Dernière édition : 9 décembre 2020

Notes prises par Téofil ADAMSKI

THÉORIE DES GROUPES ET GÉOMÉTRIE

(THGG)

Ludovic MARQUIS

M1 maths fonda Université de Rennes 1

Chapitre 1

LES BASES DE LA THÉORIE DES GROUPES

INTRODUCTION ET MOTIVATIONS. Dans le désordre, les exemples les plus importantes sont $\mathbf{Z}$, $\mathbf{Z}^d$, $\mathbf{Z}/n\mathbf{Z}$, $\mathfrak{S}(X)$ où X est un ensemble et $\mathrm{GL}(V)$ où V est un k-espace vectoriel ainsi que tous leurs sous-groupes et quotients de sous-groupes.

Le but de ce cours est de comprendre les groupes en les faisant agir sur des espaces appropriés et inversement de comprendre des espaces en utilisant des groupes qui agissent. Par exemple, le groupe des isométries de $\mathbf{R}^n$ pour la distance euclidienne agit sur $\mathbf{R}^n$.

1.1 ACTION DE GROUPE

1.1.1 C'est quoi?

DÉFINITION 1.1. Une action d'un groupe G sur un ensemble X est la donnée équivalente

– d'un morphisme $\varphi\colon G \longrightarrow \mathfrak{S}(X)$;
– d'une application $\Phi\colon G \times X \longrightarrow X$ vérifiant
  ◦ pour tout $x \in X$, on a $\Phi(e,x) = x$;
  ◦ pour tous $g,h \in G$ et $x \in X$, on a $\Phi(g,\Phi(h,x)) = \Phi(gh,x)$.

On notera $G \curvearrowright_\varphi X$ ou $G \curvearrowright_\Phi X$ selon la définition. Pour $g \in G$ et $x \in X$, on note $g \cdot x := \varphi(g)(x)$ ou $g \cdot x := \Phi(g,x)$.

Preuve On peut montrer l'équivalence en posant l'égalité $\varphi(g)(x) = \Phi(g,x)$ pour tous $g \in G$ et $x \in X$. □

DÉFINITION 1.2. Soit G un groupe agissant sur un ensemble X. L'ensemble

$$\mathscr{O}_x := \{y \in X \mid \exists g \in G, y = g \cdot x\}$$

est l'orbite de x sous l'action de G. De plus, la relation binaire $\mathscr{R}$ sur l'ensemble X définie par

$$x \mathscr{R} y \iff \exists g \in G,\ y = g \cdot x, \qquad x,y \in X$$

est une relation d'équivalence dont les classes d'équivalences sont les orbites de X sous l'action de G. On note alors l'espace quotient

$$X/G := X/\mathscr{R}.$$

1.1.2 Formule des classes

PROPOSITION 1.3. Soit G un groupe agissant sur un ensemble X. Alors

$$\sharp X = \sum_{\mathscr{O} \in X/G} \sharp \mathscr{O}.$$

DÉFINITION 1.4. Soit G un groupe agissant sur un ensemble X. Pour $x \in X$, l'ensemble

$$\mathrm{Stab}_x := \{g \in G \mid g \cdot x = x\}$$

est le stabilisateur de x dans G. Pour tout $x \in X$, l'application orbitale

$$\varphi_x : \begin{vmatrix} G \longrightarrow X, \\ g \longmapsto g \cdot x \end{vmatrix}$$

a pour image l'orbite de x et deux éléments $g, h \in G$ ont la même image si et seulement si $gh^{-1} \in \mathrm{Stab}_x$. Ainsi, cette application induit une bijection

$$\tilde{\varphi}_x : G/\mathrm{Stab}_x \longrightarrow \mathcal{O}_x.$$

PROPOSITION 1.5. Soit G un groupe fini agissant sur un ensemble fini X. Pour tout $x \in X$, on a

$$\sharp G = \sharp \mathrm{Stab}_x \sharp \mathcal{O}_x.$$

LEMME 1.6 (BURNSIDE). Soit G un groupe fini agissant sur un ensemble fini X. Alors

$$\sharp(X/G) = \frac{1}{\sharp G} \sum_{g \in G} \sharp \mathrm{Fix}(g) = \frac{1}{\sharp G} \sum_{x \in X} \sharp \mathrm{Stab}_x$$

où, pour tout $g \in G$, on note $\mathrm{Fix}(g) := \{x \in X \mid g \cdot x = x\}$.

Preuve On remarque l'égalité ensembliste

$$\begin{aligned} \{(g,x) \in G \times X \mid g \cdot x\} &= \{(g,x) \in G \times X \mid x \in \mathrm{Fix}(g)\} \\ &= \{(g,x) \in G \times X \mid g \in \mathrm{Stab}_x\}. \end{aligned}$$

On obtient alors

$$\sum_{g \in G} \sharp \mathrm{Fix}(g) = \sum_{x \in X} \sharp \mathrm{Stab}_x.$$

De plus, les orbites formant une partition de X, on a

$$\sum_{x \in X} \sharp \mathrm{Stab}_x = \sum_{\mathcal{O} \in X/G} \sum_{x \in \mathcal{O}} \sharp \mathrm{Stab}_x.$$

On rappel que, pour tous $x \in X$ et $g \in G$, on a $\mathrm{Stab}_{g \cdot x} = g\mathrm{Stab}_x g^{-1}$. En particuliers, si deux éléments $x, y \in X$ sont dans la même orbite, alors les stabilisateurs Stab_x et Stab_y sont de même ordre. On note $\{y_1, \ldots, y_n\}$ un ensemble de représentants des orbites. Finalement, on a

$$\begin{aligned} \sum_{x \in X} \sharp \mathrm{Stab}_x &= \sum_{i=1}^{n} \sum_{x \in \mathcal{O}_{y_i}} \sharp \mathrm{Stab}_x \\ &= \sum_{i=1}^{n} \sharp \mathrm{Stab}_{y_i} \sharp \mathcal{O}_{y_i} = n \sharp G \end{aligned}$$

ce qui montre la formule. □

1.1.3 Vocabulaire

DÉFINITION 1.7. L'action d'un groupe G sur un ensemble X est dite

- *fidèle* si le morphisme $\varphi : G \longrightarrow \mathfrak{S}(X)$ est injectif (on note $\mathrm{Ker}(G \curvearrowright X) := \mathrm{Ker}\,\varphi$) ;
- *libre* si, pour tout $g \in G$ et tout $x \in X$, on a $g \cdot x = x \Rightarrow g = 1$;
- *transitive* lorsqu'il n'y a qu'une seule orbite ;
- *simplement transitive* lorsque l'action est libre et transitive ;
- *k-transitive* avec $k \geqslant 1$ si l'action de G sur $X^{*k} := \{(x_1, \ldots, x_k) \in X^k \mid \forall i \neq j, x_i \neq x_j\}$ est transitive ;
- *simple k-transitive* avec $k \geqslant 1$ si l'action de G sur X^{*k} est simplement transitive.

1.1.4 Exemples

ACTION À GAUCHE. Tout groupe G agit sur lui-même par translation à gauche

$$(g,x) \in G \times G \longmapsto gx \in G.$$

Cette action est fidèle et simplement transitive. On peut en déduire qu'il existe une injection $\varphi : G \longrightarrow \mathfrak{S}(G)$. En particulier, tout groupe d'ordre $n \geqslant 1$ s'injecte dans le groupe $\mathfrak{S}_n$. Si H est un sous-groupe de G, alors on peut faire agir G par translation à gauche sur les classes à droites de G modulo H, c'est-à-dire par

$$(g, xH) \in G \times G/H \longmapsto gxH \in G/H.$$

Ainsi, il existe un morphisme $G \longrightarrow \mathfrak{S}(G/H)$.

ACTION PAR CONJUGAISON. Tout groupe agit sur lui-même par conjugaison

$$(g,x) \in G \times G \longmapsto gxg^{-1}.$$

Les orbites de cette action sont appelées les *classes de conjugaison*, son noyau est appelé le *centre* et noté

$$\mathrm{Z}(G) \coloneqq \{g \in G \mid \forall x \in X, gx = xg\}.$$

◇ REMARQUES. – Pour tout $g \in G$, l'application

$$\alpha_g : \begin{vmatrix} G \longrightarrow G, \\ x \longmapsto gxg^{-1} \end{vmatrix}$$

est un automorphisme de G, dit *intérieur*. Ainsi il existe un morphisme $\alpha : G \longrightarrow \mathrm{Aut}(G)$ de noyau $\mathrm{Z}(G)$.
– L'action par conjugaison de G sur G induit une action sur les sous-groupes de G : un sous-groupe de G fixé est dit *normal* et un sous-groupe de G fixé par $\mathrm{Aut}(G)$ est dit *caractéristique*. De plus, le stabilisateur d'un sous-groupe H de G

$$\mathrm{N}_G(H) \coloneqq \{g \in G \mid gHg^{-1} = H\}$$

est appelé le *normalisateur* de H dans G et le noyau de l'action induite par $\mathrm{N}_G(H)$ sur H

$$\mathrm{Z}_G(H) \coloneqq \{g \in G \mid \forall h \in H, ghg^{-1} = h\}$$

est appelé le *centralisateur* de H dans G.

REPRÉSENTATION LINÉAIRE. Une représentation linéaire d'un groupe G est une action de G sur un k-espace vectoriel par application linéaire, *i. e.* un morphisme $G \longrightarrow \mathrm{GL}(V)$. Par exemple, soit G un groupe agissant sur un ensemble X. Alors l'ensemble des fonctions k^X est un k-espace vectoriel de dimension $\sharp X$ et le groupe G agit sur k^X par l'application

$$(g,f) \in G \times k^X \longmapsto [x \in X \longmapsto (g \cdot f)(x) \coloneqq f(g^{-1} \cdot x)] \in k^X.$$

DES ACTIONS PLUS GÉOMÉTRIQUES. Par exemple, on a
– l'action du groupe linéaire $\mathrm{GL}(V)$ sur V ;
– l'action de groupe linéaire $\mathrm{GL}_n(\mathbf{R})$ sur $\mathbf{R}^n$;
– l'action du groupe affine $\mathrm{GA}_n(\mathbf{R})$ sur $\mathbf{R}^n$;
– l'action du groupe des isométries $\mathrm{Isom}(\mathbf{R}^n)$ sur $\mathbf{R}^n$;
– l'action de groupe spécial orthogonal $\mathrm{SO}_n(\mathbf{R})$ sur $\mathbf{S}^{n-1}$;
– l'action du groupe linéaire $\mathrm{GL}(V)$ sur l'espace projectif $\mathbf{P}(V)$.

1.2 THÉORÈME DE LAGRANGE, CAUCHY ET SYLOW

THÉORÈME 1.8 (LAGRANGE). L'ordre d'un sous-groupe divise l'ordre du groupe.

Preuve On considère l'action d'un groupe G sur lui-même par translation. On restreint cette action à un sous-groupe $H < G$. Cette action est libre. On applique la deuxième formule des classes. □

THÉORÈME 1.9 (CAUCHY). Soient G un groupe fini et p un nombre premier divisant l'ordre de G. Alors il existe un élément d'ordre p dans G.

Preuve On introduit l'ensemble $X \coloneqq \{(x_1,\dots,x_p) \in G^p \mid x_1 \cdots x_p = 1\}$. On fait agir le groupe $\mathbf{Z}/p\mathbf{Z}$ sur cet ensemble par permutation circulaire, *i. e.* définie par $\overline{1} \cdot (x_1,\dots,x_p) = (x_p,x_1,\dots,x_{p-1})$. On remarque que
– un point fixe pour l'action de $\mathbf{Z}/p\mathbf{Z}$ est un élément $(x_1,\dots,x_p) \in X^p$ tel que $x_1 = \cdots = x_p$;
– les orbites sont de cardinal p ou 1 ;
– un point fixe est de la forme $(x,\dots,x) \in X$ avec $x^p = 1$, donc soit $x = e$ soit x est d'ordre p.
Ainsi, on peut écrire $\sharp X = k_1 + pk_p$ où les entiers k_1 et k_p sont resp. les nombres d'orbites de cardinal 1 et p. De plus, on a $\sharp X = n^{p-1}$. Or $p \mid n$, donc $p \mid k_1$. Comme $k_1 \geqslant 1$, on a $k_1 \geqslant p \geqslant 2$. □

THÉORÈME 1.10 (SYLOW). Soient $\alpha \geqslant 0$, p un nombre premier et $n \geqslant 1$ tel que $\mathrm{pgcd}(n,p) = 1$. Soit G un groupe d'ordre $p^\alpha n$. On note $s_p \geqslant 0$ le nombre de p-SYLOW de G, *i. e.* de sous-groupe de G d'ordre p^α. Alors
1. on a $s_p \geqslant 1$;
2. tout sous-groupe dont l'ordre est une puissance de p est inclus dans un p-SYLOW ;

3. le groupe G agit transitivement sur l'ensemble des p-SYLOW ;
4. on a $s_p \equiv 1 \ [p]$ et $s_p \mid m$.

▷ EXEMPLE. Soit p un nombre premier. On note $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ le corps à p éléments. On pose $q := p^2$. Alors le groupe $\mathrm{U}_n(\mathbf{F}_q)$ des matrices de dimension $n \times n$ à coefficients dans $\mathbf{F}_q$ dont les diagonales sont constituées de 1 est un p-SYLOW de $\mathrm{GL}_n(\mathbf{F}_q)$.

1.3 SIMPLICITÉ

DÉFINITION 1.11. Un groupe G est dit *simple* lorsque tout sous-groupe distingué de G est trivial.

▷ EXEMPLES. Le groupe $\mathbf{F}_p$ pour un nombre premier p est simple. Le groupe alterné $\mathfrak{A}_n$ pour $n \geqslant 5$ l'est aussi.

EXERCICE 1.1. Soient p et q deux nombres premiers et $\alpha \geqslant 1$. Montrer, en utilisant le théorème de SYLOW, que toute d'ordre pq^α n'est pas simple.

1.4 GROUPE DÉRIVÉ

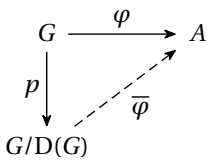
DÉFINITION 1.12. Le *groupe dérivé* d'un groupe G est le groupe engendré par les commutateurs, *i. e.* les éléments de la forme $[x, y] := xyx^{-1}y^{-1}$ pour $x, y \in G$. On le note $\mathrm{D}(G)$ ou G'.

PROPOSITION 1.13. Soit G un groupe. Alors le groupe $\mathrm{D}(G)$ est distingué et caractéristique dans G.

Preuve L'ensemble des commutateurs est préservé par les automorphismes et, en particulier, par les automorphismes intérieurs. □

PROPOSITION 1.14. 1. Soit G un groupe. Alors le groupe dérivé de G est trivial si et seulement si le groupe G est abélien. De plus, le groupe quotient $G/\mathrm{D}(G)$ est abélien.

