétriques sont caractérisées à équivalence près par leur signature (p, q).

Démonstration. — Le semi-groupe des normes est composé des nombres réels strictement positifs. On raisonne comme précédement à partir d'une décomposition orthogonale $E = vect(x_1) \oplus^{\perp} vect(x_2) \oplus^{\perp} \cdots \oplus^{\perp} vect(x_r) \oplus^{\perp} Ker(f)$. Le nombre p_x est le nombre de vecteurs x_i de norme $q(x_i) > 0$ et le nombre $q_x = r - p_x$, le nombre de vecteur x_j de norme $q(x_j) < 0$. Soit $E = vect(y_1) \oplus^{\perp} vect(y_2) \oplus^{\perp} \cdots \oplus^{\perp} vect(y_r) \oplus^{\perp} Ker(f)$ est une autre décomposition orthogonale pour f. Les deux sous-espaces engendrés par les vecteurs non-isotropes dans les décompositions forment un supplémentaire du noyau de f. Ils sont donc

isométrique au quotient $E/Ker(f)$ muni du produit $\overline{f}(x+Ker(f), y+Ker(f)) = f(x,y)$. On note u une isométrie qui envoie l'un sur l'autre. Donc avec $x'_i = u(x_i)$, on vérifie que $vect(x'_1)\oplus^{\perp} vect(x'_2)\oplus^{\perp}\cdots\oplus^{\perp} vect(x'_r) = vect(y_1)\oplus^{\perp} vect(y_2)\oplus^{\perp}\cdots\oplus^{\perp} vect(y_r)$. Soit $X_+ = Vect(x'_i, q(x'_i) > 0)$ et $Y_- = Vect(y_j, q(y_j) < 0)$. Par orthogonalité, la forme f est définie positive sur X_+ et définie négative sur Y_-. On a donc $X_+ \cap Y_- = \{0\}$ et $p_x + q_y = p_x + r - p_y \leq r$, soit $p_x \leq p_y$. De même, on obtiendrait $p_y \leq p_x$. □

Exercice. — *Montrer que l'indice d'une forme bilinéaire symétrique sur un espace vectoriel réel est* $\nu(f) = \inf(p+n-r, q+n-r)$ *où* (p,q) *est sa signature et* r *son rang.*

6.4.3. Sur les corps finis. — Soit $\mathbb{F}_q$ un corps fini de caractéristique différente de 2. Le noyau du morphisme de groupes $\mathbb{F}_q^\star \to \mathbb{F}_q^\star$, $\lambda \mapsto \lambda^2$ est $\{-1,1\}$ de cardinal 2 (car $-1 \neq 1$.) Il y a par conséquent $(q-1)/2$ éléments dans son image est donc $1+(q-1)/2 = (q+1)/2$ carrés dans $\mathbb{F}_q$. Par le théorème de Lagrange, les carrés de $\mathbb{F}_q^\star$ vérifient $x^{\frac{q-1}{2}} = 1$. Par ailleurs, comme $\mathbb{F}_q$ est un corps, il y a au plus $(q-1)/2$ solutions à cette équation polynômiale de degré $(q-1)/2$. Les carrés non nuls de $\mathbb{F}_q$ sont donc exactement les solutions de $x^{\frac{q-1}{2}} = 1$. Les non-carrés de $\mathbb{F}_q$ vérifient $x^{\frac{q-1}{2}} = -1$. En particulier, le rapport de deux non-carrés est un carré.

Lemme. — *L'équation* $ax^2 + by^2 = 1$ *avec* a, b *dans* $\mathbb{F}_q$ *admet des solutions dans* $\mathbb{F}_q$.

Démonstration. — On sait qu'il y a $(q+1)/2$ carrés dans $\mathbb{F}_q$. Puisque $(q+1)/2+(q+1)/2 > q$, l'une des $(q+1)/2$ quantités $(1-by^2)/a$ est donc un carré. □

Théorème. — *Soit* $\mathbb{F}_q$ *un corps de caractéristique différente de* 2. *Il y a deux classes d'équivalence de formes quadratiques non dégénérée sur* E, *distinguées par le fait que leur discriminant est ou pas un carré. Précisemment, pour toute forme quadratique non dégénérée, il existe une base de* E *dans laquelle la matrice de* f *est*

$$\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix} \quad \textit{ou} \quad \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & \lambda \end{pmatrix}$$

où λ *n'est pas un carrré dans* $\mathbb{F}_q$.

Démonstration. — La démonstration se fait par récurrence à partir d'une base orthogonale. Le lemme indique qu'on peut trouver un vecteur de norme 1. Dans le cas de la dimension 2, comme les non-carrés sont tous de la forme $\lambda\mu^2$, en normalisant le second vecteur, on peut assurer que sa norme est 1 ou λ. Dans le cas général, on utilise l'hypothèse de récurrence sur l'orthogonal du vecteur de norme 1 trouvé. □

6.5. Classification des formes hermitiennes

6.5.1. Sur $\mathbb{C}$. —

Théorème. — *Soit f une forme hermitienne relative à la conjugaison complexe sur un espace vectoriel complexe E. Il existe une base dans laquelle la forme hermitien est donnée par*

$$f(x,y) = \sum_{i=1}^{p} x_i \overline{y_i} - \sum_{j=1}^{q} x_j \overline{y_j}.$$

On peut trouver une base dans laquelle la matrice de f est

$$\begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \ddots & & & & & & \\ & & & 1 & & & & & \\ & & & & -1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & -1 & & \\ & & & & & & & 0 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 0 \end{pmatrix}.$$

Démonstration. — Comme le semi-groupe des normes est composé des nombres réels strictement positifs, la démonstration est la même que dans le cas des formes quadratiques sur $\mathbb{R}$. □

6.5.2. Sur les corps finis. —

Théorème. — *Soit k un corps fini de caractéristique différente de 2.*

- *Les seules involutions non égales à l'identité sur les corps finis sont les applications $\sigma(\lambda) = \lambda^q$ sur les corps $\mathbb{F}_{q^2}$.*
- *Relativement à ces involutions, les formes hermitiennes sont classifiées à équivalence près par leur rang.*

Démonstration. — Soit σ une involution d'un corps fini k. L'ensemble $k_0 := \{\lambda \in k, \lambda^\sigma = \lambda\}$ est un sous-corps de k. Soit $a \in k - k_0$ et $b = (a - a^\sigma)$. Alors $b^\sigma = -b$. L'élément $c = -bb^\sigma$ est invariant par σ. Par conséquent, b vérifie l'équation polynômiale de degré 2, $b^2 - c = 0$ avec $c \in k_0$. Le corps k est donc une extension $k = k_0[b]$ de degré 2. L'application σ est l'identité sur k_0 et transforme b en $-b$. Comme l'image de b par un automorphisme de k qui est l'identité sur k_0, doit satisfaire l'équation à coefficients dans k_0, $b^2 - c = 0$, σ est l'unique automorphisme de k autre que l'identité, qui est l'identité sur k_0. Si on note $k_0 = \mathbb{F}_q$ et $k = \mathbb{F}_{q^2}$, (on considère k_0 comme le sous-corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$) alors σ est le morphisme de Frobenius $\mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$, $\lambda \mapsto \lambda^q$. L'application $N : k^\star \to k_0^\star$, $\lambda \mapsto \lambda\lambda^\sigma = \lambda^{q+1}$ est un morphisme de groupes dont le noyau a au plus $q+1$ éléments (les solutions dans $\mathbb{F}_{q^2}$ de l'équation $X^{q+1} = 1$). Son image est donc de cardinal au moins $\frac{q^2-1}{q+1} = q - 1$. L'application N est donc surjective.

