Université de Rennes 1

THGG

THÉORIE DES GROUPES & GÉOMÉTRIES

Groupes et actions de groupes, groupes symétriques et alternés, simplicité du groupe alterné, groupe linéaire sur un corps, géométrie projective formes sesquilinéaires et quadratiques dans un corps quelconque, formes quadratiques sur $\mathbb{R}$, groupes orthogonaux.

Auteur
Matthieu Romagny

Notes de cours
Victor Lecerf

2021–2022

Table des matières

Chapitre 1

Rappels sur les groupes et les actions de groupes

1.1 Sous-groupes distingués et quotients

Définition 1.1.1. *Soit G un groupe. Un sous-groupe H de G est dit* ***distingué*** *(ou* ***normal****) dans G si $gHg^{-1} = H$ pour tout $g \in G$. On note $H \triangleleft G$.*

Remarque.

— Il est équivalent de demander que $gHg^{-1} \subset H$ pour tout $g \in G$.

— Si H est distingué dans G, les deux relations d'équivalence définies par

$$g \sim_1 g' \iff \exists h \in H,\, g' = hg, \quad \text{et} \quad g \sim_2 g' \iff \exists h \in H,\, g' = gh$$

sont identiques. On note G/H l'ensemble quotient de G par cette même relation d'équivalence. Cela permet de définir une une unique groupe sur ce quotient.

Théorème 1.1.1 (existence du quotient)**.** *Soit G un groupe et H un sous-groupe distingué dans G. Il existe une unique structure de groupe sur G/H telle que l'application canonique $\pi : G \longrightarrow G/H$ est un morphisme de groupe.*

Théorème 1.1.2 (propriété universelle du quotient)**.** *Soit G et G' des groupes, H un sous-groupe distingué dans G, et soit $\pi : G \longrightarrow G/H$ la projection canonique. Soit $f : G \longrightarrow G'$ un morphisme de groupes tel que $H \subset \ker(f)$. Alors, il existe un unique morphisme de groupe $\tilde{f} : G/H \longrightarrow G'$ tel que $f = \tilde{f} \circ \pi$. Autrement dit, le diagramme suivant commute.*

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\pi}\big\downarrow & \nearrow_{\exists!\tilde{f}} & \\ G/H & & \end{array}$$

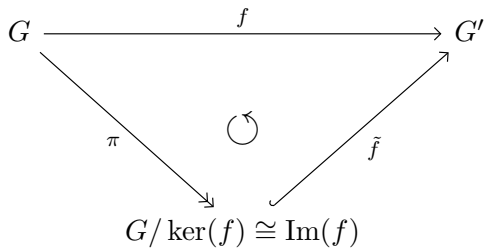
De plus, $\mathrm{Im}(f) = \mathrm{Im}(\tilde{f})$*, et le morphisme composé* $\ker(f) \xrightarrow[\pi_{|\ker(f)}]{} \ker(\tilde{f})$ *induit un isomorphisme entre* $\ker(\tilde{f})$ *et* $\ker(f)/H$ *:* $\ker(\tilde{f}) \xrightarrow{\sim} \ker(f)/H$*.*

Exercice. Il existe une bijection entre l'ensemble des sous-groupes de G contenant H vers les sous-groupes de G/H, dont le mécanisme est $K \longmapsto \pi(K)$. Si K est un sous-groupe de G contenant H, alors $\pi(K) \cong K/H$. Cette bijection préserve les sous-groupes distingués.

Remarques.

— Le théorème qu'une morphisme surjectif $f : G \longrightarrow G'$ donne naissance à un isomorphisme $G/\ker(f) \xrightarrow{\sim} G'$.

— Le théorème implique en général que tout morphisme $f : G \longrightarrow G'$ admet une factorisation unique.



Exemples. Quand on utilise le théorème de quotient, il peut se passer deux choses différentes.

(*i*) Soit k un corps et $G = \mathrm{GL}_n(k)$ et $M = \mathrm{SL}_n(k)$. On "connaît" le quotient G/M. En effet, M est le noyau du déterminant $\det : \mathrm{GL}_n(k) \longrightarrow k^\times$ surjectif de noyau $\mathrm{SL}_n(k)$. Cela induit donc l'isomorphisme

$$\mathrm{GL}_n(k)/\mathrm{SL}_n(k) \xrightarrow[\det]{\sim} k^\times.$$

(*ii*) $G = \mathrm{GL}_n(k)$, et $H = k^\times I_n$. Le quotient est noté $\mathrm{PGL}_n(k) = \mathrm{GL}_n(k)/H$ appelé *groupe projectif linéaire.*

1.2 Théorèmes d'isomorphismes (de NOETHER)

Ce sont des relations entre sous-groupes et quotients.

Théorème 1.2.1. *Les théorèmes d'isomorphismes sont les suivants.*

(i) (Premier théorème d'isomorphisme.) Tout morphisme de groupes $f : G \longrightarrow G'$ induit un isomorphisme $G/\ker(f) \xrightarrow{\sim} \mathrm{Im}(f)$.

(ii) (Deuxième théorème d'isomorphisme.) Pour tout sous-groupe distingué $H \triangleleft G$ et tout sous-groupe $K \subset G$, on a un isomorphisme $K/(H \cap K) \xrightarrow{\sim} (KH)/H$.

(iii) (Troisième théorème d'isomorphisme.) Pour tous sous-groupes distingués $H, K \triangleleft G$ avec $H \subset K$, on a un isomorphisme $G/K \xrightarrow{\sim} (G/H)/(K/H)$.

Lemme 1.2.1 (de ZASSENHAUS, quatrième théorème d'isomorphisme)**.** *Soit G un groupe, et $H' \lhd H$, $K' \lhd K$ des sous-groupes. Alors il existe un isomorphisme*

$$\frac{H'(H \cap K)}{H'(H \cap K')} \cong \frac{K'(H \cap K)}{K'(H' \cap K)}.$$

Chacun étant isomorphe avec

$$\frac{H \cap K}{(H \cap K')(H' \cap K)}.$$

Démonstration. Voir TD.

□

1.3 Groupes simples et facteurs simples de groupes

On rappelle qu'un groupe est dit simple s'il ne possède aucun sous-groupe distingué non trivial.

Définition 1.3.1. *Soit G un groupe. Une suite de composition de G est une suite d'inclusion*

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e_G\}.$$

L'entier n est appelé ***longueur de la suite*** *(le nombre d'inclusions). La suite est de* JORDAN-HÖLDER *si les quotients G_i/G_{i+1} (pour $i \in [\![0, n-1]\!]$) sont simples.*

Remarque. Dans la pratique on remplace, $\rhd$ par $\supset$ puisqu'il est sous-entendu que les groupes sont distingués les uns dans les autres. On considèrera toujours que les inclusions sont strictes (pour éviter les redondances et bien définir la longueur d'une suite). On écrit généralement $\{e_G\} = 1$ à la fin d'une suite de composition.

Exemple. $G = \mathfrak{S}_4 \supset \mathfrak{A}_4 \supset V \cong (\mathbb{Z}/2\mathbb{Z})^2 \supset 1$.

Définition 1.3.2. *Soient $\Sigma : (G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = 1)$ et $\Sigma' : (G \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_p = 1)$ deux suites de compositions. On dit que Σ' est un* ***raffinement*** *de Σ si Σ s'obtient à partir de Σ' en omettant certains sous-groupes. On dit que Σ et Σ' sont* ***équivalentes*** *si et seulement si $n = p$ et les quotients $Q_i = G_i/G_{i+1}$ et $Q'_j = H_j/H_{j+1}$ à isomorphisme et permutations des indices près.*

Théorème 1.3.1 (SCHREIER)**.** *Deux suites de compositions Σ_1 et Σ_2 de G possèdent des raffinements Σ'_1 et Σ'_2 équivalents.*

Démonstration. Soit $\Sigma_1 : (G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{n-1} = 1)$ et $\Sigma_2 : (G \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_{p-1} = 1)$. Pour tout $i \in [\![1, n]\!]$ et $j \in [\![1, p]\!]$, on pose $G_0 = H_0 = G$, ainsi que

$$G_{i,j} = G_i(G_{i-1} \cap H_j) \quad \text{et} \quad H_{j,i} = H_j(H_{j-1} \cap G_i)$$

(ce sont bien des groupes car $G_i \triangleleft G_{i-1}$ et $H_j \triangleleft H_{j-1}$ et distingués les uns dans les autres). Cela permet de raffiner Σ_1 et Σ_2 en intercalant p inclusions entre G_{i-1} et G_i de la sorte

$$G_{i-1} \supset G_{i,1} \supset \cdots \supset G_{i,p} \supset G_i \quad \text{et} \quad H_{j-1} \supset H_{j,1} \supset \cdots \supset H_{j,p} \supset G_j.$$

On peut conclure car le lemme de Zassenhaus assure que ces deux suites sont équivalentes. □

Théorème 1.3.2 (Jordan-Hölder)**.** *Soit G un groupe possédant une suite de* Jordan-Hölder *notée Σ_0.*

(i) Toute suite de composition strictement décroissante admet un raffinement qui est une suite de Jordan-Hölder*.*

(ii) Deux suites de Jordan-Hölder *de G sont équivalentes.*

Remarque. Les groupes finis vérifient l'hypothèse car une suite de G (où G est fini) a une longueur bornée par la quantité $\lceil \log_2 |G| \rceil \leq |G|$. Si Σ est de longueur n maximale, chaque G_i/G_{i+1} est simple car sinon, la préimage $\tilde{H} = \pi^{-1}(H)$ où $\pi : G_i \longrightarrow G_i/G_{i+1}$ d'un sous-groupe distingué $H \subset G_i/G_{i+1}$ non trivial rallongerait la suite Σ.

Démonstration. Soit Σ une suite de Jordan-Hölder de G.

(i) Soit Σ une suite de composition strictement décroissante. D'après le théorème de Schreier, il existe des raffinements Σ_1 de Σ et Σ_2 de Σ_0 équivalents ($\Sigma_1 \sim \Sigma_2$). Puisque Σ_0 est une suite de Jordan-Hölder, on a $\Sigma_2 = \Sigma_0$, donc $\Sigma_1 \sim \Sigma_0$.

(ii) Soit Σ_1 une suite de Jordan-Hölder et Σ' et Σ'' des raffinements respectivement de Σ_1 et Σ_0 qu'on suppose équivalents. Alors, $\Sigma'' = \Sigma_0$ et donc $\Sigma_1 \sim \Sigma'' = \Sigma_0$. Toutes les suites de Jordan-Hölder sont équivalentes à Σ_0.

□

Définition 1.3.3. *Si G possède une suite de* Jordan-Hölder*, la liste des quotients de cette suite est appelée* ***liste des facteurs de* Jordan-Hölder *de*** *G.*

Remarque. Les $Q_i = G_i/G_{i+1}$ sont des sous-quotients de G (*i.e* des quotients d'un sous-groupe de G).

1.4 Groupes résolubles

Définition 1.4.1. *Soit G un groupe. On appelle sous-groupe dérivé de G le sous-groupe engendré par les commutateurs $[x, y] = xyx^{-1}y^{-1}$ $(x, y \in G)$. On le note $D(G)$.*

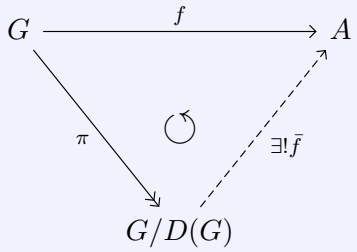
Remarque. L'ensemble des commutateurs n'est pas stable par produit en général. En revanche, le plus petit ordre d'un groupe fini dont l'ensemble des commutateurs n'est pas un groupe est 96. Plus exactement, il y a deux groupes d'ordre 96 non isomorphes tels que l'ensemble des commutateurs n'est pas un groupe. Pour plus de détails sur ces groupes, voir ici.

Proposition 1.4.1. *On a sur le groupe dérivé les propriétés suivantes.*

(i) $D(G)$ *est un sous-groupe distingué de* G*.*

(ii) $D(G) = \{e_G\}$ *si et seulement si* G *est abélien.*

(iii) Le quotient $G^{ab} = G/D(G)$ *est abélien. Il est tel que pour tout groupe abélien* A *et tout morphisme* $f : G \longrightarrow A$*, il existe un unique morphisme* $\bar{f} : G/D(G) \longrightarrow A$ *tel que* $f = \bar{f} \circ \pi$*.*



(iv) Si H *est un sous-groupe de* G *contenant* $D(G)$*. Alors,* G/H *est abélien.*

Démonstration. (i) $D(G)$ est stable pour automorphisme de G. En particulier, il est stable par automorphisme intérieur de G.

(iv) On a une bijection entre les groupes de G contenant $D(G)$ et les sous-groupes de $G/D(G)$. □

Remarques.

— G^{ab} est appelé *abélianisé* de G.

— Les groupes $H \subset Z(G)$ sont toujours distingués. On verra pour les groupes $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$ que les seuls sous-groupes distingués sont exactement ceux contenus dans le centre, ou ceux contenant le groupe dérivé.

Définition 1.4.2. *On appelle* ***suite dérivée*** *de* G *la suite définie par* $G_0 = G$ *et* $G_{i+1} = D(G_i)$*, i.e la suite*

$$G \supset D(G) \supset D^2(G) \supset \cdots \supset \cdots$$

On dit que G *est* ***résoluble*** *lorsque cette suite est stationnaire à* 1*. Dans ce cas, sa longueur est alors appelée* ***indice de résolubilité*** *de* G*.*

Exemples.

— $\mathfrak{S}_5 \supset \mathfrak{A}_5 \supset \mathfrak{A}_5 \supset \cdots$ stationne mais pas à 1.

— $\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset V \supset 1$ où V est le groupe de Klein.

Proposition 1.4.2. *Pour un groupe* G*, les assertions suivantes sont équivalentes.*

(i) G *est résoluble ;*

(ii) G *possède une suite de composition à quotients abéliens.*

Si de plus G *possède une suite de* Jordan-Hölder*, ces conditions sont aussi équivalentes à la condition suivante.*

(iii) Les facteurs de Jordan-Hölder *sont abéliens.*

Démonstration. — $(i) \implies (ii)$. La suite $G \supset D(G) \supset D^2(G) \supset \cdots \supset D^n(G) = 1$ est une suite de compositions à quotients abéliens.