2. Soient A un groupe abélien et $\varphi\colon G \to A$ un morphisme de groupes. Alors $\mathrm{D}(G) < \mathrm{Ker}\, f$ et le morphisme φ se factorise de manière unique par la projection canonique $p\colon G \to G/\mathrm{D}(G)$, c'est-à-dire qu'il existe un unique morphisme de groupes $\overline{\varphi}\colon G/\mathrm{D}(G) \to A$ tel que $\varphi = \overline{\varphi} \circ p$.



3. Pour tout sous-groupe H de G tel que le quotient G/H soit abélien, on a $\mathrm{D}(G) < H$.
4. Le groupe $G/\mathrm{D}(G)$ est le plus grand quotient abélien de G, appelé l'*abélianisé* de G.

DÉFINITION 1.15. Soit G un groupe. On définit les groupes dérivés d'ordres supérieurs de la façon suivante :
– $\mathrm{D}^0(G) = G$;
– pour tout $k \in \mathbf{N}$, on a $\mathrm{D}^{(k+1)} = \mathrm{D}(\mathrm{D}^{(k)}(G))$.
La suite $(\mathrm{D}^{(k)}(G))_{k\in\mathbf{N}}$ s'appelle la *suite dérivée* de G.

DÉFINITION 1.16. Un groupe *parfait* est un groupe G tel que $\mathrm{D}(G) = G$.

1.5 CLASSIFICATION DES GROUPES ABÉLIENS DE TYPE FINI

DÉFINITION 1.17. Un groupe G est de *type fini* s'il est engendré par un nombre fini de ses éléments.

THÉORÈME 1.18. Soit Γ un groupe abélien de type fini. Alors
1. il existe un entier $\ell \geqslant 0$ et un n-uplet $(q_1, \ldots, q_n) \in \mathbf{N}^n$ de puissances de nombres premiers, unique à permuta-

tion près, tels que

$$\Gamma \simeq \mathbf{Z}^\ell \times \frac{\mathbf{Z}}{q_1\mathbf{Z}} \times \cdots \times \frac{\mathbf{Z}}{q_n\mathbf{Z}} ;$$

2. il existe un entier $\ell \geqslant 0$ et un m-uplet $(a_1, \ldots, a_m) \in \mathbf{N}_{\geqslant 2}^m$ tels que

$$a_m \mid a_{m-1} \mid \cdots \mid a_1 \quad \text{et} \quad \Gamma \simeq \mathbf{Z}^\ell \times \frac{\mathbf{Z}}{a_1\mathbf{Z}} \times \cdots \times \frac{\mathbf{Z}}{a_m\mathbf{Z}}.$$

◇ REMARQUE. Le théorème chinois permet de passer du point 1 au point 2.

1.6 EXTENSION DE GROUPES

1.6.1 Un petit lemme

LEMME 1.19. Soient G un groupe et H et K deux sous-groupes de G dont un est distingué dans G. Alors le groupe HK est un sous-groupe de G et $HK = KH$.

Preuve Supposons que H est distingué dans G. Pour tous $h \in H$ et $k \in K$, on a $hk = kk^{-1}hk \in KH$ car $k^{-1}hk \in H$. Cela montre $HK \subset KH$. De même, on a $KH \subset HK$. D'où $HK = KH$. Avec le même genre d'argument, on montre qu'il s'agit d'un sous-groupe de G. □

1.6.2 Produit semi-direct interne

DÉFINITION 1.20. Soient G un groupe et N et K deux sous-groupes de G. On dit que le groupe G est le *produit semi-direct* (interne) de N par K lorsqu'on a les trois assertions suivantes :

– le sous-groupe N est distingué dans G ;
– on a $N \cap K = \{1\}$;
– on a $NK = G$.

On note alors $N \rtimes K = G$.

PROPOSITION 1.21. Soit G un groupe étant le produit semi-direct de N par K. Alors

1. pour tout $g \in G$, il existe un unique couple $(n, k) \in N \times K$ tel que $g = nk$;
2. pour tous $n, n' \in N$ et $k, k' \in K$, on a $(nk) \times (n'k') = n(kn'k^{-1})kk'$;
3. l'application

$$p : \left| \begin{array}{l} G \longrightarrow K, \\ nk \longmapsto k \end{array} \right.$$

est un morphisme de noyau N.

Preuve Montrons seulement le premier point. L'existence vient de l'égalité $G = NK$. L'unicité est une conséquence de l'égalité $N \cap K = \{1\}$: si quatre éléments $n, n' \in N$ et $k, k' \in K$ vérifient $nk = n'k'$, alors $n'^{-1}n = kk'^{-1}$ est un élément de $N \cap K$, donc $n = n'$ et $k = k'$. □

DÉFINITION 1.22. Soit G un groupe. On dit qu'un sous-groupe distingué N de G admet un *complément* lorsqu'il existe un sous-groupe K de G tel que $N \cap K = \{1\}$ et $NK = G$.

PROPOSITION 1.23. Soient G un groupe et N et K deux sous-groupes de G tels que $G = N \rtimes K$. Alors le groupe K est distingué dans G si et seulement si le groupe K centralise N, *i. e.* pour tous $k \in K$ et $n \in N$, on a $knk^{-1} = n$. Dans ce cas, on dit que le produit est *direct* et on note $G = N \times K$.

▷ EXEMPLES. – Soient k un corps et $n \geqslant 1$. On note

$$\mathrm{GA}_n(k) := \left\{ \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \;\middle|\; A \in \mathrm{GL}_n(k), b \in k^n \right\}.$$

Alors le groupe $\mathrm{GL}_n(k)$ s'injecte dans ce dernier. De plus, on note $\mathrm{T}_n(k)$, $\mathrm{U}_n(k)$ et $\mathrm{A}_n(k)$ les matrices de $\mathrm{GL}_n(k)$ triangulaires supérieures, triangulaires supérieures avec des 1_k sur la diagonale et diagonales. Alors on a les produits semi-direct suivant.

Groupe G	Groupe N	Groupe N
$\mathfrak{S}_n$	$\mathfrak{A}_n$	groupe engendré par une transposition
$\mathrm{GL}_n(k)$	$\mathrm{SL}_n(k)$	$\left\{ \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \middle\| \lambda \in k^\times \right\}$
$\mathbf{D}_n$	sous-groupe des rotations	un groupe engendré par une réflexion
$\mathrm{T}_n(k)$	$\mathrm{U}_n(k)$	$\mathrm{A}_n(k)$
$\mathrm{GA}_n(k)$	$\mathrm{T}_n(k)$	$\mathrm{GL}_n(k)$

1.6.3 Produit semi-direct externe

DÉFINITION 1.24. Soient N et K deux groupes et $\alpha\colon K \to \mathrm{Aut}(N)$ un morphisme de groupes. On appelle *produit semi-direct* (externe) de N par K relative à α le couple $(G,\cdot)$ où

– on a $G = N \times K$;
– l'application $\cdot\colon G^2 \to G$ est définie par $(n,k)\cdot(n',k') = (n\alpha(k)(n'), kk')$ pour tous $n,n' \in N$ et $k,k' \in K$.

PROPOSITION 1.25. Soient N et K deux groupes et $\alpha\colon K \to \mathrm{Aut}(N)$ un morphisme de groupes. Alors

1. le couple $(N \times K, \cdot)$ est un groupe noté $N \rtimes_\alpha K$;
2. le groupe $N \times \{1_K\}$ est distingué dans $N \rtimes_\alpha K$;
3. l'application $i\colon n \in N \longmapsto (n,1) \in N \rtimes_\alpha K$ est un morphisme de groupes injectif ;
4. l'application $s\colon k \in K \longmapsto (1,k) \in N \rtimes_\alpha K$ est un morphisme de groupes injectif ;
5. le groupe $\{1_N\}\cdot K$ est un sous-groupe de $N \rtimes_\alpha K$;
6. le groupe $N \rtimes_\alpha K$ est le produit semi-direct interne de $N \times \{1_K\}$ par $\{1_N\} \times K$;
7. avec les bons abus de notation, pour tous $n \in N$ et $k \in K$, on a $\alpha(k)\cdot n = knk^{-1}$.

PROPOSITION 1.26. Soient N et K deux groupes et $\alpha\colon K \to \mathrm{Aut}(N)$ un morphisme de groupes. Alors $N \rtimes_\alpha K$ est le produit direct de N par K si et seulement si le morphisme α est trivial.

Preuve Le groupe $N \rtimes_\alpha K$ est le produit direct de N par K si et seulement si le groupe K centralise N si et seulement si

$$\forall n \in N,\ \forall k \in K, \quad \alpha(k)\cdot n = knk^{-1} = n$$

si et seulement si le morphisme α est trivial. □

◇ REMARQUE. Attention, on peut tout à fait avoir $N \rtimes_\alpha K \simeq N \times K$ tout en ayant un morphisme α non trivial.

PROPOSITION 1.27. Soient $\alpha_1, \alpha_2\colon K \to \mathrm{Aut}(N)$ deux morphismes de groupes. S'il existe $\varphi \in \mathrm{Aut}(K)$ et $\gamma \in \mathrm{Aut}(N)$ tel que $\alpha_2(k) = \gamma\alpha_1 \circ \varphi(k)\gamma^{-1}$ pour tout $k \in K$, alors $N \rtimes_{\alpha_1} K \simeq N \rtimes_{\alpha_2} K$.

1.7 SUITES EXACTES

DÉFINITION 1.28. Une *suite exacte* de groupes est la donnée de trois groupes N, G et K et de deux morphismes de groupes $i\colon N \to G$ et $p\colon G \to K$ tels que

– le morphisme i est injectif ;
– le morphisme p est surjectif ;
– on a $\mathrm{Im}\, i = \mathrm{Ker}\, p$.

On note alors

$$1 \longrightarrow N \xrightarrow{\ i\ } G \xrightarrow{\ p\ } K \longrightarrow 1$$

◇ REMARQUE. Soient G un groupe et N un sous-groupe distingué de G. Alors la suite

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1.$$

est exacte.

DÉFINITION 1.29. On dit qu'un groupe G est une *extension* d'un groupe N par un groupe K s'il existe une suite exacte $1 \longrightarrow N \longrightarrow G \longrightarrow K \longrightarrow 1$.

DÉFINITION 1.30. Une suite exacte $1 \longrightarrow N \longrightarrow G \longrightarrow K \longrightarrow 1$ est dite *scindée* s'il existe un morphisme de groupes $s\colon K \to G$ tel que $p \circ s = \mathrm{Id}_K$. Un tel morphisme s s'appelle une *section* et la suite exacte est dite scindée *par* ce morphisme.

◇ REMARQUES. Une section est nécessairement injective. Une suite exacte est scindée si et seulement s'il existe un sous-groupe $\overline{K}$ de G tel que la restriction $p|_{\overline{K}}$ soit un isomorphisme.

PROPOSITION 1.31. Soient G un groupe et N et K deux sous-groupes de G tels que $G = N \rtimes K$. Alors la suite exacte canonique $1 \longrightarrow N \longrightarrow G \longrightarrow K \longrightarrow 1$ est scindée par l'inclusion de K dans G.

Preuve On prend le point de vue externe. Pour tout $k \in K$, on a $p(1,k) = k$. Donc l'application $k \in K \longmapsto (1,k)$ est une section. □

PROPOSITION 1.32. Soit $1 \longrightarrow N \longrightarrow G \longrightarrow K \longrightarrow 1$ une suite exacte scindée par une section $s\colon K \to G$. On définit une action de K sur N par la relation

$$\alpha(k) \cdot n = s(k) n s(k)^{-1}, \quad n \in N, k \in K.$$

Alors le groupe G est égale au produit semi-direct interne de $i(N)$ par $s(K)$ et, en particulier, isomorphe à $N \rtimes_\alpha K$.

Preuve On vérifie les trois points du produit semi-direct interne. Le sous-groupe $i(N) = \mathrm{Ker}\, p$ est bien distingué dans G. De plus, on a $i(N) \cap s(K) = \{1\}$ car, si $s(k) \in i(N) = \mathrm{Ker}\, p$ avec $k \in K$, alors $k = p \circ s(k) = 1$. Enfin, on a bien $i(N)s(K) = G$. En effet, soit $g \in G$. On pose $k := p(g) \in NK$ et $n := g s(k)^{-1} \in i(N)$. Alors $g = nk$. □

DÉFINITION 1.33. Une suite exacte $1 \longrightarrow N \longrightarrow G \longrightarrow K \longrightarrow 1$ est dite *triviale* si elle est scindée et l'image $s(K)$ centralise l'image de i, *i. e.* tous les éléments de $i(N)$ commutent avec tous les éléments de $s(K)$ ou, autrement dit, on a $G = i(N) \times s(K)$.

1.8 EXTENSIONS CENTRALES

DÉFINITION 1.34. Un groupe G est une *extension centrale* d'un groupe A par un groupe K lorsqu'il existe une suite exacte

$$1 \longrightarrow A \longrightarrow G \longrightarrow K \longrightarrow 1$$

telle que $i(A) < \mathrm{Z}(G)$.

◇ REMARQUES. – Pour tout groupe G, on a la suite exacte

$$1 \longrightarrow \mathrm{Z}(G) \longrightarrow G \longrightarrow G/\mathrm{Z}(G) \longrightarrow 1.$$

Donc tout groupe dont le centre est non trivial est une extension centrale. On peut prendre les exemples $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$ qui possèdent des centres non triviaux.

– Une extension centrale et scindée est triviale. En effet, si la suite

$$1 \longrightarrow A \longrightarrow G \longrightarrow K \longrightarrow 1$$

est centrale et scindée, alors $s(K)$ centralise $i(A)$ puisque $i(A) < \mathrm{Z}(G)$.

– Attention à $\mathrm{GL}_n(k)$! Les deux suites exactes

$$1 \longrightarrow \mathrm{SL}_n(k) \longrightarrow \mathrm{GL}_n(k) \longrightarrow k^\times \longrightarrow 1 \quad \text{et} \quad 1 \longrightarrow k^\times \longrightarrow \mathrm{GL}_n(k) \longrightarrow \mathrm{PGL}_n(k) := \mathrm{GL}_n(k)/\mathrm{Z}(\mathrm{GL}_n(k)) \longrightarrow 1$$

sont resp. scindée et centrale.

