Théorie des groupes et géométrie

Pierron Théo

ENS Ker Lann

Table des matières

Chapitre 0

Rappels

0.1 Actions et groupes symétriques

Définition 0.1 On définit $\#(\sigma)$ comme étant le nombre de transpositions dans une décomposition de σ.

$\varepsilon(\sigma) = (-1)^{\#(\sigma)}$ est la signature de σ, c'est l'unique morphisme de $\mathfrak{S}_n \to \{\pm 1\}$. Son noyau est le groupe alterné $\mathfrak{A}_n$.

Proposition 0.1 La donnée d'une action $(g, x) \mapsto gx$ de G sur X correspond à celle d'un morphisme $\varphi : G \to \mathfrak{S}(X)$.

Définition 0.2

- On note $G_x = \mathrm{Stab}_G(x) = \{g \in G, gx = x\}$ et l'orbite de x par $Gx = \{gx, g \in G\}$.
- Une action est transitive ssi il n'existe qu'une seule orbite.
- Une action est libre ssi tous les stabilisateurs sont réduits à $\{1\}$.
- $\mathrm{Ker}(\varphi) = \bigcap\limits_{x \in X} \mathrm{Stab}_G(x)$ et si $\mathrm{Ker}(\varphi) = \{1\}$, l'action est fidèle.

Définition 0.3 Le type d'une permutation est la liste des tailles des orbites triée dans l'ordre décroissant.

Exemple 0.1 G agit sur lui-même par translation à gauche. C'est une action libre. On en déduit que tout groupe G est sous-groupe de $\mathfrak{S}_{|G|}$ (théorème de Cayley).

Proposition 0.2 $|Gx| = (G : G_x)$.

0.2 Action par translation : groupes affines

Définition 0.4 Un espace affine E de direction un K-ev V est un ensemble non vide E avec une action de groupe de V sur E : $(E, V) \to E$ libre et transitive, ie

- pour tout $A, B \in E$ il existe $u \in V$ tel que $B = A + u$ (transitive)
- il y a de plus unicité de u (libre). On le note $\overrightarrow{AB}$.

<u>Théorème 0.1</u> Chasles $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

Démonstration.

$$A + (\overrightarrow{AB} + \overrightarrow{BC}) = (A + \overrightarrow{AB}) + \overrightarrow{BC}) = B + \overrightarrow{BC} = C$$

D'où le résultat. ■

Proposition 0.3 Soient E_1, E_2 de direction V_1 et V_2.

On dit que $f : E_1 \to E_2$ est affine ssi il existe $\varphi_f : V_1 \to V_2$ linéaire telle que

$$\forall (M, N) \in E_1, f(N) = f(M) + \varphi_f(\overrightarrow{MN})$$

ce qui revient à $\overrightarrow{f(M)f(N)} = \varphi_f(\overrightarrow{MN})$.

Remarque 0.1 La donnée d'une application affine est équivalente à celle d'un point de E_1, de son image dans E_2 et d'une application linéaire $V_1 \to V_2$.

Proposition 0.4 $\varphi_{g \circ f} = \varphi_g \circ \varphi_f$.

Démonstration.

$$\begin{aligned} g \circ f(N) - g \circ f(M) = g(f(N)) - g(f(M)) &= \varphi_g(f(N) - f(M)) \\ &= \varphi_g(\varphi_f(N - M)) \end{aligned}$$

■

<u>**Définition 0.5**</u> L'ensemble des applications affines bijectives de E dans E forment un groupe noté $GA(E)$.

On a un morphisme $\phi : GA(E) \to GL(V)$ qui à f associe φ_f. Son noyau est l'ensemble des translations.

0.3 Action par conjugaison

<u>**Définition 0.6**</u> Il s'agit de $(g, h) \to ghg^{-1}$. L'orbite de h est sa classe de conjugaison. SOn stabilisateur est le centralisateur $Z_G(h)$.

Proposition 0.5 $\omega(i_1, \dots, i_n)\omega^{-1} = (\omega(i_1), \dots, \omega(i_n))$.

Exemple 0.2 Soit $\sigma = (761)(3254)$ et $\rho = (3576)(142)$. On cherche ω tel que $\rho = \omega\sigma\omega^{-1}$.

Il suffit d'écrire $\omega(7) = 1$, $\omega(6) = 4$, ...

On trouve donc $\omega = (1752)(46)$. Il n'y a pas unicité ! (on doit avoir $\prod j = 1 l i_j!$ ω possibles où σ est de type $[i_1, \dots, i_l]$).

<u>Définition 0.7</u> On définit le centre de G par $Z(G) = \{h \in G, \forall g \in G, gh = hg\}$. G est commutatif ssi $Z(G) = G$.

Remarque 0.2 Il est clair que $\mathrm{Aut}(G) \subset \mathfrak{S}_{|G|-1}$.

<u>Définition 0.8</u> On note $\mathrm{Int}(G)$ l'ensemble des automorphismes internes ie les $\varphi_h : g \to hgh^{-1}$.

<u>Définition 0.9</u> On a une action de $\mathrm{Aut}(G)$ sur l'ensemble de sous-groupes de G donnée par $(\varphi, H) \mapsto \varphi(H)$.

<u>Définition 0.10</u> On a un morphisme

$$G \twoheadrightarrow \mathrm{Int}(G) \hookrightarrow \mathrm{Aut}(G) \to \mathfrak{S}(\{H < G\})$$

qui associe

$$g \mapsto (h \mapsto ghg^{-1}) \mapsto (h \mapsto ghg^{-1}) \mapsto (H \mapsto gHg^{-1})$$

On dit alors que $H \lhd G$ ssi H est un point fixe de l'action de $\mathrm{Int}(G)$ sur $\{H < G\}$.

On dit aussi que H est un sous-groupe caractétistique est un point fixe de l'action de $\mathrm{Aut}(G)$ sur $\{H < G\}$.

Comme on a une injection, caractéristique implique distingué.

Proposition 0.6 $\mathrm{Int}(G) \simeq G/Z(G)$.

Proposition 0.7 Soit $K < H < G$.

- Si K est caractéristique dans H et H est caractéristique dans G alors K est caractéristique dans G.
- Si K est caractéristique dans H et $H \lhd G$ alors $K \lhd G$.

Démonstration. On montre le deuxième point. On considère l'action de $\beta \in \mathrm{Int}(G)$ sur H. On a $\beta(H) = H$ donc $\beta|_H \in \mathrm{Aut}(H)$.

Comme K est caractéristique dans H, K est fixe par $\mathrm{Aut}(H)$ donc $\beta|_H$ fixe K donc β aussi. ■

<u>Définition 0.11</u> On appelle $D(G)$ le groupe engendré par les commutateurs $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$. C'est le groupe dérivé.

Proposition 0.8 $D(G)$ est caractéristique dans G.

Démonstration. Si $\alpha \in \mathrm{Aut}(G)$,

$$\alpha([g_{i_1}, g_{j_1}] \dots [g_{i_l}, g_{j_l}]) = [\alpha(g_{i_1}), \alpha(g_{j_1})] \dots [\alpha(g_{i_l}), \alpha(g_{j_l})]$$

On a donc $\alpha(D(G)) \subset D(G)$. Pour α^{-1}, on obtient $D(G) \subset \alpha^{-1}(D(G))$.

Comme l'inversion $\alpha \mapsto \alpha^{-1}$ est un antiautomorphisme, on a $D(G) \subset \alpha(D(G))$, d'où l'égalité.

$D(G)$ est donc un point fixe de l'action de $\mathrm{Aut}(G)$. ■

<u>Théorème 0.2</u> *Soit $H \subset G$.*
- *$G/D(G)$ est un groupe abélien*
- *$D(G) \subset H$ ssi $H \lhd G$ et G/H abélien.*

Exemple 0.3
- $\mathfrak{S}_3/\mathfrak{A}_3$ est abélien donc $D(\mathfrak{S}_3) \subset \mathfrak{A}_3$ donc $D(\mathfrak{S}_3) = \{1\}$ ou $\mathfrak{A}_3$.
- Pour D_4, $\langle r \rangle$ est d'indice 2 donc $D_4/\langle r \rangle$ est abélien. Alors $D(D_4) = \{e\}$, $\langle r \rangle$ ou $\langle r^2 \rangle$.
  Ça ne peut pas être $\{e\}$ sinon D_4 est abélien. De plus, $D_4/\langle r^2 \rangle$ est d'ordre 4 donc abélien (et $\langle r^2 \rangle$ est distingué car c'est le centre) donc c'est $\langle r^2 \rangle$.

0.4 Groupes simples

<u>Définition 0.12</u> G est simple ssi $\{e\}$ et G sont ses seuls sous-groupes distingués.

Proposition 0.9 $\mathfrak{A}_5$ est simple.

Démonstration. Les classes de conjugaison de $\mathfrak{S}_5$ sont
- $\{e\}$
- les 15 doubles transpositions
- les 20 3-cycles
- les 24 5-cycles
- les 30 4-cycles
- les 10 tranpositions
- les 20 produits de type $[3, 2]$.

Les quatres premiers formant $\mathfrak{A}_5$.

On a la chaîne $Z_{\mathfrak{S}_5}(\sigma) \hookrightarrow \mathfrak{S}_5 \twoheadrightarrow \{\pm 1\}$. Notons φ le morphisme associé.

Alors $Z_{\mathfrak{A}_5}(\sigma) = \operatorname{Ker}\varphi$ donc on a deux cas :

(i) S'il n'existe aucun $\omega \in \mathfrak{S}_5 \setminus \mathfrak{A}_5$ avec $\omega \in Z_{\mathfrak{S}_5}(\omega)$, alors $Z_{\mathfrak{S}_5}(\sigma) = Z_{\mathfrak{A}_5}(\sigma)$

(ii) Sinon, $Z_{\mathfrak{A}_5}$ est d'indice deux dans $Z_{\mathfrak{S}_5}$.

Les classes de conjugaisons de $\mathfrak{A}_5$ sont
- $\{1\}$
- les 3-cycles
- les doubles transpositions
- deux classes issues de la cassure de celle des 5-cycles de $\mathfrak{S}_5$.

La classe des 3-cycles ne se casse pas en deux puisque (45), on est dans le cas (ii) donc le cardinal de la classe vaut

$$(\mathfrak{S}_5 : Z_{\mathfrak{S}_5}(\sigma)) = \frac{|\mathfrak{S}_5|}{|Z_{\mathfrak{S}_5}(\sigma)|} = \frac{\frac{1}{2}|\mathfrak{A}_5}{\frac{1}{2}Z_{\mathfrak{A}_5}(\sigma)} = (\mathfrak{A}_5 : Z_{\mathfrak{A}_5}(\sigma))$$

Donc la classe dans $\mathfrak{S}_5$ et celle dans $\mathfrak{A}_5$ ont même nombre d'éléments.