— $(ii) \implies (i)$. Soit $G \supset G_1 \supset G_2 \supset \cdots \supset G_n = 1$ une suite de composition à quotients abéliens de G. On remarque par récurrence que $D^i(G) \subset G_i$ pour tout $i \in [\![1, n]\!]$ car G_i/G_{i+1} est abélien. Ainsi, $D^n(G) \subset G_n = 1$ donc G est résoluble.

□

Proposition 1.4.3. *On a les propriétés suivantes.*

(i) Tout sous-groupe et tout quotient d'un groupe résoluble est résoluble.

(ii) Si H est distingué dans G, alors G est résoluble si et seulement si H et G/H le sont.

(iii) Un groupe simple est résoluble si et seulement s'il est fini, cyclique, d'ordre premier.

Démonstration. (i) Si $H \subset G$, alors $D(H) \subset D(G)$, donc si $D^n(G) = 1$, alors $D^n(H) = 1$. Pour le deuxième point, supposons H distingué dans G. Soit $\pi : G \longrightarrow G/H$, alors on observe que $D(G/H) = \pi(D(G))$. Par récurrence, on arrive au fait que $D^n(G/H) = \pi(D^n(G)) = 1$.

□

Exemples. Quelques exemples de groupes résolubles.

— Les groupes abéliens ;

— le groupe $\mathfrak{S}_4$;

— les groupes diédraux (groupes $\mathbb{D}_n$ des isométries planes du n-gone régulier) ;

— le groupe affine de $\mathbb{R}$, *i.e* le groupe des transformations de la forme $f_{a,b} : \mathbb{R} \to \mathbb{R}, x \mapsto ax+b$ où $(a, b) \in \mathbb{R}^* \times \mathbb{R}$. On a ici

$$\mathrm{Aff}(\mathbb{R}) \supset \underbrace{\{f_{1,b} \,|\, b \in \mathbb{R}\}}_{\cong(\mathbb{R},+)} \supset 1$$

et $\mathrm{Aff}(\mathbb{R})/\{f_{1,b} \,|\, b \in \mathbb{R}\} \cong \mathbb{R}^*$.

Proposition 1.4.4. *Soit k un corps commutatif. Alors, le groupe $T_n(k)$ des matrices triangulaires supérieures est résoluble.*

Démonstration. Trop de matrices pour que j'ai le courage de l'écrire.

□

1.5 Actions de groupes

Définition 1.5.1. *Une action (ou opération) d'un groupe G sur un ensemble X est la donnée d'une application*

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

telle que

(i) pour tout $x \in X$, $e_G \cdot x = x$;

(ii) pour tout $x \in X$, et $g, h \in G$, $(gh) \cdot x = g \cdot (h \cdot x)$.

Remarques.

— Plus précisément, on parle ici d'action *à gauche*.

— L'application est une fonction de deux variables. Si on fixe la variable $g \in G$, on obtient une application $X \to X$, $x \mapsto g \cdot x$. On la note souvent g par souci de simplicité. C'est une bijection d'inverse g^{-1} grâce aux axiomes (i) et (ii).

— Il est équivalent de définir une action de groupe comme la donnée d'un morphisme de groupe $G \longrightarrow \mathfrak{S}_X$.

Terminologie.

— Si X est un espace topologique, et chaque $g : X \longrightarrow X$ est un homéomorphisme, alors on dit que G agît sur X par homéomorphismes.

— Si X est un k-espace vectoriel, et $g : X \longrightarrow X$ est un automorphisme k-linéaire, alors on dit que G agît sur X linéairement (ou par automorphisme k-linéaire).

Remarques (encore). Si l'on fixe cette fois-ci la variable $x \in X$, on obtient une application $ev_x : G \to X$, $g \mapsto gx$. L'étude d'injectivité et surjectivité de cette nous mène aux définitions suivantes.

Définition 1.5.2 (stabilisateur)**.** *Soit $x \in X$. On appelle **stabilisateur** de x dans Gle sous-groupe*

$$G_x = \{g \in G \,|\, gx = x\}.$$

Remarques.

— Le stabilisateur mesure le défaut d'injectivité de ev_x.

— G_x n'est pas distingué dans G en général.

Proposition 1.5.1. *Soit $x \in X$, alors l'application $ev_x : G \longrightarrow X$ est injective si et seulement si $G_x = \{e_G\}$.*

Démonstration. Soient $(g_1, g_2) \in G^2$. Alors, $g_1x = g_2x$ *si et seulement si* $(g_2^{-1}g_1)(x) = x$. C'est encore équivalent à demander que $g_2^{-1}g_1 \in G_x$. On conclut donc facilement sur le résultat.

□

Définition 1.5.3 (orbite)**.** *Soit $x \in X$. On appelle **orbite** de x l'image de ev_x, i.e*

$$\mathcal{O}(x) = \{gx \,|\, g \in G\}.$$

Remarque. L'orbite mesure le défaut de *surjectivité* de ev_x. Cette application est surjective *si et seulement si* $\mathcal{O}(x) = X$. On définit la relation d'équivalence $\sim$ sur X pour tout $x, y \in X$ par

$$x \sim y \iff \exists g \in G,\, y = gx \iff \mathcal{O}(x) = \mathcal{O}(y).$$

On en déduit que les orbites partitionnent X.

Théorème 1.5.1 (relation stabilisateur-orbite)**.** *Soit $x \in X$. L'application $ev_x : G \longrightarrow X$ induit une bijection*

$$\begin{array}{ccc} G/G_x & \longrightarrow & O(x) \\ gG_x & \longmapsto & gx. \end{array}$$

Remarque. Cette bijection n'est absolument pas un isomorphisme, puisque G/G_x n'est pas nécessairement un groupe. Ici, G/G_x est seulement un quotient ensembliste.

Démonstration. Notons Φ cette application, et montrons qu'elle est bien définie. Soit $h_1, h_2 \in G$ tels que $h_1 G_x = h_2 G_x$. Il existe donc $g \in G_x$ tel que $h_1 = h_2 g$. Alors, $h_1 x = h_2 g x = h_2 x$. Montrons maintenant que Φ est injective (elle est clairement surjective). Soit $gG_x, hG_x \in G/G_x$ tels que $gx = hx$. Alors, $h^{-1}gx = x$ donc $h^{-1}g \in G_x$. On en conclut que $gG_x = hG_x$.

□

Exemples.

- Par définition, $G = \mathfrak{S}_n$ agît sur $[\![1, n]\!]$. Le stabilisateur de $i \in [\![1, n]\!]$ est l'ensemble des permutations pour lesquelles i est un point fixe. Ainsi, G_i est isomorphe à $\mathfrak{S}_{n-1}$.
- Soit $\sigma \in \mathfrak{S}_n$ fixé. Alors, le groupe $H = \langle \sigma \rangle$ agît (par restriction) sur $[\![1, n]\!]$, et la partition de $[\![1, n]\!]$ en H-orbites mène à la décomposition de σ en cycles à support disjoints. Les orbites sont les supports des cycles.
- Le groupe $G = \mathrm{GL}_n(k)$ agît sur $X = k^n$ par automorphismes linéaires : $g \cdot x = gx \in k^n$. Il y a deux orbites : $\mathcal{O}(0_{k^n})$ et $\mathcal{O}(x)$, pour tout $x \in k^n$ non nul.
- Ce même groupe agît aussi sur l'ensemble des sous-espaces vectoriels de k^n, avec $g \cdot F = g(F)$. Puisque g est toujours un automorphisme, alors cette action préserve la dimension (*i.e* que $\dim F = \dim g(F)$). De plus, si F_1 et F_2 sont deux d-plans de k^n, on peut trouver $g \in \mathrm{GL}_n(k)$ tel que $F_2 = g(F_1)$. Pour cela, on prend des bases $\mathcal{B}_1 = (e_1, \ldots, e_d, e_{d+1}, \ldots, e_n)$ et $\mathcal{B}_2 = (f_1, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de k^n obtenus en complétants les bases de F_1 et F_2, et en définissant $g(e_i) = f_i$ pour tout $i \in [\![1, d]\!]$. Les orbites de $\mathrm{GL}_n(k)$ agissant sur l'ensemble des sous-espaces sont paramétrées par la dimension. Ce sont les $\mathrm{Gr}(d, n)$ (sous-espaces de k^n de dimension d). On appelle cette orbite la *grassmanienne* des d-plans dans k^n.

1.6 Extensions et produit semi-direct

L'étude des groupes finis se fait selon une stratégie en deux étapes. D'abord, on classifie les groupes simples (problème de la *classification*), puis on cherche à comprendre, étant donnés N et Q deux groupes, quels sont tous les groupes G ayant N comme sous-groupe distingué, dont le quotient G/N est isomorphe à Q. On dit alors que G est une extension de Q par N.

1.6.1 Produit semi-direct interne

Définition 1.6.1. *Soit G un groupe, et H, N deux sous-groupes de G, où N est **distingué** dans G. On dit que G est produit semi-direct (PSD) de H par N si $NH = G$, et $N \cap H = \{e_G\}$.*

Remarque.

— Dans ce cas, tout élément $g \in G$ peut s'écrire ($NH = G$) de manière unique ($N \cap H = \{e_G\}$) sous la forme $g = nh$ avec $(n, h) \in N \times H$. On note $G = N \rtimes H$.

— Si $g_1 = n_1 h_1$, et $g_2 = n_2 h_2$, on peut décomposer $g_1 g_2$ sous la forme en écrivant

$$g_1 g_2 = n_1 h_1 n_2 h_2 = \underbrace{n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\in N}}_{\in N} \underbrace{h_1 h_2}_{\in H}.$$

— On voit que l'application $\pi : G \to H$, $g = nh \mapsto h$ est un morphisme de groupes surjectif (car $h = \pi(e_G \cdot h)$) de noyau N. Le groupe G est alors une extension de G par N.

Proposition 1.6.1. *Soient N et H des sous groupes de G, où N est distingué. Alors, les conditions suivantes sont équivalentes.*

(i) H est distingué dans G.

(ii) N centralise H : tout élément de N commute avec tout élément de H.

(iii) L'application $N \times H \to G$, $(n, h) \mapsto nh$ est un isomorphisme de groupes.

Démonstration. — $(i) \implies (ii)$. Soient $n \in N$ et $h \in H$. On a

$$H \ni nhn^{-1} = \underbrace{nhn^{-1}h^{-1}}_{\in N} \underbrace{h}_{\in H}.$$

Par unicité de l'écriture, on a nécessairement $nhn^{-1} = h$, donc $nh = hn$.

— $(ii) \implies (iii)$. Notons φ cet application, puisque (ii) est vrai, il est clair que φ est un morphisme de groupe. Il est injectif, car si $nh = 1$, alors $n = h = 1$ car $H \cap N = 1$. Il est aussi surjectif car $G = NH$.

□

Exemple. On étudie le n-ième groupe diédral $\mathbb{D}_n$ composé des isométries planes du n-gone régulier. Il est engendré par r et s, où r est la rotation d'angle $2\pi/n$ et s la réflexion de droite d'axe (Ox). En effet, il est clair que $\langle r, s\rangle \subset \mathbb{D}_n \subset O_2(\mathbb{R})$. Réciproquement, soit $g \in \mathbb{D}_n$, et A un sommet du n-gone. Alors, $g(A)$ est aussi un sommet, donc $g(A) = r^i(A)$ pour un certain $i \in [\![0, n-1]\!]$ (le sous-groupe $\langle r\rangle$ agît sur l'ensemble des sommets, et n'a qu'une orbite). Posons $h = r^{-i}g$, alors $h(A) = A$. Comme h est une isométrie, alors si $B = r(A)$, $h(B)$ est un sommet voisin de $h(A) = A$. Donc, $h(B) = B$, ou alors c'est un sommet $B' = s(B)$. Posons $k = h$ si $h(B) = B$, ou $k = s^{-1}h$ si $h(B) = B'$. Maintenant, k fixe A et B. Comme de plus $k(0) = 0$, cette isométrie fixe un repère affine $(0, A, B)$, donc $k = \mathrm{id}$.

Ainsi, $g = r^i$ ou $g = r^i s$ donc $g \in \langle r, s\rangle$. On a donc montré qu'un élément $g \in \mathbb{D}_n$ s'écrit de manière unique sous la forme $g = r^i s^\varepsilon$ ($i \in [\![0, n-1]\!]$, $\varepsilon \in \{0, 1\}$). De plus, on a $srs^{-1} = r^{-1}$. En effet, si l'on note $A_0, \ldots, A_n$ les n sommets du n-gone, alors

$$(srs^{-1})(A_0) = (sr)(A_0) = s(A_1) = A_{n-1} = r^{-1}(A_0)$$

et

$$(srs^{-1})(A_1) = (sr)(A_{n-1}) = s(A_0) = A_0 = r^{-1}(A_1).$$

Ainsi, srs^{-1} et r^{-1} sont égales sur le repère $(0, A_0, A_1)$. Cela suffit à montrer que

$$srs^{-1} = r^{-1}.$$

Cette relation implique que $sr^is^{-1} = r^{-i}$. Ainsi, $N := \langle r \rangle \cong \mathbb{Z}/n\mathbb{Z}$ est distingué. On pose $H = \langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}$. On a bien $NH = \mathbb{D}_n$ et $N \cap H = \{1\}$ car $\det(s) = -1$. Ainsi,

$$\mathbb{D}_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}.$$

C'est un produit non direct, et non commutatif. On pourrait définir $\mathbb{D}_n$ de manière abstraite comme un groupe engendré par r et s deux objets tels que r soit d'ordre n, s d'ordre 2, et srs^{-1}.

1.6.2 Produit semi-direct externe

La structure d'un produit semi-direct $G = N \rtimes H$ est entièrement déterminée lorsqu'on connaît N, H, et la manière de commuter les éléments de N et H, *i.e* la formule

$$n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2.$$

Cela revient donc à connaître l'action de H sur N par conjugaison dans G. On peut renverser ce point de vue pour construire G à partir de N, H et φ.

Proposition 1.6.2. *Soit H, N deux groupes, et $\varphi : H \longrightarrow \mathrm{Aut}(N)$ une action de H sur N par automorphisme de groupes.*

(i) L'ensemble $G = N \times H$ muni de la loi de composition interne définie pour tout $(n_1, h_1), (n_2, h_2) \in G$ par

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$$

est un groupe de neutre (e_N, e_H). On le note $N \rtimes_\varphi H$.

(ii) L'ensemble $N' = N \times \{e_H\}$ est un sous-groupe distingué isomorphe à N.