1.9 GROUPES DIÉDRAUX

DÉFINITION 1.35. Soit $n \geqslant 1$ un entier. Le *groupe diédral* d'ordre $2n$ est le produit-semi-direct de $\mathbf{Z}/n\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$ *via* l'action

$$\begin{aligned} &\mathbf{Z}/2\mathbf{Z} \longrightarrow \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}), \\ &\quad 1 \longmapsto \alpha(1) := [x \longmapsto -x]. \end{aligned}$$

Le *groupe diédral infini* est le produit semi-direct de $\mathbf{Z}$ par $\mathbf{Z}/n\mathbf{Z}$ *via* l'action

$$\begin{vmatrix} \mathbf{Z}/2\mathbf{Z} \longrightarrow \mathrm{Aut}(\mathbf{Z}), \\ 1 \longmapsto \alpha(1) := [x \longmapsto -x]. \end{vmatrix}$$

On les note resp. $\mathbf{D}_n$ et $\mathbf{D}_\infty$.

PROPOSITION 1.36. Soient G un groupe et $n \geqslant 1$ un entier. Alors le groupe G est isomorphe à $\mathbf{D}_n$ (resp. $\mathbf{D}_\infty$) si et seulement s'il existe des éléments $a, b \in G$ d'ordre 2 (resp. infini) et n tels que $bab^{-1} = a^{-1}$ et $G = \langle a, b\rangle$.

Preuve Il s'agit d'une simple réécriture de la définition. □

PROPOSITION 1.37. Soit G un groupe engendré par deux éléments d'ordre 2. Alors le groupe G est un groupe diédral.

Preuve On note b et c ses deux générateurs d'ordre 2. On pose $a := bc$. Alors $G = \langle b, c\rangle$ et il faut juste vérifier la relation $bab^{-1} = a^{-1}$ et, en effet, on a $bab^{-1} = b(bc)b = cb = a^{-1}$. Il s'agit donc d'un groupe diédral. □

PROPOSITION 1.38. Soit $n \geqslant 3$ un entier. Alors le groupe diédral d'ordre $2n$ est le groupe est des isométries du polygone régulier à n côtés.

Preuve On note $\mathscr{P}_n \subset \mathbf{R}^2$ l'enveloppe convexe des racines n-ième de l'unité. Alors on montre l'isomorphie

$$\mathbf{D}_n \simeq \mathrm{Isom}(\mathscr{P}_n) := \{g \in \mathrm{Isom}(\mathbf{R}^2) \mid g(\mathscr{P}_n) = \mathscr{P}_n\}.$$

En effet, le groupe de droite est bien engendré par les deux isométries de matrices

$$\begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

□

EXERCICE 1.2. Soit $n \geqslant 1$ un entier. Montrer que

1. le centre de $\mathbf{D}_n$ est trivial si et seulement si n est pair ou l'infini ;
2. si n est pair, alors $\mathrm{Z}(\mathbf{D}_n) = \{1, a^{d/2}\}$;
3. si n est impair, alors $\mathrm{D}(\mathbf{D}_n) = \langle a\rangle$;
4. si n est pair ou l'infini, alors $\mathrm{D}(\mathbf{D}_n) = \langle a^2\rangle$;
5. si n est impair ou l'infini, alors il y a une seule classe de conjugaison d'éléments d'ordre 2 ;
6. si n est pair, alors il y a deux classes de conjugaison pour les réflexions.

1.10 GROUPES SYMÉTRIQUES ET ALTERNÉES

PROPOSITION 1.39. Soit $n \geqslant 1$ un entier. Le groupe $\mathfrak{S}_n$ est engendré par les transpositions.

PROPOSITION 1.40. La signature d'une permutation $\sigma \in \mathfrak{S}_n$ est la quantité $\epsilon(\sigma) = (-1)^k$ où l'entier k est le nombre de transpositions dans la décomposition de σ en produit de transpositions. La signature est bien définie et donne un morphisme $\epsilon\colon \mathfrak{S}_n \longmapsto \{\pm 1\}$. On pose alors $\mathfrak{A}_n := \mathrm{Ker}\,\epsilon$.

Transitivité multiple

PROPOSITION 1.41. 1. L'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ est simplement n-transitive.
2. L'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$ est simplement $n-2$-transitive.

Preuve Le point 1 est évident. Soient $x_1, \ldots, x_{n-2} \in \mathfrak{A}_n$ des éléments deux à deux distincts et $y_1, \ldots, y_{n-2} \in \mathfrak{A}_n$ des éléments deux à deux distincts. Soient $x_{n-1}, x_n, y_{n-1}, y_n \in \mathfrak{A}_n$. Il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(x_i) = y_i$ pour $i \in [\![1, n-2]\!]$. Si $\sigma \in \mathfrak{A}_n$,c'est fini. On suppose désormais $\sigma \notin \mathfrak{A}_n$. On considère la transposition $\tau := (y_{n-1}\ y_n) \in \mathfrak{S}_n$. Alors la permutation $\tau\sigma \in \mathfrak{A}_n$ convient. De plus, l'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$ est simplement $n-2$-transitive car

$$\{\sigma \in \mathfrak{S}_n \mid \forall i \in [\![0, n-2]\!],\ g(i) = i\} = \{\mathrm{Id}\}.$$

□

Les 3-cycles dans $\mathfrak{A}_n$

PROPOSITION 1.42. Soit $n \geqslant 5$ un entier. Alors les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Preuve Pour tous $i_1, \dots, i_k \in [\![1, n]\!]$ et $g \in \mathfrak{S}_n$, le principe de conjugaison donne

$$g(i_1 \cdots i_k)g^{-1} = (g(i_1) \cdots g(i_k)).$$

Soient $i, j, k \in [\![1, n]\!]$ trois entiers distincts. L'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$ est $n-2$-transitive, donc elle est 3-transitive. Alors il existe $g \in \mathfrak{A}_n$ telle que $g(1) = i$, $g(2) = j$ et $g(3) = k$. Alors $g(1\ 2\ 3)g^{-1} = (i\ j\ k)$. On en conclut que tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$. □

PROPOSITION 1.43. Soit $n \geqslant 3$ un entier. Alors les 3-cycles engendrent $\mathfrak{A}_n$.

◇ REMARQUE. L'ensemble $X \subset \mathfrak{A}_n$ des trois cycles vérifie les trois points suivants :

- il engendre $\mathfrak{A}_n$;
- il est stable par conjugaison ;
- ses éléments ont le maximum de points fixes possibles.

Centres

PROPOSITION 1.44. 1. Soit $n \geqslant 3$ un entier. Alors $\mathrm{Z}(\mathfrak{S}_n) = \{1\}$.
2. Soit $n \geqslant 4$ un entier. Alors $\mathrm{Z}(\mathfrak{A}_n) = \{1\}$.

Preuve Montrons uniquement le premier point. Raisonnons par l'absurde et supposons qu'il existe une permutation $\sigma \in \mathrm{Z}(\mathfrak{S}_n) \setminus \{\mathrm{Id}\}$. On peut supposer $\sigma(1) = 2$. En conjuguant par la transposition $(1\ 3)$, on a

$$(1\ 3) = \sigma(1\ 3)\sigma^{-1} = (\sigma(1)\ \sigma(2)) = (2\ \sigma(3))$$

ce qui est impossible. □

Groupes dérivés

PROPOSITION 1.45. 1. Soit $n \geqslant 1$ un entier. Alors $\mathrm{D}(\mathfrak{S}_n) = \mathfrak{A}_n$.
2. Soit $n \geqslant 5$ un entier. Alors $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$.

Preuve 1. Si $n \in \{1, 2\}$, la proposition est évident. On suppose alors $n \geqslant 3$. Comme $[(1\ 2), (1\ 3)] = (2\ 3\ 1)$, le groupe dérivé $\mathrm{D}(\mathfrak{S}_n)$ contient un 3-cycle. Les 3-cycles étant conjugués et le groupe $\mathrm{D}(\mathfrak{S}_n)$ étant normal, ce dernier contient tous les 3-cycles. Or les 3-cycles engendrent $\mathfrak{A}_n$, donc $\mathfrak{A}_n \subset \mathrm{D}(\mathfrak{S}_n)$. Mais l'inclusion réciproque est triviale car tous les commutateurs appartiennent à $\mathfrak{A}_n$. D'où l'égalité.
2. On peut remarquer $[(1\ 2\ 3), (1\ 4\ 5)] = (1\ 4\ 2)$. Avec les mêmes arguments, on obtient $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$. □

◇ REMARQUE. Le groupe $\mathrm{D}(\mathfrak{A}_4)$ est le sous-groupe d'ordre 4 composé des doubles transpositions, noté V_4. Il est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

Simplicité

THÉORÈME 1.46. Soit $n \geqslant 5$ un entier. Alors le groupe $\mathfrak{A}_n$ est simple.

Idée de la preuve Soit N un sous-groupe normal non trivial de $\mathfrak{A}_n$. Montrons que $N = \mathfrak{A}_n$. Pour cela, montrons qu'il contient un 3-cycle. Si on choisit un 3-cycle $k \in \mathfrak{A}_n$ et une permutation $n \in N$, alors les permutations nkn^{-1} et k^{-1} sont des 3-cycles, donc le commutateur $[n, k]$ est un 3-cycle. □

EXERCICE 1.3. On note

$$\mathfrak{S}_\infty := \{g \in \mathfrak{S}(\mathbf{N}) \mid \exists N \geqslant 0,\ \forall k \geqslant N,\ g(k) = k\}.$$

Montrer que la signature $\epsilon \colon \mathfrak{S}_\infty \longrightarrow \{\pm 1\}$ a encore un sens et que son noyau $\mathfrak{A}_\infty := \mathrm{Ker}\,\epsilon$ est simple.

PROPOSITION 1.47. Soit $n \geqslant 5$ un entier. Alors les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

1.11 GROUPES RÉSOLUBLES

1.11.1 Définition et caractérisations

DÉFINITION 1.48. Soit G un groupe. Une *suite de composition* de G est une suite finie $(G_0,\dots,G_n)$ de sous-groupes de G tels que

$$G = G_0 > G_1 > \cdots > G_n = \{1\} \quad \text{et} \quad G_{i+1} \lhd G_i,\ \forall i \in [\![0, n-1]\!].$$

Les quotients G_i/G_{i+1} sont les *facteurs* de cette suite. Une suite de composition est dite de JORDAN-HÖLDER si tous ses facteurs sont simples et non triviaux.

THÉORÈME 1.49 (JORDAN-HÖLDER). Tout groupe fini admet une suite de composition de JORDAN-HÖLDER. De plus, les facteurs d'une suite de JORDAN-HÖLDER sont uniques à permutations près.

DÉFINITION 1.50. Un groupe G est dit *résoluble* s'il admet une suite de compositions dont les facteurs sont abéliens.

PROPOSITION 1.51. Un groupe G est résoluble si et seulement s'il existe un entier $k \in \mathbf{N}$ tel que $\mathrm{D}^{(k)}(G) = \{1\}$.

Preuve $\Leftarrow$ On suppose qu'il existe un entier $k \in \mathbf{N}$ tel que $\mathrm{D}^{(k)}(G) = \{1\}$. Alors la suite $(\mathrm{D}^{(0)}(G),\dots,\mathrm{D}^{(k)}(G))$ est bien une suite de composition de G dont les facteurs sont abéliens.

$\Leftarrow$ On suppose que le groupe G est résoluble. Soit $(G_0,\dots,G_n)$ une suite de compositions de G dont les facteurs sont abéliens. Comme G_0/G_1 est abélien, on a $\mathrm{D}^{(1)}(G) < G_1$ car le groupe dérivé est le plus petit sous-groupe tels que $G/\mathrm{D}(G)$ soit abélien. Comme G_1/G_2 est abélien, on a $\mathrm{D}(G_1) < G_2$, donc $\mathrm{D}^{(2)}(G) < G_2$. Ainsi de suite, on montre que, pour tout $k \in [\![1, n]\!]$, on a $\mathrm{D}^{(k)}(G) < G_k$. En particulier, on a $\mathrm{D}^{(n)}(G) < G_n$, donc $\mathrm{D}^{(n)}(G) = \{1\}$. □

PROPOSITION 1.52. Un groupe fini G est résoluble si et seulement s'il admet une suite de compositions dont tous les facteurs sont cycliques d'ordre premier.

1.11.2 Propriétés

PROPOSITION 1.53. 1. Tout sous-groupe ou quotient d'un groupe résoluble est résoluble.

2. Soient G un groupe et N un sous-groupe distingué de G. Alors le groupe G est résoluble si et seulement si les groupes N et G/N le sont.

3. Un groupe résoluble et simple est cyclique d'ordre premier.

LEMME 1.54. Soient $K \lhd L < G$ et $f\colon G \longrightarrow H$ un morphisme. Alors $f(K) \lhd f(L)$ et le morphisme $f\colon L \longrightarrow f(L)$ induit un morphisme surjectif $f\colon L/K \longrightarrow f(L)/f(K)$.

Preuve Montrons que $f(K) \lhd f(L)$. Soient $g \in L$ et $k \in K$. Alors $f(g)f(k)f(g)^{-1} = f(gkg^{-1}) \in f(K)$ car $K \lhd L$. Le sous-groupe $f(K)$ est bien distingué dans $f(L)$.

Le morphisme $f\colon L \longrightarrow f(L)$ est bien surjectif. Il induit donc un morphisme $f\colon L \longrightarrow f(L)/f(K)$ qui est surjectif et de noyau contenant K, donc ce dernier induit un morphisme surjectif $f\colon L/K \longrightarrow f(L)/f(K)$. □

Preuve 1. Pour tout sous-groupe H d'un groupe résoluble G, il suffit de trouver $n \in \mathbf{N}$ tel que $\mathrm{D}^{(n)}(H) = \{1\}$ et c'est évident car G est résoluble.

Soit H un sous-groupe distingué d'un groupe résoluble G. Il suffit de montrer que, si $f\colon G \longrightarrow H$ est un morphisme surjectif, alors H est résoluble. Soit $\{1\} = G_n < \cdots < G_0 = G$ une suite de composition dont les facteurs sont abéliens. Alors la suite $\{1\} = f(G_n) < \cdots < f(G_0) = H$ est bien une suite de composition d'après le lemme. Soit $i \in [\![1, n-1]\!]$. Il reste à montrer que le quotient $f(G_i)/f(G_{i+1})$ est abélien. Celui-ci est un quotient de G_i/G_{i+1} d'après le lemme. Or G_i/G_{i+1} est abélien, donc $f(G_i)/f(G_{i+1})$ est bien abélien. Ceci montre que H est résoluble.