Au contraire, l'autre classe se casse puisque $Z_{\mathfrak{S}_5}(12345)$ contient $\langle(12345)\rangle$ et est d'ordre 5 $(= \frac{120}{24})$. Ainsi, le calcul précédent donne :

$$(\mathfrak{S}_5 : Z_{\mathfrak{S}_5}(\sigma)) = \frac{|\mathfrak{S}_5|}{|Z_{\mathfrak{S}_5}(\sigma)|} = \frac{\frac{1}{2}|\mathfrak{A}_5}{Z_{\mathfrak{A}_5}(\sigma)} = \frac{(\mathfrak{A}_5 : Z_{\mathfrak{A}_5}(\sigma))}{2}$$

D'où la cassure.

On écrit donc l'équation aux classes de $\mathfrak{A}_5$:

$$60 = 1 + 12 + 12 + 15 + 20$$

Or un sous-groupe distingué est uen union de classes de conjugaison contenant $\{1\}$. Or aucune somme d'une sous famille de $(1, 12, 12, 15, 20)$ contenant 1 ne divise 60. On n'a donc pas de sous-groupe distingué. ■

0.5 Produit semi-direct

Définition 0.13 Soient N et K deux groupes et $\varphi : K \to \mathrm{Aut}(N)$. Sur $G = N \times K$, on définit la loi du produit semi-direct externe par

$$(n_1, k_1)(n_2, k_2) = (n_1\varphi(k_1)(n_2), k_1k_2)$$

Remarque 0.3 *En notant $K \simeq \{(1, k), k \in K\} =: K_1 < G$ et $N \simeq \{(n, 1), n \in N\} =: N_1 < G$, on a $N_1K_1 = G$ et $N_1 \cap K_1 = \{1\}$.*

Proposition 0.10

(i) Si $K \subset N_G(N)$ ou $N \subset N_G(K)$ alors $NK = KN$ est un sous-groupe.

(ii) Si $N \cap K = \{e\}$, $K \subset N_G(N)$ et $N \subset N_G(K)$ alors $NK \simeq N \times K$.

Exemple 0.4 $Q_8 = \langle I\rangle\langle J\rangle$.

Exemple 0.5 Si $|G| = 6$, il existe g_2 et g_3 d'ordre 2 et 3 par Cauchy. Notons $H = \langle g_3\rangle$ et $K = \langle g_2\rangle$.

On a $H \lhd G$, $HK = G$ et $H \cap K = \{e\}$ donc $G = H \rtimes K$.

Théorème 0.3 Correspondance des sous-groupes *Soit $\varphi : G \to \Gamma$ et $N = \mathrm{Ker}\,\varphi$.*

- *Si $K \subset G$, alors $\varphi^{-1}(\varphi(K)) = NK$.*
- *Il y a une correspondance bijective entre les sous-groupes de G contenant N et les sous-groupes de $\varphi(G)$.*
- *Si φ est surjective, elle envoie un sous-groupe distingué sur un sous-groupe distingué.*

Théorème 0.4 *Soient K et H deux sous-groupes de G, $K \subset N_G(H)$. Alors $KH = HK$ est un sous-groupe de G, $H \lhd HK$ et $(K \cap H) \lhd K$. De plus*

$$HK/H \simeq K/(H \cap K)$$

Démonstration. ■

Exemple 0.6

$$\mathfrak{S}_4/V \simeq \mathfrak{S}_3V/V \simeq \mathfrak{S}_3/\mathfrak{S}_3 \cap V \simeq \mathfrak{S}_3$$

Théorème 0.5 *Tout groupe simple à 60 éléments est isomorphe à $\mathfrak{A}_5$.*

Démonstration. Soit $H < G$ tel que $(G : H) = n > 1$. G agit par translation à gauche sur $\{gH, g \in G\}$. On a donc un morphisme $\varphi : G \to \mathfrak{S}_n$.

$\operatorname{Ker}(\varphi) \lhd G$ donc $\operatorname{Ker}(\varphi) = \{1\}$. φ est injectif donc $n \geqslant 5$ ($\mathfrak{S}_4$ est trop petit car $60 \nmid |\mathfrak{S}_4|$).

- Si $n = 5$, supposons $G \neq \mathfrak{A}_5$. On a alors $\mathfrak{S}_5 = G\mathfrak{A}_5$. G est distingué car d'indice deux et on a

$$\mathfrak{S}_5/G_simeqG\mathfrak{A}_5/G = \mathfrak{A}_5G/G \simeq \mathfrak{A}_5/\mathfrak{A}_5 \cap G$$

  Alors $\mathfrak{A}_5 \cap G$ est un sous-groupe d'indice 2 donc distingué. Contradiction. Donc $G = \mathfrak{A}_5$.
- On suppose que G ne possède pas de sous-groupe d'indice inférieur à 5. Le nombre n_5 de 5-Sylows de G vérifie

$$n_5 \mid 12 \text{ et } n_5 \equiv 1 \mod 5$$

  Donc $n_5 = 1$ ou 6. Or $n_5 \neq 1$ car si on n'a qu'un 5-Sylow, il est distingué. Donc $n_5 = 6$. On a de même $n_3 \mid 20$ et $n_3 \equiv 1 \mod 3$ donc $n_3 \in \{4, 10\}$. Or n_3 est l'indice du normalisateur des 3-Sylows dans G. Donc on ne peut pas avoir $n_3 = 4$ d'après notre hypothèse. Alors $n_3 = 10$.
  On a de même $n_2 = 15$.
  Chaque p-Sylow nous fournit n_p éléments d'ordre p. Comme l'intersection de deux p-Sylow est réduite à $\{1\}$, on obtient $(p-1)n_p$ éléments distincts.
  Pour $p = 5$, on a 24 éléments. $p = 3$ donne 20 éléments et $p = 2$ donne des problèmes. Supposons qu'on ait deux 2-Sylows S_2 et S_2' qui ont une intersection K d'ordre 2.
  On a $K \lhd S_2$ et $K \lhd S_2'$ donc $K \lhd \langle S_2, S_2'\rangle$ donc $\langle S_2, S_2'\rangle \neq G$. Notons $n = (\langle S_2, S_2'\rangle, S_2)$ et $m = (G : \langle S_2, S_2'\rangle)$.
  On a forcément $nm = 15$, $n \neq 1$ et $n \wedge 2 = 1$. Donc $n \geqslant 3$ et alors $m \leqslant 5$. Or on n'a pas de sous-groupes d'indice inférieur à 5. Contradiction. K

n'est donc pas d'ordre 2. Les intersections de 2-Sylow sont donc réduites à $\{\mathrm{Id}\}$, ce qui donne 45 éléments d'ordre 2.
On totalise alors $45+20+24>60$ éléments. Contradiction : il existe donc un sous-groupe H d'indice 5, ce qui assure le résultat par le point précédent. ■

Chapitre 1

Groupe résoluble

Définition 1.1 On définit par récurrence $G^{(0)} = G$ et $G^{(i)} = D(G^{(i-1)})$. On dit que G est résoluble ssi il existe n tel que $G^{(n)} = \{\mathrm{Id}\}$.

Proposition 1.1
- Les groupes abéliens sont résolubles.
- Un groupe simple non abélien n'est pas résoluble.
- $\mathfrak{A}_5 = D(\mathfrak{S}_5)$

Proposition 1.2 Si $\varphi : G \to \Gamma$ alors $\varphi(G^{(i)}) \subset \Gamma^{(i)}$.
Si φ est surjectif, alors il y a égalité.

Théorème 1.1 *Les assertions suivantes sont équivalentes :*

(i) *G est résoluble*

(ii) *il existe une suite $H_i \lhd G$*

$$G = H_0 \rhd \ldots \rhd H_n = \{e\}$$

avec H_i/H_{i+1} abélien.

(iii) *il existe une suite*

$$G = H_0 \rhd \ldots \rhd H_n = \{e\}$$

avec H_i/H_{i+1} abélien.

Démonstration. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) sont claires.

On montre (iii) $\Rightarrow$ (i) par récurrence en montrant que pour tout i, $G^{(i)} \subset H_i$.

$G \rhd H_1$ et G/H_1 est abélien donc $D(G) \subset H_1$. Si $G^{(i)} \subset H_i$, on a

$$G^{(i+1)} = D(G^{(i)}) \subset D(H_i) \subset H_{i+1}$$

car H_i/H_{i+1} est abélien. Par récurrence (finie), $G^{(n)} \subset H_n = \{e\}$ donc G est résoluble. ∎

Proposition 1.3 Soit $H < G$ et $N \lhd G$.

(i) Si G est résoluble alors H l'est

(ii) Si G est résoluble alors G/N l'est

(iii) G est résoluble ssi N et G/N le sont

(iv) Si H et N sont résolubles alors HN l'est

Démonstration.

(i) $H^{(n)} \subset G^{(n)} = \{e\}$ donc H est résoluble

(ii) On a $\{\overline{e}\} = \pi(G^{(n)}) = D^{(n)}(\pi(G)) = (G/N)^{(n)}$ car π est surjectif (surjection canonique).

(iii) Un sens est clair. Supposons N et G/N sont résolubles. Il existe n, m tel que $N^{(n)} = \{e\}$ et $D^m(G/N) = \{e\}$. On a $\pi(G^{(m)}) = (G/N)^{(m)} = \{e\}$. Alors $G^{(m)} \subset N$ donc

$$D^{n+m}(G) = D^n(G^{(m)}) \subset D^n(N) = \{e\}$$ ■

<u>THÉORÈME 1.2</u> BURNSIDE *Tout groupe d'ordre $p^a q^b$ est résoluble.*

<u>THÉORÈME 1.3</u> *Un p-groupe fini est résoluble.*

Démonstration. Par récurrence sur $|G| = p^n$. Si $n = 0$, c'est bon. Sinon, on sait que $Z(G) \neq \{1\}$.

On a deux cas : si $Z(G) = G$, c'est bon, G est abélien.

Sinon, $G/Z(G)$ est un p-groupe d'ordre $< |G|$ et $Z(G)$ est résoluble car abélien. Donc G est résoluble. ■

<u>THÉORÈME 1.4</u> *Si G est résoluble fini alors il existe une suite*

$$G = G_0 \rhd \ldots \rhd G_n = \{e\}$$

avec G_i/G_{i+1} cycliques d'ordre premier.

Démonstration. G est résoluble donc on a déjà une suite G_i avec G_i/G_{i+1} abélien.

On va montrer que si G_i/G_{i+1} n'est pas cyclique d'ordre premier, il existe N tel que $G_i \rhd N \rhd G_{i+1}$, G_i/N abélien et N/G_{i+1} cyclique d'ordre premier. Ceci concluera car on pourra réappliquer à $N \rhd G_{i+1}$, etc.

Supposons donc que G_i/G_{i+1} n'est pas cyclique d'ordre premier. Soit p un diviseur de $|G_i/G_{i+1}|$. Par le théorème de Cauchy, il existe un élément d'ordre p donc un sous-groupe U d'ordre p.

$U \lhd G_i/G_{i+1}$ car icelui est abélien. Le morphisme canonique $G_i \to G_i/G_{i+1}$ est surjective donc $G_{i+1} \lhd \underbrace{\pi^{-1}(U)}_{=N} \lhd G_i$.

On a $G_i/N_simeq(G_i/G_{i+1})/(N/G_{i+1}) = (G_i/G_{i+1})/U$ qui est donc le quotient d'un groupe abélien donc abélien. On a de plus $N/G_{i+1} = U$ cyclique. ■

Chapitre 2

Groupes linéaires

2.1 Générateurs

On prend K un corps, V un K-ev. H et W désigneront souvent un hyperplan.