Soit maintenant f une forme hermitienne sur un espace vectoriel E sur $\mathbb{F}_{q^2}$. Soit (e_i) une base orthogonale. Comme les $f(e_i, e_i)$ sont des éléments de k_0, pour ceux qui sont non-nuls, on peut trouver des λ_i dans k tels que $f(1/\lambda_i e_i, 1/\lambda_i e_i) = 1$. □

6.6. Théorème de Witt

Définition. — *Une isométrie entre deux espaces (E, f) et (E', f') est un isomorphisme linéaire qui respecte les formes bilinéaires.*

Donnons d'abord une généralisation du lemme sur les paires symplectiques et hyperboliques.

Proposition. — *Soit (E, f) un espace muni d'une forme symétrique (resp. anti-symétrique) non-dégénérée. Pour tout sous-espace V de E, on choisit un supplémentaire W de $rad(V)$ dans V ($V = rad(V) \oplus^{\perp} W$) et une base $N_1 \cdots N_q$ de $rad(V)$. Alors, il existe des vecteurs $M_1, \cdots, M_q$ tels que chaque plan $vect(N_i, M_i)$ soit hyperbolique (resp. symplectique) et que ces plans ainsi que W soient deux à deux orthogonaux. En particulier, V est un sous-espace du sous-espace non-singulier*

$$\overline{V} := vect(N_1, M_1) \oplus^{\perp} \cdots \oplus^{\perp} vect(N_1, M_1) \oplus^{\perp} W.$$

De plus, toute isométrie de V dans un espace non-singulier E' peut-être prolongée en une isométrie de $\overline{V}$ dans E'.

Démonstration. — Il suffit de raisonner par récurrence sur q. Si $q = 0$, il n'y a rien à faire. Considérons le sous-espace $V' := vect(N_1, \cdots, N_{q-1}) \oplus^{\perp} W$. Noter que W est non-isotrope car W est orthogonal à $rad(V)$ et d'intersection vide avec $rad(V)$. Donc, $rad(V') = vect(N_1, \cdots, N_{q-1})$ Le vecteur N_q est dans $(V')^{\perp}$ mais pas dans $rad((V')^{\perp}) = rad(V') = vect(N_1, \cdots, N_{q-1})$. Il y a donc dans $(V')^{\perp}$ un vecteur A tel que $f(N_q, A) \neq 0$. Le plan $P_q := vect(N_q, A) \subset (V')^{\perp}$ est donc engendré par une paire hyperbolique (resp. symplectique) (N_q, M_q). L'espace V' est inclus dans l'espace non-singulier $P_q^{\perp}$ et son radical est de dimension $q - 1$. Par hypothèse de récurrence, il existe des vecteurs M_i ($i \leq q - 1$) dans $P_q^{\perp}$ tels que les plans $vect(N_i, P_i)$ et W soient deux à deux orthogonaux dans $P_q^{\perp}$. En ajoutant le plan P_q on obtient l'espace non-singulier $\overline{V}$ souhaité. Pour prolonger une isométrie σ de V à $\overline{V}$, on applique la première partie aussi à l'image de V dans E' et on impose les conditions $\sigma(M_i) = M_i'$. □

Théorème **(Théorème de Witt)**. — *Soit E et E' deux espaces non-singuliers isométriques. Toute isométrie d'un sous-espace V de E sur un sous-espace de E' peut-être prolongée en une isométrie de E sur E'.*

Démonstration. — Soit σ une isométrie de V sur un sous-espace V' de E'. Par le corollaire précédent, on peut supposer V non-singulier et donc $E = V \oplus^{\perp} V^{\perp}$. De même, l'image V' est non-singulière et $E' = V' \oplus^{\perp} V'^{\perp}$. Reste à montrer que $V^{\perp}$ et $V'^{\perp}$ sont isométriques. Ils sont non-singuliers et de même dimension. Dans le cas anti-symétrique, ceci suffit à dire qu'ils sont isométriques (puisque isométriques à une sommes directe orthogonale de plans symplectiques).

Dans le cas symétrique, on raisonne par récurrence sur la dimension de V. Supposons d'abord que V est une droite $vect(x)$. Notons ρ l'isométrie de E sur E' et $x' = \sigma(x) = \rho(y)$. Il reste à trouver une isométrie τ de E qui envoie x sur y, de sorte que l'isométrie de E $\rho \circ \tau$ envoie x sur x'. Notons que $f(x, x) = f(y, y) = f(x', x')$. Les vecteurs $x + y$ et $x - y$ sont orthogonaux et l'un des deux disons $x + \varepsilon y$ est non-isotrope puisque $2x$ est non-isotrope. L'hyperplan

$H = (x + \varepsilon y)^\perp$ contient $x - \varepsilon y$. Soit μ la réflexion d'hyperplan H. Alors,

$$2\mu(x) = \mu(x + \varepsilon y + x - \varepsilon y) = -x - \varepsilon y + x - \varepsilon y = -2\varepsilon y.$$

Quitte encore à composer avec l'isométrie de E qui change tout vecteur en son opposé, on obtient une isométrie de E qui envoie x sur y.

Supposons maintenant le résultat pour les sous-espaces de dimension strictement inférieure à n et soit V de dimension $n > 1$. On peut écrire par la décomposition en irréductibles, $V = V_1 \oplus^\perp V_2$. On applique d'abord l'hypothèse de récurrence au sous-espace V_1. On peut donc prolonger $\sigma_{|V_1}$ à E. Ainsi $V_1^\perp$ et $\sigma(V_1)^\perp$ sont isométriques. L'isométrie $\sigma_{|V_2}$ définie sur $V_2 \subset V_1^\perp$ se prolonge donc à tout $V_1^\perp$ en une application notée θ. L'isométrie $\sigma_{|V_1} \perp \theta$ est donc un prolongement de σ à tout E. □

Il y a maintenant une multitude de reformulations du théorème de Witt.

Corollaire. — *Soit (E, f) un espace non-singulier et V, V' deux sous-espaces. Pour qu'il existe une isométrie de E qui envoie V sur V', il faut et il suffit que $(V, f_{|V\times V})$ et $(V', f_{|V'\times V'})$ soient équivalentes. Autrement dit, le groupe orthogonal de E agit transitivement sur les sous-espaces équivalents de E.*

Corollaire. — *Tous les sous-espaces isotropes maximaux pour la relation d'inclusion ont la même dimension, $\nu(f)$ appelée* indice *de la forme f.*

$\nu(f) = \max\{\dim V, V \text{ sous-espace totalement isotrope de } E\}$.