(iii) L'ensemble $H' = \{e_N\} \times H$ est un sous-groupe isomorphe à H.

(iv) Le groupe $G = N \rtimes_\varphi H$ est le produit semi-direct de H' par N', et dans G, l'action de conjugaison de H' sur N' est définie par

$$(e_G, h) \cdot (n, e_H) \cdot (e_G, h)^{-1} = (\varphi(h)(n), e_H).$$

Démonstration. Exercice pour les gens au troisième rang.

□

Définition 1.6.2. *Le groupe $N \rtimes_\varphi H$ ainsi construit est appelé **produit semi-direct externe** de H par N selon l'action φ.*

Exemple. Soit $G = \mathbb{D}_n = \langle r, s \rangle$ avec $r^n = s^2 = 1$ et $srs^{-1} = r^{-1}$. Le groupe $H = \langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}$ agît sur $N = \langle r \rangle \cong \mathbb{Z}/n\mathbb{Z}$ (distingué car d'ordre $|\mathbb{D}_n|/2$) par la formule $srs^{-1} = r^{-1}$. Rappelons que l'application

$$\begin{array}{ccccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) & & \\ k & \longmapsto & m_k : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & & & x & \longmapsto & kx \end{array}$$

est un isomorphisme (où $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ désigne le groupe des automorphismes de *groupe* de $\mathbb{Z}/n\mathbb{Z}$). On en déduit que le groupe diédral est un produit semi-direct externe.

1.6.3 Suites exactes

Définition 1.6.3. *Une suite de morphismes de groupes*

$$\cdots G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow \cdots$$

est dite exacte si pour tout $i \in \mathbb{N}$, $\mathrm{Im}(f_i) = \ker(f_{i+1})$.

Exercice. Montrer que la suite

$$1 \to N \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

est exacte *si et seulement si* i est injectif, p est surjectif, et $\mathrm{Im}(i) = \ker(p)$. Une suite vérifiant l'une des deux conditions est appelée *suite exacte courte*. Cela signifie que l'on a un isomorphisme $G/N \cong Q$ (de G/N vers Q).

Chapitre 2

Groupes symétriques et alternés

2.1 Signature

Soit $n \geq 1$ un entier. On définit une action du groupe $\mathfrak{S}_n$ sur $\mathbb{C}[X_1, \ldots, X_n]$ en posant

$$(\sigma \cdot P)(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Exercice. Vérifier que l'action définie est une action par automorphismes de $\mathbb{C}$-algèbre, *i.e* que l'action est la donnée d'un morphisme

$$\mathfrak{S}_n \longrightarrow \mathrm{Aut}_{\mathbb{C}\text{-alg}}(\mathbb{C}[X_1, \ldots, X_n]).$$

Soit $V_1 = 1$ et $V_n = \prod_{1 \leq i < j \leq n}(X_j - X_i)$ pour $n \geq 2$. C'est le déterminant de la matrice Vandermonde

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \end{pmatrix}$$

Remarquons que $V_3 = (X_2 - X_1)(X_3 - X_1)(X_3 - X_2)$, et que si $\sigma = (1, 2)$, alors $\sigma V_3 = -V_3$.

Proposition 2.1.1. *Pour tout $\sigma \in \mathfrak{S}_n$, il existe un unique $\varepsilon(\sigma) \in \{-1, 1\}$ tel que $\sigma V_n = \varepsilon(\sigma) V_n$. L'application*

$$\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$$

est un morphisme de groupes.

Définition 2.1.1. *Le morphisme σ est appelée la* ***signature****.*

Remarque. $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$ est surjectif dès lors que $n \geq 2$, mais est trivial quand $n = 1$. On peut d'ailleurs définir (lorsque $n \geq 2$) la signature comme l'unique morphisme de groupes non trivial de $\mathfrak{S}_n$ vers $\{-1, 1\}$.

Définition 2.1.2 (groupe alterné)**.** *On appelle groupe alterné d'ordre n le sous-groupe de $\mathfrak{S}_n$, $\mathfrak{A}_n = \ker \varepsilon$.*

Remarque. C'est un sous-groupe distingué d'ordre 2. On a la suite exacte

$$1 \longrightarrow \mathfrak{A}_n \longrightarrow \mathfrak{S}_n \xrightarrow{\varepsilon} \{-1,1\} \longrightarrow 1.$$

2.2 Générateurs de $\mathfrak{S}_n$ et $\mathfrak{A}_n$

Rappels. Par définition du groupe $\mathfrak{S}_n$, il agît sur $[\![1,n]\!]$. Ainsi, pour tout $\sigma \in \mathfrak{S}_n$, le groupe $H = \langle\sigma\rangle$ agît sur $[\![1,n]\!]$ aussi. Les orbites de cette nouvelle action sont de la forme

$$\{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{d-1}(a)\}$$

où d est un diviseur de l'ordre de σ supposé minimal. La partition de $[\![1,n]\!]$ en σ-orbites s'écrit

$$[\![1,n]\!] = \mathcal{O}_{i_1} \sqcup \cdots \sqcup \mathcal{O}_{i_k}$$

où les entiers i_j sont des représentants des orbites de cette partition, avec

$$\mathcal{O}_{i_j} = \{i_j, \sigma(i_j), \sigma^2(i_j), \ldots, \sigma^{d-1}(i_j)\}.$$

Cette observation donne lieu à la décomposition en cycles à supports disjoints [1].

Exercice. Vérifier que $\varepsilon(\sigma) = (-1)^{n-k}$, où k est le nombre d'orbites (qui comprend les orbites ponctuelles, *i.e* à un élément).

Proposition 2.2.1. *On a sur $\mathfrak{S}_n$ les propriétés suivantes.*

(i) $\mathfrak{S}_n$ *est engendré par les cycles.*

(ii) $\mathfrak{S}_n$ *est engendré par les transpositions (i.e les 2-cycles)*

(iii) $\mathfrak{S}_n$ *est engendré par les* $(1,i)$ *(pour* $i \in [\![2,n]\!]$*).*

(iv) $\mathfrak{S}_n$ *est engendré par les* $(i,i+1)$ *(pour* $i \in [\![1,n-1]\!]$*).*

(v) $\mathfrak{S}_n$ *est engendré par le doubleton* $\{(1,2),(1,2,\ldots,n)\}$*.*

Rappel. Si $(a_1,\ldots,a_k)$ est un k-cycle, alors pour tout $\sigma \in \mathfrak{S}_n$,

$$\sigma(a_1,\ldots,a_k)\sigma^{-1} = (\sigma(a_1),\ldots,\sigma(a_k)).$$

Rappelons aussi qu'on appelle support de $\sigma \in \mathfrak{S}_n$ l'ensemble $\{i \in [\![1,n]\!] \mid \sigma(i) \neq i\}$.

Proposition 2.2.2. *On a sur $\mathfrak{A}_n$ les propriétés suivantes.*

(i) $\mathfrak{A}_n$ *est engendré par les k-cycles avec k impair.*

(ii) $\mathfrak{A}_n$ *est engendré par les 3-cycles (lorsque* $n \geq 3$*).*

(iii) $\mathfrak{A}_n$ *est engendré par les 3-cycles (lorsque* $n \geq 3$*) de la forme* $(1,i,j)$

(iv) Si $n > 3$ *est pair (resp. impair), alors* $\mathfrak{A}_n$ *est engendré par* $(1,2,3)$ *et* $(1,2)(3,4,\ldots,n)$ *(resp.* $(1,2,3)$ *et* $(3,4,\ldots,n)$*).*

Proposition 2.2.3. *Si* $n \geq 5$*, les 3-cycles sont conjugués dans* $\mathfrak{A}_n$*.*

1. Un cycle est un permutation avec une seule σ-orbite non réduite à un élément

Démonstration. Cours d'algèbre, D. Perrin, chapitre I proposition 4.10.

□

Remarques. Il existe des contre-exemples lorsque $n \leq 4$. Remarquons aussi que les 3-cycles sont conjugués dans $\mathfrak{A}_n$ mais pas nécessairement dans $\mathfrak{S}_n$.

2.3 Simplicité de $\mathfrak{A}_n$

Théorème 2.3.1. *Si $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.*

Démonstration. Montrons d'abord le résultat suivant : si a et b sont deux éléments de $\mathfrak{A}_5$ d'ordre 5 alors b est conjugué dans $\mathfrak{A}_5$ à a ou à a^2. Notons $a = (a_1\, a_2 \ldots a_5)$ et $b = (b_1\, b_2 \ldots b_5)$, on a alors $a^2 = (a_1\, a_3\, a_5\, a_2\, a_4)$. Soit $\sigma = (a_2\, a_3\, a_5\, a_4)$ le 4-cycle conjuguant a et a^2. Si on suppose que a et b ne sont pas conjugués dans $\mathfrak{A}_n$, alors ils sont conjugués par un permutation τ de signature -1. On a alors $a^2 = \sigma a \sigma^{-1}$ et $a = \tau b \tau^{-1}$, donc $\sigma\tau$ est une permutation de signature 1 conjuguant a^2 et b. Montrons maintenant le résultat principal.

- Pour $n = 5$. $\mathfrak{A}_5$ est un groupe d'ordre 60, en particulier il contient :
  - L'élément neutre ;
  - 15 éléments d'ordre 2 (les éléments d'ordre 2 sont des produits de deux transpositions disjointes : cela revient à choisir 2 éléments parmi 5, puis 2 parmi 3, soit 30 possibilités que l'on divise par 2 pour s'affranchir de l'ordre de multiplication) ;
  - 20 éléments 3-cycles ;
  - 24 éléments d'ordre 5 (pour choisir un 5-cycles, il suffit de choisir l'image de 1, puis l'image de $\sigma(1)$, ..., ce qui donne 4! possibilités (puisqu'on ne peut pas envoyer 1 sur lui-même)).

  Ce qui nous donne bien un total de 60 éléments. On sait que les 3-cycles sont conjugués dans $\mathfrak{A}_n$, il en est de même pour les produits de deux transpositions (la démonstration est la même que pour les 3-cycles et consiste à exhiber la conjugaison). Soit maintenant H un sous-groupe distingué dans $\mathfrak{A}_5$, qu'on suppose non-trivial. Si H contient un élément d'ordre 2 (*resp.* 3), il les contient tous par ce qui précède (car H est stable par conjugaison dans $\mathfrak{A}_n$). Si H contient un élément a d'ordre 5, il contient aussi a^2, mais tout autre élément de $\mathfrak{A}_5$ d'ordre 5 est conjugué à a ou a^2 dans $\mathfrak{A}_5$, donc H contient tous les autres éléments de $\mathfrak{A}_5$ d'ordre 5.

  Or, H ne peut pas contenir qu'un seul de ces trois types d'éléments (en effet $16 = 15 + 1$, $21 = 20 + 1$, et $25 = 24 + 1$ ne divisent pas 60). Donc H est au minimum d'ordre $36 = 20 + 15 + 1$, il est donc d'ordre 60 et $H = \mathfrak{A}_5$.

- Soit $n > 5$. On pose $E = [\![1, n]\!]$. Soit $H \triangleleft \mathfrak{A}_n$ tel que $H \neq \{\mathrm{id}_E\}$. Soit $\sigma \in H$, $\sigma \neq \mathrm{id}_E$. On souhaite en fait se ramener au cas $n = 5$. Soit $\tau \in \mathfrak{A}_n$, et $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$. Si l'on écrit $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$, alors on voit que $\rho \in H$. Mais en écrivant $\rho = \tau(\sigma\tau^{-1}\sigma^{-1})$, on voit que si τ a des points fixes, alors ρ aussi. Plus précisément : $\sigma \neq \mathrm{id}_E$, donc il existe $a \in E$ un point non fixe. On note $b = \sigma(a) \neq a$. Soit $c \in E \backslash \{a, b, \sigma(b)\}$. Soit alors le 3-cycle $\tau = (a\, c\, b)$, on a $\tau^{-1} = (a\, b\, c)$, et soit $\rho = [\tau, \sigma] = (a\, c\, b)(\sigma(a)\, \sigma(b)\, \sigma(c))$. Soit $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$. Puisque $b = \sigma(a)$, on a $\mathrm{card}\, F \leq 5$. Enfin, ρ n'est pas l'identité car $\rho(b) = \tau\sigma(b) \neq b$, car $c = \tau^{-1}(b) \neq \sigma(b)$. De plus, on a $\rho(F) = F$ et $\rho_{|F\backslash E} = \mathrm{id}_{F\backslash E}$. Quitte à rajouter des éléments, on peut supposer $\mathrm{card}\, F = 5$. On va maintenant considérer $\mathfrak{A}(F)$. $\mathfrak{A}(F)$ est clairement isomorphe à $\mathfrak{A}_5$, et se plonge dans $\mathfrak{A}_n$ par l'application :

$$\begin{array}{ccc} \mathfrak{A}_5 & \longrightarrow & \mathfrak{A}_n \\ u & \longmapsto & \overline{u} = \left\{ \begin{array}{ccc} \overline{u}_{|_F} & = & u \\ \overline{u}_{|_{E\setminus F}} & = & \mathrm{id}_{E\setminus F} \end{array} \right. \end{array}$$

Posons $H_0 = \{u \in \mathfrak{A}(F) \,|\, \overline{u} \in H\} = H \cap \mathfrak{A}(F)$. H_0 est clairement distingué dans $\mathfrak{A}(F)$. On sait de plus que $\rho_{|_F} \in H_0$ et $\rho_{|_F} \neq \mathrm{id}_F$. Puisque $\mathfrak{A}(F) \cong \mathfrak{A}_5$ est simple, on voit que $H_0 = \mathfrak{A}(F)$. Soit alors u un 3-cycle de $\mathfrak{A}(F)$. Alors $\overline{u} \in H$ et est un 3-cycle aussi. Or, les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$ et l'engendrent. Puisque H contient un 3-cycle et que c'est un sous-groupe distingué, il va contenir tous les 3-cycles. Donc H contient $\mathfrak{A}_n$. D'où $H = \mathfrak{A}_n$.

□

Chapitre 3

Géométrie vectorielle et affine

3.1 Comment fait-on de la géométrie ?

J'étais en train de manger mon pain au chocolat, le prof a tout dit à l'oral. Tant pis.