<u>Définition 2.1</u> Une homologie linéaire est une $\varphi \in GL_n(K)$ qui a un hyperplan de points fixes. Si $\det \varphi = 1$ on parle de transvection, sinon on parle de dilatation.

Proposition 2.1 Soit φ une homologie linéaire et W son hyperplan de points fixes. On a équivalence entre

- $\det \varphi = 1$
- φ n'est pas diagonalisable
- $\mathrm{Im}(\varphi - \mathrm{Id}) \subset W$
- Pour toute forme linéaire de noyau $>$, il existe $w \in W$ tel que $\varphi(v) = v + f(v)w$ pour tout $v \in V$.
- Il existe une vase de V tel que $\varphi = \mathrm{Id} + E_{n-1,n}$.

Démonstration. • (i)⇔(ii)⇔ (iii) c'est de l'algèbre linéaire

(i)⇒(iv) On écrit $V = W \oplus \langle v$ avec $f(v) \neq 0$. On pose $v_1 = \frac{v}{f(v)}$ et $w = \varphi(v_1) - v_1$.
$\psi : V \to V$ est donnée par $\psi(v_1) = v_1 + f(v_1)w$ et $\psi(v') = v'$ pour $v' \in W$.
On a $\varphi = \psi$ sur W et v_1 donc sur V. ∎

Remarque 2.1 On note maintenant $t_{f,w}$ les transvections.

Lemme 2.0.1
Si $\varphi \in GL_n(K)$, on cosidère $t_{f,w}$. On sait que $f\varphi^{-1}$ est une forme linéaire et $\varphi(w) \in \mathrm{Ker}(f\varphi^{-1}) \setminus \{0\}$ et

$$\varphi \circ t_{f,w} \circ \varphi^{-1} = t_{f\varphi^{-1},\varphi(w)}$$

Proposition 2.2 Par pivot de Gauss, $GL_n(K)$ est engendré par les transvections et les dilatations et $SL_n(K)$ est engendré par les transvections.

Proposition 2.3 $Z(GL_n(k))$ est l'ensemble des matrices scalaires.
$Z(SL_n(K))$ est l'ensemble des matrices scalaires de $SL_n(K)$ ie λI_n avec $\lambda^n = 1$.

Démonstration. Si $\varphi \in Z(SL_n(K))$, φ commute avec les transvections donc $t_{f,w} = t_{f\varphi^{-1},\varphi(w)}$ ie $\varphi(w) = \lambda_w w$ pour tout f, w. En écrivant sur une base, on a λ_w qui ne dépend pas de w donc φ est une homothétie. ∎

2.2 Groupe dérivé

Proposition 2.4 Si $n \geqslant 2$, toutes les transvections sont conjuguées dans $GL_n(K)$

(i) Pour $n \geqslant 3$, elles sont aussi conjuguées dans $SL_n(K)$

(ii) Pour $n = 2$, une matrice de transvection est conjuguée dans $SL_2(K)$ à $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ avec $a \in K$.

Démonstration.

(i) Toutes les matrices de $SL_n(K)$ sont conjuguées à $I_n + E_{n-1,n}$ dans $GL_n(K)$ via φ. En prenant $D = \mathrm{diag}(\frac{1}{\det \varphi}, 1, \dots, 1)$, $D\varphi \in SL_n(K)$ et $D(I_n + E_{n-1,n})D^{-1} = I_n + E_{n-1,n}$ donc c'est bon.

(ii) Pour $n = 2$, la matrice $I_2 + E_{n-1,n} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et on peut s'y ramener en conjugant par $\varphi \in GL_n(K)$.
En prenant D comme avant, on trouve qu'on est conjugué à $\begin{pmatrix} 1 & \frac{1}{\det \varphi} \\ 0 & 1 \end{pmatrix}$ dans $SL_n(K)$. ∎

Proposition 2.5 Si $n \geqslant 3$, $D(GL_n) = D(SL_n) = SL_n$.

Démonstration. $\det([g,h]) = 1$ donc $D(GL_n) \subset SL_n$. On va montrer qu'il existe une transvection dans $D(SL_n(K))$. On aura alors tous ses conjugués (ie toutes les transvections) dans $D(SL_n)$. On aura donc $D(SL_n) = SL_n$.

Soient f_1, f_2 deux formes linéaires indépendantes et $w \neq 0$ dans $\operatorname{Ker} f_1 \cap \operatorname{Ker} f_2$. Il existe $\varphi \in SL_n(K)$ tel que

$$t_{f_1,w} = \varphi \circ t_{f_2,w} \circ \varphi^{-1}$$

Ainsi, $t_{f_1-f_2,w} = [\varphi, t_{f_2,w}]$. ∎

Proposition 2.6 Si $|K| > 3$, $D(SL_2(K)) = SL_2(K)$.

Démonstration. Il suffit de montrer que toutes les $I_2 + aE_{1,2} \in D(SL_2(K))$. On a

$$\begin{pmatrix} 1 & c(1-b^2) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & \frac{1}{b} \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}$$

Comme $|K| > 3$, $1 - b^2 \neq 0$ donc $c(1-b^2)$ est inversible pour un certain b. On a donc le résultat. ∎

2.3 Groupes linéaires finis

Définition 2.2 On note $GL_n(q)$ le groupe $GL_n(\mathbb{F}_q)$.

Proposition 2.7

$$|GL_n(q)| = \prod_{i=0}^{n-1} (q^n - q^i) = q^{\frac{n(n-1)}{2}}(q^n - 1)\dots(q-1)$$

Définition 2.3 On appelle groupe projectif linéaire et on note $PGL_n(K) = GL_n(K)/Z(GL_n(K))$.

On définit de même $PSL_n(K)$.

Remarque 2.2 $|SL_n(K)| = \frac{|GL_n(K)|}{q-1}$ *car c'est le noyau de* $\det$ *qui est surjectif donc* $\frac{|GL_n(K)|}{|SL_n(K)|} = |K^*| = q - 1$.

Proposition 2.8 $|PGL_n(K)| = \frac{|GL_n(K)|}{q-1}$ et

$$|PSL_n(K)| = \frac{|SL_n(K)|}{n \wedge q - 1} = \frac{|GL_n(K)|}{(q-1)(n \wedge (q-1))}$$

Exemple 2.1 $|GL_2(5)| = 2^5 \times 3 \times 5$ et $|SL_2(5)| = 2^3 \times 3 \times 5 = 120$.

2.4 Drapeaux

Définition 2.4 On appelle drapeau une suite de sous-espaces vectoriels

$$\{0\} = V_0 \subsetneq \ldots \subsetneq V_k = V$$

de dimensions d_i. Si $d_i = i$ pour tout i, on parle de drapeau complet. On note $\mathcal{F}$ l'ensemble des drapeaux complets.

Proposition 2.9 À toute base on peut associer à drapeau et inversement, on peut associer une base à tout drapeau.

On a une action de $GL_n(K)$ sur $\mathcal{F}$ donnée par

$$(g, (V_0, \ldots, V_k)) \mapsto (g(V_0), \ldots, g(V_k))$$

Cette action est transitive (clairement en passant aux bases) et le stabilisateur d'un drapeau est le groupe $\mathbb{B}$ (dit dgroupe de Borel standard) des matrices triangulaires supérieures de $GL_n(K)$.

Proposition 2.10 Tout groupe fini s'identifie à un sous-groupe d'un groupe $GL(n, K)$ pour n, K bien choisis.

Démonstration. On a une injection de $\mathfrak{S}_n$ dans $GL(n, K)$ qui à σ associe $\varphi(e_i) = e_{\sigma(i)}$. ■

L'image du morphisme précédent est notée W et appellée groupe de Weyl.

2.5 Bruhat

Théorème 2.1 Bruhat *Tout $A \in GL(n, K)$ s'écrit comme UPT avec $P \in W$ et $T \in \mathbb{B}$ et $U \in \mathbb{B}$ à diagonale de 1 avec P unique.*

Démonstration. On fait un pivot de Gauss et on obtient $A = UPV$ avec U, V triangulaires à diagonales de 1 et $P = P'D$ avec P' une matrice de permutation.

On a donc $A = UP'(DV)$ qui est sous la bonne forme.

Lemme 2.1.1
Si $T_1, T_2 \in \mathbb{B}$ et P_{σ_1}, P_{σ_2} dans W telles que $P_{\sigma_1}T_1 = T_2P_{\sigma_2}$.

Alors $\sigma_1 = \sigma_2$.

Démonstration. Si $\sigma_1 \neq \sigma_2$ il existe i tel que $\sigma_1(i) > \sigma_2(i)$. On a $T_1 = P_{\sigma_1^{-1}}T_2P_{\sigma_2}$.

Le coefficient (i, i) de T_2 est non nul car T_2 est inversible. Le coefficient de T_1 en position $(\sigma_1(i), \sigma_2(i))$ est non nul, ce qui contredit que T_1 est triangulaire. ■

■

Corollaire 2.1 Décomposition de Bruhat $GL(n,K) = \mathbb{B}W\mathbb{B}$.

Chapitre 3

Groupes linéaires projectifs

3.1 Espaces projectifs

<u>Définition 3.1</u> Soit K un corps et V un K-ev de dimension $n+1$. L'espace projectif est l'ensemble des droites vectorielles de K^{n+1} et on le note $\mathbb{P}_n(K)$.

Proposition 3.1 $\mathbb{P}_n(K) = K^{n+1} \setminus \{0\} / \sim$ où $v \sim w$ ssi il existe $\lambda \neq 0$ tel que $v = \lambda w$.

<u>Définition 3.2</u> On appelle coordonnées homogènes d'un point projectif les coordonnées d'un élément de la classe de ce point. On les note

$$(x_1 : \ldots : x_{n+1})$$

et on a $(x_1 : \ldots : x_{n+1}) = (\lambda x_1 : \ldots : \lambda x_{n+1})$.

<u>Définition 3.3</u> Un sous-espace projectif de $\mathbb{P}(V)$ est un $\pi(W \setminus \{0\})$ pour un sev W de V (π surjection canonique).

Remarque 3.1 *Soit* $(x_1 : \ldots : x_{n+1}) \in \mathbb{P}_n(K)$. *Si* $x_{n+1} \neq 0$, *on peut se ramener à* $x_{n+1} = 1$ *et dans ce cas, les* $x_1, \ldots, x_n$ *sont fixes et on se retrouve avec nos bonnes vieilles coordonnées* $(x_1, \ldots, x_n)$.

Si $x_{n+1} = 0$, *on retrouve* $\mathbb{P}_{n-1}(K)$. *On a donc*

$$\mathbb{P}_n(K) = \mathbb{P}_{n-1}(K) \cup K^n$$

Proposition 3.2 Soit $V = K^{n+1}$, $\mathbb{P}(W_1)$ et $\mathbb{P}(W_1)$ deux sous-espaces-projectifs de $\mathbb{P}(V)$. Si

$$\dim(\mathbb{P}(V)) \leqslant \dim(\mathbb{P}(W_1)) + \dim(\mathbb{P}(W_2))$$

alors $\mathbb{P}(W_1) \cap \mathbb{P}(W_2) \neq \{0\}$.