Démonstration. — Soit V_1 et V_2 deux espaces totalement isotropes maximaux, avec $\dim V_1 \leq \dim V_2$. Toute injection de V_1 isotrope dans V_2 isotrope est une isométrie. Par le théorème de Witt, elle se prolonge en une isométrie σ de E. Maintenant, l'inclusion V_1 isotrope maximal dans $\sigma^{-1}(V_2)$ isotrope, montre l'égalité $V_1 = \sigma^{-1}(V_2)$ et donc l'égalité $\dim V_1 = \dim V_2$. □

En complétant un sous-espace isotrope maximal en un sous-espace non-singulier de dimension double, on montre que la dimension d'un sous-espace symplectique ou hyperbolique maximal est $2\nu(E) \leq \dim E$.

Exercice. — *Montrer que dans un espace E non-singulier, si V_1 et V_2 sont deux sous-espaces isométriques, $V_1^\perp$ et $V_2^\perp$ aussi.*

CHAPITRE 7

GROUPES ORTHOGONAUX EUCLIDIENS

On suppose dans tout ce chapitre que f est une forme bilinéaire symétrique définie positive sur un espace vectoriel de dimension finie sur $\mathbb{R}$. On notera q sa forme quadratique associée.

7.1. Structure des groupes orthogonaux euclidiens

Par des arguments plus simples que dans le cas général, puisqu'il n'y a pas de droites isotropes, on obtient le

Théorème. — – *Le centre de $O(q)$ est $\{\mathrm{Id}, -\mathrm{Id}\}$.*
– *Si $n \geq 3$ et pair, le centre de $SO(q)$ est $\{Id, -\mathrm{Id}\}$. Si $n \geq 3$ et impair, le centre de $SO(q)$ est $\{Id\}$.*

7.1.1. Réduction des endomorphismes orthogonaux. —

Théorème. — *Soit u un endomorphisme orthogonal de (E, q). Il existe une décomposition de E comme somme directe orthogonale*

$$E = E_1(u) \oplus^{\perp} E_{-1}(u) \oplus^{\perp} P_1 \oplus^{\perp} P_2 \oplus^{\perp} \cdots \oplus^{\perp} P_r$$

où les P_i sont des plans stables par u sur lesquels u se restreint en une rotation différente de Id *et* $-\mathrm{Id}$.

7.1.2. Prolongement des isométries. —

Théorème. — *Soit V un espace vectoriel, A une partie de V contenant le vecteur nul. Soit φ une application de A dans A qui conserve le vecteur nul et telle que*

$$\forall (P, Q) \in A^2, \|\varphi(P) - \varphi(Q)\| = \|P - Q\|.$$

Alors il existe un produit de réflexions orthogonales qui coïncide avec φ sur A.

L'énoncé le plus naturel est dan un cadre affine.

Théorème. — *Soit E un espace affine, A une partie de E. Soit φ une application de A dans A telle que*

$$\forall (P, Q) \in A^2, d(\varphi(P), \varphi(Q)) = d(P, Q).$$

Alors il existe un produit de réflexions orthogonales qui coïncide avec φ sur A.

Démonstration. — Si A est un ensemble fini, on raisonne par récurrence sur son cardinal. Si $\mathrm{card}\, A = 0$ il suffit de choisir l'identité. Si $\mathrm{card}\, A = 1$, $A = \{P\}$ il suffit de choisir la réflexion orthogonale par rapport à l'hyperplan médiateur de $[P, \varphi(P)]$ si $\varphi(P) \neq P$ et l'identité sinon. Supposons que le résultat est démontré pour n points quelconques et considérons une partie $A = \{a_1, \cdots, a_{n+1}$ avec $n+1$ points. Soit ψ un produit de reflexions orthogonales qui coïncide avec φ sur $\{a_1, \cdots, a_n$. Soit s la réflexion orthogonale par rapport à l'hyperplan H médiateur de $[\psi(a_{n+1}), \varphi(a_{n+1})]$. Le produit $s \circ \psi$ envoie a_{n+1} sur $\varphi(a_{n+1})$. Reste à montrer que les points $\psi(a_i)$ sont sur H, c'est à dire équidistants de $\psi(a_{n+1})$ et $\varphi(a_{n+1})]$. Mais

$$d(\psi(a_i), \psi(a_{n+1})) = d(a_i, a_{n+1}) = d(\varphi(a_i), \varphi(a_{n+1})) = d(\psi(a_i), \varphi(a_{n+1})).$$

Si maintenant A est infini, soit B une partie finie de A qui engendre le même sous-espace affine que A. Soit ψ un produit de réflexions qui coïncide avec φ sur B. Montrons que ψ

coïncide avec φ sur tout A. Soit P un point de A. Soit $Q \in B$. Soit H l'ensemble des points équidistants de $\psi(P)$ et $\varphi(P)$.

$$d(\psi(Q), \psi(P) = d(\varphi(Q), \varphi(P)) = d(\psi(Q), \varphi(P)).$$

Par conséquent, pour tous les $\psi(Q)$ sont sur le sous espace affine H, et $Aff(B) \subset \psi^{-1}(H)$. En particulier, $\psi(P)$ est équidistant de $\psi(P)$ et $\varphi(P)$. Donc, $\psi(P) = \varphi(P)$. □

Corollaire. — *Toute isométrie d'un espace euclidien est produit de réflexions, en particulier affine et bijective.*

7.2. Le groupe $SO(2)$ et les nombres complexes

Théorème. — *L'application*

$$U \to SO(2, \mathbb{R}), e^{it} \mapsto \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

est un isomorphisme de groupes du groupe des nombres complexes de module 1 *sur le groupe spécial orthogonal* $SO(2, \mathbb{R})$.

7.3. Le groupe $SO(3)$ et les quaternions

Théorème. — *Il existe une algèbre* H *de dimension* 4 *sur* $\mathbb{R}$ *munie d'une base* $1, \imath, \jmath, k$ *telle que* 1 *est l'élément neutre de la multiplication,*

$$\imath^2 = \jmath^2 = k^2 = -1, \jmath k = -k\jmath = i, k\imath k = -\jmath k = j, \imath\jmath = -\jmath\imath = k.$$

Le corps des nombres réels est isomorphe à la sous-algèbre engendrée par 1. On identifiera donc le quaternion $a1$ et le nombre réel a.