2. Il suffit de montrer la réciproque. On suppose que les groupes N et G/N sont résolubles. On note

$$\{1\} = N_m < \cdots < N_0 = N \quad \text{et} \quad \{1\} = K_n < \cdots < K_0 = G/N$$

deux suites de composition à facteurs abéliens. En considérant la projection $\pi\colon G \longrightarrow G/N$, on obtient une bijection entre l'ensemble des sous-groupes de G contenant N et l'ensemble des sous-groupes de G/N. On relève la seconde suite de composition. On obtient une suite $N = L_n < \cdots < L_0 = G$. En concaténant les deux suites, on récupère une suite de composition

$$\{1\} = N_m < \cdots < N_1 < N < L_{n-1} < \cdots < L_0 = G.$$

En effet, on doit vérifier $L_{i+1} \triangleleft L_i$ pour tout $i \in [\![0, n-2]\!]$ et c'est le cas puisque $K_{i+1} \triangleleft K_i$ et la bijection entre les sous-groupes de G contenant N et les sous-groupes de G/N préserve la normalité. Puis les quotients sont bien abéliens car

$$\frac{L_i}{L_{i+1}} \simeq \frac{L_i/n}{L_{i+1}/N} = \frac{K_i}{K_{i+1}}.$$

3. Soit G un groupe résoluble. Montrer qu'il est isomorphe à un groupe $\mathbf{Z}/p\mathbf{Z}$ pour un nombre premier p. Comme G est résoluble, on a $\mathrm{D}(G) < G$. Or $\mathrm{D}(G) \triangleleft G$ et G est simple, donc $\mathrm{D}(G) = \{1\}$, donc G est abélien.

Soit $g \in G \setminus \{1\}$. Alors $\langle g \rangle \neq \{1\}$ et $\langle g \rangle \triangleleft G$. Or G est simple, donc $G = \langle g \rangle$. Ceci montre que le groupe G est monogène. Or $\mathbf{Z}$ n'est pas simple, donc le groupe G est isomorphe à un groupe $\mathbf{Z}/n\mathbf{Z}$ pour un entier n. Enfin, pour tout diviseur premier p de n, le groupe $\mathbf{Z}/n\mathbf{Z}$ possède un élément d'ordre p par le théorème de CAUCHY et celui-ci doit engendrer G. Donc l'entier n est premier.

□

1.11.3 Exemples

◇ REMARQUES. – Les groupes abéliens sont résolubles.
– Les extensions de groupes abéliens sont résolubles.
– Les produits directs et semi-directs sont résolubles.

PROPOSITION 1.55. Le groupes des matrices triangulaires supérieures sur un corps quelconque et ses sous-groupes sont résolubles.

Preuve Soit k un corps. On note
– $\mathrm{T}_n(k) \subset \mathrm{GL}_n(k)$ l'ensemble des matrices triangulaires supérieures ;
– $\mathrm{U}_n(k) \subset \mathrm{T}_n(k)$ l'ensemble des matrices triangulaires supérieures contenant des 1 sur la diagonale ;
– $\mathrm{U}_n^{-\ell}(k) \subset \mathrm{U}_n(k)$ l'ensemble des matrices dont les ℓ sur-diagonales sont nulles pour tout $\ell \in [\![1, n-1]\!]$.

Alors des calculs donnent $[\mathrm{T}_n(k), \mathrm{T}_n(k)] < \mathrm{U}_n(k)$ et $[\mathrm{U}_n^{-\ell}(k), \mathrm{U}_n^{-\ell}(k)] < \mathrm{U}_n^{-(\ell+1)}(k)$ pour tout $\ell \in [\![1, n-2]\!]$. On en déduit $\mathrm{D}^{(n)}(\mathrm{T}_n(k)) = \{1\}$. □

PROPOSITION 1.56. Les p-groupes sont résolubles.

Preuve Soit G un p-groupe. On procède par récurrence sur l'entier $n \geqslant 1$ tel que $|G| = p^n$. Dans le cas $n = 1$, le groupe $G \simeq \mathbf{Z}/p\mathbf{Z}$ est abélien. Soit $n \geqslant 2$. On suppose que c'est vrai pour des groupes de d'ordres p^k avec $k < n$. Soit G un groupe d'ordre p^n. Le centre $\mathrm{Z}(G)$ est non trivial car G est un p-groupe. Les groupes $\mathrm{Z}(G)$ et $G/\mathrm{Z}(G)$ sont tous les deux résolubles, donc le groupe G est résoluble. □

PROPOSITION 1.57. Tout d'ordre inférieur à $60 = |\mathfrak{A}_5|$ est résoluble.

THÉORÈME 1.58 (BURNSIDE, 1904). Soient p et q deux nombres premiers et $\alpha, \beta \geqslant 1$ deux entiers. Alors tout groupe d'ordre $p^\alpha q^\beta$ est résoluble.

THÉORÈME 1.59 (FEIT-THOMPSON, 1963). Tout groupe d'ordre impair est résoluble.

CONTRE-EXEMPLE. La réciproque est fausse. En effet,
– les groupes $\mathfrak{S}_n$ et $\mathfrak{A}_n$ ne sont pas résolubles pour $n \geqslant 5$;
– pour un corps quelconque k, les groupes $\mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$, $\mathrm{PSL}_n(k)$ et $\mathrm{PGL}_n(k)$ ne sont pas résolubles sauf dans les cas $n = 1$ ou $n = 2$ et $k \in \{\mathbf{F}_2, \mathbf{F}_3\}$ (ceci sera montré plus tard) ;
– le groupe libre n'est pas résoluble.

1.11.4 Pourquoi le mot « résoluble » ?

Soit $P \in \mathbf{Q}[X]$ un polynôme de degré $n \geqslant 1$. On peut associer à ce polynôme une extension K_P de $\mathbf{Q}$ de telle sorte qu'il possède n racines dans K_P. Le but est de trouver une formule simple permettant de trouver les racines de P. Par exemple, pour $n = 2$, en notant $P = aX^2 + bX + c$, si $b^2 - 4ac \geqslant 0$, ses racines sont données par

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

En 1535, TARTAGLIA a trouvé une formule pour $n = 3$, puis vint FERARRI en 1555 pour $n = 4$. Pour $n = 5$, respectivement en 1824 et 1830, ABEL et GALOIS ont montré qu'il n'existait pas de formule.

On note $\mathrm{Gal}(K_p/\mathbf{Q})$ l'ensemble des automorphismes de corps $\sigma : K_P \longrightarrow K_P$ qui fixent les rationnels. Alors on a le résultat admis suivant : le groupe $\mathrm{Gal}(K_P/\mathbf{Q})$ est résoluble si et seulement si l'équation $P(x) = 0$ est résoluble par radicaux. Ainsi, le polynôme $P := x^5 - 4x + 2$ est résoluble par radicaux car $\mathrm{Gal}(K_P/\mathbf{Q}) \simeq \mathfrak{S}_5$.

Chapitre 2
GÉOMÉTRIE AFFINE

2.1 C'EST QUOI ?

La géométrie affine réelle est la géométrie qu'on a pratiquée avant la découverte de l'algèbre linéaire. Cependant, on va utiliser l'algèbre linéaire pour construire la géométrie affine.

DÉFINITION 2.1. Un ensemble $\mathbb{A}$ est muni d'une structure d'*espace affine* par la donnée d'une action simplement transitive d'un espace vectoriel E sur $\mathbb{A}$. Cet espace vectoriel est la *direction* de $\mathbb{A}$

On note $\alpha : E \longrightarrow \mathfrak{S}(\mathbb{A})$ cette action. Pour $A \in \mathbb{A}$ et $u \in E$, on notera $A + u := \alpha(u)(A)$. Comme l'action est simplement transitive, il existe une application

$$\Theta : \begin{vmatrix} \mathbb{A} \times \mathbb{A} \longrightarrow E, \\ (A, B) \longmapsto \overrightarrow{AB} \end{vmatrix}$$

telle que, pour tous $A, B \in \mathbb{A}$, le vecteur $\Theta(A, B) \in E$ est l'unique vecteur tel que $A + \Theta(A, B) = B$.

PROPOSITION 2.2. 1. Pour tout $A \in \mathbb{A}$, l'application $\Theta_A := \Theta(A, \cdot)$ est une bijection.
2. Pour tous $A, B, C \in \mathbb{A}$, on a $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

Preuve Montrons le second point. Soient $A, B, C \in \mathbb{A}$. On a

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

Comme l'action est simplement transitive, on obtient la relation de CHASLES. □

◇ REMARQUE. La relation de CHASLES peut se reformuler sous la forme

$$\forall u, v \in E,\ \forall A \in \mathbb{A}, \quad (A + u) + v = A + (u + v).$$

DÉFINITION 2.3. Les éléments de $\mathbb{A}$ s'appellent les *points* et les éléments de E les *vecteurs*. On appelle dimension de $\mathbb{A}$ la dimension de E, notée $\dim \mathbb{A}$.

▷ EXEMPLES. – L'ensemble $\emptyset$ est un espace affine dirigé par n'importe quel espace vectoriel. On convient qu'il n'a pas de dimension.

– Tout espace vectoriel E agit sur lui-même par translation à gauche. Cette action étant simplement transitive, l'espace vectoriel est muni d'une structure d'espace affine. L'application $\Theta : E \times E \longrightarrow E$ est alors donnée par la relation $\Theta(u, v) = v - u$ pour tous points $u, v \in E$.

– Soient $\mathbb{A}_1$ et $\mathbb{A}_2$ deux espaces affines dirigées par des espaces vectoriels E_1 et E_2. Alors l'ensemble $\mathbb{A}_1 \times \mathbb{A}_2$ est un espace affine dirigé par l'espace vectoriel $E_1 \times E_2$ *via* l'application

$$\Theta : \begin{vmatrix} (\mathbb{A}_1 \times \mathbb{A}_2) \times (\mathbb{A}_1 \times \mathbb{A}_2) \longrightarrow E_1 \times E_2, \\ ((A_1, B_1), (A_2, B_2)) \longmapsto (\overrightarrow{A_1 A_2}, \overrightarrow{B_1 B_2}). \end{vmatrix}$$

2.2 PROPRIÉTÉS

Dans toute la suite, on fixe un espace affine $\mathbb{A}$.

PROPOSITION 2.4. Soient $A, A', B, B' \in \mathbb{A}$. Alors
1. $\overrightarrow{AA} = 0$;
2. $\overrightarrow{AB} = -\overrightarrow{BA}$;

3. $\overrightarrow{AA'} = \overrightarrow{BB'}$ si et seulement si $\overrightarrow{AB} = \overrightarrow{A'B'}$.

Preuve 1. On a $A + 0 = \alpha(0)(A) = \{0\} + A = A$. Comme α est simplement transitive, on en déduit $\overrightarrow{AA} = 0$.
2. On a $A + \overrightarrow{AB} = B = \alpha(\overrightarrow{AB})(A)$, donc $A = \alpha(-\overrightarrow{AB})(B) = B + (-\overrightarrow{AB})$. Par unicité, on a donc $\overrightarrow{BA} = -\overrightarrow{AB}$.
3. Il suffit d'appliquer la relation de CHASLES et le point précédent. □

◇ REMARQUE. Soit $A \in \mathbb{A}$. Avec le point 1 de la proposition 2.2, on en tire une structure de $\mathbb{A}$-espace vectoriel où l'on décrète $M + N = Q$ lorsque $\overrightarrow{AM} + \overrightarrow{AN} = \overrightarrow{AQ}$ pour tous $M, N, Q \in \mathbb{A}$. On note $\mathbb{A}_A$ cette structure. Elle dépend du point A et ce dernier devient le neutre de l'espace vectoriel $\mathbb{A}_A$. Ainsi tout espace affine est muni d'une structure d'espace vectoriel par le choix d'une origine A, mais cette structure n'est pas canonique.

2.3 SOUS-ESPACES AFFINES

DÉFINITION 2.5. Une partie $\mathscr{F}$ de $\mathbb{A}$ est un *sous-espace affine* de $\mathbb{A}$ s'il est vide ou s'il existe un point $A \in \mathscr{F}$ tel que l'image $\Theta_A(\mathscr{F})$ soit un sous-espace vectoriel de E.

PROPOSITION 2.6. 1. Soit F un sous-espace affine de $\mathbb{A}$. Alors il existe un unique sous-espace vectoriel F de E telle que $\Theta_B(\mathscr{F}) = F$ pour tout $B \in \mathscr{F}$. On dit que le sous-espace affine $\mathscr{F}$ est dirigé par F et on note $\overrightarrow{\mathscr{F}} = F$.
2. Soient F un sous-espace vectoriel de E et $A \in \mathbb{A}$. Alors il existe un sous-espace affine dirigé par F et passant par A.

Preuve 1. Soit $A \in \mathscr{F}$ un point fixé. On note $F := \Theta_A(\mathscr{F})$. Soit $B \in \mathscr{F}$. Montrons $\Theta_B(\mathscr{F}) = F$ par double inclusion. Pour l'inclusion directe, pour tout $M \in \mathscr{F}$, on a

$$\Theta_B(M) = \overrightarrow{BM} = -\overrightarrow{AB} + \overrightarrow{AM} \in F.$$

Réciproquement, soit $u \in F$. Comme Θ_A est une bijection, il existe $M \in \mathscr{F}$ tel que $\overrightarrow{AM} = u$. On pose $N := M + \overrightarrow{AB}$. Comme $\overrightarrow{MN} = \overrightarrow{AB}$, on a $\overrightarrow{BN} = \overrightarrow{BA} + \overrightarrow{AM} + \overrightarrow{MN} = \overrightarrow{AM} = u$, donc $u \in \Theta_B(\mathscr{F})$. Ceci montre $\Theta_B(\mathscr{F}) = F$ et conclut.
2. Il suffit de poser $\mathscr{F} := \{A + u \mid u \in F\}$. □

◇ REMARQUE. Pour tout sous-espace affine $\mathscr{F}$ et tous points $M, N \in \mathscr{F}$, on a $\overrightarrow{MN} \in \overrightarrow{\mathscr{F}}$.

▷ EXEMPLES. – Un sous-espace affine de $\mathbb{A}$ de dimension nulle est constitué d'un point.
– Les sous-espaces affines de $\mathbb{A}$ de dimensions une, deux ou $\dim \mathbb{A}$ sont respectivement appelés les droites affines, les plans affines et les hyperplans affines de $\mathbb{A}$.
– Soient $f : E \to F$ une application linéaire entre deux espaces vectoriels. Pour tout $v \in F$, la préimage $f^{-1}(\{v\})$ est un sous-espace affine dirigé par $\operatorname{Ker} f$.
– Les sous-espaces vectoriels de la forme $F + u_0 \subset E$ sont les sous-espaces affines de E. Les sous-espaces vectoriels sont les sous-espaces affines contenant l'élément neutre.

◇ REMARQUE. Une intersection quelconque de sous-espaces affines est un sous-espace affine. On peut donc définir le sous-espace affine engendré par une partie.

2.4 PARALLÉLISME

DÉFINITION 2.7. Deux sous-espaces affines $\mathscr{F}$ et $\mathscr{G}$ d'un espace affine sont *parallèle* s'ils ont la même direction. On note alors $\mathscr{F} \parallel \mathscr{G}$.