3.2 Transitivité des actions

Définition 3.2.1. *Soit G un groupe opérant sur un ensemble X. Cette action est dite*

(i) ***fidèle*** *si le morphisme $G \longrightarrow \mathfrak{S}(G)$ est injectif ;*

(ii) ***libre*** *si tous les stabilisateurs de G_x sont triviaux ;*

(iii) ***transitive*** *si pour tout $x, y \in X$, il existe $g \in G$ tel que $y = gx$.*

(iv) ***simplement transitive*** *si l'action est libre et transitive.*

(v) ***k-transitive*** *(resp. simplement k-transitive) si l'action de G sur $X^k \backslash \Delta_k$ définie par $g(x_1, \dots, x_k) = (gx_1, \dots, gx_k)$ est transitive (resp. simplement transitive), où*

$$\Delta_k = \{(x_1, \dots, x_k) \in X^k \mid \exists i \neq j,\ x_i = x_j\}.$$

Remarques.

— L'action de G sur X est fidèle *si et seulement si*

$$\bigcap_{x \in X} G_x = \{e_G\}.$$

— Une action 1-transitive est une action transitive. De plus, une action est transitive *si et seulement si* elle n'est qu'une seule orbite, *i.e* pour tout $x \in X$, $X = \mathcal{O}(x)$. C'est encore équivalent à dire que pour tout $x \in X$, l'évaluation

$$ev_x : \left| \begin{array}{ccc} G & \longrightarrow & X \\ g & \longmapsto & gx \end{array} \right.$$

est surjective.

— Une action est simplement transitive *si et seulement si* il existe un x tel que ev_x soit bijective. Il est encore équivalente de demander que pour tout $x \in X$, ev_x est bijective.

— Pour agir k-transitivement, le groupe G doit être assez grand. Par exemple, si X et G sont finis et $|X| = n$ alors si l'action est k-transitive, on a nécessairement

$$|G| \geq n(n-1) \cdots (n-k+1).$$

Définition 3.2.2 (espace homogène)**.** *Soit G un groupe opérant sur un ensemble X. On dit que X est un espace homogène (resp. principalement homogène) s'il est non vide, et G agît transitivement (resp. simplement transitivement).*

Exemple.

- L'ensemble des jours de la semaine est un espace principalement homogène sous l'action de $\mathbb{Z}/7\mathbb{Z}$.
- L'ensemble des bases d'un k-espace vectoriel E est un espace principalement homogène sous l'action de $\mathrm{GL}(E)$.
- Une droite affine du plan est un espace principalement homogène sous l'action de $(\mathbb{R}, +)$.
- $\mathbb{S}^1$ est un espace principalement homogène sous l'action de $\mathrm{SO}_2(\mathbb{R})$. On ne peut pas totalement généraliser ce résultat. En effet $\mathbb{S}^n$ est un espace homgène *non principal* sous l'action de $\mathrm{SO}_{n+1}(\mathbb{R})$ dès lors que $n \geq 2$. Les stabilisateurs de cette action sont de la forme $G_x \cong \mathrm{SO}(\mathrm{Vect}(x)^\perp)$.

3.3 Le groupe linéaire et quelques sous-groupes

Soit k un corps, et E un k-espace vectoriel de dimension finie. Remarquons que $\mathrm{GL}(E)$ est de dimension n^2 au sens des sous-variétés. En effet, c'est un ouvert dense de $\mathscr{L}(E)$ (qui est de dimension n^2).

Définition 3.3.1. *Soit $r \geq 1$ et $d = (d_1, \ldots, d_r) \in (\mathbb{N}^*)^r$ avec $d_i \geq 1$ pour tout $i \in [\![1, r]\!]$ et $\sum_{i=1}^r d_i = n$. On appelle décomposition de E de type d la donnée d'un r-uplet sous-espaces $(F_1, \ldots, F_r)$ tels que*

$$E = F_1 \oplus \cdots \oplus F_r$$

et $\dim F_i = d_i$ pour tout $i \in [\![1, r]\!]$. On note $\mathrm{Dec}_d(E)$ l'ensemble des ces décompositions.

Le groupe $\mathrm{GL}(E)$ agît sur $\mathrm{Dec}_d(E)$ *via*

$$g \cdot (F_1, \ldots, F_r) = (g(F_1), \ldots, g(F_r)).$$

Proposition 3.3.1. *Soit $\mathcal{D} = (F_1, \ldots, F_r) \in \mathrm{Dec}_d(E)$. On a les propriétés suivantes.*

(i) Le stabilisateur de $\mathcal{D}$ est

$$G_{\mathcal{D}} = \{g \in \mathrm{GL}(E) \,|\, \forall i \in [\![1, r]\!]\,,\, g(F_i) = F_i\}$$

(ii) L'action est transitive.

Démonstration. (i) Clair.

(ii) Si $\mathcal{D} = (F_1, \ldots, F_r)$ et $\mathcal{D}' = (F'_1, \ldots, F'_r)$ sont deux décompositions de E de type d, on peut choisir des bases pour tout $i \in [\![1, r]\!]$ des bases $(e_{i,j})_{1 \leq j \leq d_i}$ de F_i et $(e'_{i,j})_{1 \leq j \leq d_i}$ de F'_i, alors $\mathcal{B} = (e_{i,j})$ et $\mathcal{B} = (e'_{i,j})$ sont des bases de E. Soit alors $g : E \longrightarrow E$ définie par $g(e_{i,j}) = e'_{i,j}$. Alors, g est une transformation dans $\mathrm{GL}(E)$ telle que $g(\mathcal{D}) = g(\mathcal{D}')$.

□

Remarque. Dans une base telle que $\mathcal{B} = (e_{i,j})$, les éléments de $G_{\mathcal{D}}$ ont pour matrice des matrices triangulaires supérieures par blocs.

Définition 3.3.2. *Soit $r \geq 1$ et $d = (d_1, \ldots, r) \in \mathbb{N}$ avec $d_i \geq 1$ pour tout $i \in [\![1, r]\!]$ et $\sum_{i=1}^{r} d_i = n$. On appelle drapeau de type d une chaîne de sous-espaces $F_1 \subset F_2 \subset \cdots \subset F_r$ telle que $\dim F_i = d_1 + \cdots + d_i$ pour tout $i \in [\![1, r]\!]$. Un drapeau est dit être* ***complet*** *si $d_i = 1$ pour tout $i \in [\![1, r]\!]$.*

Remarque (une différence entre drapeaux complets et incomplets). Pour les drapeaux, dans un base adaptée à un drapeau $\mathcal{D}$

$$\mathcal{D} : F_1 \subset F_2 \subset \cdots \subset F_n = E,$$

le stabilisateur $G_{\mathcal{D}}$ est $\mathrm{T}_n(k)$, l'ensemble des matrices triangulaires supérieures. On a montré dans le chapitre 1 que ce groupe est *résoluble*. Ce n'est pas le cas pour les drapeaux incomplets. Pour s'en convaincre, admettons un résultat ultérieur. Pour tout $n \in \mathbb{N}^*$,

$$D(\mathrm{GL}_n(k)) = D(\mathrm{SL}_n(k)) = \mathrm{SL}_n(k)$$

sauf lorsque $(n, k) \in \{(2, \mathbb{F}_2), (2, \mathbb{F}_3)\}$. Pour $n = 3$, on considère le drapeau $\mathcal{D} = (D \subset E)$, où D est une droite dans un espace vectoriel E de dimension 3. Alors, $G_{\mathcal{D}}$ est l'ensemble des matrice la forme

$$\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,2} \\ 0 & a_{2,2} & a_{2,3} \\ 0 & a_{3,2} & a_{3,3} \end{pmatrix}$$

Or les matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a_{2,2} & a_{2,3} \\ 0 & a_{3,2} & a_{3,3} \end{pmatrix}$$

en font parti, et leur ensemble est isomorphe en tant que groupe à $\mathrm{GL}_2(k)$. Pour tout $i \geq 1$,

$$D^i(G_{\mathcal{D}}) \supset D^i(\mathrm{GL}_2(k)) = \mathrm{SL}_2(k)$$

si $|k| \geq 5$, où $\mathrm{GL}_2(k)$ est vu comme le sous-groupe des matrices de la forme donnée ci-dessus.

3.4 Générateurs de $\mathrm{GL}(E)$ et $\mathrm{SL}(E)$

Pour tout vecteur $a \in E$ et tout forme linéaire $f \in E^*$, on définit une application linéaire

$$u_{a,f} : \left| \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x + f(x)a \end{array} \right.$$

On note par la suite $u := u_{a,f}$.

Lemme 3.4.1. *On a sur u les propriétés suivantes.*

(i) $u \neq \mathrm{id}_E$ si et seulement si a et f sont tous deux non nuls.

(ii) $u \in \mathrm{GL}(E)$ si et seulement si $f(a) \neq -1$.

Démonstration. (*i*) Si $a = 0$ ou $f = 0$, alors $u(x) = x$. Si $a \neq 0$ et $f \neq 0$ alors il existe $x \in E$ tel que $f(x) \neq 0$, donc $u(x) = x + f(x)a \neq x$.

(*ii*) On peut supposer que $f \neq 0$ (sinon $u = \mathrm{id}_E \in \mathrm{GL}(E)$). Ainsi, $H := \ker f$ est un hyperplan. On observe d'abord que pour tout $x \in E$, $u(x) - (1 + f(a))x \in H$ car f envoie cet élément sur 0_E. Soit $x \in E \backslash H$, et $\mathcal{B}$ une base de H telle qu'elle est la concaténation d'une base de H et $de\{x\}$. Alors, la matrice de u est de la forme

$$\mathrm{mat}_B(u) = \left(\begin{array}{c|c} I_{n-1} & * \\ \hline 0 & 1 + f(a) \end{array}\right).$$

En effet, $u_{|H} = \mathrm{id}_H$, et $u(x) = (1 + f(a))x + h$ avec $h \in H$. En en déduit que $\det(u) = 1 + f(a)$, d'où le résultat.

□

Par la suite on supposera toujours que les $u_{a,f}$ vérifient ces conditions.

Définition 3.4.1. *Si $u = u_{a,f}$ est tel que $a \neq 0$, $f \neq 0$, et $f(a) \neq -1$, on appelle droite de u la droite $D = \mathrm{Vect}(a)$ et hyperplan de u l'hyperplan $H = \ker f$.*

Exercice. Si $(a, f), (a', f')$ sont non nuls, alors $u_{a,f} = u_{a',f'}$ si et seulement s'il existe $\lambda \in k^\times$ tel que $(a', f') = (\lambda a, \lambda^{-1} f)$.

Proposition 3.4.1. *Avec les mêmes notations que la définition précédente, les conditions suivantes sont équivalentes.*

(i) *u est diagonalisable.*

(ii) *$D \not\subset H$*

(iii) *$f(a) \neq 0$.*

(iv) *La matrice de u dans une certaine base est*

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & 0 \\ & & \ddots & & \\ & 0 & & 1 & \\ & & & & 1 + f(a) \end{pmatrix}.$$

*Dans ce cas, u est appelée **dilatation** et $\lambda := 1 + f(a)$ est son rapport. Dans le cas contraire, u est appelée **transvection** et sa matrice dans une certaine base est*

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

appelée matrice de transvection.

Démonstration. Comme $u_{|H} = \mathrm{id}_H$, la valeur propre 1 est de multiplicité supérieure ou égale à $n - 1$. La dernière est $1 + f(a)$ car $\det u = 1 + f(a)$.

— Si u est diagonalisable, $1 + f(a) \neq 1$, *i.e* que $f(a) \neq 0$, *i.e* $D \not\subset H$ ce qui se traduit par $\mathrm{Vect}(a) \not\subset \ker f$. Dans ce cas, dans une base $\mathcal{B}$ concaténation d'une base de H et d'un vecteur propre pour $1 + f(a)$. La matrice de u est donc comme indiquée une fois diagonalisée. Enfin l'implication $(iv) \implies (i)$ est claire.

— $(i) \iff (ii) \iff (iii)$: c'est clair d'après le point précédent. Reste à montrer l'équivalence $(i) \iff (iv)$. On a montré dans la démonstration du lemme 3.4.1 que pour tout choix de vecteur $e_n \in E\backslash H$, on définit par récurrence la base $\mathcal{B} = (e_1, \ldots, e_n)$ définie par récurrence par $e_{i-1} = u(e_i) - e_i$. Alors, $(e_1, \ldots, e_{n-1})$ est une base de H. La matrice de u dans cette base aura la forme donnée par l'énoncé. Enfin (iv) implique (i) car cette matrice n'est pas l'identité, et pourtant son spectre se réduit à $\{1\}$. Elle n'est donc pas diagonalisable.

□

Corollaire 3.4.1. *Les transvections sont conjuguées dans* $\mathrm{GL}(E)$.

Remarque. Pour étudier $\mathrm{SL}(E)$, on est en présence d'une famille (les transvections) avec une grande quantité de points fixes sur E, et dont les éléments sont tous conjugués dans $\mathrm{GL}(E)$.

Lemme 3.4.2. *Soit $u \neq \mathrm{id}_E$ une transformation du type précédent (dilatation ou transvection). Soit D sa droite, H son hyperplan, et $g \in \mathrm{GL}(E)$. Alors, gug^{-1} est une transformation du même type que u, de droite $D' = g(D)$, et d'hyperplan $H' = g(H)$.*

Démonstration. Soient $(a, f) \in E \times E^*$ non nul tel que $u = u_{a,f}$. On a $D = \mathrm{Vect}(a)$ et $H = \ker f$. Alors, pour tout $x \in E$,

$$(gug^{-1})(x) = g(u(g^{-1}(x))) = x + f(g^{-1}(x))g(a).$$

La transformation $u' = gug^{-1}$ est du type voulu, avec pour droite $D' = \mathrm{Vect}(g(a)) = g(D)$ et pour hyperplan $H' = \ker f \circ g^{-1} = g(H)$.

□

On peut utiliser les transvections pour déterminer les centres de $\mathrm{GL}(E)$ et $\mathrm{SL}(E)$ avec le lemme suivant.

Lemme 3.4.3. *Un endomorphisme $g : E \longrightarrow E$ qui préserve toutes les droites (i.e que toute droite vectorielle est stable par g) est une homothétie.*

Démonstration. On peut supposer E non réduit à $\{0_E\}$. Soit $e \in E$ un vecteur non nul. Alors, il existe $\lambda \in k$ tel que $g(e) = \lambda e$. Montrons que $g = \lambda \mathrm{id}_E$. Si $\dim E = 1$, c'est clair. Plus généralement, l'égalité tient toujours sur $\mathrm{Vect}(e)$. Si $x \in E\backslash \mathrm{Vect}(e)$, alors il existe $\mu, \nu \in k$ tels que

$$g(e + x) = \mu(e + x) = g(e) + g(x) = \lambda e + \nu x.$$

Puisque la famille $\{e, x\}$ est libre, on en déduit que $\mu = \lambda = \nu$. On en conclue que $g = \lambda \mathrm{id}_E$.