Démonstration. — Il suffit de vérifier que l'ensemble

$$\left\{ M \in M_2(\mathbb{C}) / \exists (a, b) \in \mathbb{C}^2, M = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \right\}$$

est une $\mathbb{R}$-sous-algèbre de $M_2(\mathbb{C})$ de base

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

satisfaisant les relations précédentes. □

Définition. — – *Le conjugué d'un quaternion* $q = a1 + b\imath + c\jmath + dk$ *est* $\overline{q} = a1 - b\imath - c\jmath - dk$.
– *Un quaternion est dit pur si* $\overline{q} = -q$, *c'est à dire s'il est de la forme* $b\imath + c\jmath + dk$.
– *La norme d'un quaternion* $q = a1 + b\imath + c\jmath + dk$ *est* $N(q) = a^2 + b^2 + c^2 + d^2 = q\overline{q}$.

Lemme 7.3.1. — *La forme polaire* f *associée à la norme vérifie*

$$q\overline{q'} + q'\overline{q} = 2f(q, q').$$

Lemme 7.3.2. — *L'application norme est un morphisme de* $(H^\star, \times) \to \mathbb{R}^{+\star}$. *Son noyau* G, *l'ensemble des quaternions de norme* 1, *est un groupe.*

Démonstration. —

$$N(qq') = qq\overline{qq'} = qq'\overline{q'}\overline{q} = qN(q')\overline{q} = q\overline{q}N(q') = N(q)N(q').$$

□

Théorème. — *On a un isomorphisme de groupes* $G/\{1,-1\} \to SO(3,\mathbb{R})$ *et donc un*

$$1 \to \{-1,1\} \to G \to SO(3,\mathbb{R}) \to 1.$$

Démonstration. — On considère l'action de G sur H par automorphismes intérieurs

$$\begin{array}{rcl} G \times H & \to & H \\ (g,q) & \mapsto & gqg^{-1} = gq\overline{g}. \end{array}$$

Soit $\Phi : G \to Bij(H)$ le morphisme associé. Puisque, $q \mapsto gq\overline{g}$ est linéaire, le morphisme Ψ est à valeurs dans $GL(4,\mathbb{R})$. Son noyau est $centre(H) \cap G = \{-1,1\}$. Comme $N(\Psi(g)(q)) = N(gq\overline{g}) = N(q)$, $\Psi(g)$ est une transformation orthogonale. Donc, Ψ est à valeurs dans $O(4,\mathbb{R})$. La restriction de $\Psi(g)$ à la droite $vect(1)$ est l'identité. L'orthogonal de cette droite, l'ensemble des quaternions purs, est donc aussi invariant par $\Psi(g)$. On obtient donc un morphisme $\psi : G \to O(3,\mathbb{R})$ dont le noyau est $\{-1,1\}$. Par un argument de continuité, puisque G est connexe et que $\det : O(3,\mathbb{R}) \to \{1,-1\}$ et $\psi : G \to O(3,\mathbb{R})$ sont polynômiales donc continues, ψ est en fait à valeurs dans $SO(3,\mathbb{R})$. Pour $p \in G$ pur, $\psi(p)$ fixe la droite $vect(p)$ et est une involution. C'est donc un renversement d'axe $vect(p)$. Comme les renversements engendrent $SO(3)$, $\psi : G \to SO(3,\mathbb{R})$ est surjective. □

7.4. Le groupe $SO(3)$ et le groupe de Moebius

L'application

$$\begin{array}{rcl} P^1(\mathbb{C}) & \to & S^2 \subset \mathbb{R}^3 \\ [Z_1 : Z_0] & \mapsto & \left(\dfrac{2 < Z_0, Z_1 >}{|Z|^2 + |Z_0|^2}, \dfrac{2Z_0 \wedge Z_1}{|Z|^2 + |Z_0|^2}, \dfrac{|Z|^2 - |Z_0|^2}{|Z|^2 + |Z_0|^2} \right) \\ [Z_1 = x + iy : Z_0 = x_0 + iy_0] & \mapsto & \left(\dfrac{2(xx_0 + yy_0)}{|Z|^2 + |Z_0|^2}, \dfrac{2(x_0 y - y_0 x)}{|Z|^2 + |Z_0|^2}, \dfrac{|Z|^2 - |Z_0|^2}{|Z|^2 + |Z_0|^2} \right) \end{array}$$

est une bijection de la droite projective complexe $P^1(\mathbb{C})$ sur la sphère euclidienne $S^2 \subset \mathbb{R}^3$.

Théorème. — *Par cette bijection, le sous-groupe* $PSU(2,\mathbb{C}) \subset PGL(2,\mathbb{C})$ *correspond au groupe des rotations de* S^2. *On a donc un isomorphisme* $PSU(2,\mathbb{C}) \to SO(3,\mathbb{R})$.

Démonstration. — Voir Beardon □

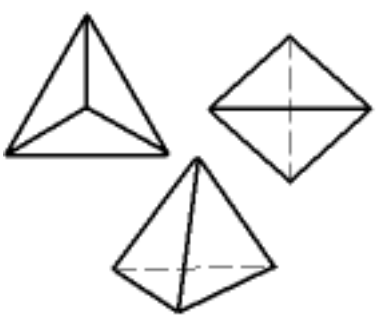
Les deux points de vue se rejoingnent en notant que le groupe G des quaternions de norme 1 est isomorphe au groupe spécial unitaire $SU(2,\mathbb{C})$. Par définition,

$$G = \left\{ M \in M_2(\mathbb{C}) / \exists (a,b) \in \mathbb{C}^2, M = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}, |a|^2 + |b|^2 = 1 \right\}$$

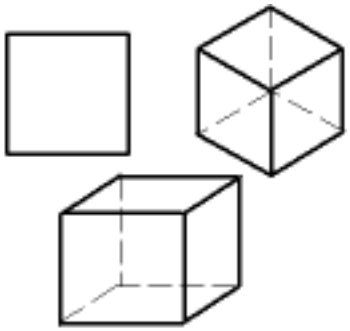
est l'ensemble $\left\{ M \in M_2(\mathbb{C}) / M\,{}^t\overline{M} = \mathrm{Id}, \det M = 1 \right\}$.

7.5. Sous-groupes finis de $SO(3)$

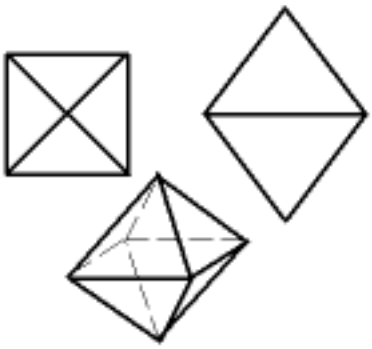
Définition. — *Un polyèdre régulier de l'espace euclidien $\mathbb{R}^3$ est un polyèdre convexe dont toutes les faces sont des polygones réguliers isométriques entre eux et tel que les figures formées par les arêtes aboutissant en un sommet sont toutes isométriques.*