Démonstration. Notons $\dim(W_i) = m_i + 1$. L'hypothèse donne

$$n+2 \leqslant m_1+m_2+2 \leqslant \dim(W_1+W_2)+\dim(W_1\cap W_2) \leqslant n+1+\dim(W_1\cap W_2)$$

Donc $\dim(W_1 \cap W_2) > 0$. ∎

Proposition 3.3 Si $K = \mathbb{F}_q$, on a $|\mathbb{P}_n(K)| = \frac{q^{n+1}-1}{q-1}$.

Remarque 3.2 Le plus petit plan projectif est le plan de Fano $\mathbb{P}_2(\mathbb{F}_2)$.

Remarque 3.3 On a une action naturelle de $GL(n+1, K)$ sur $\mathbb{P}_n(K)$ qui induit une action de $PGL(n+1, K)$ et de $PSL(n+1, K)$ sur $\mathbb{P}_n(K)$ (en factorisant le morphisme canonique $GL(n+1, K) \to \mathfrak{S}(\mathbb{P}_n(K))$).

3.2 Actions k-transitives

Définition 3.4 On note $Y_{\neq}$ l'ensemble des éléments de $Y = X^k$ dont toutes les composantes sont distinctes.

Si G agit sur X, il agit aussi sur $Y_{\neq}$. L'action de G sur X est dite k-transitive ssi l'action de G sur $Y_{\neq}$ est transitive.

Proposition 3.4 Si V est de dimension supérieure à 2, l'action de SL et PSL sur $\mathbb{P}(V)$ est 2-transitive.

Démonstration. Si $[v_1] \neq [v_2] \in \mathbb{P}(V)$ et $[w_1] \neq [w_2] \in \mathbb{P}_2$, on complète (v_1, v_2) et (w_1, w_2) en bases de V et la matrice de changement de base g est bien inversible.

Si $\det(g) = \lambda$, on pose $w_1' = \frac{1}{\lambda} w_1$. On a toujours $[w_1] = [w_1']$ et en prenant g' qui passe de $(v_1, v_2, \ldots)$ à $(w_1', w_2, \ldots)$, $g' \in SL(n, K)$. ∎

Proposition 3.5 Si G opère 2-transitivement sur X alors pour tout $x \in X$, G_x est un sous-groupe maximal.

Démonstration. Supposons qu'il existe K tel que $G_x \subsetneq K \subsetneq G$ avec $g \in G\backslash K$ et $k \in K \setminus G_x$.

Comme k et g n'appartiennent pas à G_x, $gx \neq x \neq kx$. Il existe donc h qui envoie (x, gx) sur (x, kx).

On a $hx = x$ et $hgx = kx$ donc $k^{-1}hg \in G_x \subset K$. Or $k, h \in K$ donc $g \in K$. Contradiction. ∎

Définition 3.5 Soit X un G-ensemble, $B \subset X$ est un bloc ssi pour tout $g \in G$, $g(B) = B$ ou $g(B) \cap B = \varnothing$.

Les blocs triviaux sont $\varnothing$, X et les singletons.

L'action de G sur X est dite primitive si les seuls blocs sont les blocs triviaux.

Proposition 3.6 Si G agit 2-transitivement sur X alors l'action est primitive.

Démonstration. Supposons qu'il existe un bloc B non trivial. Il existe $x \neq y \in B$ et $z \in X \setminus B$ tel que $gx = x$ et $gy = z$ avec $g \in G$.

On a $x \in g(B) \cap B$ qui est donc non vide et $z \in g(B) \cap B^c$. ∎

Lemme 3.0.2
Soit $H \lhd G$ et X un G-ensemble. Toute orbite sous H est un bloc non vide.

Démonstration. Soit Hx une orbite. On a $g(Hx) = Hgx$ donc les orbites sous H partitionnent X. ∎

Proposition 3.7 Soit $\varphi : G \to \mathfrak{S}(X)$ avec $H \lhd G$ et $H \not\subset \operatorname{Ker} \varphi$.

L'action de H sur X est transitive et pour tout $x \in X$, $G = HG_x$.

Démonstration. Soit $x \in X$. $Hx \neq \varnothing$ est un bloc pour G. Comme l'action est primitive on a $Hx = \{x\}$ ou $Hx = X$.

Si $Hx = \{x\}$, $H \subset G_x$ et si c'est le cas pour tout x, on a $H \subset \bigcap\limits_{x \in X} G_x = \operatorname{Ker} \varphi$. Contradiction.

Il existe donc x tel que $Hx = X$. Soit $g \in G$. Il existe $h \in H$ tel que $hx = gx$. On a donc $h^{-1}g \in G_x$ et ainsi tout $g \in G$ se décompose en hg_x avec $h \in H$ et $g_x \in G_x$. D'où $G = HG_x$. ∎

<u>Théorème 3.1</u> Iwasawa *Soit G agissant pimitivement et fidèlement sur X et tel que $D(G) = G$.*

Soit $x \in X$. Si $K \lhd G_x$ avec K résoluble et $\langle gKg^{-1}, g \in G\rangle = G$ alors G est simple.

Démonstration. Soit $H \lhd G$ non vide. On veut montrer que $H = G$.

- Montrons que $HK \lhd G$. On sait que $G = HG_x$.

$$
\begin{aligned}
hg_xHK(hg_x)^{-1} &= \underbrace{hg_xH(hg_x)^{-1}}_{=H} hg_xK(hg_x)^{-1} \\
&= Hhg_xK(hg_x)^{-1} = HhKh^{-1}
\end{aligned}
$$

  car $K \lhd G_x$. De plus $HK = KH$ car H est distingué donc on a h' tel que $h'K = Kh^{-1}$. Alors

$$hg_xHK(hg_x)^{-1} = Hhh'K = HK$$

  Donc $HK \lhd G$.

- Montrons que $HK = G$.
  Pour tout $g \in G$, $gKg^{-1} \subset gHKg^{-1} = HK$ donc $G = \langle gKg^{-1}, g \in G\rangle \subset HK$.
- Montrons que $D(KH) \subset D(K)H$. Considérons $[g_1h_1, g_2, h_2]$. On écrit $h_ig_i = g_ig_i^{-1}h_ig_i = g_i\overline{h}_i$ et on obtient

  $$[g_1h_1, g_2, h_2] = g_1g_2g_1^{-1}g_2^{-1}\overline{h} = [g_1, g_2]\overline{h}$$

  En prenant $g_1, g_2 \in K$, on a $D(KH) \subset D(K)H$.
  On a donc $G = D^i(G) = D^i(KH) \subset D^i(K)H$ et K est résoluble donc pour n assez grand, $G \subset D^n(K)H = H$, ce qui assure que $G = H$ donc que G est simple. ■

<u>Théorème 3.2</u> Jordan-Dickson *Soit K un corps et V-ev de dimension n. Si $n \geqslant 3$ ou si $n = 2$ et $|K| > 3$, alors $PSL(V)$ est simple.*

Remarque 3.4 À un élément g de $SL(V)$, on peut associer une permutation des classes de $\mathbb{P}(V)$: $[v] \mapsto [gv]$. Le noyau de ce morphisme est $Z(SL(V))$.
On en déduit un morphisme $\overline{\varphi}$ injectif entre $PSL(V)$ et $\mathfrak{S}(\mathbb{P}(V))$.

Démonstration. Dans $SL(V)$, on fixe $u \in V$ et donc $[u] \in \mathbb{P}(V)$. Soit $A = \{t_{f,u}, f \neq 0, u \in \operatorname{Ker} f\} \cup \{\mathrm{Id}\}$. On montre que A est un groupe abélien :

$$t_{f_1,u} \circ t_{f_2,u}^{-1} = t_{f_1-f_2,u} \in A$$

ce qui montre au passage que A est abélien donc résoluble.

Soit $\varphi \in SL(v)_{[u]}$. $\varphi t_{f,u}\varphi^{-1} = t_{\varphi f\varphi^{-1},u} \in A$ donc $A \lhd SL(V)_{[u]}$.

Si $n \geqslant 3$, $\langle gAg^{-1}, g \in SL(V)\rangle = SL(V)$ car toutes les transvections sont conjuguées et qu'elles engendrent $SL(V)$. Si $n = 2$ et $|K| > 3$, A contient les transvections car il contient toutes les $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ donc on a aussi

$$\langle gAg^{-1}, g \in SL(V)\rangle = SL(V)$$

On passe maintenant dans $PSL(V)$. Notons π la surjection canonique. $\pi(SL(V)_{[u]})$ s'identifie à $PSL(V)_{[u]}$.

Comme $A \lhd SL(V)_{[u]}$, $AZ(SL(V)) \lhd SL(V)_{[u]}$ et que $\pi : SL(V)_{[u]} \to PSL(V)_{[u]}$ reste surjective, $K := \pi(AZ(SL(V)))$ est distingué et par ailleurs abélien donc résoluble. ■

Chapitre 4

Géométrie projective

<u>Définition 4.1</u> Soient V_1, V_2 deux ev, $\psi : V_1 \to V_2$ linéaire. À ψ correspond l'application projective

$$[\psi] : \begin{cases} \mathbb{P}(V_1) \setminus \mathbb{P}(\operatorname{Ker}\psi)) & \to & \mathbb{P}(V_2) \\ [v] & \mapsto & [\psi(v)] \end{cases}$$

appelée projectivisation de ψ.

Si ψ est bijective on dit que $[\psi]$ est une homographie.

Proposition 4.1 Les applications projectives transforment des points alignés en des points alignés.

Démonstration. Soient $P_i = \mathbb{P}(V_i)$ les trois points alignés. $\langle V_1, V_2, V_3\rangle$ est de dimension 2 donc $\dim\langle \varphi(V_1), \varphi(V_2), \varphi(V_3)\rangle \leqslant 2$.

Ainsi, $\dim \mathbb{P}(\langle \varphi(V_1), \varphi(V_2), \varphi(V_3)\rangle) \leqslant 1$ donc les P_i sont alignés. ■

<u>Définition 4.2</u> Soit d et d' deux droites du plan projectif qui se coupent en 0 et S un point n'appartenant ni à d ni à d'. On appelle perspective de centre S l'application qui à $M \in d$ associe l'unique point d'intersection de d' et (MS).

Proposition 4.2 Une perspective est une homographie.

Démonstration. On note H et H' les plans associés à d et d', v_S le vecteur qui dirige la droite associée à S.

On appelle ρ la projection de $V = H' \oplus \langle v_S\rangle$ sur V. On a $[\rho|_H] : d \to d'$ qui est une homographie (car $\operatorname{Ker}\rho \cap H = \{0\}$.

Pour tout M', les vecteurs du plan $\langle v_{M'}, v_S\rangle$ sont tous envoyés sur $v_{M'}$ par $\rho|_H$. En particulier, si $v_M \in H$ est associé à $M \in d$, l'image de v_M est $v_{M'}$ associé au $M' \in d'$ intersection de (MS) avec H'.

$[\rho_H]$ correspond donc bien à la perspective. ■

Définition 4.3 Le groupe projectif $GP(V)$ est l'ensemble des homographies de $\mathbb{P}(V) \to \mathbb{P}(V)$. Il est isomorphe à $GL(V)/Z(GL(V))$.