□

Proposition 3.4.2. *On a les résultats suivants.*

(i) Le centre de $\mathrm{GL}(E)$ *est le sous-groupe des homothéties, isomorphe à* $k^\times$.

(ii) Le centre de $\mathrm{SL}(E)$ *est le sous-groupe des éléments de* $\mathrm{GL}(E)$ *de déterminant* 1 *isomorphe à* $\mathbb{U}_n(k)$ *(le groupe des racines n-ièmes de* 1_k*).*

Démonstration. Soit $g \in \mathcal{Z}(\mathrm{GL}(E))$. Puisque g commute avec tous les éléments de $\mathrm{GL}(E)$, il commute avec toutes les transvections. Ainsi, pour tout $u = u_{a,f}$ avec $(a, f) \neq 0$ et $f(a) = 0$, $g = gug^{-1}$. On en déduit que g est à la fois une transvection de droite D et de droite $g(D)$. Ainsi, pour toute droite $D \subset E$, le choix d'une transvection de droite D (pour toute droite, on peut trouver une transvection correspondante) montre que $g(D) = D$. Compte tenu de ce qui précède, le lemme précédent montre que g est une homothétie. Ceci montre donc clairement le point (i). Il montre aussi le point (ii) car $g = \lambda id_E \in \mathrm{SL}(E)$ *si et seulement si* $\lambda^n = 1$.

□

Théorème 3.4.1. *Les transvections engendrent* $\mathrm{SL}(E)$*. Les dilatations et transvections engendrent* $\mathrm{GL}(E)$*.*

On utilisera pour cela deux lemmes.

Lemme 3.4.4. *Soit* $x \in E$ *un élément non nul, et* H_1*,* H_2 *deux hyperplans distincts de* E *tels que* $x \notin H_1 \cup H_2$*. Alors, il existe une transvection* $u \in \mathrm{SL}(E)$ *telle que* $u(x) = x$ *et* $u(H_1) = H_2$*.*

Démonstration. L'hypothèse sur les plans impose que $n = \dim E \geq 2$, et $\dim(H_1 \cap H_2) = n-2$ par la formule de Grassman. Soit $H = H_1 \cap H_2 \neq \mathrm{Vect}(x)$. C'est un hyperplan différent de H_1 et H_2. En particulier, $H + H_1 = E = H + H_2$. Soit $z \in H_2 \backslash H$, qu'on écrit $z = a + y$ avec $(a, y) \in H \times H_1$. On remarque que z n'est pas élément de H, donc y non plus. Ainsi, il existe une unique forme $f \in E^*$ telle que $H = \ker f$ et donc $f(y) = 1$. Soit $u : H \to H$, $t \mapsto t + f(t)a$. Par définition de f, on a $u_{|H} = \mathrm{id}_H$ et en particulier $f(x) = x$. De plus, $u(y) = y + f(y)a = y + a = z \in H_2$. De plus, $u(H_1 \cap H_2) \subset H_1 \cap H_2$, donc $u(H_1) = H_2$.

□

Lemme 3.4.5. *Supposons* $\dim E \geq 2$ *et soient* $x, y \in E\backslash\{0_E\}$*. Alors, il existe* $u \in \mathrm{GL}(E)$*, produit d'une ou deux transvections, tel que* $u(x) = y$*.*

Démonstration. Supposons x et y non colinéaires, alors $y - x$ et x ne le sont pas non plus. Ainsi, il existe un hyperplan qui contient $y - x$ mais pas x. Soit $f \in E^*$ une forme linéaire telle que $H = \ker f$ et $f(x) = 1$. Si $u(t) = t + f(t)a$ avec $a = y - x$, alors $u(x) = x + f(x)a = x + a = y$.

Si maintenant x et y sont colinéaires, puisque $\dim E \geq 2$, il existe $z \in \mathrm{Vect}(x)$, soit donc un tel z. En utilisant ce que nous avons déjà montré dans le cas non colinéaire, il existe u_1 et u_2 deux transvections telles que $u_1(x) = z$ et $u_2(z) = y$. On pose alors $u = u_2 u_1$.

□

Démonstration (du théorème). Montrons le résultat par récurrence sur $n = \dim E$.

— Si $n = 1$, alors $\mathrm{SL}(E) = \{\mathrm{id}_E\}$: il n'y a rien à démontrer.

— Soit $n \geq 2$, supposons le théorème vraie pour tout espace de dimension $n-1$ et soit E un k-espace vectoriel de dimension n. Soit $v \in \mathrm{SL}(E)$. Montrons que $v \in T$, où T est l'espace engendré par les transvections. Pour cela, il est possible de remplacer v par vu ou uv, où u est une transvection (que l'on va déterminer). Soit $x \in E$ un élément non nul. Selon le second lemme, il existe $u \in \mathrm{GL}(E)$ un produit d'une ou deux transvections telle que $u(x) = v(x)$, donc $(u^{-1}v)(x)$. Quitte à remplacer v par $u^{-1}v$, on peut supposer que $v(x) = x$. Soit un hyperplan H tel que $x \notin H$ (cet hyperplan existe puisque $\dim E \geq 2$). Si $v(H) \neq H$, il existe d'après le premier lemme, il existe une transvection u telle que $u(x) = x$ et $u(H) = v(H)$. Ainsi, $(u^{-1}v)(H) = H$ et $(u^{-1}v)(x) = x$. On peut donc supposer dans tous les cas que $v(x) = x$ et $v(H) = H$. Par hypothèse de récurrence appliquée à $v_{|H}$, on sait que $v_{|H}$ est un produit de transvections sur H : on note

$$v_{|H} = u_{1,H} \cdots u_{d,H}.$$

On a donc que v a une matrice de la forme

$$\left(\begin{array}{c|c} v_{|H} & 0 \\ \hline 0 & 1 \end{array}\right)$$

où une base de H a été complétée avec x. Pour tout $i \in [\![1, d]\!]$, on peut étendre $u_{i,H}$ en une transvection de H en posant $u_{i|H} = u_{i,H}$ et $u_i(x) = x$. On a donc

$$v_{|H} = u_{1,H} \circ \cdots \circ u_{d,H} = (u_1 \circ \cdots \circ u_d)_{|H}$$

et

$$v(x) = (u_1 \circ \cdots \circ u_d)(x)$$

Ainsi, $v = u_1 \cdots u_d$.

□

3.5 Conjugaison des transvections, commutateurs

Proposition 3.5.1. *Deux transvections sont conjugués dans* $\mathrm{GL}(E)$. *Si* $\dim E \geq 3$, *elles le sont aussi dans* $\mathrm{SL}(E)$.

Démonstration. Soit $n = \dim E$. On a vu que toute transvection a pour matrice dans une certaine base

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

Puisque les transvections ont même matrice *modulo* un changement de base (donc sont conjuguées dans $\mathrm{GL}_n(k)$ par une matrice de passage), elles sont conjuguées dans $\mathrm{GL}(E)$. Si $n \geq 3$, et soient

u et v deux transvections. Soit $g \in \mathrm{GL}(E)$ tel que $v = gug^{-1}$, et soit $\mathcal{B}$ une base de E dans laquelle

$$\mathrm{mat}_{\mathcal{B}}(v) = \begin{pmatrix} 1 & & & & & \\ & 1 & & & 0 & \\ & & \ddots & & & \\ & & & 1 & & \\ & 0 & & & 1 & 1 \\ & & & & 0 & 1 \end{pmatrix}.$$

Soit $\lambda = \det g$ et $s \in \mathrm{GL}(E)$ tel que

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

(c'est possible car $\dim E \geq 3$). On a $sv = vs$ et $\det s = \lambda^{-1}$. Donc $\det(sg) = 1$, et

$$v = svs^{-1} = sgug^{-1}s^{-1} = (sg)u(sg)^{-1}.$$

□

Proposition 3.5.2 (conjugaison dans un espace plan)**.** *(i) Dans $\mathrm{SL}_2(k)$, toute transposition est conjuguée à une matrice*

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

avec $\lambda \in k^\times$.

(ii) Les matrices

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \textit{et} \quad \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$

sont conjuguées dans $\mathrm{SL}_2(k)$ si et seulement si $\lambda/\mu \in (k^\times)^2$, i.e que λ/μ est un carré de $k^\times$.

On en déduit le calcul des sous-groupes dérivés.

Théorème 3.5.1. *On a sur les groupes dérivés de $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$ les cas suivants.*

(i) On a $D(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k)$ sauf dans le cas $(n = 2, k = \mathbb{F}_2)$.

(ii) On a $D(\mathrm{SL}_n(k)) = \mathrm{SL}_n(k)$ sauf dans les deux $(n = 2, k = \mathbb{F}_2)$ et $(n = 2, k = \mathbb{F}_3)$.

Démonstration. Si $n \geq 3$, il suffit de montrer que $D(\mathrm{GL}_n(k))$ et $D(\mathrm{SL}_n(k))$ contiennent une transvection. Rappelons qu'une matrice de transvections élémentaires est une matrice $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ pour $i \neq j$ avec $\lambda \in k$. Pour tout $i \neq$, l'application $(k, +) \to \mathrm{SL}(E)$, $\lambda \mapsto T_{i,j}(\lambda)$ est un morphisme de groupes. Puisque $n \geq 3$, on peut les matrices de transvections éléments $h = T_{1,2}(1)$ et $h = T_{2,3}(1)$. On a

$$\begin{aligned} ghg^{-1}h^{-1} &= (I_n + E_{1,2})(I_n - E_{1,2})(I_n - E_{2,3}) \\ &= (I + E_{1,2} + E_{2,3} + E_{1,3})(I - E_{1,2} - E_{2,3} + E_{1,3}) \\ &= I_n + E_{1,3} \end{aligned}$$

qui est une matrice de transvection.

□

Cas exceptionnels.

— $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}(\mathbb{F}_2) \cong \mathfrak{S}_3$ dont le groupe dérivé est $\mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$.

— $\mathrm{SL}_2(\mathbb{F}_3)$ est une groupe de cardinal $24 = 8 \times 3$ non isomorphe à $\mathfrak{S}_4$, donc le groupe dérivé est son unique 2-Sylow (donc distingué) est isomorphe au groupe des quaternions

$$\mathbb{H} = \{-1, 1, -i, i, -j, j, -k, k\}$$

avec $i^2 = j^2 = k^2 = -1$, $jk = -kj = i$, $ik = -ki = j$, et $ij = -ij = k$.

3.6 Simplicité de $\mathrm{PSL}(E)$

Définition 3.6.1. *On appelle* ***groupe projectif linéaire*** *le groupe*

$$\mathrm{PGL}(E) = \mathrm{GL}(E)/\mathcal{Z}(\mathrm{GL}(E)).$$

De même, on définit

$$\mathrm{PSL}(E) = \mathrm{SL}(E)/\mathcal{Z}(\mathrm{SL}(E)).$$

Remarque. Le mot *projectif* vient que les homothéties sont exactement les transformations linéaires qui préservent toutes les droites, ce qui exprime le fait que le centre de $\mathrm{GL}(E)$ est le noyau de l'action de $k^\times$ sur $\mathrm{GL}(E)$. De manière générale, on définit le groupe projectif d'un espace vectoriel comme

$$\mathbb{P}(E) = E/k^\times$$

où l'action de $k^\times$ sur E est définie par $\lambda \cdot x = \lambda x$ pour tout $(\lambda, x) \in k^\times \times E$.

Théorème 3.6.1. *Le groupe* $\mathrm{PSL}(E)$ *est simple sauf dans les cas* $(n = 2, k = \mathbb{F}_2)$ *et* $(n = 2, k = \mathbb{F}_3)$.

Démonstration. Supposons $n \geq 3$, et soit $\bar{N} \triangleleft \mathrm{PSL}(E)$ un groupe non trivial. Montrons que $\bar{N} = \mathrm{PSL}(E)$, et soit N sa préimage par la surjection canonique $\mathrm{SL}(E) \longrightarrow \mathrm{PSL}(E)$. Cette préimage est distingué dans $\mathrm{SL}(E)$ et contient $\mathcal{Z}(\mathrm{SL}(E))$. Puisque cette application est surjective, montrons que $N = \mathrm{PSL}(E)$. Il suffit de trouver une transvection dans N. Soit donc $\sigma \in N$ avec $\sigma \notin \mathbb{Z}(\mathrm{SL}(E))$. Il existe donc $a \in E$, tel $b := \sigma(a) \notin \mathrm{Vect}(a)$. Soit τ une transvection de droite $\mathrm{Vect}(a)$, et

$$\rho := \sigma\tau\sigma^{-1}\tau^{-1}.$$

Soit $H \subset E$ un hyperplan contenant $\mathrm{Vect}(a, b)$ (c'est un 2-plan car $n \geq 3$). On a trois propriétés.

(*i*) $\rho \in N$ et diffère de l'identité. En effet,

$$\rho = \underbrace{\sigma}_{\in N}\underbrace{(\tau\sigma^{-1}\tau^{-1})}_{\in N} \in N$$

(*ii*) Pour tout $x \in E$, $\rho(x) - x \in H$. En effet, si l'on note $\tau(x) = x + f(x)a$ alors $\tau^{-1}(x) = x - f(x)a$ donc

$$(\sigma\tau\sigma^{-1})(x) = x + f(\sigma^{-1}(x))\sigma(a).$$

Ainsi,

$$\rho(x) = (\sigma\tau\sigma^{-1})(\tau^{-1}(x)) = x - f(x)a + f(\sigma^{-1}(x - f(x)a))b$$

ce qui est la somme de x et d'un élément de $\mathrm{Vect}(a, b)$. Ainsi,

$$\rho(x) - x \in \mathrm{Vect}(a, b) \subset H.$$

(*iii*) $\rho(H) = H$. En effet, si $x \in H$, alors $h := \rho(x) - x \in H$, donc $\rho(x) = x + h \in H$.

On distingue maintenant deux cas.