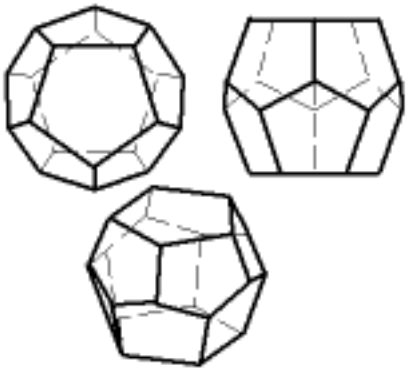
tétraèdre



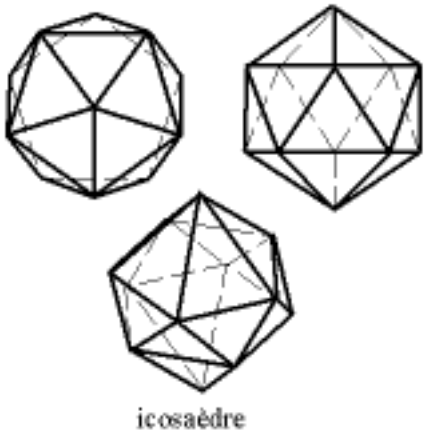
cube



octaèdre



dodécaèdre



icosaèdre

Théorème. — *Tout sous-groupe fini de $SO(3)$ et soit un groupe cyclique, soit un groupe dihédral, soit le groupe de symétrie d'un polyèdre régulier.*

Démonstration. — Soit G un groupe fini de $SO(3)$, composé donc de rotations. Chaque élément autre que l'identité fixe globalement la sphère unité S, et possède exactement deux points

fixes sur cette sphère. Soit X l'ensemble fini des points de S fixé par un des éléments de G différent de l'identité. Le groupe G agit sur X, car si x est fixé par $f \neq \mathrm{Id}$, $g(x)$ est fixé par $gfg^{-1} \neq \mathrm{Id}$. On note N le nombre d'orbite de cette action et n_j le cardinal du stabilisateur d'un quelconque des éléments de l'orbite $\mathcal{O}_j$. Par la première formule des classes, $\sum_j \operatorname{card} \mathcal{O}_j = \operatorname{card} X$ et par la seconde, $\operatorname{card} \mathcal{O}_j = \operatorname{card} G/n_j$. Donc,

$$\operatorname{card} X = \operatorname{card} G \sum_j 1/n_j.$$

Par le théorème de Burnside,

$$N \operatorname{card} G = \sum_{g \in G} \operatorname{card}(Fix(g)) = 2(\operatorname{card} G - 1) + \operatorname{card} X.$$

En éliminant $\operatorname{card} X$, on aboutit à

$$2 - \frac{2}{\operatorname{card} G} = \sum_j \left(1 - \frac{1}{n_j}\right).$$

Comme $1/2 \leq 1 - 1/n_j < 1$ et $\operatorname{card} G \geq 2$, on trouve que N vaut 2 ou 3.

Si $N = 2$, $2/\operatorname{card} G = 1/n_1 + 1/n_2$ et comme $n_j \leq \operatorname{card} G$, on trouve $n_1 = n_2 = \operatorname{card} G$. Il y a deux orbites, chacune contenant un point. Le groupe G est donc un groupe cyclique engendré par une rotation.

Si $N = 3$, les possibilités sont

- $(n_1, n_2, n_3) = (2, 2, n)$ et $\operatorname{card} G = 2n$. On montre que G est le groupe D_{2n}.
- $(n_1, n_2, n_3) = (2, 3, 3)$ et $\operatorname{card} G = 12$. On montre que G est le groupe des isométries directes du tétraèdre régulier (isomorphe à $\mathfrak{A}_4$ par l'action sur les quatre sommets)
- $(n_1, n_2, n_3) = (2, 3, 4)$ et $\operatorname{card} G = 24$. On montre que G est le groupe des isométries directes du cube (isomorphe à $\mathfrak{S}_4$ par l'action sur les quatre grandes diagonales).
- $(n_1, n_2, n_3) = (2, 3, 5)$ et $\operatorname{card} G = 60$. On montre que G est le groupe des isométries directes du dodécaèdre ou de l'icosaèdre isomorphe à $\mathfrak{A}_5$.

Lire [**?**] page 163. □

CHAPITRE 8

GROUPES ORTHOGONAUX

8.1. Groupes orthogonaux, unitaires, et symplectiques

Définition. — *Soit f une forme sesquilineaire réflexive sur un espace vectoriel E. Les isomorphismes (linéaires) de E qui vérifient*

$$\forall (x,y) \in E^2, \;\; f(u(x),u(y)) = f(x,y)$$

sont appelés les isométries de (E,q). Dans les cas symétrique et hermitien, pour un corps de caractérisitque différente de 2, il est équivalent de demander

$$\forall x \in E, \;\; q(u(x)) = q(x)$$

Les isométries forment un sous-groupe de $GL(E)$ noté

- *groupe orthogonal $O(f)$ ou $O(q)$ si f est symétrique.*
- *groupe symplectique $Sp(f)$ si f est anti-symétrique*
- *groupe unitaire $U(f)$ ou $U(q)$ si f est hermitienne.*

Lemme. — *Les groupes d'isométries de deux formes équivalentes sont conjugués.*

L'écriture matricielle montre que le déterminant d'une isométrie vérifie $(\det u)(\det u)^\sigma = 1$. Dans le cas symplectique, toutes les isométries sont de déterminant 1. Dans les cas symétrique ou hermitien, les isométries de déterminant 1 forment le groupe spécial orthogonal ou unitaire.

Proposition. — – *Une involution est une isométrie si et seulement si ses espaces propres sont orthogonaux (donc non-isotropes).*

– *Si F est un sous-espace non isotrope de E alors il existe une unique involution isométrique de E telle que $E_1(u) = F$. Elle sera appelée symétrie orthogonale par rapport à F.*

Les symétries orthogonales par rapport à des hyperplans sont appelées réflexions. Les symétries orthogonales par rapport à des espaces de codimension 2 sont appelées renversements. Noter que si u est une isométrie, us_Fu^{-1} est la symétrie orthogonale par à rapport à $u(F)$.

Démonstration. — – Soit u une involution de E d'espaces propres orthogonaux. Comme le polynôme X^2-1 annulateur de u est scindé avec racines simples, u est diagonalisable. Avec $E_+ := ker(u - \mathrm{Id})$ et $E_- := ker(u + \mathrm{Id})$ on a $E_\oplus E_- = E$. Si u est une isométrie, si $x_+ \in E_+$ et $x_- \in E_-$ alors

$$f(x_+,x_-) = f(u(x_+),u(x_-)) = f(x_+,-x_-) = -f(x_+,x_-)$$

et donc E_+ et E_- sont orthogonaux. Si E_+ et E_- sont orthogonaux, si $x = x_+ + x_-$ et $y = y_+ + y_-$,

$$f(u(x),u(y)) = f(x_+ - x_-, y_+ - y_-) = f(x_+,y_+) + f(x_-,y_-) = f(x,y)$$

et u est une isométrie.