◇ REMARQUES. – Dans un plan affine, deux droites affines sont parallèles si et seulement si elles sont disjointes. Ce n'est pas vrai en dimension supérieure à 3. Montrons le sens réciproque par contraposée. Soient $\mathscr{D}$ et $\mathscr{D}'$ deux droites non parallèles dirigées par des espaces vectoriels D et D'. Alors ces espaces vectoriels sont des droites vectorielles d'un plan et $D \neq D'$, donc $D \cap D' = \{0\}$ et, en notant P la direction du plan affine, on a $P = D + D'$. Soient $A \in \mathscr{D}$ et $A' \in \mathscr{D}'$. Alors il existe un unique couple de vecteurs $(u, v) \in D \times D'$ tel que $A + u = A' + v$. Alors l'intersection $\mathscr{D} \cap \mathscr{D}'$ est non vide et réduite à un point.
– Deux sous-espaces affines $\mathscr{F}$ et $\mathscr{G}$ parallèles sont égaux ou disjoints.
– Pour tout point d'un espace affine, il passe une unique droite parallèle à une droite donnée.

PROPOSITION 2.8. Soient $\mathscr{F}$ et $\mathscr{G}$ deux sous-espaces affines d'un espace affine $\mathbb{A}$, de direction F, G et E. On suppose que $F+G=E$. Alors tout sous-espace affine parallèle à $\mathscr{G}$ rencontre $\mathscr{F}$. De plus, si $\mathscr{F}\cap\mathscr{G}=\{0\}$, alors l'intersection de $\mathscr{F}$ avec tout sous-espace affine $\mathscr{G}'$ parallèle à $\mathscr{G}$ est réduite à un point.

2.5 APPLICATION AFFINE

2.5.1 Définition

DÉFINITION-PROPOSITION 2.9. Une application $\varphi\colon \mathscr{E}\longrightarrow\mathscr{F}$ entre deux sous-espaces affines de directions respectives E et F est dite *affine* lorsqu'il existe un point $O\in\mathscr{E}$ et une application linéaire $f\colon E\longrightarrow F$ tels que

$$\forall M\in\mathscr{E},\quad \overrightarrow{\varphi(O)\varphi(M)}=f(\overrightarrow{OM}).$$

L'application f ne dépend pas du choix du point O et est unique. On dit que cette application est le *linéarisé* de l'application affine φ, on le note $\vec{\varphi}$. Elle vérifie

$$\forall M,N\in\mathscr{E},\quad \overrightarrow{\varphi(M)\varphi(N)}=\vec{\varphi}(\overrightarrow{MN}).$$

Preuve L'application $f\colon E\longrightarrow F$ est donnée par la relation $f(u)=\overrightarrow{\varphi(O)\varphi(O+u)}$ pour tout $u\in E$ ce qui assure son unicité. Montrons la dernière relation. Soient $A,M\in\mathscr{E}$. Alors la relation de CHASLES donne

$$\begin{aligned}\overrightarrow{\varphi(A)\varphi(M)}&=\overrightarrow{\varphi(A)\varphi(O)}+\overrightarrow{\varphi(O)\varphi(M)}\\&=f(\overrightarrow{AO})+f(\overrightarrow{OM})\\&=f(\overrightarrow{AO}+\overrightarrow{AM})\\&=f(\overrightarrow{AM}).\end{aligned}$$

□

▷ EXEMPLES. – Les applications constantes sont affines.

– Soit k un corps. Alors les applications affines de k dans lui-même sont exactement de la forme $x\longmapsto ax+b$ avec $a,b\in k$. De même, pour tous entiers $e,d\geqslant 1$, les applications affines de k^d dans k^e sont exactement de la forme $x\longmapsto Ax+b$ avec $A\in\mathscr{M}_{e,d}(k)$ et $b\in k^e$.

En effet, montrons cela. Soit $\varphi\colon k^d\longmapsto k^e$ une application affine. On note $b:=\varphi(0)\in k^e$ et $A\in\mathscr{M}_{e,d}(k)$ la matrice du linéarisé $\vec{\varphi}$ dans la base canonique. Alors $\varphi(x)=Ax+b$ pour tout $x\in k^d$. Réciproquement, toute application de cette forme est bien affine.

– Les applications affines entre deux espaces vectoriels E et F sont exactement celles de la forme $x\longmapsto f(x)+u_0$ avec $f\in\mathscr{L}(E,F)$ et $u_0\in F$. Les applications linéaires de E dans F sont exactement les applications affines qui envoient 0 sur 0.

PROPOSITION 2.10. Soient $\mathscr{F}$ et $\mathscr{G}$ deux sous-espaces affines d'un espace affine $\mathscr{E}$, de direction F, G et E. On suppose que $E=F\oplus G$. Pour tout $x\in\mathscr{E}$, on note $\pi(x)\in\mathscr{F}$ l'unique point d'intersection de $\mathscr{F}$ et du sous-espace affine parallèle à G et contenant x. Alors l'application $x\in\mathscr{E}\longmapsto\pi(x)\in\mathscr{F}$ est affine, appelée la projection sur $\mathscr{F}$ parallèlement à $\mathscr{G}$. Son linéarisé est la projection sur F parallèlement à G.

Preuve Soit $A\in\mathscr{E}$ l'unique point telle que $\mathscr{F}\cap\mathscr{G}=\{A\}$. Il est fixé par l'application π. On le choisit pour origine de $\mathscr{E}$. Ainsi l'ensemble $\mathscr{E}$ est muni d'une structure d'espace vectoriel où les sous-ensembles $\mathscr{F}$ et $\mathscr{G}$ deviennent des sous-espaces vectoriels. Alors l'application π est la projection sur $\mathscr{F}$ parallèlement à $\mathscr{G}$ ce qui en fait une application linéaire et donc une application affine. □

2.5.2 Translations et homothéties

DÉFINITION 2.11. Une application affine $\varphi\colon\mathscr{E}\longrightarrow\mathscr{E}$ est une *translation* lorsque $\vec{\varphi}=\mathrm{Id}_E$.

◇ REMARQUE. Une telle application est bien de la forme $\varphi(M)=M+u$ pour tout $M\in\mathscr{E}$ où le vecteur $u:=\overrightarrow{A\varphi(A)}$ où $A\in\mathscr{E}$ ne dépend pas de ce point A. On note $t_u:=\varphi$ cette translation.

DÉFINITION 2.12. Soient $O\in\mathscr{E}$ et $\lambda\in k$. Alors l'application $\varphi\colon\mathscr{E}\longrightarrow\mathscr{E}$ définie par

$$\overrightarrow{O\varphi(M)}=\lambda\overrightarrow{OM},\quad M\in\mathscr{E}$$

est affine, son linéarisé est l'homothétie de rapport λ. On l'appelle l'homothétie de centre O et de rapport λ. On la note $h_{O,\lambda}$.

2.5.3 Propriétés

PROPOSITION 2.13. 1. L'image d'un sous-espace affine par une application affine est un sous-espace affine.
2. Les images de trois points alignés par une application affine sont alignées.
3. L'image réciproque d'un sous-espace affine par une application affine est un sous-espace affine.

PROPOSITION 2.14. La composée de deux applications affines est une application affine. De plus, pour toutes applications affines $\varphi : \mathscr{E} \longrightarrow \mathscr{F}$ et $\psi : \mathscr{F} \longrightarrow \mathscr{G}$, on a $\overrightarrow{\psi \circ \varphi} = \vec{\psi} \circ \vec{\varphi}$.

Preuve Montrons uniquement la relation. Soient $M, N \in \mathscr{E}$. On a

$$\overrightarrow{\psi(\varphi(M))\psi(\varphi(N))} = \psi(\overrightarrow{\varphi(M)\varphi(N)}) = \vec{\psi}(\vec{\varphi}(\overrightarrow{MN}))$$

ce qui donne bien $\overrightarrow{\psi \circ \varphi} = \vec{\psi} \circ \vec{\varphi}$. □

2.6 GROUPE AFFINE

PROPOSITION 2.15. Une application affine φ est bijective si et seulement si l'application $\vec{\varphi}$ est bijective. Dans ce cas, sa réciproque φ^{-1} est affine de linéarisé $\vec{\varphi}^{-1}$.

Preuve Pour tous points $X, Y \in \mathscr{E}$, on a $f(X) = f(Y) \Leftrightarrow \overrightarrow{\varphi(X)\varphi(Y)} = \vec{0} \Leftrightarrow \vec{\varphi}(\overrightarrow{XY}) = \vec{0}$. Donc l'application φ est injective si et seulement si son linéarisé l'est.

Soit $O \in \mathscr{E}$. On pose $O' := \varphi(O) \in \mathscr{F}$. Soit $M' \in \mathscr{F}$. L'équation $\varphi(M) = M'$ pour $M \in \mathscr{E}$ est équivalente à avoir la relation $\vec{\varphi}(\overrightarrow{OM}) = \overrightarrow{\varphi(O)\varphi(M)}$. Donc l'application φ est surjective si et seulement si son linéarisé l'est.

On suppose que l'application φ est bijective. Montrons que sa réciproque est affine. En effet, pour tous points $A, B \in \mathscr{E}$, on a

$$\overrightarrow{AB} = \overrightarrow{\varphi(\varphi^{-1}(A))\varphi(\varphi^{-1}(B))} = \vec{\varphi}(\overrightarrow{\varphi^{-1}(A)\varphi^{-1}(B)}),$$

donc

$$\vec{\varphi}^{-1}(\overrightarrow{AB}) = \overrightarrow{\varphi^{-1}(A)\varphi^{-1}(B)}.$$

□

COROLLAIRE 2.16. Les bijections affines d'un espace affine $\mathscr{E}$ dans lui-même forme un groupe, appelé le *groupe affine* et noté $\mathrm{GA}(\mathscr{E})$.

PROPOSITION 2.17. L'application $\vec{\cdot} : \mathrm{GA}(\mathscr{E}) \longrightarrow \mathrm{GL}(E)$ est surjective, de noyau le groupe $\mathrm{T}(\mathscr{E})$ des translations. La suite exacte

$$\{\vec{0}\} \longrightarrow \mathrm{T}(\mathscr{E}) \longrightarrow \mathrm{GA}(\mathscr{E}) \longrightarrow \mathrm{GL}(E) \longrightarrow \{1\}$$

est scindée. On obtient le produit semi-direct $\mathrm{GA}(\mathscr{E}) = \mathrm{T}(E) \rtimes \mathrm{GL}(E)$.

Preuve On peut supposer $\mathscr{E} = E$ en choisissant une origine $O \in \mathscr{E}$ Ainsi le groupe $\mathrm{GL}(E)$ est le stabilisateur de O dans $\mathrm{GA}(\mathscr{E})$. En particulier, l'application $\vec{\cdot}$ restreinte au stabilisateur de O est l'identité, donc elle est surjective. Il reste à montrer le produit semi-direct $\mathrm{GA}(E) = \mathrm{T}(E) \rtimes \mathrm{GL}(E)$. Premièrement, on a bien $\mathrm{T}(E) \cap \mathrm{GL}(E) = \{\mathrm{Id}\}$. Deuxièmement, montrons que $\mathrm{T}(E)\,\mathrm{GL}(E) = \mathrm{GA}(E)$. Soit $g \in \mathrm{GA}(E)$. Comme $\mathrm{T}(E)$ agit transitivement sur E, il existe $u \in E$ tel que $g(O) = t_u(O)$, donc l'application $t_{-u} \circ g$ fixe le point O, donc $f := t_{-u} \circ g \in \mathrm{GL}(E)$. On a donc obtenu $g = t_u \circ f$ avec $f \in \mathrm{GL}(E)$. D'où $\mathrm{T}(E)\,\mathrm{GL}(E) = \mathrm{GA}(E)$. Cela montre le produit semi-direct. □

COROLLAIRE 2.18. Soit $\varphi : E \longrightarrow E$ une application affine d'un espace vectoriel E dans lui-même. Alors il existe un unique couple $(u, v) \in E \times E$ telle que $\varphi = t_u \circ \vec{\varphi} = \vec{\varphi} \circ t_v$.

2.7 LE THÉORÈME DE THALÈS

DÉFINITION-PROPOSITION 2.19. Soient (A, B, C) un triplet de points distincts et alignés sur une droite affine. Alors il existe un unique scalaire $\lambda \in k$ tel que $\overrightarrow{AB} = \lambda \overrightarrow{AC}$. On note alors

$$\frac{\overline{AB}}{\overline{AC}} := \lambda.$$

THÉORÈME 2.20 (THALÈS, version générale). Soient d, d' et d'' trois droites parallèles d'un plan affine quelconque. Soient $\mathscr{D}_1$ et $\mathscr{D}_2$ deux droites non parallèles à d et d'. Pour $i \in \{1,2\}$ et $\dagger \in \{\emptyset, ', ''\}$, on note $A_i^\dagger$ le point

d'intersection des droites $d^\dagger$ et $\mathscr{D}_i$. Alors

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

Réciproquement, tout point B vérifiant

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

est égal à A_2''.

Preuve On note π la projection sur $\mathscr{D}_2$ parallèlement à d. On a $\pi(A_1) = A_2$, $\pi(A_1') = A_2'$ et $\pi(A_1'') = A_2''$. On note

$$\lambda := \frac{\overline{A_1A_1''}}{\overline{A_1A_1'}}.$$

Alors $\overrightarrow{A_1A_1''} = \lambda\overrightarrow{A_1A_1'}$, donc

$$\overrightarrow{A_2A_2''} = \overrightarrow{\pi(A_1)\pi(A_1'')} = \vec{\pi}(\overrightarrow{A_1A_1''}) = \lambda\vec{\pi}(\overrightarrow{A_1A_1'}) = \lambda\overrightarrow{\pi(A_1)\pi(A_1')} = \lambda\overrightarrow{A_2A_2'}.$$

Par unicité du rapport, on a

$$\lambda = \frac{\overline{A_2A_2''}}{\overline{A_2A_2'}}.$$

Montrons la réciproque. Soit B un tel point. Alors

$$\frac{\overline{A_1B}}{\overline{A_1A_1'}} = \frac{\overline{A_2A_2''}}{\overline{A_2A_2'}} = \frac{\overline{A_1A_1''}}{\overline{A_1A_1'}} = \lambda,$$

donc $\overrightarrow{A_1B} = \lambda\overrightarrow{A_1A_1'}$. Par unicité, on en déduit $B = A_2''$. □

THÉORÈME 2.21 (THALÈS, version troisième). Soient $\mathscr{D}_1$ et $\mathscr{D}_2$ deux droites sécantes en un point A et d et d' deux droites parallèles non parallèles à $\mathscr{D}_1$ et $\mathscr{D}_2$. Pour $i \in \{1,2\}$ et $\dagger \in \{\emptyset, '\}$, on note $A_i := \mathscr{D}_i \cap d^\dagger$. Alors

$$\frac{\overline{AA_1'}}{\overline{AA_1}} = \frac{\overline{AA_2'}}{\overline{AA_2}}.$$

Preuve On applique le théorème précédent. □

Chapitre 3
GÉOMÉTRIE PROJECTIVE

3.1 ESPACES PROJECTIFS

3.1.1 Définition

DÉFINITION 3.1. Soient k un corps et E un k-espace vectoriel de dimension finie. L'*espace projectif* sur E est l'ensemble des droites vectorielles de E, noté $\mathbf{P}(E)$. Autrement dit, c'est le quotient de $E \setminus \{0\}$ par l'action de $k^\times$ par homothétie.