— *Cas 1.* S'il existe une transvection d'hyperplan H tel que $u\rho \neq \rho u$ alors on pose

$$v = \underbrace{\rho u^{-1}}_{\in N}\underbrace{\rho^{-1}u^{-1}}_{\in N} \in N$$

qui diffère de l'identité. Ainsi, v est produit de $\rho u\rho^{-1}$ (avec $\rho(H) = H$) et u^{-1} qui est une transvection d'hyperplan H. Or, on vérifie que le produit de deux transvections de même hyperplan H en est encore une.

— *Cas 2.* Si non, ρ commute avec toutes les transvections d'hyperplan H. Soit $f \in E^*$ une forme linéaire telle que $H = \ker f$, $c \in H$, et $u(x) = u_{c,f}(x) = x + f(x)c$ pour tout $x \in E$. Par hypothèse, $\rho u = u\rho$ donc $f(x)\rho(c) = f(\rho(x))c$ pour tout $x \in E$. Si $x \notin H$, on a $\rho(x) - x \in H$, donc $f(\rho(x)) = f(x) \neq 0$ puisque $x \notin H$. L'égalité $f(x)\rho(c) = f(x)c$ implique que $\rho(c) = c$ pour tout $c \in H$. On a donc montré que $\rho_{|H} = \mathrm{id}_H$. Puisque $\det\rho = 1$, on en déduit que ρ est une transvection.

□

3.7 Cas des corps finis

Soit $k = \mathbb{F}_q$ un corps fini avec $q = p^\alpha$ une puissance d'un nombre premier. On rappelle que $\mathrm{car}\,\mathbb{F}_q = p$.

Proposition 3.7.1. *On a les résultats suivants. Si $n \geq 1$,*

— $|\,\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-2})(q^n - q^{n-1})$;

— $|\,\mathrm{SL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-2})q^{n-1} = |\,\mathrm{PGL}(\mathbb{F}_q)|$;

— $|\,\mathrm{PSL}(\mathbb{F}_q)| = |\,\mathrm{SL}_n(\mathbb{F}_q)|/d$ *où* $d = n \wedge q - 1 = \mathrm{card}\,\mu_n(\mathbb{F}_q)$.

Démonstration. (*i*) $\mathrm{GL}_n(\mathbb{F}_q)$ est bijection avec les bases de $\mathbb{F}_q^n$. Si $(e_1, \ldots, e_n)$ est une telle base, alors il y a $q^n - 1$ choix possible (tout sauf $0_{\mathbb{F}_q^n}$). Pour e_2, on peut tout choisir sauf les éléments de la droite portée par e_1 ce qui donne $q^n - q$ choix. En itérant, on peut choisir e_{k+1} dans $\mathbb{F}_q \setminus \mathrm{Vect}(e_1, \ldots, e_k)$ qui est de cardinal $q^n - q^k$.

(*ii*) On a les suites exactes

$$1 \longrightarrow \mathrm{SL}_n(\mathbb{F}_q) \longrightarrow \mathrm{GL}_n(\mathbb{F}_q) \xrightarrow{\det} \mathbb{F}_q^\times \longrightarrow 1$$

et

$$1 \longrightarrow \underbrace{\mathcal{Z}(\mathrm{GL}_n(\mathbb{F}_q))}_{\cong \mathbb{F}_q^\times} \longrightarrow \mathrm{GL}_n(\mathbb{F}_q) \longrightarrow \mathrm{PGL}_n(\mathbb{F}_q) \longrightarrow 1.$$

(*iii*) Exercice.

□

Ces résultats permettent entre autres de montrer un théorème de Sylow.

Théorème 3.7.1 (Sylow)**.** *Tout groupe fini G d'ordre $n = p^s m$ avec $p \not| m$ possède un sous-groupe de cardinal p^s (appelé p-Sylow).*

Lemme 3.7.1. *Sous les mêmes hypothèses que le théorème précédent, et si H possède un p-Sylow S, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Démonstration. G agît par translation à gauche sur G/S l'ensembles des aS, *i.e* que $g\cdot(aS) = gaS$ pour tout $g \in G$. Remarquons que G/S est de cardinal m premier avec p. Le stabilisateur de aS pour l'action de G est

$$\mathrm{Stab}_G(aS) = aSa^{-1}.$$

En effet, si $g \in \mathrm{Stab}(aS)$, alors $gaS = aS$ donc $ga \in gaS = aS$, donc $g \in aSa^{-1}$. Réciproquement, si $g \in aSa^{-1}$, alors il existe $s \in S$ tel que $g = asa^{-1}$ donc $gaS = asa^{-1} = asS = aS$. Par restriction H agît sir G/S et $\mathrm{Stab}_H(aS) = H \cap aSa^{-1}$. La partition en orbite de l'action de H donne

$$G/S = \sum_{i=1}^{d} |\mathcal{O}_H(a_i)| = \sum_{i=1}^{d} \frac{|H|}{|H \cap a_i S a_i^{-1}|}$$

Or $|G/S|$ est premier avec p donc il existe $i_0 \in [\![1, d]\!]$ tel que $\frac{|H|}{|H \cap a_{i_0} S a_{i_0}^{-1}|}$ est premier avec p. Puisque $H \cap a_{i_0} S a_{i_0}^{-1}$ est un p-groupe d'indice dans H premier avec p, c'est un p-Sylow de H.

□

Chapitre 4

Géométries projective et affine

4.1 Structure de l'espace

En mécanique classique, l'espace où l'on vit est un $\mathbb{R}$-espace affine de dimension 3.

4.2 Espaces affines et sous-espaces affines

Soit k un corps commutatif.

4.2.1 Définitions

Définition 4.2.1. *Un k-espace affine de dimension est un ensemble non vide $\mathcal{E}$ sur lequel agît **transitivement** un espace vectoriel E*

Remarques et notations.

- Les éléments de $\mathcal{E}$ sont appelés *points* et ceux de E *vecteurs*.
- E est appelé la *direction* de $\mathcal{E}$, parfois noté $\vec{\mathcal{E}}$.
- On note l'action $E \times \mathcal{E} \to \mathcal{E}$, $(u, A) \mapsto A+u$. Ainsi, les axiomes d'action s'écrivent "$A+0 = A$" et "$A + (u + v) = (A + u) + v$".
- Pour tout $u \in \mathcal{E}$, l'application $\tau_u : \mathcal{E} \to \mathcal{E}$, $A \mapsto A + u$ est appelée *translation de vecteur u*.

L'action de E sur $\mathcal{E}$ est simplement transitive (*i.e* libre et transitive). Ainsi, pour tout $A, B \in \mathcal{E}$, il existe un unique $u \in E$ tel que $B = A + U$. Ce vecteur est noté $\overrightarrow{AB}$. On a donc toujours la formule

$$A + \overrightarrow{AB} = B.$$

Proposition 4.2.1 (relation de Chasles)**.** *Pour tout A, B et $C \in \mathcal{E}$, on a*

$$\overrightarrow{AB} + \overrightarrow{BC} = \vec{AC}.$$

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

□

On peut aussi définir ces espaces d'une manière équivalente.

Définition 4.2.2 (équivalente d'un k-espace affine)**.** *Soit E un k-espace vectoriel. Un k-espace affine de direction E est un ensemble non vide $\mathcal{E}$ muni d'une application*

$$\begin{array}{ccc} \mathcal{E} \times \mathcal{E} & \longrightarrow & \mathcal{E} \\ (A, B) & \longmapsto & \overrightarrow{AB} \end{array}$$

telle que

(i) pour tout $A \in \mathcal{E}$, l'application $\mathcal{E} \to E$, $M \mapsto \overrightarrow{AM}$ est bijective ;

(ii) pour tout $(A, B) \in \mathcal{E}^2$, on a $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

Exemples.

(*i*) Soit $(a, b) \in \mathbb{R}^2$ un vecteur non nul. Alors on peut voir $D = \mathbb{R}(a, b) \subset \mathbb{R}^2$ comme la direction d'une droite dans l'espace.

(*ii*) Si $\mathcal{E} = E$, alors E peut être vu comme un k-espace affine en opérant sur lui-même *via* $E \times E \to E$, $(u, v) \mapsto u + v$.

Définition 4.2.3. *Si $\mathcal{E}$ est un espace affine sur lequel agît un espace vectoriel E, on appelle dimension d'un l'espace affine $\mathcal{E}$ la dimension de E.*

4.2.2 Vectorialisation en un point.

Soit $\mathcal{E}$ un espace affine de dimension $\dim E$, et soit $A \in \mathcal{E}$. La bijection $f_A : E \to \mathcal{E}$, $u \mapsto A+u$ permet de munir $\mathcal{E}$ d'une structure d'espace vectoriel noté $\mathcal{E}_A$ par transport de structure de la manière suivante. C'est-à-dire que l'on pose

$$M +_{\mathcal{E}_A} N = f_A(f_A^{-1}(M) +_E f_A^{-1}(N)) \quad \text{et} \quad \lambda \cdot_{\mathcal{E}_A} = f_A(\lambda \cdot_E f_A^{-1}(M))$$

pour tout $M, N \in \mathcal{E}$ et $\lambda \in k$. Par construction, on observe que f_A^{-1} est un isomorphisme de k-espaces vectoriels.

Proposition 4.2.2. *L'application $f_A : E \longrightarrow \mathcal{E}_A$ est un isomorphisme de k-espaces vectoriels.*

Remarque. $\mathcal{E}_A$ est appelé vectorialisé de $\mathcal{E}$ en A.

4.2.3 Sous-espaces affines

Proposition 4.2.3. *Soit $\mathcal{E}$ un k-espace affine, $\mathcal{F} \subset \mathcal{E}$ et $A \in \mathcal{F}$. Sont équivalents.*

(i) L'ensemble $\left\{\overrightarrow{AM} \,|\, M \in \mathcal{F}\right\}$ est un sous-espace vectoriel de E.

(ii) $\mathcal{F}$ est une orbite d'une sous-espace vectoriel F de E, i.e qu'il existe F un sous-espace vectoriel de E tel que $\mathcal{F} = \mathcal{O}_F(A) = \{A + u \,|\, u \in F\}$.

(iii) $\mathcal{F}$ est un sous-k-espace vectoriel du vectorialisé $\mathcal{E}_A$.

Démonstration. — (*i*) $\implies$ (*ii*). Soit $F = \left\{\overrightarrow{AM} \,|\, M \in \mathcal{F}\right\}$ qu'on suppose être un sous-espace vectoriel de E. Soit $M \in \mathcal{F}$, alors $\overrightarrow{AM} \in F$ et $M = A + \overrightarrow{AM} \in \mathcal{O}_F(A)$. Réciproquement si

$M = A + u \in \mathcal{O}_F(A)$ avec $u \in F$, alors $u = \overrightarrow{AM} \in F$. S'il existe $M' \in \mathcal{F}$ tel que $u = \overrightarrow{AM'}$, donc $M = A + u = A + \overrightarrow{AM'} = M' \in \mathcal{F}$.

— $(ii) \implies (iii)$. Par définition de F, on a $f_A(F) = \mathcal{F}$ qui est donc l'image par l'isomorphisme linéaire $f_A : E \longrightarrow \mathcal{E}_A$ du sous-espace vectoriel F. Ainsi, $\mathcal{F}$ est un sous-espace vectoriel de $\mathcal{E}_A$.

— $(iii) \implies (i)$. On a $\left\{\overrightarrow{AM} \,|\, M \in \mathbb{F}\right\} = f_A^{-1}(\mathcal{F})$, donc si $\mathcal{F} \subset \mathcal{E}_A$ est un sous-espace vectoriel alors $\left\{\overrightarrow{AM} \,|\, M \in \mathbb{F}\right\}$ en est un de E.

□

Définition 4.2.4. *On appelle sous-espace affine de $\mathcal{E}$ une partie non vide $\mathcal{F} \subset \mathcal{E}$ vérifiant ces conditions équivalentes.*

Remarque. F est alors la direction de $\mathcal{F}$.

Définition 4.2.5. *Soit $\mathcal{F}_1, \mathcal{F}_2$ deux sous-espaces affines de $\mathcal{E}$. On dit que $\mathcal{F}_1$ et $\mathcal{F}_2$ sont parallèles si $F_1 = F_2$ (i.e s'ils sont de même direction). Plus généralement, on dit que $\mathcal{F}_1$ est faiblement parallèle à $\mathcal{F}_2$ si $F_1 \subset F_2$.*

Remarques (exercices).

(i) Deux sous-espaces affines parallèles sont égaux ou disjoints.

(ii) Un sous-espace affine faiblement parallèle à un autre y est inclus ou en est disjoint.

(iii) Si $\mathcal{F} \subset \mathcal{E}$ est un sous-espace affine et $A \in \mathcal{E}$, alors il existe un unique sous-espace affine $\mathcal{F} \subset \mathcal{E}$ parallèle à $\mathcal{F}$ contenant A.

4.3 Applications affines, groupe affine

Proposition 4.3.1. *Soient $\mathcal{E}$ et $\mathcal{F}$ deux espaces affines de directions respectives E et F, et soit $f : \mathcal{E} \longrightarrow \mathcal{F}$ une application. Sont équivalents.*

— *Il existe une application linéaire $\varphi : E \longrightarrow F$ telle que pour tout $A \in \mathcal{E}$ et $u \in E$, $f(A + u) = f(A) + \varphi(u)$.*

— *Il existe $A \in \mathcal{E}$ tel que l'application*

$$\varphi_A \left| \begin{array}{ccc} E & \longrightarrow & F \\ u & \longmapsto & \overrightarrow{f(A)f(A+u)} \end{array} \right.$$

est linéaire.

— *Pour tout $A \in \mathcal{E}$, l'application φ_A est linaire.*

Démonstration. La démonstration est en exercice. Observons néanmoins que φ_A ne dépend pas de A. En effet, si $B \in \mathcal{E}$ et $B = A + v$ avec $v = \overrightarrow{AB} \in E$, alors

$$f(B) + \overrightarrow{f(A)f(A+u)} = f(A) + \varphi_A(V) + \overrightarrow{f(A)f(A+u)} = f(A+u) + \varphi_A(V)$$

mais aussi,

$$f(B) = \varphi_A(u) = f(A) + \varphi(u) + \varphi(v) = f(A+v) + \varphi(u) = f(B+u).$$

Ainsi, $\varphi_A(u) = \varphi_B(u)$.