– Si F est non-isotrope, $F \cap F^\perp = \{0\}$ et par suite $F \oplus^\perp F^\perp = E$. Il suffit alors de poser $u_{|F} = \mathrm{Id}_{|F}$ et $u_{|F^\perp} = -\mathrm{Id}_{|F^\perp}$.

□

8.2. Groupe symplectique

8.2.1. Générateurs. — ??????????????????????????

8.2.2. Simplicité. — ??????????????????????????

8.3. Théorème de Cartan-Dieudonné

Désormais dans ce chapitre, f sera une forme bilinéaire symétrique non-dégénérée sur un espace vectoriel E de dimension finie n sur un corps k de caractéristique différente de 2. On notera q la forma quadratique associée.

Les démonstrations se simplifient dans le cas euclidien puisque qu'alors il n'y a pas de vecteurs ou d'espaces isotropes non nuls. (voir TD, livre de Daniel Perrin).

8.3.1. Centre de $O(q)$ et $SO(q)$. —

Lemme. — *Si $n \geq 3$, toute droite est intersection de deux plans non isotropes.*

Démonstration. — Soit $d = vect(x)$ une droite de E. Si x est isotrope, si y est un vecteur de E tel que $f(x, y) \neq 0$ (f est non-dégénérée), le plan $P = vect(x, y)$ est non isotrope. Il en est donc de même pour $P^\perp$. Soit donc z (non-isotrope ?) dans $P^\perp$. Notons que z et donc $y + z$ n'appartiennent pas à $vect(x, y)$ puisque $P \cap P^\perp = \{0\}$. La droite d est l'intersection des deux plans hyperboliques non-isotrope $vect(x, y)$ et $vect(x, y + z)$.

Si x n'est pas isotrope, soit y et z deux vecteurs non-isotropes linéairement indépendants de $x^\perp$ (par exemple d'une base orthogonale de $x^\perp$ qui est non-isotrope de dimension au moins 2. La droite d est l'intersection des deux plans $vect(x, y)$ et $vect(x, z)$, non-isotropes. □

Proposition. — *Si $n \geq 3$, le centre de $O(q)$ est $\{Id, -\mathrm{Id}\}$. Si $n \geq 3$ et pair, le centre de $SO(q)$ est $\{Id, -\mathrm{Id}\}$. Si $n \geq 3$ et impair, le centre de $SO(q)$ est $\{Id\}$.*

Démonstration. — Soit u dans le centre de $O(q)$. Soit P un plan non-isotrope et $r_P \in SO(P)$ le renversement de plan P. Comme $ur_Pu^{-1} = r_P$, $u(P) = P$. Par le lemme précédent, u conserve donc toutes les droites et u est une homothétie. □

Théorème **(Théorème de Cartan-Dieudonné)**. — *Toute isométrie de (E, q) est composée d'au plus $dimE$ réflexions.*

Démonstration. — – Si $n = 1$, $O(q) = \{\mathrm{Id}, -\mathrm{Id}\}$.

– Si $n = 2$, soit $u \in O(q)$ et $x \in E$ non-isotrope.

Comme $q(u(x) - x) + q(u(x) + x) = 4q(x) \neq 0$, soit $u(x) - x$ soit $u(x) + x$ est non-isotrope. Si $u(x)+x$ est non-isotrope, on considère la réflexion r de droite $vect(u(x)+x)$. Comme $f(u(x)-x, u(x)+x) = q(u(x))-q(x) = 0$, $u(x)-x$ est dans $vect(u(x)+x)^\perp$. Par conséquent, $2ru(x) = r(u(x)+x+u(x)-x) = -(u(x)+x)+u(x)-x = -2x$. La droite $x^\perp$ est aussi conservée par ru. Si u est de déterminant -1, comme $\det ru = 1$, $ru = -\mathrm{Id}$, $u = -r$ est une réflexion. Si u est de déterminant 1, si t est une réflexion, $\det tu = -1$. Par le cas précédent, tu est une réflexion et u le produit ttu de deux réflexions.

– Si $n \geq 3$, soit $u \in O(q)$. On notera $v = u - \mathrm{Id}$.

– Si $kerv$ n'est pas totalement isotrope, il existe $x \in ker(v)$ non-isotrope. Comme $u(x) = x$, l'hyperplan $x^\perp$ est aussi stable par u. Par récurrence, on obtient que u est composé d'au plus $n-1$ réflexions (étendues par l'identité sur $vect(x)$). On supposera désormais que $kerv$ est totalement isotrope.

– S'il existe $x \in E$ non isotrope tel que $v(x) = u(x) - x$ ne soit pas isotrope. Soit r la réflexion de droite $vect(v(x))$. On calcule comme précédemment $ru(x) = x$. Par le cas précédent appliqué à ru, u est produit d'au plus n réflexions.
– On suppose maintenant que $v(x)$ est isotrope pour tout x non isotrope. Montrons qu'en fait Imv est totalement isotrope. Soit x isotrope. Comme dim $x^\perp = n - 1 \geq n/2$, il y a dans $x^\perp$ un vecteur y non isotrope. Ainsi, y, $x + y$ et $x - y$ sont non-isotropes. Par hypothèse, on obtient que leur image par v sont isotropes.

$$2q(v(x)) = q(v(x + y)) + q(v(x - y)) - 2q(v(y)) = 0.$$

Par conséquent, $v(x)$ est isotrope et par suite Imv est totallement isotrope. Par la formule du rang, et l'inégalité $Indice(q) \leq n/2$, on en déduit que $Kerv$ et Imv sont deux sous-espaces totallement isotropes maximaux et que f est hyperbolique.
On choisit une base e_i de $kerv$ et des éléments ε_i de E tels que les plans $vect(e_i, \varepsilon_i)$ soient hyperboliques. Notons que $u(e_i) = e_i$. En écrivant $u(\varepsilon_i) = \sum a_{ij}e_j + \sum b_{ij}\varepsilon_j$,

$$b_{ij} = f(u(\varepsilon_i), e_j) = f(u(\varepsilon_i), u(e_j)) = f(\varepsilon_j, e_i) = \delta_{ij}.$$

Par conséquent, la matrice de u dans la base (e_i, ε_j) a deux matrices identités sur sa diagonale : elle est donc de détermiant 1.
En particulier, le théorème est démontré pour les transformations de déterminant -1. Si u est de déterminant 1, et r une réflexion, ru est de déterminant -1, donc produit d'au plus n réflexions et même $n - 1$ réflexions (puisque n est pair).

□

8.4. L'algèbre de Clifford d'une forme quadratique

Ce paragraphe est inclus à titre culturel.