NOTATION. On note $\pi\colon E \setminus \{0\} \longrightarrow \mathbf{P}(E)$ la projection. La quantité $\dim \mathbf{P}(E) := \dim E - 1$ est la dimension de l'espace projectif sur E.

▷ EXEMPLES. – On a $\mathbf{P}(\{0\}) = \emptyset$ et $\mathbf{P}(E) = \{E\}$ pour un espace vectoriel E de dimension 1.
– Pour un espace vectoriel E de dimension 2 (respectivement 3), on dit que son espace projectif est une *droite projective* (respectivement un *plan projectif*).
– Pour tout entier $n \geqslant 0$, l'espace projectif standard sur k de dimension n est l'espace projectif $\mathbf{P}^n(k) := \mathbf{P}(k^{n+1})$.

3.1.2 Topologie lorsque $k = \mathbf{R}$ ou $\mathbf{C}$

On suppose $k = \mathbf{R}$ ou $\mathbf{C}$. Soit E un k-espace vectoriel de dimension finie. On munit E de la topologie usuelle donnée par une base et on munit $\mathbf{P}(E)$ de la topologie quotient, c'est-à-dire de la topologie la plus fine telle que la projection $\pi\colon E \setminus \{0\} \longrightarrow \mathbf{P}(E)$ soit continue.

EXERCICE 3.1. Montrer que la projection π est une application ouverte. On pourra utiliser le fait que $\mathbf{P}(E)$ est un quotient de $E \setminus \{0\}$ par une action de groupe.

En pratique, une suite $(\ell_n)_{n\in\mathbf{N}}$ de $\mathbf{P}(E)$ converge vers un élément $\ell_\infty \in \mathbf{P}(E)$ si et seulement s'il existe une suite $(u_n)_{n\in\mathbf{N}} \in \prod_{n\in\mathbf{N}} \ell_n$ et un élément $u_\infty \in \ell_\infty$ tous non nuls tels que $u_n \to u_\infty$.

EXERCICE 3.2. On suppose $k = \mathbf{R}$.

1. Montrons que la projection $\pi\colon \mathbf{S}^d \longrightarrow \mathbf{P}^d(\mathbf{R})$ induit un homéomorphisme $\mathbf{S}^d / \{\pm \mathrm{Id}\} \simeq \mathbf{P}^d(\mathbf{R})$.
2. En déduire que $\mathbf{P}^1(\mathbf{R})$ est homéomorphe à $\mathbf{S}^1$.
3. Trouver un ouvert de $\mathbf{P}^2(\mathbf{R})$ homéomorphe à un ruban de MÖBIUS.
4. Trouver un recollement des côtés d'un carré homéomorphe à $\mathbf{P}^2(\mathbf{R})$.

On suppose maintenant $k = \mathbf{C}$.

5. Montrons que l'application $\pi\colon \mathbf{S}^{2d+1} \subset \mathbf{C}^{d+1} \longrightarrow \mathbf{P}^d(\mathbf{R})$ induit un homéomorphisme $\mathbf{S}^{2d+1}/\mathbf{S}^1 \simeq \mathbf{P}^d(\mathbf{C})$ où l'action de $\mathbf{S}^1$ sur $\mathbf{S}^{2d+1}$ est donnée par $(\lambda, x) \longmapsto \lambda x$.
6. En déduire que $\mathbf{P}^1(\mathbf{C})$ est homéomorphe à $\mathbf{S}^2$.

LEMME 3.2. Soit $f\colon X \longrightarrow Y$ une bijection continue entre deux espaces topologiques séparés. Si X est compact, alors f est un homéomorphisme.

3.1.3 Sous-espaces projectifs

DÉFINITION 3.3. Une partie $V \subset \mathbf{P}(E)$ est un *sous-espace projectif* s'il existe un sous-espace vectoriel $\overline{V}$ de E tel que $\pi(\overline{V} \setminus \{0\}) = V$. Ce sous-espace vectoriel $\overline{V}$ est unique.

◇ REMARQUE. Par définition, on a une bijection entre les sous-espaces projectifs de dimension k et les sous-espaces vectoriels de dimension $k+1$.

PROPOSITION 3.4. Soient V et W deux sous-espaces projectifs de $\mathbf{P}(E)$.

1. Si $\dim V + \dim W \geqslant \dim \mathbf{P}(E)$, alors $V \cap W \neq \emptyset$.
2. En particulier, si $\dim \mathbf{P}(E) = 2$, alors deux droites quelconques de $\mathbf{P}(E)$ sont concourantes.
3. Soient H un hyperplan projectif de $\mathbf{P}(E)$ et $m \in \mathbf{P}(E) \setminus H$. Alors toute droite contenant m rencontre H en un unique point.

Preuve 1. On suppose $\dim V + \dim W \geqslant d := \dim \mathbf{P}(E)$. On sait que

$$\dim \overline{V} + \dim \overline{W} = \dim(\overline{V} + \overline{W}) + \dim(\overline{V} \cap \overline{W}).$$

Par ailleurs, on a les inégalités

$$\begin{cases} \dim \overline{V} + \dim \overline{W} = \dim V + \dim W + 2 \geqslant d + 2, \\ \dim(\overline{V} + \overline{W}) \leqslant \dim E = d + 1. \end{cases}$$

On en déduit $\dim(\overline{V} \cap \overline{W}) \geqslant (d+2) - (d+1) = 1$, donc $V \cap W \neq \emptyset$.

2. C'est immédiat avec le point 1.
3. On applique le point 1 avec $W := H$ et $V := (mA)$ avec $A \in \mathbf{P}(E)$. Pour montrer l'unicité, on a

$$\begin{aligned} 2 + d = \dim \overline{V} + \dim \overline{W} &= \dim(\overline{V} + \overline{W}) + \dim(\overline{V} \cap \overline{W}) \\ &= d + 1 + \dim(\overline{V} \cap \overline{W}) \end{aligned}$$

car $\overline{V} + \overline{W} = E$. On en déduit $\dim(\overline{V} \cap \overline{W}) = 1$ et l'intersection $V \cap W$ est réduite à un point. □

◇ REMARQUE. Une intersection quelconque de sous-espaces projectifs est un sous-espace projectif. On peut alors définir le sous-espace projectif engendré par une partie.

3.2 LIAISON AFFINE/PROJECTIF

On va voir que la géométrie affine est incluse dans la géométrie projective. Plus précisément, on va montrer que l'espace projection de dimension n est le « complété » de l'espace affine de dimension.

3.2.1 La droite projective

Soit E un k-espace vectoriel de dimension 2. On choisit une base (e_1, e_2) de E. Toutes les droites vectorielles de E rencontre la droite $\{y = 1\}$ en un unique point, sauf la droite $\{y = 0\}$. Il existe donc une bijection entre la droite projective $\mathbf{P}(E)$ privée du point $\infty := \{y = 0\}$ et la droite affine $\{y = 1\}$. On peut donc identifier la droite affine à la droite projective privée d'un point. On peut aussi dire qu'on a obtenu la droite projective en ajoutant un point (dit à l'infini) à la droit affine. En résumé, la bijection est

$$\left|\begin{array}{rl} \{y = 1\} \cup \{\infty\} & \longrightarrow \mathbf{P}(E), \\ (x, 1) & \longmapsto \mathrm{Vect}\{(x, 1)\}, \\ \infty & \longmapsto \mathrm{Vect}\{(1, 0)\}. \end{array}\right.$$

De même, lorsque $E = k^2$, elle s'écrit

$$\left|\begin{array}{rl} \hat{k} := k \cup \{\infty\} & \longrightarrow \mathbf{P}^1(k), \\ x & \longmapsto \mathrm{Vect}\{(x, 1)\}, \\ \infty & \longmapsto \mathrm{Vect}\{(1, 0)\}. \end{array}\right.$$

◇ REMARQUE. Lorsque $k \in \{\mathbf{R}, \mathbf{C}\}$, on munit $\hat{k}$ de la topologie suivante : les ouverts de $\hat{k}$ contiennent les ouverts de k et les ensemble $k \setminus K \cup \{\infty\}$ pour des compacts K de k. Alors l'ensemble $\hat{k}$ est un compact, appelée le *compactifié* d'ALEXANDROV.

EXERCICE 3.3. Montrons qu'on a des homéomorphismes $\hat{\mathbf{R}} \simeq \mathbf{S}^1$ et $\hat{\mathbf{C}} \simeq \mathbf{S}^2$. On pourra utiliser la projection stéréographique.

3.2.2 Le plan projectif

Soit E un k-espace vectoriel de dimension 3. On choisit une base (e_1, e_2, e_3) de E. On considère l'espace affine $\mathscr{F} := \{z = 1\}$ dont on note F sa direction. Alors on a l'alternative suivante : pour toute droite D de E, on a

– soit $\sharp(D \cap \mathscr{F}) = 1$;
– soit $D \subset F$.

On a donc deux bijections entre $\mathbf{P}(E) \setminus \mathbf{P}(F)$ et $\mathscr{F}$ et entre $\mathscr{F} \sqcup \mathbf{P}(F)$ et $\mathbf{P}(E)$.

3.2.3 Cas général : la complétion projective d'un espace affine

DÉFINITION 3.5. Soit $\mathscr{F}$ un k-espace affine de direction F. L'espace projectif $\mathbf{P}(F \times k)$ est le *complété projectif* de $\mathscr{F}$ et le sous-espace projectif $\mathbf{P}(F \times \{0\})$ est l'*hyperplan à l'infini* de $\mathscr{F}$.

◇ REMARQUE. Cette construction est canonique. Soit $O \in \mathscr{F}$. On plonge $\mathscr{F}$ dans $F \times k$ par l'injection

$$\begin{vmatrix} \mathscr{F} \longrightarrow F \times k, \\ M \longmapsto (\overrightarrow{OM}, 1). \end{vmatrix}$$

Ainsi on peut identifier $\mathscr{F}$ à $F \times \{1\}$ et F à $F \times \{0\}$. Toute droite vectorielle de $F \times k$ vérifie l'alternative suivante :

– soit elle rencontre $\mathscr{F}$ en un point ;
– soit elle est incluse dans $\mathscr{F} \times \{0\}$.

On peut donc écrire $\mathbf{P}(F \times k) = \mathscr{F} \sqcup \mathbf{P}(F \times \{0\})$. L'hyperplan à l'infini de $\mathscr{F}$ est constitué des droites de F, c'est-à-dire des directions des droites de $\mathscr{F}$. Par exemple, avec $k = \mathbf{R}$ et $F = \mathscr{F} = \mathbf{R}^2$, on obtient $\mathbf{P}^2(\mathbf{R}) = \mathbf{R}^2 \sqcup \mathbf{P}^1(\mathbf{R})$.

3.2.4 Droites affines, droites projectives

Soient $\mathscr{F}$ un espace affine de direction F et $\mathscr{D}$ une droite affine. On note $P_{\mathscr{D}} := \mathrm{Vect}\,\mathscr{D}$ et $d := \pi(P_{\mathscr{D}})$. Alors d est une droite projective égale à $\mathscr{D}$. En notant $\infty_{\mathscr{D}} \in \mathbf{P}(F)$ la direction de $\mathscr{D}$, on a $\mathscr{D} = \{\infty_{\mathscr{D}}\}$. Ainsi d est le complété projectif de la direction D de $\mathscr{D}$.

◇ REMARQUE. L'hyperplan à l'infini $\mathbf{P}(F)$ est composé des points $\infty_{\mathscr{D}}$ pour toutes droites affines $\mathscr{D}$.

3.2.5 Intersection de droites dans le plan

Soit $\mathscr{F}$ un espace affine de direction F. Les éléments de $\mathbf{P}(F \times k)$ sont

– $d = \mathscr{D} \cup \{\infty_{\mathscr{D}}\}$ pour toute droite affine $\mathscr{D}$ de F ;
– $\mathbf{P}(F \times \{0\})$ la droite à l'infini.

Soient $\mathscr{D}$ et $\mathscr{D}'$ deux droites affines de $\mathscr{F}$ se recoupant en un seul point $m \in \mathscr{F}$, *i. e.* on a $\mathscr{D} \cap \mathscr{D}' = \{m\}$. Alors en notant $d := \mathscr{D} \cup \{\infty_{\mathscr{D}}\}$ et $d' := \mathscr{D}' \cup \{\infty_{\mathscr{D}'}\}$, on a $d \cap d' = \{m\}$, donc $P_{\mathscr{D}} \cap P_{\mathscr{D}'} = (Om)$. Maintenant, si $\mathscr{D}$ et $\mathscr{D}'$ sont parallèles, alors $d \cap d' = \{\infty_{\mathscr{D}}\}$, donc $P_{\mathscr{D}} \cap P_{\mathscr{D}'} = D$.

3.2.6 Choix de l'infini

Dans un espace projectif, il n'y a pas d'hyperplan à l'infini. Autrement dit, on peut choisir n'importe quel hyper comme étant l'hyperplan à l'infini. Soit H un hyperplan de E. Alors $\mathbf{P}(E) \setminus \mathbf{P}(H)$ est en bijection est n'importe quel hyperplan affine de E parallèle à H ne contenant pas l'origine.

3.2.7 Le théorème de TAPPAS

THÉORÈME 3.6. Soient D et D' deux droites du plan projectif P. Soient $a, b, c \in D$ et $a', b', c' \in D'$. Alors les trois points

$$\alpha := (b'c) \cap (bc'), \quad \beta := (ac') \cap (a'c) \quad \text{et} \quad \gamma := (ab') \cap (a'b)$$

sont alignés.

Preuve On envoie la droite $(\alpha\gamma)$ à l'infini. Autrement dit, on étudie ce problème dans le plan affine $\mathscr{P} := P \setminus (\alpha\gamma)$. Dire que le point α est à l'infini signifie que, dans le plan affine $\mathscr{P}$, les droites $(b'c)$ et (bc') puis (ab') et $(a'b)$ sont parallèles. On veut montrer que $\beta \in (\alpha\gamma)$.