Proposition 4.3 Soit $W \subset V$ un hyperplan. L'ensemble G composé de l'identité et des homographies qui fixent exactement $\mathbb{P}(W)$ est un groupe isomorphe à $(W, +)$ qui agit simplement transitivement sur $\mathbb{P}(V) \setminus \mathbb{P}(W)$.

Démonstration. Montrons que les éléments φ distincts de l'identité de G sont des transvections dont l'homographie est la projectivisation.

Si φ est diagonalisable, alors on fixe non seulement $\mathbb{P}(W)$ mais aussi le supplémentaire de W ce qui contredit le fait qu'on fixe uniquement $\mathbb{P}(W)$. Ainsi, φ est une transvection (hyperplan de points fixes et non diagonalisable).

On peut donc écrire $G = \{t_{f,w}, \mathrm{Ker}(f) = W, w \in W\} \cup \{\mathrm{Id}\}$ et on a déjà vu qu'on pouvait fixer f de noyau W et on a

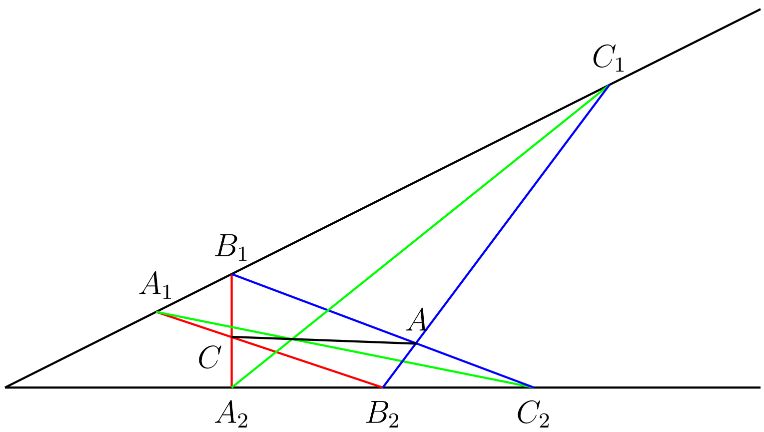
$$G = \{t_{f,w}, w \in W\} \cup \{\mathrm{Id}\}$$

Comme $t_{f,w_1} \circ t_{f,w_2} = t_{f,w_1+w_2}$, on a bien l'isomorphisme entre G et $(W, +)$.

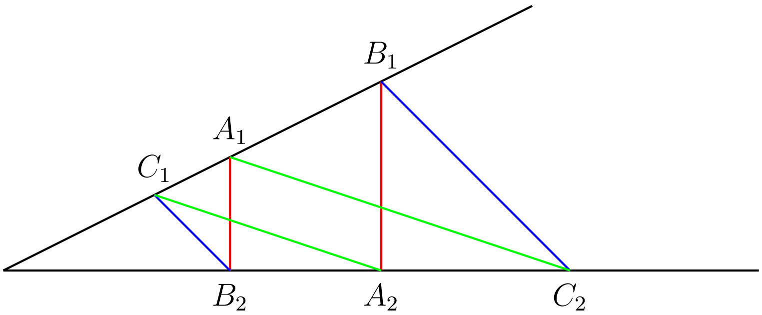
Soit $[\psi] \in G$. $[\psi]$ agit transitivement sur $\mathbb{P}(V) \setminus \mathbb{P}(W)$ et le stabilisateur de v dans G est $\{\mathrm{Id}\}$ car si ψ fixe x, ψ fixe W et une droite donc ψ fixe V donc $\psi = \mathrm{Id}$. ■

<u>Théorème 4.1</u> Pappus *Soient d et d' deux droites d'un plan projectif et A_1, B_1, C_1 sur d et A_2, B_2, C_2 sur d'. Alors $(A_1B_2) \cap (A_2B_1)$, $(B_1C_2) \cap (B_2C_1)$ et $(A_1C_2) \cap (A_2C_1)$ sont alignés.*

Démonstration.



On met la droite (AC) à l'infini et le dessin devient



On sait alors que $(A_1B_2) \parallel (A_2B_1)$ et $(A_1C_2) \parallel (A_2C_1)$ et par une application de Thalès, on obtient que $(B_1C_2) \parallel (B_2C_1)$ ce qui assure que B est à l'infini, donc sur (AC). ■

Définition 4.4 Un repère projectif de $\mathbb{P}(V)$ de dimension n est la donnée de $n+2$ points tels que tout sous ensemble de $n+1$ d'entre eux est projectivement libre.

Lemme 4.1.1
Les points $P_0, \ldots, P_{n+1}$ forment un repère projectif ssi il existe une base $(e_1, \ldots, e_{n+1})$ de V avec $P_i = [e_i]$ et $P_0 = [e_1 + \ldots + e_{n+1}]$.

Proposition 4.4 Il existe une unique homographie qui envoie un repère projectif sur un autre.

Démonstration.

$\exists$ Soit $(e_1, \ldots, e_{n+1})$ une base de V et $(e'_1, \ldots, e'_{n+1})$ une base de V'. Il existe $\varphi : V \to V'$ qui envoie e_i sur e'_i. En particulier, la somme des e_i est envoyée sur la somme des e'_i.
Ainsi, $[\varphi]$ convient.

! Si $[\varphi]$ et $[\psi]$ conviennent, on a $\varphi(e_i) = \lambda_i \psi(e_i)$ pour tout i.

$$\sum \lambda_i \psi(e_i) = \varphi(e_0) = \lambda_0 \psi(e_0) = \sum \lambda_0 \psi(e_i)$$

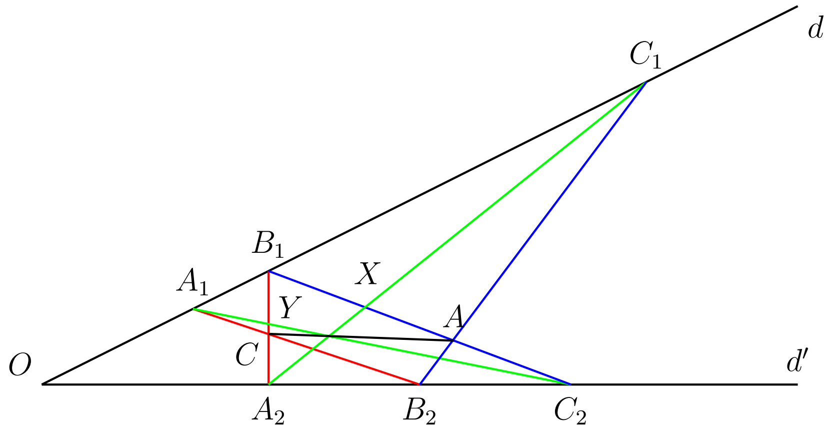
Donc $\lambda_i = \lambda_0$ et l'unicité. ■

Proposition 4.5 Une homographie entre d et d' qui se coupent en O est une perspective ssi elle fixe O.

Démonstration.

$\Rightarrow$ Clair

$\Leftarrow$ Soit φ qui fixe O. On a la situation



On considère p_{A_1} la perspective de sommet A_1 qui envoie d' sur (A_2B_1) et p_{C_1} celle de sommet C_1 qui envoie (B_1C_2) sur d'.
p_{A_1} envoie O sur B_1, A_2 sur A_2, B_2 sur C et C_2 sur Y. p_{C_1} envoie B_1 sur O, X sur A_2, A sur B_2 et C_2 sur C_2.
On remarque que $f = p_{A_1} \circ p_{C_1}$ coïncide avec la perspective p_B qui envoie (B_1C_2) sur (A_2B_1) en trois points ($B_1 \to B_1$, $X \to A_2$ et $C_2 \to Y$).
Ainsi, C est l'image de A par f donc par une perspective de centre B donc A, B et C sont alignés. ■

Proposition 4.6 Une homothétie de la droite projective est donnée par $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc \neq 0$. On écrit $z \mapsto \frac{az+b}{cz+d}$ avec la convention $\frac{1}{0} = \infty$.

<u>Définition 4.5</u> Pour tout (a, b, c) finis, il existe une unique homographie qui les envoie sur $(\infty, 0, 1)$. Si d est un autre point, on appelle son image $[a, b, c, d]$ le birapport des points (a, b, c, d). Il vaut

$$\frac{\frac{d-b}{d-a}}{\frac{c-b}{c-a}}$$

Proposition 4.7 Les homographies préservent le birapport et les bijections entre deux droites qui préservent le birapport sont des homographies.

Démonstration.

- Soit φ une homographie, a, b, c trois points distincts et d un point. Soit φ_1 l'unique homographique envoie $(\varphi(a), \varphi(b), \varphi(c))$ sur $(\infty, 0, 1)$. $\varphi_1(\varphi(d))$ est le birapport $[\varphi(a), \varphi(b), \varphi(c), \varphi(d)]$. Or $\varphi_1 \circ \varphi$ envoie (a, b, c) sur $(\infty, 0, 1)$ donc $[a, b, c, d] = (\varphi_1 \circ \varphi)(d)$.
- Soit f une bijection qui conserve le birapport. $(\infty, 0, 1)$ forment un repère projectif donc il existe une unique homographie telle que $\varphi = f$

sur $(\infty, 0, 1)$. On a

$$\begin{aligned} d = [\infty, 0, 1, d] &= [\varphi^{-1} \circ f(\infty), \varphi^{-1} \circ f(0), \varphi^{-1} \circ f(1), \varphi^{-1} \circ f(d)] \\ &= \varphi^{-1}(f(d)) \end{aligned}$$

Ainsi, $f(d) = \varphi(d)$ pour tout d. ∎

Définition 4.6 $\mathbb{P}(V^*)$ est l'espace projectif dual de $\mathbb{P}(V)$.

Théorème 4.2 *Il existe une bijection canonique entre les hyperplans de $\mathbb{P}(V)$ et les points de $\mathbb{P}(V^*)$.*

Proposition 4.8 Si $W \subset V$, la restriction des formes linéaires $V^* \to W^*$ est une application linéaire de noyau $W^\perp = \{f \in V, f|_W = 0\}$. On a alors $W^* = V^*/W^\perp$ et $\dim W + \dim W^\perp = \dim V$.

Exemple 4.1 Trois points sont alignés dans $\mathbb{P}(V)$ ssi les droites associées sont concourrantes dans $\mathbb{P}(V^*)$.

Théorème 4.3 Dualisation de Pappus *Soient P et P' deux points.*

Soient a_1, b_1, c_1, trois droites concourrantes en P, a_2, b_2, c_2 concourrantes en P'.

Soit c la droite qui relie l'intersection de a_1 et b_2 avec l'intersection de a_2 et b_1. Soit b la droite qui relie l'intersection de a_1 et c_2 avec l'intersection de a_2 et c_1. Soit a la droite qui relie l'intersection de c_1 et b_2 avec l'intersection de c_2 et b_1.

Alors a, b et c sont concourrantes.

Définition 4.7 Une homologie de $\mathbb{P}(V)$ est une homographie qui admet un hyperplan de points fixes.