Théorème. — *Soit f une forme bilinéaire symétrique non dégénérée sur un espace vectoriel E de dimension n sur un corps k. Alors, il existe une algèbre $C(f)$ appelée algèbre de Clifford de f de dimension 2^n sur k et une application linéaire injective $\iota : E \to c(f)$ telle que toute application linéaire $\varphi : E \to L$ de E vers une k-algèbre L vérifiant pour tout $x \in E$, $\psi(x) \times_L \psi(x) = q(x) \times 1_L$ se prolonge de façon unique en un morphisme d'algèbres de $\psi_\star : C(f) \to L$ (i. e. $\psi = \psi_\star \circ \iota$.)*

Démonstration. — L'algèbre $C(f)$ est le quotient de l'algèbre tensorielle $T(E)$ par l'idéal bilatère engendré par les éléments de la forme $x \otimes y + y \otimes x - 2f(x, y)1$. □

On ommettra la notation ι. Dans l'algèbre de Clifford, la quantité $x \cdot y + y \cdot x$ vaut $f(x, y)1$ notée $f(x, y)$.

Théorème. — – *Pour toute transformation orthogonale $u \in SO(f)$, il existe un élément inversible s_u de $C(f)$ (unique à multiplication près par un scalaire non nul) tel que pour tout $x \in E$,*

$$u(x) = s_u \cdot x \cdot s_u^{-1}$$

le produit $\cdot$ étant calculé dans l'algèbre de Clifford $C(f)$.

– *Pour toute transformation orthogonale $u \in O(f)$ de déterminant -1, il existe un élément inversible s_u de $C(f)$ (unique à multiplication près par un scalaire non nul) tel que pour tout $x \in E$,*

$$u(x) = -s_u \cdot x \cdot s_u^{-1}.$$

Démonstration. — Si u est une réflexion par rapport à un hyperplan orthogonal à un vecteur non isotrope a, on a

$$u(x) = x - 2\frac{f(x,a)}{f(a,a)} \cdot a = x - (x \cdot a + a \cdot x) \cdot a^{-2} \cdot a = -a \cdot x \cdot a^{-1}.$$

Le cas général se fait en utilisant une décomposition de u comme produit de réflexions (théorème de Cartan-Dieudonné). □

CHAPITRE 9

GROUPE LINÉAIRE SUR $\mathbb{R}$ OU $\mathbb{C}$ (ASPECTS TOPOLOGIQUES)

9.1. Groupes topologiques

Définition. — *Un groupe topologique est un groupe G muni d'une topologie telle que les applications $G \times G \to G, (g, g') \mapsto gg'$ et $G \to G, g \mapsto g^{-1}$ soient continues.*

Soit E un espace vectoriel réel ou complexe muni d'une norme $\| \ \|$. L'espace vectoriel $End(E)$ des endomorphismes de E est muni de la norme associée

$$\| \ u \ \| := \sup_{x \in E, \|x\|=1} \|u(x)\| = \max_{x \in E, \|x\|=1} \|u(x)\|.$$

C'est une norme d'algèbre (i.e. pour tout $(u, v) \in End(E)^2$ $\| \ uv \ \| \leq \| \ u \ \| \| \ v \ \|$). Noter que cette norme est équivalente à toute autre norme en particulier celle donnée par le maximum des coefficients dans une base choisie.

Proposition. — *Pour la topologie induite sur $GL(E)$ par la topologie métrique de la norme $\| \ \|$, le groupe $GL(E)$ est un groupe topologique.*

Démonstration. — La multiplication est donnée coefficient par coefficient par des formules polynômiales. Elle est donc continue. C'est aussi le cas du passage à l'inverse si on utilise l'expression avec le quotient de la comatrice par le déterminant. □

Nous aurons en fait besoin du résultat plus précis suivant.

Lemme. — *Si $M \in End(E)$ un endomorphisme de norme d'opérateur $\| \ A \ \|$ strictement inférieure à 1. Alors $I - M$ est inversible. Par conséquent, $GL(E)$ est un ouvert de $End(E)$.*

Démonstration. — Comme $\| \ M^i \ \| \leq \| \ M \ \|^i$, la série $\sum M^i$ est normalement convergente donc convergente dans $End(E)$ complet. Sa limite est un inverse de $I - A$. Si $A \in GL(E)$, comme $A + M = A(I + A^{-1}M)$ et $\| \ A^{-1}M \ \| \leq \| \ A^{-1} \ \| \| \ M \ \|$, la boule ouverte de centre A et de rayon $\| \ A^{-1} \ \|^{-1}$ est un voisinage ouvert de A dans $GL(E)$. □

Corollaire. — *Les sous-ensembles $\{A \in GL(E), \| \ A \ \| \leq C, \| \ A^{-1} \ \| \leq C\}$ sont compacts et tout compact de $GL(E)$ est inclus dans un tel sous-ensemble.*

Démonstration. — Si K est un compact de $GL(E)$ la fonction continue $A \mapsto \| \ A \ \|$ atteint son maximum sur K, de même pour la fonction continue $A \mapsto \| \ A^{-1} \ \|$. Ceci montre la seconde assertion. L'ensemble $\{A \in GL(E), \| \ A \ \| \leq C, \| \ A^{-1} \ \| \leq C\} \subset \{A \in End(E) \ \| \ A \ \| \leq C\}$ est borné dans $M(n)$. Si A_n est une suite de matrices de $\{A \in GL(E), \| \ A \ \| \leq C, \| \ A^{-1} \ \| \leq C\}$ qui converge dans $End(E)$ vers A alors par continuité $\| \ A \ \| \leq C$. Comme $\| \ A_n^{-1} \ \| \leq C$, il existe une constante strictement positive c telle que pour tout n, $\det A_n^{-1} = (\det A_n)^{-1} \leq c$. Par conséquent, $\det A \geq 1/c$ et A appartient à $GL(E)$. Par continuité, $\| \ A_n^{-1} \ \| \leq C$. L'ensemble $\{A \in GL(E), \| \ A \ \| \leq C, \| \ A^{-1} \ \| \leq C\}$ est donc fermé dans $End(E)$. □

Corollaire. — *Le groupe orthogonal $O(E, \| \ \|)$ est compact.*

Démonstration. — On peut fixer une base orthonormée de E et identifier le groupe $O(E, \| \ \|)$ des endomorphismes orthogonaux au groupe $O(n)$ des matrices telles que ${}^tMM = \mathrm{Id}$. Comme image réciproque du singleton $\{\mathrm{Id}\}$ par l'application continue $M \mapsto {}^tMM$, le groupe $O(n)$ est fermé dans $M(n)$. Par ailleurs, il est dans le borné $\{A \in M(n), \| \ A \ \| \leq 1\}$. □

9.2. Décomposition polaire de $GL(n,\mathbb{R})$ et de $GL(n,\mathbb{C})$

Théorème. — *Toute matrice M de $GL(n,\mathbb{R})$ s'écrit de façon unique comme produit OS d'une matrice orthogonale O et d'une matrice S symétrique définie positive.*

L'application $O(n,\mathbb{R}) \times \mathbb{SDP} \to GL(n,\mathbb{R})$ est un homéomorphisme.