On suppose $\mathscr{D} \cap \mathscr{D}' \neq \emptyset$. Soit $O \in \mathscr{D} \cap \mathscr{D}'$. Les droites (bc') et $(b'c)$ sont parallèles, donc le théorème de THALÈS assure qu'il existe une homothétie h de centre O telle que $h(b) = c$ et $h(c') = b'$. De même, il existe une homothétie k de centre O telle que $k(a) = b$ et $k(b') = a'$. Alors $h \circ k(a) = c$ et $k \circ h(c') = a'$. Mais comme ces homothéties ont le même centre, elle commute et donc l'homothétie $h \circ k$ vérifie $k \circ k(a) = c$ et $h \circ k(c') = a'$. On en déduit $h \circ k(ac') = (a'c)$. Or l'image d'une droite par une homothétie est une droite parallèle, donc les droites (ac') et $(a'c)$ sont parallèles. Ainsi le point β est à l'infini. On en déduit que les points α, β et γ sont alignés.

Dans le cas $\mathscr{D} \cap \mathscr{D}' = \emptyset$, *i. e.* les droites $\mathscr{D}$ et $\mathscr{D}'$ sont parallèles, on remplace les homothéties h et k par des translations. □

3.2.8 Le théorème de DESARGUES

THÉORÈME 3.7. Soient abc et $a'b'c'$ deux triangles du plan projectif. Alors les droites (aa'), (bb') et (cc') sont concourantes si et seulement si les points

$$u := (bc) \cap (b'c'), \quad v := (ac) \cap (a'c') \quad \text{et} \quad w := (ab) \cap (a'b')$$

sont alignés.

3.3 DUALITÉ PROJECTIVE

3.3.1 Dualité vectorielle

Pour un sous-espace vectoriel F d'un espace vectoriel E, on peut définir son orthogonal F° comme l'ensemble $F^\circ := \{\varphi \in E^* \mid \varphi|_F = 0\}$, ce dernier est de dimension $\dim F^\circ = \dim E - \dim F$. De même, pour un sous-espace vectoriel G de E^*, on peut définir son orthogonal G° comme l'ensemble $G^\circ := \{x \in E \mid \forall \varphi \in G, \varphi(x) = 0\}$, ce dernier est également de dimension $\dim G^\circ = \dim E - \dim G$.

Un énoncé de géométrie projective est une assertion où les hypothèses portent sur des relations d'inclusion ou d'intersection entre des points, des droites, des plans, des coniques, … et les conclusions apportent de nouvelles informations sur d'autres inclusions ou intersections entre ces objets. Par conséquent, si on a un énoncé dans $\mathbf{P}(E)$, on peut le « dualiser ». Pour cela, on commence par traduire les hypothèses dans $\mathbf{P}(E^*)$, puis on traduit les conclusions toujours dans $\mathbf{P}(E^*)$. Comme $\mathbf{P}(E^*)$ est un espace projectif comme les autres, c'est-à-dire isomorphe à $\mathbf{P}(E)$, on a obtenu un nouveau théorème !

3.3.2 Métamorphose de théorèmes

Énonçons d'abord le théorème de PAPPUS.

THÉORÈME 3.8 (PAPPUS). Soient D et D' deux droites d'un plan projectif, a, b et c trois points de E et a', b' et c' trois points de D'. Soient u, v et w les points d'intersection entre $(b'c)$ et $(c'b)$, $(c'a)$ et $(a'c)$ et (a', b) et $(b'a)$. Alors les points u, v et w sont alignés.

On peut alors métamorphoser ce théorème pour obtenir le théorème suivant.

THÉORÈME 3.9 (BRIANCHON). Soient d et d' deux points d'un plan projectif, A, B et C trois droites concourantes en d et A', B' et C' trois droites concourantes en d'. Soient U, V et W les droites joignant $B' \cap C$ et $C' \cap B$, $C' \cap A$ et $A' \cap C$ et $A' \cap B$ et $B' \cap A$. Alors les droites U, V et W sont concourantes.

De même, le sens direct du théorème de DESARGUES se métamorphose comme ce qui suit.

THÉORÈME 3.10. Soient A, B, C, A', B' et C' six droites. Soient U, V et W les droites passant par $B \cap C$ et $B' \cap C'$, $C \cap A$ et $C' \cap A'$ et $A \cap B$ et $A' \cap B'$. Si les droites U, V, W, alors les points $A \cap A'$, $B \cap B'$ et $C \cap C'$ sont alignés.

3.4 HOMOGRAPHIES

3.4.1 Transformations projectives et groupe projectif

Soient E et E' deux espaces vectoriels et $f : E \longrightarrow E'$ une application linéaire. Pour toute droite D de E telle que $D \cap \operatorname{Ker} f = \{0\}$, l'image $f(D)$ est une droite de E'. Ainsi l'application f induit une *application projective*

$$\mathbf{P}(f) : \mathbf{P}(E) \setminus \mathbf{P}(\operatorname{Ker} f) \longrightarrow \mathbf{P}(E')$$

vérifiant $\pi' \circ f = \mathbf{P}(f) \circ \pi$. En d'autres termes, le diagramme

$$\begin{array}{ccc} E & \xrightarrow{f} & E' \\ \pi \downarrow & & \downarrow \pi' \\ \mathbf{P}(E) & \xrightarrow{f'} & \mathbf{P}(E') \end{array}$$

commute. Presque toujours, on se limitera à des isomorphismes f et, dans ce cas, l'application $\mathbf{P}(f)$ est appelée une *homographie* de E. On peut vérifier que l'ensemble $\mathrm{PGL}(E)$ des homographies de E est un groupe.

PROPOSITION 3.11. L'application $\mathbf{P} : \mathrm{GL}(E) \longrightarrow \mathrm{PGL}(E)$ est un morphisme de groupes surjectif dont le noyau est le groupe des homothéties de E.

Preuve Il reste à vérifier que le noyau de $\mathbf{P}$ est le groupe de homothétie. D'abord, toutes homothéties est clairement dans le noyau. Réciproquement, soit $f \in \operatorname{Ker} \mathbf{P}$. Alors pour toute droite D de E, on a $f(D) = D$. En particulier, pour tout $u \in E \setminus \{0\}$, il existe $\lambda_u \in k$ tel que $f(u) = \lambda_u u$. Soient $u, v \in E$ deux vecteurs non colinéaires. Alors $\lambda_u u + \lambda_v v = f(u) + f(v) = f(u+v) = \lambda_{u+v} u + \lambda_{u+v} v$. Comme u et v ne sont pas colinéaires, on en déduit que $\lambda_u = \lambda_{u+v}$ et $\lambda_v = \lambda_{u+v}$. Ainsi l'application $u \neq 0 \longmapsto \lambda_u$ est constante ce qui montre que l'application f est une homothétie. □

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

3.4.2 Homographie de la droite

COORDONNÉES HOMOGÈNES. Soit $(e_1, \ldots, e_{n+1})$ une base de E. Un point $m \in \mathbf{P}(E)$ peut-être décrit par les coordonnées $(x_1, \ldots, x_{n+1})$ d'un vecteur dans la base qui engendre cette droite m. On note alors

$$m := [x_1 : \ldots : x_{n+1}].$$

HOMOGRAPHIE DE LA DROITE PROJECTIVE. Soit E un espace vectoriel de dimension 2 et soit (e_1, e_2) une base. Cette base induit une bijection canonique

$$\varphi : \begin{cases} \mathbf{P}^1(k) \longrightarrow \hat{k} := k \cup \{\infty\}, \\ [x, y] \longmapsto x/y \qquad \text{si } y \neq 0, \\ [1:0] \longmapsto \infty. \end{cases}$$

À présent, décrivons les homographies de $\mathbf{P}(E)$ dans $\hat{k}$. Une homographie de la droite projection vient d'un isomorphisme $f : E \longrightarrow E$ d'un plan vectoriel. Dans une base (e_1, e_2), on peut écrire

$$f(x, y) = (ax + by, cx + dy), \quad x, y \in k$$

où $ad - bc \neq 0$. Pour tous $x, y \in k$ avec $y \neq 0$, on a $[x : y] = [z : 1]$ avec $z := x/y$ de telle sorte que

$$f(z, 1) = (az + b, cz + d) \sim \left(\frac{az+b}{cz+d}, 0 \right)$$

dès que $cz + d \neq 0$. L'homographie induite par f sera alors notée

$$f : \begin{cases} \hat{k} \longrightarrow \hat{k}, \\ z \longmapsto \dfrac{az+b}{cz+d} \end{cases}$$

en posant $f(\infty) = f([1:0]) = a/c$ et $f(-d/c) = \infty$ et, de plus, en adoptant la convention $\lambda/0 = \infty$ et $0/\lambda = 0$ pour tout $\lambda \in k^\times$. Ces conventions sont cohérentes. En effet,

– si $y = 0$, alors $f(1, 0) = (a, c)$ et

- si $c \neq 0$, alors $(a,c) \sim (a/c, 1)$;
- si $c = 0$, alors $(a,c) \sim (1,0)$ car $a \neq 0$ puisque $ad - bc \neq 0$;

– si $cz + d = 0$, alors

- si $c \neq 0$, alors $z = -d/c$ et $f(z,1) = ((bc-ad)/c, 0) \sim (1,0)$ car $ad - bc \neq 0$;
- si $c = 0$, alors $d = 0$ ce qui est impossible.

CHOIX DE L'INFINI (SUITE). Revenons à la question de l'expédition d'objets à l'infini. Une autre façon de voir les choses est de dire qu'on applique une homographie à une figure pour la transformer en une nouvelle figure plus simple à analyser.

3.4.3 Homographies et transformations affines

PROPOSITION 3.12. Soit $\mathscr{F}$ un espace affine dirigé par une espace vectoriel E. Alors toute homographie préservant l'hyperplan à l'infini définit une transformation affine de $\mathscr{F}$. Inversement, toute transformation affine $\mathscr{F}$ se prolonge de façon unique en une homographie de $\mathbf{P}(F \times k)$ qui préserve l'hyperplan à l'infini.

Preuve Soit $g\colon \mathbf{P}(F \times k) \longrightarrow \mathbf{P}(F \times k)$ une homographie préservant l'hyperplan à l'infini $\mathbf{P}(F)$. Elle préserve également le complémentaire $\mathscr{F} = \mathbf{P}(F \times k) \setminus \mathbf{P}(F)$. Montrons que $g|_{\mathscr{F}}$ est affine. Notons $f\colon F \times k \longrightarrow F \times k$ l'automorphisme linéaire induisant g. Alors il existe un automorphisme linéaire $h\colon F \longrightarrow F$, un vecteur $v \in F$ et un scalaire $a \in k^\times$ tels que

$$f(u,0) = (h(u),0) \quad \text{et} \quad f(0,1) = (v,a), \quad u \in F.$$

Quitte à multiplier f par a^{-1}, on peut supposer $a = 1$. Ainsi l'hyperplan affine $\mathscr{F}$ est préservé par f. Comme l'application f est linéaire, l'application induit $g|_{\mathscr{F}}$ est affine. En effet, fixons le point $O := (0,1)$ comme origine de $\mathscr{F}$. Alors pour tout point $M := (u,1) \in \mathscr{F}$, on a

$$\overrightarrow{g(O)g(M)} = f(u,1) - f(0,1) = (h(u) + v, 1) - (v,1) = (h(u),0).$$

Cela montre que l'application g est affine de linéarisé g.

Réciproquement, soit $\varphi\colon \mathscr{F} \longrightarrow \mathscr{F}$ une application affine. En notant $h\colon F \to F$ son linéarisé, l'application

$$f\colon \begin{vmatrix} F \times k \longrightarrow F \times k, \\ (u,a) \longmapsto a\varphi(0,1) + (h(u),0) \end{vmatrix}$$

est linéaire, préserve $\mathscr{F}$ et induit φ. L'homographie induite par f possède alors les propriétés attendues.

L'unicité d'une telle homographie φ est claire puisqu'on a $g = \varphi$ sur $\mathscr{F}$ et, sur l'hyperplan à l'infini, elle doit envoyer l'ensemble des droites parallèles à D sur l'ensemble des droites parallèles à $\varphi(D)$, *i. e.* elle doit envoyer la droite d sur la droite $\vec{\varphi}(d)$. Autrement, l'application $g|_{\mathbf{P}(F)}$ est l'homographie induite par $\vec{\varphi}$ sur $\mathbf{P}(F)$ ce qui montre l'unicité. □

Cette démonstration permet d'identifier le groupe affine avec un sous-groupe du groupe linéaire ou du sous-groupe projectif linéaire.

PROPOSITION 3.13. Pour tout entier $d \geqslant 1$, on a

$$\mathrm{GA}(k^d) = \left\{ \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \;\middle|\; A \in \mathrm{GL}_d(k), b \in k^d \right\}.$$

3.4.4 Action de PSL(E) sur P(E)

Le *groupe spécial linéaire* $\mathrm{SL}(E)$ de E est le sous-groupe des automorphismes linéaires de E dont le déterminant vaut 1. En notant $Z := \mathrm{Z}(\mathrm{GL}(E)) \simeq k^\times$ le groupe des homothéties de E, le sous groupe $Z \cap \mathrm{SL}(E)$ est distingué dans $\mathrm{SL}(E)$: c'est le centre de $\mathrm{SL}(E)$. Le quotient $\mathrm{PSL}(E) := \mathrm{SL}(E)/(Z \cap \mathrm{SL}(E))$ s'appelle le *groupe projectif spécial linéaire*. L'action de $\mathrm{PSL}(E)$ sur $\mathbf{P}(E)$ est fidèle.

PROPOSITION 3.14. Cette action est 2-transitive.

Preuve On peut suppose $E = k^{n+1}$. Soient $m, m' \in \mathbf{P}^n(k)$ deux points distincts. Soient $u \in m$ et $u' \in m'$. Alors les vecteurs u et u' ne sont pas colinéaires et on peut compléter le couple (u,u') en une base $(u_1, \ldots, u_{n+1})$ de E. Quitte à multiplier le vecteur u_1 par un bon scalaire $\lambda \in k^\times$, on peut supposer que le déterminant de cette base vaut 1. Les vecteurs u_1 et e_2 engendrent toujours les droites m et m'. En notant $g \in \mathrm{SL}(E)$ la matrice de cette base dans la base canonique de E, on obtient $g(e_1) = u_1$ et $g(e_2) = u_2$. Cela montre la 2-transitivité. □

PROPOSITION 3.15. En dimension 2, cette action est 3-transitive.

Preuve Grâce à la proposition précédente, il suffit de montrer que le stabilisateur de 0 et ∞ agit simplement et transitivement sur $k^\times$ (cf. TD). Or ce stabilisateur est le groupe des matrices de la forme $\mathrm{diag}(\lambda, 1)$ avec $\lambda \in k^\times$: il s'identifie donc à $k^\times$ et l'action du stabilisateur sur $k^\times$ s'identifie à l'action par translation de $k^\times$ sur lui-même. Elle est donc simplement transitive. □

3.5 BIRAPPORT

En géométrie euclidienne, la distance entre deux points est essentielle. En géométrie affine, les rapports de « distances » entre deux points sont essentiels. En géométrie projective, les rapports de rapport de distance entre quatre points seront essentiels, on les appelle les birapports !