Proposition 4.9 Si l'homologie $\pi(\varphi)$ de $\mathbb{P}(V)$ d'hyperplan $\mathbb{P}(W)$ admet un autre point fixe $O \in \mathbb{P}(V) \setminus \mathbb{P}(W)$ alors il s'agit de la projectivisation d'une dilatation.

Démonstration. $\pi(\psi)|_{\mathbb{P}(W)}$ est l'identité donc l'application linéaire ψ_W est une multiplication scalaire sur W. ∎

Définition 4.8 On appelle élation les projectivisations des transvections.

Lemme 4.3.1
Si $\dim(\mathbb{P}(V)) \geqslant 2$, $\pi(\psi) \in GP(V)$ une homologie. On note $O = \pi(\psi - \mathrm{Id})$ le sommet de l'homologie.

Alors O est l'unique point de $\mathbb{P}(V)$ tel que pour tout M, (O, M, M') sont alignés (où $M' = \pi(\varphi(M))$).

Démonstration. Pour tout $v \in V$, on a que $\psi(v) - v \in \mathrm{Im}(\psi - \mathrm{Id}) = \pi^{-1}(O)$ donc les vecteurs $\psi(v)$, v et $\pi^{-1}(O)$ sont liés donc appartiennent à un même plan.

Donc $O, [v]$ et $[\varphi(v)]$ sont alignés. ■

Définition 4.9 Soit $f : V_1 \to V_2$ est dite σ-linéaire (pour $\sigma \in \mathrm{Aut}(K)$) ssi $f(v + w) = f(v) + f(w)$ et $f(\lambda v) = \sigma(\lambda)f(v)$.

Si f est σ-linéaire et g est τ -linéaire alors $g \circ f$ est $\tau \circ \sigma$-linéaire. On note ΓL le groupe des fonctions σ-linéaires et $P\Gamma L$ le groupe projectif associé.

Chapitre 5

Formes sesquilinéaires

Définition 5.1 Soit K un corps, V un K-ev. Une forme σ-sesquilinéaire est une application $B : V \times V \to K$ telle que B est linéaire en la première variable et σ-linéaire en la deuxième.

Définition 5.2 B est

- hermitienne ssi $\sigma(B(v, w)) = B(w, v)$
- alternée ssi $B(v, v) = 0$
- réflexive dès que $B(v, w) = 0$ ssi $B(w, v) = 0$.

$GL(V)$ agit sur l'ensemble des formes σ-sesquilinéaires par $(gB)(v, w) = B(g(v), g(w))$. On dit que deux formes sont équivalentes ssi elles appartiennent à la même orbite.

On note $\mathrm{Iso}(B) = \mathrm{Stab}_G(B)$.

Définition 5.3 On définit la matrice M de B par $m_{i,j} = B(e_i, e_j)$ dans la base $(e_1, \dots, e_n)$.

ALors $B(v, w) = v^t M_B w^\sigma$.

Définition 5.4 Soit S une matrice de changement de bases.

$M' = S^t M \sigma(S)$ donc $\det(M') = \det(M)\det(S)\det(\sigma(S))$.

Pour $\sigma = \mathrm{Id}$, on a $\det(M') = \det(M)\det(S)^2$ donc $\det(M) \in K^*/(K^*)^2$ ou $\det(M) = 0$.

On appelle discriminant de B la classe de $\det(M)$ dans ce quotient.

Définition 5.5 Soit B sesquilinéaire. L'adjoint de B est l'application σ-sesquilinéaire $B^* : w \mapsto B(\cdot, w)$.

Définition 5.6 Soit B réflexive. v et w sont orthogonaux ssi $B(v, w) = 0$. On définit l'orthogonal de $X \subset V$ par

$$X^\perp = \{v \in V, \forall w \in X, B(v, w) = 0\}$$

Le radical de B noté $\mathrm{Rad}(B)$ est $V^\perp = \mathrm{Ker}\, B^*$.

Définition 5.7

- B est non dégénérée ssi son radical est nul.
- v est dit isotrope ssi $B(v,v)=0$ et $v\neq 0$.
- Une paire v,w est dite hyperbolique ssi $B(v,v)=B(w,w)=0$ et $B(v,w)=1$.
- Un espace $W\subset V$ est non isotrope si 0 est le seul vecteur de W orthogonal à tous les vecteurs de W.
- Un espace $W\subset V$ est isotrope ssi il existe $v\neq 0$ de W qui est orthogonal à W ($W\cap W^\perp\neq\{0\}$).
- Un espace $W\subset V$ est totalement isotrope ssi $W\subset W^\perp$.

Exemple 5.1 Soit (v,w) une paire hyperbolique. Si B est symétrique on parle d'un plan hyperbolique. Si B est alternée on parle d'un plan symplectique.

Proposition 5.1 Si B est réflexive alors $X^\perp$ est un sev.

Définition 5.8 Soit B sesquilinéaire réflexive sur V et U,W deux sev de V tels que $V=U\oplus W$. On dit que $U\oplus W$ est une décomposition orthogonale et on note $U\perp W$ ssi pour tout $u\in U, w\in W$, $B(u,w)=0$.

Proposition 5.2 Soit B réflexive, $U\subset V$ telle que $\dim U+\dim U^\perp\geqslant\dim V$.

Si de plus U est non isotrope alors $V=U\perp U^\perp$.

Proposition 5.3 Soit B σ-sesquilinéaire réflexive sur V et $U\subset V$.

$$\dim U+\dim(U^\perp)\geqslant\dim V$$

Si de plus U est non isotrope, $B|_{U\times U}$ est non dégénérée donc $V=U\perp U^\perp$.

Démonstration. On considère $\overline{B}^*: V\to U^*$ qui à w associe $B(\cdot,w)$.

$\operatorname{Ker}(\overline{B}^*)=U^\perp$ donc

$$\dim V=\dim(\operatorname{Im}\overline{B}^*)+\dim\operatorname{Ker}\overline{B}^*\leqslant\dim(U^*)+\dim(U^\perp)=\dim U+\dim U^\perp$$

Si $B|_{U\times U}$ est non dégénérée alors $\operatorname{Rad}(B|_{U\times U})=U\cap U^\perp=\{0\}$. On a donc

$$\dim U+\dim U^\perp\leqslant\dim V$$

Donc $V=U\perp U^\perp$. ∎

Corollaire 5.1 *Si B est réflexive et non dégénérée alors*

- $\dim U+\dim U^\perp=\dim V$
- $U=U^{\perp\perp}$
- *Si $V=U\perp W$ alors $W=U^\perp$*

- $\{0\} = \operatorname{Rad} V = \operatorname{Rad} U + \operatorname{Rad} W$.

Démonstration. On sait déjà que $\dim V \leqslant \dim U + \dim U^\perp$.

De plus, $B^* : V \to V^*$ est injective car B est non dégénérée donc B est bijective.

Soit $e_1, \dots, e_n$ une base de V telle que $e_1, \dots, e_m$ soit une base de U.

$B^*(U^\perp)$ est inclus dans l'espace des formes linéaire nulles sur U qui est de dimension $n - m = \dim V - \dim U$ (une base est $e_{m+1}^*, \dots, e_n^*$). On a donc

$$\dim U^\perp = \dim B(U^\perp) \leqslant n - m = \dim V - \dim U \qquad \blacksquare$$

<u>Définition 5.9</u> Soit B sesquilinéaire réflexive non dégénérée. L'indice de Witt de V est la dimension d'un sous-espace totalement isotrope maximal (setim).

Proposition 5.4 L'indice de Witt est inférieur à $\frac{\dim V}{2}$.

Démonstration. Si $W \subset V$ est setim donc $W \subset W^\perp$ donc

$$\dim V = \dim W + \dim W^\perp \geqslant 2 \dim W^\perp \qquad \blacksquare$$

<u>Théorème 5.1</u> Birkhoff von Neumann *Soit B σ-sesquilinéaire réflexive non dégénérée. Alors on a l'alternative.*

- $\sigma = \mathrm{Id}$ *et B est symétrique*
- $\sigma = \mathrm{Id}$ *et $B(v, v) = 0$ pour tout v.*
- $\sigma \neq \mathrm{Id}$, $\sigma^2 = \mathrm{Id}$ *et om existe $\lambda \neq 0$ tel que λB est hermitienne.*

<u>Théorème 5.2</u> *Si (K est de caractéristique différente de deux et B symétrique) ou (B hermitienne) alors il existe une base orthogonale pour B.*

Si B est alternée alors il existe une base dans laquelle la matrice de B est de la forme

$$\begin{pmatrix} 0 & \mathrm{Id} & 0 \\ -\mathrm{Id} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad ou \quad \begin{pmatrix} R & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & R & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

avec $R = \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}$.

Démonstration.
- Si V n'est pas totalement isotrope et pour tout v, $B(v, v) = 0$ on aurait (dans le cas symétrique)

$$0 = B(v + w, v + w) = B(v, w) + B(w, v)$$

Dans le cas symétrique, on a donc $B(v,w)=0$ pour tout v,w, ce qui est absurde. Et dans le cas hermitien,

$$\lambda B(v,w) = B(\lambda v, w) = -B(w,\lambda v) = -\sigma(\lambda)B(w,v) = \sigma(\lambda)B(v,w)$$

Donc ($\sigma \neq \mathrm{Id}$) $B(v,w)=0$, ce qui est absurde car B serait totalement isotrope.

Il existe donc v tel que $B(v,v)\neq 0$. Alors $B|_{\langle v\rangle^2}$ est de matrice (d_1) avec $d_1 \neq 0$ donc $V=\langle v\rangle \perp \langle v\rangle^\perp$ et on recommence dans $\langle v\rangle^\perp$ tant qu'il n'est pas totalement isotrope.

- Si B n'est pas totalement isotrope, il existe v,w tel que $B(v,w)=\lambda\neq 0$. On a $B(\frac{v}{\lambda},w)=1$ et $B(w,\frac{v}{\lambda})=-1$. Ainsi, la matrice de $B|_{\langle \frac{v}{\lambda},w\rangle}$ est R.
  On réitère alors le procédé sur $\langle \frac{v}{\lambda},w\rangle^\perp$. En réordonnant les colonnes, on tombe sur le deuxième type de matrices. ■

Définition 5.10 Un espace symplectique est une somme de plans symplectiques.

Proposition 5.5 Un espace symplectique est toujours de dimension paire.

Démonstration. La décomposition de la matrice de B n'a que des blocs R donc la dimension de l'espace est paire. ■

Définition 5.11 Si B est symétrique ou hermitienne, on pose $Q(x)=B(x,x)$ la forme quadratique associée. En caractéristique différente de 2,

$$B(x,y)=\frac{Q(x+y)-Q(x)-Q(y)}{2}$$

THÉORÈME 5.3
- *Si K est algébriquement clos alors les formes symétriques alors les formes symétriques non dégénérées sont toutes équivalentes à une forme de matrice* Id.
- *Si $K=\mathbb{R}$, alors les formes sont équivalentes à* $\begin{smallmatrix} \mathrm{Id}_p & 0 \\ 0 & -\mathrm{Id}_{n-p}\end{smallmatrix}$. *On appelle $(p,n-p)$ la signature de la forme.*
- *On a aussi le résultat précédent si $K=\mathbb{C}$ et $\sigma=\bar{\cdot}$. À congruence près, il y a donc $n+1$ formes.*

THÉORÈME 5.4 *Si $K=\mathbb{F}_q$ avec q impair. Toute forme symétrique non dégénérée est équivalente à* Id *ou* $\mathrm{diag}(1,\dots,1,\alpha)$.