□

Remarque. Dans la seconde définition (équivalente) des espaces affines, les trois propriétés équivalentes énoncés ci-dessus signifie qu'on a le diagramme commutatif suivant

$$\begin{array}{ccc} \mathcal{E}^2 & \longrightarrow & E \\ \downarrow & \circlearrowleft & \downarrow \exists!\varphi \\ \mathcal{F}^2 & \longrightarrow & F \end{array}$$

où l'application $\mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{F} \times \mathcal{F}$ est définie par $(x, y) \longmapsto (f(x), f(y))$.

Définition 4.3.1. *On appelle application affine de $\mathcal{E}$ dans $\mathcal{F}$ toute application vérifiant l'une des conditions de la proposition précédente. L'application $\varphi : E \longrightarrow F$ est appelée partie linéaire (ou linéarisée) de f notée $\vec{f}$ ou* lin(f).

Proposition 4.3.2. *Soit $f : \mathcal{E} \longrightarrow \mathcal{F}$ une application affine. Alors f est injective (resp. surjective, resp. bijective) si et seulement si sa partie linéaire est injective (resp. surjective, resp. bijective).*

Démonstration. Montrons uniquement l'équivalence des injectivités. Supposons f injective et soit $u \in E$ tel $\varphi(u) = 0$ et soit $A \in \mathcal{E}$. Alors, $f(A+u) = f(A)+\varphi(u) = f(A)$ donc $A+u = A$, *i.e* $u = 0$. Supposons maintenant φ injective et soit $A, B \in \mathcal{E}$ tels que $f(A) = f(B)$. Soit $u = \overrightarrow{AB}$. Alors, $B = A + u$ et donc $f(B) = f(A) + \varphi(u)$. Ainsi, $\varphi(u) = 0$ par injectivité de φ et donc $A = B$.

□

Exemples.

(*i*) Les translation $\tau_u : \mathcal{E} \to \mathcal{E}$, $A \mapsto A + u$ sont des applications affines. Dans ce cas, sa linéarisée est l'identité.

(*ii*) Si $\mathcal{E} = E$ et si $(a, b) \in \mathrm{GL}(E) \times E$, alors l'application $E \to E$, $x \mapsto a(x) + b$ est une application affine, dont la linéarisée est a.

(*iii*) *Homothéties.* Soit $O \in \mathcal{E}$ et $\lambda \in k$. L'application $h_{O,\lambda}\mathcal{E} \to \mathcal{E}$, $M \mapsto O + \lambda\overrightarrow{OM}|$ est une application linéaire. Elle est telle que pour tout $M \in \mathcal{E}$, $h(M)$ est l'unique point N tel que $\overrightarrow{ON} = \lambda\overrightarrow{OM}$.

Exercices.

— Soit $f : \mathcal{E} \longrightarrow \mathcal{F}$ et $g : \mathcal{F} \longrightarrow \mathcal{G}$ deux applications affines de parties linéaires respectives φ et ψ. Alors, $g \circ f : \mathcal{E} \longrightarrow \mathcal{G}$ est une application affine de partie linéaire $\psi \circ \varphi$.

— Si f est une application affine bijective de partie linéaire φ, alors f^{-1} est affine de partie linéaire φ^{-1}.

Définition 4.3.2. *Soit $\mathcal{E}$ un k-espace affine. On appelle groupe affine de $\mathcal{E}$ (noté* $\mathrm{GA}(\mathcal{E})$*) l'ensemble des applications affines bijectives $\mathcal{E} \longrightarrow \mathcal{E}$ muni de la composition, et de neutre* id_E.

Proposition 4.3.3. *On a les propriétés suivantes.*

(i) L'ensemble $T(\mathcal{E})$ des translation de $\mathcal{E}$ est sous-groupe distingué de $\mathrm{GA}(\mathcal{E})$ isomorphe à la direction de E via l'application

$$\tau : \left| \begin{array}{ccc} E & \longrightarrow & T(\mathcal{E}) \\ u & \longmapsto & \tau_u. \end{array} \right.$$

(ii) Le morphisme

$$\mathrm{lin} : \left| \begin{array}{ccc} \mathrm{GA}(\mathcal{E}) & \longrightarrow & \mathrm{GL}(E) \\ f & \longmapsto & \overrightarrow{f} = \mathrm{lin}(f) \end{array} \right.$$

est surjectif de noyau $T(\mathcal{E})$. On a donc une suite exacte

$$1 \longrightarrow T(\mathcal{E}) \longrightarrow \mathrm{GA}(\mathcal{E}) \longrightarrow \mathrm{GL}(E) \longrightarrow 1.$$

(iii) Pour tout $A \in \mathcal{E}$ l'ensemble des applications affines qui fixent A

$$\mathrm{GA}(\mathcal{E})_A = \{f \in \mathrm{GA}(\mathcal{E}) \,|\, f(A) = A\}$$

est sous-groupe de $\mathrm{GA}(\mathcal{E})$ isomorphe à $\mathrm{GL}(E)$ via

$$\mathrm{GA}(\mathcal{E})_A \hookrightarrow \mathrm{GA}(\mathcal{E}) \longrightarrow \mathrm{GL}(E).$$

De plus, on a le produit semi-direct

$$\mathrm{GA}(\mathcal{E}) = T(\mathcal{E}) \rtimes \mathrm{GA}(\mathcal{E})_A.$$

Démonstration. (i) Soit $f : \mathcal{E} \longrightarrow \mathcal{E}$ tel que $\overrightarrow{f} = \mathrm{id}_E$, *i.e* que pour tout $(A, u) \in \mathcal{E} \times E$, $f(A+u) = f(A)+u$. Alors, $u_0 := \overrightarrow{Af(A)}$ ne dépend pas de A. On a alors que $f(A) = A+u_0$ pour tout $A \in \mathcal{E}$, *i.e* que $f = \tau_{u_0}$. Réciproquement, on a vu que si $\sigma \in T(\mathcal{E})$ alors $\mathrm{lin}(\sigma) = \mathrm{id}_E$. On a donc montré le point (i).

(ii) Montrons que

$$\mathrm{GA}(\mathcal{E})_A \hookrightarrow \mathrm{GA}(\mathcal{E}) \longrightarrow \mathrm{GL}(E)$$

est un isomorphisme. Soit $\varphi \in \mathrm{GL}(E)$, on définit $f : \mathcal{E} \to \mathcal{E}$ tel que $f(A + u) = A + \varphi(u)$ pour tout $(A, u) \in \mathcal{E} \times E$. C'est une application affine fixant A et telle que $\mathrm{lin}(f) = \varphi$. Soit maintenant $f \in \mathrm{GA}(\mathcal{E})$ telle que $f(A) = A$ et $\varphi := \mathrm{lin}(f) = \mathrm{id}_E$. Alors, pour tout $u \in E$, $\varphi(A + u) = f(A) + \varphi(u) = A + u$ donc $f = \mathrm{id}_E$.

(iii) Si $f \in T(\mathcal{E}) \cap \mathrm{GA}(\mathcal{E})_A$, alors $f(A) = A + u$ mais f fixe A donc $u = 0$, *i.e* que $f = \mathrm{id}_{\mathcal{E}}$. Ainsi, $T(\mathcal{E}) \cap \mathrm{GA}(\mathcal{E})_A = \{\mathrm{id}_{\mathcal{E}}\}$

□

On termine avec un exemple d'application affine : les projections.

Lemme 4.3.1. *Soit $\mathcal{E}$ un espace affine, et $\mathcal{F}$ et $\mathcal{G}$ des sous-espaces affines de direction respective E, F, et G. Si $E = F \oplus G$, alors, $\mathcal{F} \cap \mathcal{G}$ est un singleton.*

Démonstration. Soient $A \in \mathcal{F}$ et $B \in \mathcal{G}$ deux points, et $u = \overrightarrow{AB} = v + w$, où $(v, w) \in F \times G$. On a donc $A + v = B - w \in \mathcal{F} \cap \mathcal{G}$. Soit maintenant $C, C' \in \mathcal{F} \cap \mathcal{G}$, et $u = \overrightarrow{CC'}$. On a que $u \in F \cap G = \{0\}$, donc $C = C'$.

□

Proposition 4.3.4. *Soit $\mathcal{E}$ un espace affine, et $\mathcal{F}$ et $\mathcal{G}$ des sous-espaces affines de direction respective E, F, et G. On suppose de plus que $E = F \oplus G$. Soit $M \in \mathcal{E}$, et soit $\pi(M)$ l'unique point dans l'intersection de $\mathcal{F}$ et de l'unique sous-espace affine parallèle à $\mathcal{G}$ passant par M. Alors, $\pi : \mathcal{E} \longrightarrow \mathcal{E}$ est une application affine appelée projection sur $\mathcal{F}$ parallèlement à $\mathcal{G}$, de partie linéaire $p \in \mathscr{L}(E)$ la projection sur F parallèlement à G.*

4.4 Deux théorèmes classiques et le simplexe régulier

Le théorème de Thalès porte sur des rapports de longueurs (dans un corps k quelconque) qui ont un sens grâce au concept suivant.

Définition 4.4.1. *Soit $\mathcal{D}$ une droite affine (i.e un espace affine de dimension 1). Soit u un vecteur directeur de sa direction D (i.e $D = ku$). Si $A, B \in \mathcal{D}$, on appelle norme algébrique de (A, B) relativement à u le scalaire λ tel que $\overrightarrow{AB} = \lambda u$.*

Notation. On note $\overline{AB}$, et alors $\overrightarrow{AB} = \overline{AB}u$.

Remarque. Une norme algébrique est quasi-entièrement dépendante de u. En effet, pour tout $\alpha \in k^\times$, et $u' = \alpha u$. Alors, $\overrightarrow{AB} = \lambda u = \lambda\alpha^{-1}u'$. C'est-à-dire que la mesure algébrique relativement à u' est multipliée par α^{-1}. En revanche, des rapports de mesures algébriques $\frac{\overline{AB}}{\overline{AC}}$ où $A, B, C \in \mathcal{D}$ et $A \neq C$, sont bien définies indépendamment de u.

Théorème 4.4.1 (Thalès)**.** *Soient d, d', et d'' trois droites parallèles dans un plan affine $\mathcal{E}$. Soient $\mathcal{D}_1$ et $\mathcal{D}_2$ deux droites non parallèles à d. Soit $A_i = \mathcal{D}_i \cap d$, $A'_i = \mathcal{D}_i \cap d'$, et $A''_i = \mathcal{D}_i \cap d''$ pour tout $i \in \{1, 2\}$. Alors,*

$$\frac{\overline{A_1A''_1}}{\overline{A_1A'_1}} = \frac{\overline{A_2A''_2}}{\overline{A_2A'_2}}.$$

Réciproquement si $B \in \mathcal{D}_1$ est tel que

$$\frac{\overline{A_1B}}{\overline{A_1A'_1}} = \frac{\overline{A_1B}}{\overline{A_2A'_2}},$$

alors $B \in d''$ et $B = A''_1$.

Remarque. Contrairement au théorème de collège, $\mathcal{D}_1$ et $\mathcal{D}_2$ ne sont pas nécessairement concourantes. Cependant, le théorème de Thalès du collège où $\mathcal{D}_1$ et $\mathcal{D}_2$ sont concourants en sont une conséquence.

Démonstration. Soit π la projection sur $\mathcal{D}_2$ parallèlement à d. On a $\pi(1_A) = A_2$, $\pi(A'_1) = A'_2$, et $\pi(A''_1) = A''_2$). Soit p sa partie linéaire, et soit $\lambda = \frac{\overline{A_1A''_1}}{\overline{A_1A'_1}}$, de sorte que $\overrightarrow{A_1A''_1} = \lambda\overrightarrow{A_1A'_1}$. On a alors

$$p\left(\overrightarrow{A_1A_1''}\right) = p\left(\lambda\overrightarrow{A_1A_1'}\right) = \lambda p\left(\overrightarrow{A_1A_1'}\right) = \lambda p\left(\overrightarrow{A_2A_2'}\right).$$

Or, $p\left(\overrightarrow{A_1A_1''}\right) = \overrightarrow{A_2A_2''}$. On a donc que $\lambda = \frac{\overline{A_2A_2''}}{\overline{A_2A_2'}}$. Pour la réciproque, on a

$$\overrightarrow{A_1B} = \frac{\overline{A_2A_2''}}{\overline{A_2A_2'}}\overrightarrow{A_1A_1'} = \frac{\overline{A_1A_1''}}{\overline{A_1A_1'}}\overrightarrow{A_1A_1'} = \overrightarrow{A_1A_1''}.$$

On en déduit que

$$B = A_1 + \overrightarrow{A_1B} = A_1 + \overrightarrow{A_1A_1''} = A_1''.$$

□

Théorème 4.4.2 (Pappus). *Soient $\mathcal{D}, \mathcal{D}'$ deux droites d'un plan $\mathcal{E}$, et $A, B, C \in \mathcal{D}$, $A', B', C' \in \mathcal{D}'$. On suppose que les droites (AB') et $(A'B)$ sont parallèles, ainsi que les droites (BC') et $(B'C)$. Alors, (AC') et $(A'C)$ sont parallèles.*

Démonstration.
— *Premier cas.* Si $\mathcal{D}$ et $\mathcal{D}'$ sont concourantes en $O \in \mathcal{E}$ (donc non parallèles), soit φ l'homothétie de centre O qui envoie A sur B et ψ l'homothétie de centre O qui envoie B sur C . D'après Thalès, φ envoie B' sur A' et ψ envoie C' sur B'. Alors, $\psi \circ \varphi$ envoie A sur C. Or, deux homothéties de même centre commutent, donc $\psi \circ \varphi = \varphi \circ \psi$, qui envoie donc C' sur A'. Selon la réciproque du théorème de Thalès, (AC') et $(A'C)$ sont parallèles (puisque l'on a trouvé une homothétie $\chi = \varphi\psi = \psi\varphi$ qui envoie A sur C et C' sur A').

— *Second cas.* Si $\mathcal{D}$ et $\mathcal{D}'$ sont parallèles, on utilise des translations au lieu d'homothéties, ainsi que le fait que les translation commutent entre elles.

□

On termine par une application de la géométrie affine à la géométrie euclidienne : la construction du simplexe régulier de dimension n et le calcul de ses isométries.