Démonstration. —
- Existence : Soit $M \in GL(n,\mathbb{R})$. La matrice ${}^tMM$ est symétrique définie positive. Il existe une matrice orthogonale o et une matrice diagonale D à diagonale strictement positive telles que ${}^tMM = oDo^{-1}$. La matrice $S := o\sqrt{D}o^{-1}$ est symétrique définie positive. La matrice $O := MS^{-1}$ qui vérifie ${}^tOO = S^{-1}{}^tMMS^{-1} = o\sqrt{D}^{-1}D\sqrt{D}^{-1}o^{-1} = \mathrm{Id}$ est donc orthogonale.
- Unicité : Montrons que si $M = OS$ alors M et S commutent. ${}^tMM = S^2$. Par interpolation de Lagrange, on peut donc écrire S comme polynôme en ${}^tMM$. Si $M = O'S'$, S' est aussi un polynôme en ${}^tMM$. Par conséquent, S et S sont deux matrices symétriques définies positives qui commutent. Elles sont diagonalisables dans une même base, avec des valeurs propres positives qui ont même carré. Elles sont donc égales.
- Continuité : L'application $O(n,\mathbb{R}) \times \mathbb{SDP} \to GL(n,\mathbb{R})$ est donc bijective et continue. Soit A_n une suite convergente dans $GL(n,\mathbb{R})$ vers une matrice A. On écrit $A_n = O_nS_n$. Comme le groupe orthogonal $O(n)$ est compact, la suite O_n admet une valeur d'adhérence, soit O_∞. La sous-suite correspondante $S_{n_j} := O_{n_j}^{-1}A_{n_j}$ converge vers une matrice symétrique positive S_∞ et on a par continuité $A = O_\infty S_\infty$. La matrice S_∞ est donc (symétrique positive) inversible et donc définie positive. Par unicité de la décomposition, la suite O_n admet une unique valeur d'adhérence ; elle est donc convergente ainsi que la suite S_n. La bijection réciproque est donc continue.

□

On montre de façon analogue le

Théorème. — *Toute matrice de $GL(n,\mathbb{C})$ s'écrit de façon unique comme produit UH d'une matrice unitaire U et d'une matrice H hermitienne définie positive.*

Comme corollaire on obtient

Corollaire **(Décomposition de Cartan)**. — *Toute matrice de $SL(n,\mathbb{R})$ s'écrit comme produit ODO', d'une matrice O spéciale orthogonale, d'une matrice diagonale D de déterminant 1 et d'une matrice O' spéciale orthogonale.*

Démonstration. — On écrit la décomposition polaire $A = O_1S$. Comme S est symétrique réelle, il existe O_2 spéciale orthogonale telle que $S = O_2DO_2^{-1}$. □

9.3. Décomposition de Gramm et d'Iwasawa

On rappelle que $\mathcal{B}$ désigne le sous-groupe de Borel des matrices triangulaires supérieures. À l'aide du procédé de Gramm-Schmidt, on montre

***Théorème* (Décomposition de Gramm).** — *Toute matrice de $GL(n,\mathbb{R})$ s'écrit de façon unique comme produit OU, d'une matrice O spéciale orthogonale et d'une matrice U triangulaire supérieure. L'application $O(n) \times \mathcal{B} \to GL(n,\mathbb{R})$ est un homéomorphisme.*

Démonstration. — Soit $A \in GL(n,\mathbb{R})$. La matrice $A = Mat(\mathrm{Id}, B, B_{can})$ est la matrice de passage de la base canonique vers la base $B = (A\varepsilon_i)$. Par orthonormalisation, il existe une base B' orthonormée adaptée à B. Alors $U := Mat(\mathrm{Id}, B, B')$ est triangulaire supérieure et $O := Mat(\mathrm{Id}, B', B_{can})$ est orthogonale. Ainsi, $A = OU$. □

Cette décomposition peut être affinée en

***Corollaire* (Décomposition d'Iwasawa).** — *Toute matrice de $SL(n,\mathbb{R})$ s'écrit de façon unique comme produit ODU, d'une matrice O spéciale orthogonale, d'une matrice diagonale D de déterminant 1 et d'une matrice unipotente U triangulaire supérieure de diagonale identité.*

On montre de façon analogue le

***Théorème*.** — *Toute matrice de $GL(n,\mathbb{C})$ s'écrit de façon unique comme produit UH d'une matrice unitaire U et d'une matrice U triangulaire supérieure ayant des éléments diagonaux réels positifs.*

9.4. Sous-groupes fermés et compacts du groupe linéaire

***Théorème*.** — *Tout sous groupe compact du groupe linéaire $GL(n,\mathbb{R})$ est conjugué à un sous-groupe du groupe orthogonal $O(n)$.*

Démonstration. — Par la classification des formes quadratiques sur $\mathbb{R}$, il suffit de trouver une forme quadratique définie positive q sur $\mathbb{R}^n$ telle que le groupe compact G soit un sous-groupe de $O(q)$. Matriciellement, on cherche une matrice symétrique définie positive s (matrice de q) telle que ${}^t gsg = s$ pour tout $g \in G$.

On considère l'action à droite du groupe G sur l'espace vectoriel S_n des matrices symétriques $n \times n$ et l'application associée $\Phi : G \to GL(S_n) \subset \Sigma(S_n), g \mapsto (s \mapsto {}^t gsg)$. Il suffit de trouver un point fixe s de cette action, qui soit dans l'ensemble SDP_n des matrices symétriques définies positive. Cet ensemble est un convexe stable par $\Phi(G)$. Si G est un groupe fini, il suffit de prendre pour s la moyenne des images par les $\Phi(g)$ d'un élément s_0 quelconque de SDP_n. On considère l'orbite de Id sous l'action précédente de G et son enveloppe convexe dans le convexe SDP_n. Puisque G est compact et Φ continue, puisque l'enveloppe convexe d'un compact est un compact (théorème de Caractéodory), ce sont des compacts de SDP_n, stables par $\Phi(G)$. En appliquant le lemme suivant à $E = S_n$, on peut conclure □

***Lemme*.** — *Soit G un sous-groupe compact de $GL(E)$, K un compact convexe non vide de E stable par G. Alors G a un point fixe dans K.*

Démonstration. — On fixe une norme euclidienne $\| \ \|_0$ sur E et on pose $\|x\| := \max\{\|g(x)\|_0, g \in G\}$, bien définie par compacité de G et continuité de la norme euclidienne $\| \ \|_0$. C'est une

norme invariante par G. Soit $x \neq y \in E$ et $g \in G$ tel que $\|x+y\| = \|g(x+y)\|_0$.

$$\|\frac{x+y}{2}\|^2 = \frac{1}{4}\|g(x+y)\|_0^2 = \frac{1}{2}(\|g(x)\|_0^2 + \|g(y)\|_0^2) - \frac{1}{4}\|\frac{x-y}{2}\|_0^2 < \frac{\|x\|+\|y\|^2}{2}.$$

Soit alors $x_m \in K$ qui réalise le minimum de $\|\ \|$ sur K. Un tel élément est unique par l'inégalité précédente. Par invariance de K sous le groupe G, on déduit que x_m est invariant par G. $\square$