THÉORÈME 5.5 WITT *Soit V un K-ev de dimension finie et B une forme σ-sesquilinéaire non dégénérée qui est soit hermitienne, soit alternée soit (symétrique avec K de caractéristique différente de 2).*

Toute isométrie de $W\to W'$ entre deux sous-espaces s'étend en une isométrie de V.

Lemme 5.5.1
Soit B alternée non dégénérée sur V et $v_1, \dots, v_r$ des vecteurs isotropes linéairement indépendants avec $B(v_i, v_j) = 0$ pour $i \leqslant j$. Alors il existe $w_1, \dots, w_r$ linéairement indépendants tels que $H_i = \langle v_i, w_i \rangle$ est un plan symplectique et

$$V = H_1 \perp \dots \perp F_r \perp M$$

avec $(2r < \dim V)$.

Démonstration. B^* est bijectif et comme $v_1, \dots, v_r$ sont linéairement indépendants, il existe $w_1, \dots, w_r$ tel que $B(v_1, w_1) = 1$ et $B(v_i, w_i) = 0$.

$H_1 = \langle v_1, w_1 \rangle$ est un plan symplectique et on réapplique à $H_1^{\perp}$. ■

Corollaire 5.2 *Soit B comme dans Witt, W_1, W_2 deux setim. Alors $\dim W_1 = \dim W_2$.*

Démonstration. Par symétrie, $\dim W_1 \leqslant \dim W_2$. Il existe une isométrie de W_1 dans un sous espace de dimension $\dim W_1$ de W_2.

Par Witt, on a *p.s.* un isométrie de l'espace entier avec $\psi(W_1) \subset W_2$. On a donc $W_1 \subset \psi^{-1}(W_2)$ donc $\dim(W_1) \geqslant \dim(\psi^{-1}(W_2))) \dim W_2$, ce qui assure l'égalité. ■

Chapitre 6

Groupes classiques

Définition 6.1 Soit V un K-ev de dimension au moins 2 et B une forme σ-sesquilinéaire réflexive non dégénérée sur V.

- Si B est symétrique avec $\sigma = \mathrm{Id}$ alors le groupe des isométries de B est le groupe orthogonal $O_B(V)$. On note SO_B le sous-groupe de ces endomorphismes qui sont de déterminant 1.
- Si $\sigma = \mathrm{Id}$ et B alternée alors le groupe des isométries est le groupe symplectique $\mathrm{Sp}_B(V)$.
- Si B est σ-hermitienne alors le groupe des isométries de B est le groupe unitaire $U_B(V)$. On note $SU_B(V)$ comme pour $SO_B(V)$.

6.1 Groupes symplectiques

Corollaire 6.1 *À conjugaison près, il existe un unique groupe symplectique sur V.*

Proposition 6.1 $\mathrm{Sp}(2, K) = SL(2, K)$.

Démonstration. On se place dans le cas où la forme est $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Soit A une matrice de changement de base. On a $B(Av_1, Av_2) = B(v_1, v_2) = 1$ et

$$\begin{aligned} B(Av_1, Av_2) &= B(a_{1,1}v_1 + a_{2,1}v_2, a_{1,2}v_1 + a_{2,2}v_2) \\ &= B(a_{1,1}v_1, a_{2,2}v_2) + B(a_{2,1}v_2, a_{1,2}v_1) \\ &= a_{1,1}a_{2,2} - a_{1,2}a_{2,1} = \det(A) \end{aligned}$$

Donc A est une isométrie pour B ssi $\det(A) = 1$. ∎

Proposition 6.2 Soit B alternée réflexive non dégénérée sur $V \simeq \mathbb{F}_q^{2n}$.

(i) Il existe $(q^{2n} - 1)q^{2n-1}$ paires hyperboliques

(ii) $|\operatorname{Sp}(2n,q)| = \prod_{i=1}^{n}(q^{2i}-1)q^{2i-1} = q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$.

Démonstration.

(i) Si v_1, v_2 forment une paire hyperbolique, on a $q^{2n}-1$ choix et $v_2 \notin v_1^\perp$ donc on a $q^{2n}-q^{2n-1}$ choix pour v_2.
On a alors $B(v_1,v_2)=\lambda \neq 0$ et il y a $q-1$ valeurs possibles de λ donc il y a en fait
$$\frac{q^{2n}-q^{2n-1}}{q-1} = q^{2n-1}$$
choix pour v_2. Il y a donc $(q^{2n}-1)q^{2n-1}$ paires.

(ii) Par récurrence sur n. Pour $n=1$, on obtient $|SL(2,K)|$.
Soient $H=\langle v_1,v_2\rangle$ et $H' = \rangle v_1', v_2'\rangle$ deux paires hyperboliques. Il existe une isométrie de $H \to H'$ donnée par $\varphi(v_i)=v_i'$.
Par le théorème de Witt, on peut étendre φ à une isométrie de V, ce qui prouve que $\operatorname{Sp}(2n,K)$ agit transitivement sur les paires hyperboliques.
Un élément φ du stabilisateur d'une paire hyperbolique $H=\langle v_1,v_2\rangle$ s'identifie à un élément de $\operatorname{Sp}(H^\perp)$ puisque $\varphi|_H = \mathrm{Id}$ et $H \perp H^\perp = V$.
Réciproquement, tout élément de $\operatorname{Sp}(H^\perp)$ s'étend par Witt en une isométrie qui fixe H. Ainsi, le stabilisateur est isomorphe à $\operatorname{Sp}(2(n-1),K)$.
La relation orbite stabilisateur donne
$$|\operatorname{Sp}(2n,K)| = (q^{2n}-1)q^{2n-1}|\operatorname{Sp}(2n-2,K)|$$
ce qui conclut. ∎

Proposition 6.3 Une transvection de GL est dans Sp ssi elle est de la forme $t(v)=v+\alpha B(v,u)u$ pour $\alpha \in K^*$. On note T le sous-groupe de Sp engendré par les transvections symplectiques.

Proposition 6.4 T agit transitivement sur $V\setminus\{0\}$ et sur l'ensemble des paires hyperboliques.

Démonstration.

- Soit u_1,u_2 non nuls. Si $B(u_1,u_2)\neq 0$, on prend $t(v)=v-\frac{B(u_1-u_2,v)}{B(u_1,u_2)}(u_1-u_2)$ et $t(u_1)=u_2$.
Si $B(u_1,u_2)=0$, on cherche $w\in V$ avec $B(u_1,w)\neq 0 \neq B(u_2,w)$. Si $u_1 \notin \langle u_2\rangle$ alors $w \in V\setminus u_2^\perp$ fait l'affaire. Sinon (u_1,u_2) engendrent un espace isotrop donc il existe w_1,w_2 tels que $\langle u_i,w_i\rangle$ soient symplectiques et w_1+w_2 convient.
Il existe alors une transvection qui envoie u_1 sur w et une qui envoie w sur u_2 donc c'est bon.

- Soient (u_1, v_1) et (u_2, v_2) deux paires hyperboliques.
  Il existe une transvection t qui envoie u_1 sur u_2. Si on montre qu'il existe une transvection qui envoie $v_3 := t(v_1)$ sur v_2 en fixant u_2, on a gagné. On se restreint donc à $u_1 = u_2$.
  Si $B(v_1, v_2) \neq 0$, on prend $t(v) = v - \frac{B(v_1 - v_2, v)}{B(v_1, v_2)}(v_1 - v_2)$. Si $B(v_1, v_2) = 0$, alors on a $B(v_1, u_2 + v_1) \neq 0 \neq B(u_2 + v_1, u_2 + v_2)$ et on prend des transvections pour faire $(u_2, v_1) \to (u_2, u_2 + v_1) \to (u_2, v_2)$. ■

Proposition 6.5 $\mathrm{Sp}(V)$ est engendrée par les transvections symplectiques.

Démonstration. Par récurrence sur n. $n = 2$ c'est bon car c'est SL.

Si $n = 2m$ avec $m > 1$. Soit (u, v) une paire hyperbolique et $g \in \mathrm{Sp}(2m, K)$. $(g(u), g(v))$ est aussi une paire hyperbolique.

Soit $t \in T$ envoyant $(g(u), g(v))$ sur (u, v). $t \circ g \in \mathrm{Sp}(2n, K)$ et fixe (u, v). Alors $t \circ g|_{\langle u,v\rangle^\perp}$ est un élément de $\mathrm{Sp}(2n-2, K)$ donc par hypothèse de récurrence, il s'écrit comme produit de transvections symplectiques de $\mathrm{Sp}(\langle u, v\rangle^\perp)$.

On remarque alors qu'une transvection de $\langle u, v\rangle^\perp$ peut être convertie en une transvection de V qui fixe $\langle u, v\rangle$. Ainsi, $t \circ g = t_1 \circ \ldots \circ t_n$ donc g est un produit de transvections. ■

Corollaire 6.2 $\mathrm{Sp} \subset SL$.

Théorème 6.1 *Soit V de dimension $2m$. Alors $D(\mathrm{Sp}(2m, K)) = \mathrm{Sp}(2m, K)$ sauf pour $\mathrm{Sp}(2, 2)$, $\mathrm{Sp}(2, 3)$ et $\mathrm{Sp}(4, 2)$.*

Démonstration. On fait une récurrence sur m en supposant que c'est vrai pour $\mathrm{Sp}(6, 2)$, $\mathrm{Sp}(4, 3)$ et $\mathrm{Sp}(2, K)$ pour $|K| > 3$ (cf TD).

L'idée est de montrer que toute transvection $t_{\alpha,u}$ est dans $D(\mathrm{Sp}(2n, K))$. On considère un plan hyperbolique H dans $u^\perp \setminus \langle u\rangle$ (qui est de dimension au moins $2n - 2$ donc un tel plan existe).

$t_{\alpha,u}|_{H^\perp}$ est une transvection de $H^\perp$. Par hypothèse de récurrence, c'est un produit de commutateurs $[g_i, g_j]$.

Les g_i s'étendent comme précédemment à des isométries de $\mathrm{Sp}(V)$ et donc $t_{\alpha,u}$ est un produit de commutateurs donc il appartient au groupe dérivé. Alors $\mathrm{Sp}(V) \subset D(\mathrm{Sp}(V))$ d'où le résultat. ■

On s'intéresse à l'action de $\mathrm{Sp}(V)$ sur $\mathbb{P}(V)$. Le noyau du morphisme associé est $Z(SL(V)) \cap \mathrm{Sp}(V)$.

Proposition 6.6 L'action de $\mathrm{Sp}(V)$ sur $\mathbb{P}(V)$ est primitive.