Définition 4.4.2. *Soit $k = \mathbb{R}$. Un espace affine euclidien de dimension finie est un espace affine réel $\mathcal{E}$ dont la direction E est muni d'un produit scalaire.*

Remarque. Sur un tel espace, on peut définir une distance par

$$d(A, B) = \left\|\overrightarrow{AB}\right\|_2$$

pour tout $A, B \in \mathcal{E}$. On peut alors définir la notion d'isométrie : une isométrie $f : \mathcal{E} \longrightarrow \mathcal{E}$ est une application telle que pour tout $A, B \in \mathcal{E}$, $d(f(A), f(B)) = d(A, B)$. Il équivalent de dire que $\overrightarrow{f} \in \mathcal{O}(E)$. Compte tenu du théorème de structure de $\mathrm{GA}(\mathcal{E})$, le groupe affine euclidien de $\mathcal{E}$ (qui est le groupe des isométries) est

$$\mathrm{GAE}(\mathcal{E}) \cong T(\mathcal{E}) \rtimes \mathcal{O}(E)$$

(remarquons qu'une isométrie est nécessairement bijective).

Théorème 4.4.3. *Soit $\mathcal{E} = E = \mathbb{R}^n$ l'espace affine euclidien standard de dimension n. Alors, il existe un polyèdre Σ_n non dégénéré (i.e non inclus dans un sous-espace affine strict) dont toutes les diagonales A_iA_j ont longueur 1. De plus, Σ_n est unique à isométrie près. On l'appelle* ***simplexe régulier*** *de dimension n (ou simplexe régulier de dimension n). Toutes ses faces de dimension $i \leq n$ sont des i-simples réguliers. Le groupe $\mathrm{Iso}_{\mathbb{R}^n}(\Sigma_n)$ de ses isométries affines est isomorphe à $\mathfrak{S}_{n+1}$.*

Remarque. Il n'est pas facile de définir un polyhèdre. Pour les polyhèdres convexes, c'est plus facile (c'est l'enveloppe convexe d'un nombre fini de points). Pour plus de précisions sur les polyhèdres, on pourra voir le *Mathématiques d'école* de Daniel Perrin aux éditions Cassini, ou le *Géométrie* de Marcel Berger aux éditions Nathan.

Démonstration. Soit $\mathcal{E}' = \mathbb{R}^{n+1}$, $(e_0, \dots, e_n)$ la base canonique de $\mathbb{R}^{n+1}$, et $A_i = (0, \dots, 1, 0, \dots) = O + e_i$. Soit $\mathcal{H}$ un hyperplan affine contenant $A_0, \dots, A_n$ d'équation $x_0 + \cdots + x_n = 1$. C'est l'unique hyperplan affine passant par A_0 de direction $H = \{(x_0, \dots, x_n) \in \mathbb{R}^{n+1} \mid x_0 + \cdots + x_n = 0\}$. On note $\Sigma_n \subset \mathcal{H}$ le polyhèdre de sommets $A_0, \dots, A_n$. On a les longueurs $A_iA_j = \sqrt{2}$ dès lors que $i \neq j$, et les injections

$$\begin{array}{ccc} \mathfrak{S}_{n+1} & \longrightarrow & \mathrm{Iso}(\Sigma_n) \\ \sigma & \longmapsto & M_\sigma = (\delta_{i,\sigma(j)})_{i,j} \end{array}$$

et

$$\begin{array}{ccc} \mathrm{Iso}(\Sigma_n) & \longrightarrow & \mathfrak{S}_{n+1} \\ f & \longmapsto & f_{\{A_0,\dots,A_n\}} \end{array}$$

est un morphisme de groupes injectif car si $f(A_i) = A_i$ pour tout $i \in [\![1, n]\!]$, alors f fixe A_0 et $\overrightarrow{A_0A_1}, \dots, \overrightarrow{A_0A_n}$ qui forment une base de la direction H de $\mathcal{H}$, donc $f = \mathrm{id}_{\mathcal{H}}$. Finalement, $\mathrm{Iso}_{\mathcal{H}}(\Sigma_n) \cong \mathfrak{S}_{n+1}$ pour des raisons de cardinalité. Enfin, on pose $\Sigma'_n = \frac{1}{\sqrt{2}}\Sigma_n$.

□

4.5 Espaces projectifs, sous-espaces

Définition 4.5.1. *L'espace projectif associé à un espace vectoriel E est l'ensemble $\mathbb{P}(E)$ des droites vectorielles de E. Sa dimension est l'entier $\dim \mathbb{P}(E) = \dim E - 1$.*

Puisque toute droite peut être engendrée par un vecteur directeur non nul, on a une surjection

$$\begin{array}{ccc} E\backslash\{0\} & \longrightarrow & \mathbb{P}(E) \\ u & \longmapsto & \mathrm{Vect}(u). \end{array}$$

Or, $k^\times$ agît librement sur $E\backslash\{0\}$ et les orbites de cette action sont les droites de E. Elle induit donc une bijection $(E\backslash\{0\})/k^\times \longrightarrow \mathbb{P}(E)$.

Remarques.

— Si k est fini de cardinal q et $n = \dim \mathbb{P}(E)$, alors on trouve

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

— Lorsque $k \in \{\mathbb{R}, \mathbb{C}\}$, on peut munir $E\backslash\{0\}$ de la topologie euclidienne et le quotient de la topologie quotient.

Définition 4.5.2. *Soit X et Y des ensembles, et $f : X \longrightarrow Y$ une application surjective. La relation $\mathscr{R}$ définie pour tout $x_1, x_2 \in X$ par*

$$x_1 \mathscr{R} x_2 \iff f(x_1) = f(x_2)$$

est une relation d'équivalence. Supposons X muni d'une topologie. On appelle topologie quotient la topologie sur Y telle que $V \subset Y$ est ouvert si et seulement si $f^{-1}(V)$.

Remarque. Le nom de cette topologie vient du fait qu'une surjection $f : X \longrightarrow Y$ induit une bijection de $X/\sim$ sur Y.

Proposition 4.5.1. *Soit $k \in \{\mathbb{R}, \mathbb{C}\}$ et E un k-espace vectoriel. L'espace projectif $\mathbb{P}(E)$ est compact. Si E est euclidien (resp. hermitien) et $S(E)$ désigne la sphère unité pour la norme associée, alors la surjection $\pi : E\backslash\{0\}\mathbb{P}(E)$ induit un homéomorphisme de $S(E)/\{-1, 1\}$ vers $\mathbb{P}(E)$ (resp. de $S(E)/\mathbb{U}$ vers $\mathbb{P}(E)$ où $\mathbb{U}$ est le cercle unité).*

Remarque. Il faut comprendre ici que $S(E)/\{-1, 1\}$ est la sphère unité où les points antipodaux sont identifiés (lorsque $k = \mathbb{R}$), et que $S(E)/\mathbb{U}$ est la sphère unité où deux points sont identifiés lorsqu'ils ont pour rapport un complexe de norme 1.

Démonstration. Si $k = \mathbb{R}$, puisque chaque droite de E peut être engendrée par exactement deux vecteurs directeurs de norme 1 opposés l'un l'autre (on peut en fait voir $S(E)$ comme l'ensemble des demi-droites de E). Montrons maintenant que $\mathbb{P}(E)$ est séparé. Soient $y, y' \in \mathbb{P}(E)$ deux points distincts, et soient $x, x' \in S(E)$ deux vecteurs directeurs normés pour les droites $D = \pi^{-1}(y) \cup \{0\}$ et $D' = \pi^{-1}(y') \cup \{0\}$. Puisque la sphère $S(E)$ est séparée, il existe deux ouverts disjoints W et W' dans $S(E)$ contenant respectivement x et x'. Les cônes engendrés $U = \mathbb{R}^*W$ et $U' = \mathbb{R}^*W'$ sont des ouverts disjoints de $E\backslash\{0\}$ et on a $U = \pi^{-1}(\pi(U))$ et $U' = \pi^{-1}(\pi(U'))$. Ceci montre que $V = \pi(U)$ et $V' = \pi(U')$ sont deux ouverts disjoints dans $\mathbb{P}(E)$ (muni de la topologie quotient) contenant respectivement y et y'. Enfin, l'application $S(E) \hookrightarrow E\backslash\{0\} \xrightarrow{\pi} \mathbb{P}(E)$ est continue comme composée d'applications continues, donc $\mathbb{P}(E)$ est séparé et image continue du compact $S(E)$, il est donc compact.

Lorsque $k = \mathbb{C}$, le raisonnement est le même avec la différence que deux vecteurs directeurs normés d'une droite complexe diffèrent par un complexe de module 1, *i.e* un élément de $\mathbb{U}$. □

Exercices.

— Soit $\pi : X \longrightarrow Y$ une application où X est un espace topologique et Y un ensemble munit de la topologie quotient, et Z un espace topologique. Montrer que pour toute application continue $f : X \longrightarrow Z$ constante sur les classes de $\sim$-équivalence, l'application induite $\bar{f} : Y \longrightarrow Z$ est continue.

— On suppose de plus que Y est le quotient de X par un groupe G agissant sur X par homéomorphismes. Montrer que $\pi : X \longrightarrow Y = X/G$ est ouverte.

Remarque. Nous avons défini les espaces projectifs $\mathbb{P}(E)$, par exemple l'espace $E = k^{n+1}$ donne naissance à l'espace projectif standard $\mathbb{P}^n(k) = \mathbb{P}(k^{n+1})$. Nous introduisons maintenant les sous-espaces projectifs.

Définition 4.5.3. *Un sous-espace projectif de E est l'image par $\pi : E\backslash\{0\} \longrightarrow \mathbb{P}(E)$ de $F\backslash\{0\}$ où F est sous-espace vectoriel de E. Un tel sous-espace est donc l'ensemble $\mathbb{P}(F) \subset \mathbb{P}(E)$ des droites F.*

Remarque. On a donc une bijection entre l'ensemble des sous-espaces projectifs de dimension m de $\mathbb{P}(E)$ et l'ensemble des sous-espaces vectoriels de dimension $m+1$ de E.

Proposition 4.5.2. *On a les propriétés suivantes.*

(i) Soient V et W deux sous-espaces projectifs de $\mathbb{P}(E)$. Si $\dim V + \dim W \geq \dim \mathbb{P}(E)$, alors $V \cap W \neq \varnothing$.

(ii) Deux droites projectifs distinctes d'un plan projectif sont concourantes.

(iii) Soit $H \subset \mathbb{P}(E)$ un hyperplan projectif et $x \in \mathbb{P}(E)\backslash H$. Alors, toute droite passant par x coupe H en unique point.

Démonstration. On applique une stratégie très classique lorsqu'on travaille dans un espace projectif : prendre les préimages par π puis faire de l'algèbre linéaire.

(i) Soient F, G les sous-espaces vectoriels préimages par π, *i.e* que $V = \mathbb{P}(F)$ et $W = \mathbb{P}(G)$, et soient n, m, p les dimensions de $\mathbb{P}(E)$, $\mathbb{P}(F)$, et $\mathbb{P}(G)$. L'hypothèse est que $m + n \geq n$. On a par la formule de Grassman

$$\begin{aligned} \dim(F \cap G) &= \dim F + \dim G - \dim(F+G) \\ &\geq (m+1) + (p+1) - (n+1) = m + p - n + 1 \\ &\geq 1. \end{aligned}$$

$F \cap G$ contient donc une droite et alors $V \cap W = \mathbb{P}(F) \cap \mathbb{P}(G) = \mathbb{P}(F \cap G)$ contient au moins un point.

(ii) Prendre $n = 2$ et $m = p = 1$.

(iii) Soit $H = \mathbb{P}(F)$ et $D = \mathbb{P}(G)$ une droite passant par x. On a donc que $\dim E = n+1$, $\dim F$ et $\dim G = 2$. Puisque $x \notin H$, on a que $D \not\subset F$ d'où $F + G = E$. Ainsi,

$$\dim(F \cap G) = \dim(F) + \dim(G) - \dim(F+G) = 1,$$

c'est-à-dire que $H \cap D = \mathbb{P}(F \cap G)$ est un point.

□

Remarque. Soit A l'ensemble des sous-espaces vectoriels de E et B l'ensemble des sous-espaces projectifs de $\mathbb{P}(E)$. La bijection

$$\begin{array}{ccc} A & \longrightarrow & B \\ F & \longmapsto & \mathbb{P}(F) \end{array}$$

est une fonction croissante, d'inverse $B \to A$, $P \mapsto \mathrm{Vect}((\pi^{-1}(x))_{x \in P})$. En particulier, on voit que si $x \in \mathbb{P}(E)$e st fixé alors l'ensemble des droites projectives de $\mathbb{P}(E)$ passant par x est un espace projectif de dimension $\dim(E) - 1$. En effet, si $D \subset E$ désigne la droite vectorielle correspondante à x, on a des bijections entre l'ensemble droites projectives passant par x, l'ensemble des 2-plans vectoriels $F \subset E$ contenant D, et l'ensemble des droites vectorielles $F/D \subset E/D$ (qui est en fait $\mathbb{P}(E/D)$). Plus généralement, l'ensemble des sous-espaces projectifs de $\mathbb{P}(E)$ contenant un sous-espace projectif fixé $\mathbb{P}(F)$ est (en bijection naturelle) avec l'espace projectif $\mathbb{P}(E/F)$.

4.6 Hyperplans à l'infini, espaces affines à distance finie

Nous allons voir maintenant que le choix d'un hyperplan vectoriel $F \subset E$ (de manière équivalente, un hyperplan projectif $H = \mathbb{P}(F) \subset \mathbb{P}(E)$) permet de voir $\mathbb{P}(E)$ comme réunion d'un espace affine "à distance finie" et d'un hyperplan "à l'infini".

Proposition 4.6.1. *Soit $P = \mathbb{P}(E)$ un espace projectif de dimension n, et soit $H = \mathbb{P}(F)$ un hyperplan projectif. Alors, l'ensemble $P\backslash H = \mathbb{P}(E)\backslash\mathbb{P}(F)$ possède une structure naturelle d'espace affine de direction F (et donc de dimension n).*

Démonstration. Soit $\varphi \in E^*$ une forme linéaire non nulle sur F, et $\mathcal{F} = \{x \in E \,|\, \varphi(x) = 1\}$. Il s'agît d'un hyperplan affine de E de direction l'hyperplan F (par exemple si l'on complète une base $(e_0, \ldots, e_{n-1})$ de F avec un vecteur e_n en une base de E, on peut prendre $\varphi = e_n^*$ et alors $\mathcal{F} = \{x = \sum_{i=0}^{n} x_i e_i \in E \,|\, x_n = 1\}$). Les points de $P\backslash H$ correspondent aux droites de E non incluses dans F. Une telle droite D intersecte $\mathcal{F}$ en un unique point M_D et l'application

□