Démonstration. On partitionne $\mathbb{P}(V)$ en

$$[v] \cup \underbrace{\{[w], B(v,w)=0, [w] \neq [v]\}}_{E_1} \cup \underbrace{\{[w], B(v,w)=1\}}_{E_2}$$

Soit $[w_i] \neq [v]$ avec $B(v, w_i) = 0$. La restriction de B à $\langle v, w_1\rangle$ et $\langle v, w_2\rangle$ est 0. Il existe φ qui envoie v sur v et w_1 sur w_2 qui s'étend par Witt en une isométrie ψ de V.

$\psi(v) = v$ et $\psi(w_1) = w_2$ donc ψ stabilise v et $\psi([w_1]) = [w_2]$. Donc E_1 est bine une orbite.

Dans le cas de E_2, on sait que $\mathrm{Sp}(V)$ agit transitivement sur les couples hyperboliques et par Witt (comme avant) on étend l'application et E_2 devient une orbite.

Soit B un bloc avec $|B| > 1$. On doit montrer que B est l'espace entier. Soit $[v] \in B$.

Si B contient un point de E_1 alors B contient E_1 (c'est une orbite). Idem pour E_2. B ne peut pas contenir un point de E_1 et E_2 sinon il contiendrait tout le monde. Ainsi, les seuls blocs non triviaux possibles sont E_1 et E_2.

Supposons que B contienne E_1. On considère $w_1 \in V \setminus v^\perp$ non nul. On a $[w_1] \in E_2$.

Soit $w_2 \in (\langle v\rangle + \langle w_1\rangle)^\perp \subset v^\perp \cap w_1^\perp$ donc $w_2 \in E_1$.

On faut jouer à $[w_2]$ le rôle dans v dans la définition de E_1, ce qui donne que $\pi(w_2^\perp) \subset E_1$. Comme $w_1 \in (w_2)^\perp$, $w_1 \in B$. B contient donc un point de E_1 et E_2 donc B est bien trivial. Par symétrie, ça marche aussi si B contient E_2 donc l'action est primitive. ∎

<u>Théorème 6.2</u> *Les $PSp(V)$ sont simples sauf $PSp(2,2)$, $PSp(2,3)$ et $PSp(4,2)$.*

Démonstration. $H = \{t_{a,u}, a \in K^*\} \cup \{\mathrm{Id}\}$ est isomorphe à $(K, +)$ qui est distingué dans $\mathrm{Stab}([u])$ (car H abélien) car si φ stabilise u, $\varphi t_{a,u}\varphi^{-1} = t_{a,\varphi(u)} = t_{a,u}$.

$\displaystyle\bigcup_{\varphi \in Sp(V)} \varphi H \varphi^{-1}$ engendre $Sp(V)$ puisqu'il contient toutes les transvections.

On passe maintenant au quotient. $\pi(H)$ est toujours distingué et $\displaystyle\bigcup_{\varphi \in Sp(V)} \varphi\pi(H)\varphi^{-1}$ engendre PSp donc par Iwasawa, on a gagné. (Les exceptions proviennent des exception précédentes quand on a montré que l'action est fidèle et primitive et que $PSp = D(PSp)$.) ∎

6.2 Groupes orthogonaux

On se place en caractéristique différente de 2.

Soit $\varphi \in O(V)$ et B une forme bilinéaire symétrique non dégénérée sur V. Alors $M_B = M_\varphi^T M_B M_\varphi$ donc $\det(M_\varphi)^2 = 1$.

Définition 6.2 Une symétrie de V est un élément de $GL(V)$ dont l'ordre divise 2. On note V^+ et V^- les espaces propres associés. La symétrie est dite orthogonale ssi elle est dans $O_B(V)$.

Proposition 6.7 Une symétrie est orthogonale ssi $V^+ \perp V^-$. Si B est non dégénérée, dans ce cas, $V = V^+ \perp V^-$.

Démonstration. $B(x,y) = B(\varphi(x), \varphi(y)) = B(x, -y) = -B(x,y)$ donc $B(x,y) = 0$. ∎

Proposition 6.8 Soit $W \subset V$ non isotrope alors il existe une unique symétrie orthogonales avec $W \subset V^+$.

Démonstration. On prend $\varphi|_W = \mathrm{Id}$ et $\varphi|_{W^\perp} = -\mathrm{Id}$. ∎

Lemme 6.2.1
Si B est bilinéaire symétrique non dégénérée alors il existe un vecteur non isotrope.

Lemme 6.2.2
Soit $x, y \in V$, Si $Q(x) = Q(y) \neq 0$ alors $Q(x+y) = 0$ implique $Q(x-y) \neq 0$.

Démonstration. Par l'absurde, si $Q(x+y) = Q(x-y) = 0$, on a $Q(x+y) = 2Q(x)+2B(x,y)$ et $Q(x-y) = 2Q(x)-2B(x,y)$ donc $4Q(x) = 0$, absurde. ∎

<u>Théorème 6.3</u> Cartant-Dieudonné *Dans $O(V)$, tout élément est produit d'au plus $n := \dim V$ réflexions.*

Démonstration. Par récurrence sur $\dim(V)$. Si $\dim(V) = 1$, c'est bon. Sinon, si c'est vrai pour les dimensions $< n$, soit $\varphi \in O(V)$.

- Si φ possède un vecteur fixe non isotrope. Posons $H = x^\perp$. Alors $\varphi(H) = H$.
  Par hypothèse de récurrence, $\varphi|_H = \tau_1 \circ \ldots \circ \tau_r$ avec $r < n$. Alors $\varphi = (\mathrm{Id}_{\langle x\rangle} + \tau_1) \circ \ldots \circ (\mathrm{Id}_{\langle x\rangle} + \tau_r)$.
- Sinon, tout vecteur non isotrope x vérifie $y := \varphi(x) \neq x$. Alors $Q(x) = Q(y) \neq 0$.
  Soit $Q(x-y) \neq 0$, soit $Q(x+y) \neq 0$. On se place dans le premier cas (le second est similaire), on pose $H = \langle x - y\rangle^\perp$. H contient $x+y$ car :
  $$B(x+y, x-y) = Q(x) - Q(y) - B(x,y) + B(y,x) = 0$$
  Notons τ_H la réflexion d'hyperplan H.
  $\tau_H(x-y) = y - x$ et $\tau(x+y) = x+y$ donc $\tau_H(y) = x$ et $\tau_H \circ \varphi$ fixe x et on se ramène au cas précédent. ∎

6.3 Sous-groupes finis de SO_2 et SO_3

det est un morphisme (surjectif) de $O(\mathbb{R}^n)$ dans $\{\pm 1\}$ et son noyau (SO_n) est d'indice 2 donc $O(\mathbb{R}^n) = SO(\mathbb{R}^n) \rtimes \langle s \rangle$ où s est une symétrie.

Proposition 6.9 $g \in O(\mathbb{R}^2)$ a pour matrice

$$\begin{pmatrix} \rho_\theta = \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

ou

$$\begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

Démonstration. Il suffit d'écrire que l'image d'une BON est une BON. ■

Proposition 6.10 Les sous-groupes finis de SO_2 sont cycliques et les sous-groupes finis de O_2 qui ne sont pas dans SO_2 sont diédraux.

Démonstration. $f : \rho_\theta \mapsto \mathrm{e}^{i\theta}$ est un morphisme de groupes injectif et les sous-groupes finis du groupe multiplicatif d'un corps sont cycliques.

Soit H un sous-groupe fini de O_2. $H \cap SO_2$ est soit H soit un sous-groupe d'indice 2 cyclique engendré par ρ_θ.

Alors $H \cap SO_2 \lhd H$ est d'indice deux. On a alors un s qui vérifie $s\rho_\theta s^{-1} = \rho_\theta^{-1}$. ■

Proposition 6.11 Les points fixes de $g \in SO_3$ ($g \neq \mathrm{Id}$) forment une droite vectorielle appellée axe de la rotation.

Démonstration. g est produit d'au plus 3 réflexions. Ça peut pas être 3 car $g \in SO_3$. On écrit donc $g = s_{H_1} \circ s_{H_2}$.

Les points fixes de g sont donc dans $H_1 \cap H_2$ qui est de dimension au moins 1.

Ça ne peut pas faire 2 sinon, $H_1 = H_2$ donc $g = \mathrm{Id}$. ■

Définition 6.3 On appelle pôle d'un élément de SO_3 différent de l'identité l'intersection de son axe avec la sphère de rayon 1. On note $P(G)$ l'ensemble des pôles des éléments d'un groupe G distincts de l'identité.

Proposition 6.12 G agit sur $P(G)$ et le stabilisateur d'un pôle est un groupe cyclique.

Proposition 6.13 On rappelle la formule des classes

$$|X| = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$$

et

$$r = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

où X^g est l'ensemble de spoints fixes de $\langle g\rangle$.

<u>Théorème 6.4</u> *Si $G \subset SO_3$ est fini alors G est isomorphe à D_m, $\mathbb{Z}/m\mathbb{Z}$, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{S}_5$.*

Démonstration. Soit $X = P(G)$. Si $G \neq \{\mathrm{Id}\}$, $|X| \geqslant 2$. Soit $n = |G|$.

$$r = \frac{1}{n}\left(|X^{\mathrm{Id}}| + \sum_{g\neq \mathrm{Id}}|X^g|\right) = \frac{|X| + 2(n-1)}{n}$$

Or $|X| \in [\![2, 2n-2]\!]$ donc $2 \leqslant r \leqslant \frac{4(n-1)}{n} < 4$.

Ainsi, $r = 2$ ou $r = 3$.

- $r = 2$: On a deux orbites X_1 et X_2. On réécrit la formule précédente :

  $$2n = |X_1| + |X_2| + 2(n-1)$$

  Donc X_1 et X_2 ont un seul élément. Ainsi, tous les éléments ont les mêmes pôles donc $G \simeq \mathbb{Z}/m\mathbb{Z}$ (car c'est donc un sous-groupe fini de SO_2).
- $r = 3$: On a trois orbites X_1, X_2 et X_3 et on note n_i l'ordre des stabilisateurs associés. On ordonne les X_i par cardinal décroissant (donc $n_1 \leqslant n_2 \leqslant n_3$).

  La formule précédente donne $|X| = n + 2 = \frac{n}{n_1} + \frac{n}{n_2} + \frac{n}{n_3}$. Ainsi, $\frac{3}{n_1} \geqslant 1 + \frac{2}{n} > 1$.

  Donc $n_1 = 2$. On refait pareil en réinjectant et on trouve $\frac{2}{n_2} > \frac{1}{2}$ donc $n_2 = 2$ ou $n_2 = 3$.

  Si $n_2 = 2$, n est pair et si $n_2 = 3$, $n_3 \in \{3, 4, 5\}$, ce qui correspond à des groupes d'ordre $12, 24, 60$.
- Cas 12 : tout élément de G est dans un stabilisateur donc ils sont tous d'ordre 2 ou 3 (taille des stabilisateurs). Alors G n'est pas abélien et X_1 contient 6 pôles qui correspondent aux trois axes d'un stabilisateur qui est d'ordre 2.

  On n'a donc que 3 éléments d'ordre 2 qui forment (avec l'identité) l'unique 2-Sylow qui est isomorphe à V_4 (tous les éléments sont d'ordre 2). Donc $G \simeq V_4 \rtimes \mathbb{Z}/3\mathbb{Z} \simeq \mathfrak{A}_4$. ■