3.5.1 C'est quoi ?

En appliquant la proposition précédente, on peut définir le birapport.

DÉFINITION-PROPOSITION 3.16. Soient a, b et c trois points distincts d'une droite projective D et d un autre point. Alors il existe une unique homographie $g : D \longrightarrow \hat{k}$ telle que

$$g(a) = \infty, \quad g(b) = 0 \quad \text{et} \quad g(c) = 1.$$

Le *birapport* du quadruplet (a, b, c, d) est l'élément

$$[a, b, c, d] := g(d) \in \hat{k}.$$

◇ REMARQUE. Par définition, on a $[a, b, c, d] = \infty$, $[a, b, c, b] = 0$ et $[a, b, c, c] = 1$. Ainsi le birapport $[a, b, c, d]$ appartient à $k \setminus \{0, 1\}$ si et seulement si les quatre points sont distincts. De plus, pour tous points distincts a, b et c et tout $x \in \hat{k}$, il existe un unique point d tel que $[a, b, c, d] = x$.

PROPOSITION 3.17 (conservation du birapport). Soient D et D' deux droites projectives, $a_1, a_2, a_3, a_4 \in D$ et $a'_1, a'_2, a'_3, a'_4 \in D'$ dont les trois premiers points sont respectivement deux-à-deux distincts. Alors il existe une homographie $f : D \longrightarrow D'$ telle que $f(a_i) = a'_i$ pour tout $i \in \{1, 2, 3, 4\}$ si et seulement si

$$[a_1, a_2, a_3, a_4] = [a'_1, a'_2, a'_3, a'_4].$$

Preuve $\Leftarrow$ On suppose qu'il existe une telle homographie $f : D \longrightarrow D'$. Notons $g' : D \longrightarrow \hat{k}$ l'unique homographie telle que $g'(a'_1) = \infty$, $g'(a'_2) = 0$ et $g'(a'_3) = 1$. Par définition du birapport, on a

$$[a'_1, a'_2, a'_3, a'_4] = g'(a'_4).$$

Or l'homographie $g' \circ f$ envoie a_1 sur ∞, a_2 sur 0 et a_3 sur ∞. Par unicité, on a

$$[a_1, a_2, a_3, a_4] = g' \circ f(a_4) = g'(a'_4) = [a'_1, a'_2, a'_3, a'_4].$$

$\Rightarrow$ Réciproquement, on suppose $[a_1, a_2, a_3, a_4] = [a'_1, a'_2, a'_3, a'_4]$. Par 3-transitivité de l'action, il existe une homographie $f : D \longrightarrow D'$ telle que $f(a_i) = a'_i$ pour tout $i \in \{1, 2, 3\}$. La dernière égalité du sens directe donne alors $f(a_4) = a'_4$. □

3.5.2 Calcul du birapport

PROPOSITION 3.18. Soient $a, b, c, d \in \hat{k}$ quatre points dont les trois premiers sont distincts. Alors

$$[a, b, c, d] = \frac{(d-b)(c-a)}{(d-a)(c-b)}.$$

Preuve D'abord, on suppose $a, b, c \in k$. Alors l'unique homographie envoyant le triplet (a, b, c) sur $(\infty, 0, 1)$ est

$$z \longmapsto \frac{(z-b)(c-a)}{(z-a)(c-b)}.$$

Il suffit alors de l'évaluer au point d. Si $a = \infty$, alors cette telle unique homographe est

$$z \longmapsto \frac{z-b}{c-b}.$$

De même si $c = \infty$ ou $d = \infty$ □

◇ REMARQUE. Soient a, b et c trois points distincts d'une droite affine. On peut retrouver le rapport de longueur par la relations

$$[a,b,c,\infty] = \frac{\overline{ca}}{\overline{cb}}.$$

PROPOSITION 3.19. Soient a, b, c et d quatre points alignés distincts. Alors

$$[a,b,c,d] = [b,a,c,d]^{-1} = [a,b,d,c]^{-1} \quad \text{et} \quad [a,b,c,d] + [a,c,b,d] = 1.$$

3.5.3 Birapport de quatre droites concourantes

DÉFINITION-PROPOSITION 3.20. Soient D et D' deux droites d'un plan projectif et o un point en dehors de ces droites. Alors l'application bien définie

$$\begin{vmatrix} D \longrightarrow D' \\ x \longmapsto (ox) \cap D' \end{vmatrix}$$

est une homographie. Une telle application est appelée une *perspective*.

NOTATION. Pour tout sous-espace projectif X de $\mathbf{P}(E)$, on note $\overline{X} \subset E$ l'unique sous-espace vectoriel de E tel que $\mathbf{P}(\overline{X}) = X$. Montrons à présent l'énonce de la définition précédente en se servant du lemme suivant.

LEMME 3.21. L'application

$$\varphi_{o,D'} : \begin{vmatrix} \mathbf{P}^2(k) \setminus \{o\} \longrightarrow D', \\ m \longmapsto m' \coloneqq (om) \cap D' \end{vmatrix}$$

est induite par la projection sur $\overline{D'}$ parallèlement à la droite o.

Preuve Soit $m \in \mathbf{P}^2(k) \setminus \{0\}$. En projectif, le point m' est caractérisé par les deux assertions

$$(om) = (om') \quad \text{et} \quad m' \in D'.$$

En repassant en vectoriel, la droite vectorielle m' est caractérisé par ces deux-là

$$o + m = o + m' \quad \text{et} \quad m' \subset \overline{D'}.$$

Soit $x \in m \setminus \{0\}$. Comme $E = o \oplus \overline{D'}$, on peut écrire $x = u + v$ avec $u \in \overline{D'}$ et $v \in o$. On obtient alors

$$o + m = \text{Vect}(o,u) \quad \text{et} \quad u \in \overline{D'}.$$

On en déduit $m' = \text{Vect}\, u$. □

Preuve de la définition L'application annoncé est simplement la restriction de $\varphi_{o,D'}$ à la droite D. Cette dernière est une homographie induite par la projection $p_{o,\overline{D'}|\overline{D'}} : \overline{D} \longrightarrow \overline{D'}$ qui est un isomorphisme car son noyau est $o \cap \overline{D} = \{0\}$. □

COROLLAIRE 3.22. Soient ℓ_1, ℓ_2, ℓ_3 et ℓ_4 quatre droites d'un plan projectif concourantes en un point z dont les trois premières sont distinctes. Soient D et D' deux droites. Pour $i \in [\![1,4]\!]$, on note $x_i \coloneqq \ell_i \cap D$ et $x'_i \coloneqq \ell_i \cap D'$. Alors

$$[x_1,x_2,x_3,x_4] = [x'_1,x'_2,x'_3,x'_4]$$

Ce nombre, ne dépendant donc pas des droites D et D', est noté $[\ell_1,\ell_2,\ell_3,\ell_4]$.

Division harmonique

DÉFINITION 3.23. On dit que quatre points alignés forment une *division harmonique* lorsque leur birapport à égal à -1.

◇ REMARQUES. – Pour tous points a, b et c d'une droite affine, ces trois points avec l'infini forment une division harmonique si et seulement si le point c est le milieu du segment $[a,b]$.

– Pour tout quadruplet harmonique (a,b,c,d), les quadruplets (b,a,c,d) et (a,b,d,c) en sont aussi.

PROPOSITION 3.24. Soient a, b et c trois points alignés d'un plan projectif. La construction indiqué dans la figure 3.1 suivante construit l'unique point d tel que le quadruplet (a,b,c,d) soit harmonique.

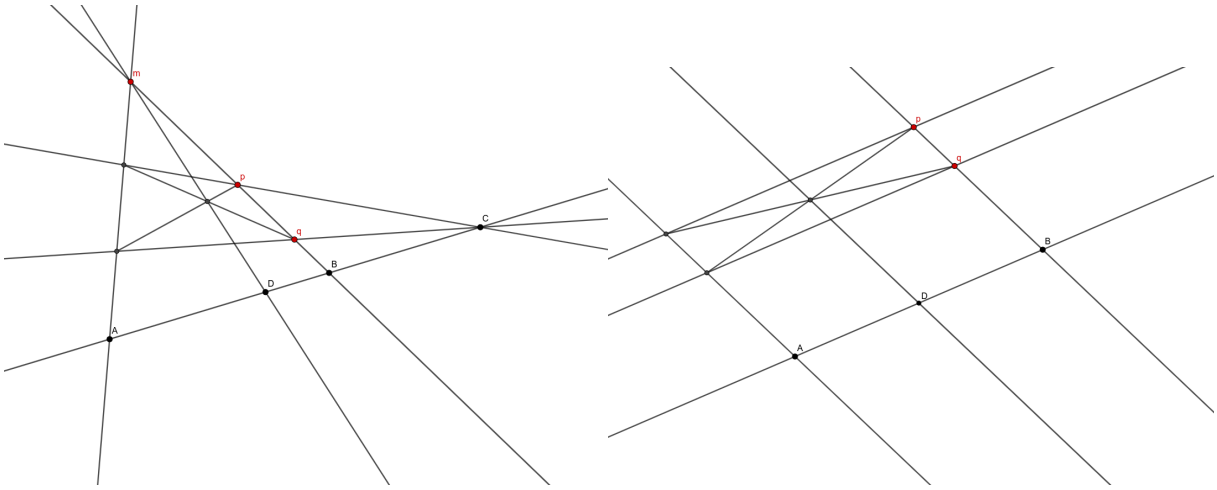


FIGURE 3.1 – Construction du quatrième point d

Preuve Il suffit de vérifier $[a,b,c,d]=-1$. Envoyons la droite (mc) à l'infini : on obtient la figure de droite. Alors le quadrilatère $qprs$ de la construction devient un parallélogramme et la droite (md) devient la droite parallèle aux côtés pq et rs passant par l'intersection de diagonale du parallélogramme. Ainsi, le point $(md)\cap(ps)$ est le milieu de $[ps]$ et le point $(md)\cap(qr)$ est le milieu de $[qr]$. Le quadrilatère $bqra$ est aussi un parallélogramme. La droite (md) est parallèle aux côtés bq et ra et donc le point d est le milieu de $[ab]$. □

3.6 LE THÉORÈME FONDAMENTALE DE LA GÉOMÉTRIE PROJECTIVE

DÉFINITION 3.25. Une *collinéation* d'un espace projectif $\mathbf{P}^d(k)$ est une bijection $\varphi\colon \mathbf{P}^d(k)\longrightarrow\mathbf{P}^d(k)$ préservant l'ensemble des droites projectifs.

DÉFINITION 3.26. Soit E un k-espace vectoriel. Une application $u\colon E\longrightarrow E$ est dite *semi-linéaire* s'il existe un automorphisme de corps $\sigma\colon k\longrightarrow k$ tel que

– pour tous $x,y\in E$, on ait $u(x+y)=u(x)+u(y)$;
– pour tous $x\in E$ et $\lambda\in k$, on ait $u(\lambda x)=\sigma(\lambda)u(x)$.

Si $u\neq 0$, alors un tel automorphisme σ est unique, noté σ_u.

▷ EXEMPLE. Pour toute matrice $M\in\mathscr{M}_n(\mathbf{C})$, l'application $X\in\mathbf{C}^n\longmapsto\overline{MX}\in\mathbf{C}^n$ est une application semi-linéaire.

◇ REMARQUE. Pour toutes applications $u,v\colon E\longrightarrow E$ non nulles, on a $\sigma_{u\circ v}=\sigma_u\circ\sigma_v$. Ainsi l'application $u\longmapsto\sigma_u$ est un morphisme du groupe des isomorphismes semi-linéaires de E vers le groupe des automorphismes de k

Donnons le théorème suivant à titre culturel.

THÉORÈME 3.27. Soient k un corps différent de $\mathbf{F}_2$ et $d\geqslant 2$ un entier. Alors toute collinéation de $\mathbf{P}^d(k)$ est induite par un isomorphisme semi-linéaire.

COROLLAIRE 3.28. 1. Soient $p\geqslant 3$ un nombre premier, $d\geqslant 2$ un entier et $k\in\{\mathbf{Q},\mathbf{R},\mathbf{F}_p\}$. Alors toute collinéation de $\mathbf{P}^d(k)$ est une homographie.
2. Soit $d\geqslant 2$ un entier. Alors toute collinéation continue de $\mathbf{P}^d(\mathbf{C})$ est une homographie ou une anti-homographie (*i. e.* l'automorphisme de $\mathbf{C}$ correspondant est la conjugaison complexe).

3.7 LA DROITE PROJECTION COMPLEXE

◇ REMARQUE. On peut voir $\mathbf{C}$ comme le plan $\mathbf{R}^2$ et donc comme un espace vectoriel réel de dimension 2. Mais alors on le voit comme un plan affine réel et sa complétion naturelle est alors le plan projectif réel $\mathbf{P}^2(\mathbf{R})$. On peut aussi le point comme un espace vectoriel complexe de dimension 1 et alors sa complétion naturelle est la droite projective complexe $\mathbf{P}^1(\mathbf{C})$. Ces deux constructions cohabitent sans souci et peuvent même se compléter.

3.7.1 Birapport et cercles

PROPOSITION 3.29. Le birapport de quatre points alignés sur une droite affine réelle contenue dans $\mathbf{C}$ coïncide avec leur birapport comme point de la droite projective complexe $\mathbf{P}^1(\mathbf{C})$.

Preuve Soient a, b, c et d quatre points alignés sur une droite affine réel D de $\mathbf{C}$. Le groupe Is engendré par les rotations et les translations de $\mathbf{R}^2$ est à la fois un sous-groupe des transformations affines de $\mathbf{R}^2$, *i. e.* un sous-groupe de $\mathrm{PGL}_3(\mathbf{R}) = \mathrm{Aut}(\mathbf{P}^2(\mathbf{R}))$, et un sous-groupe des similitudes de $\mathbf{C}$, *i. e.* un sous-groupe de $\mathrm{PGL}_2(\mathbf{C}) = \mathrm{Aut}(\mathbf{P}^1(\mathbf{C}))$. Quitte à appliquer un élément de Is, on peut supposer que la droite D est l'axe réel. Alors il existe une unique homographie $f \in \mathrm{PGL}_2(\mathbf{R})$ envoyant les points a, b et c sur les points ∞, 0 et 1. Mais $\mathrm{PGL}_2(\mathbf{R}) < \mathrm{PGL}_2(\mathbf{C})$, donc l'application f est aussi l'unique homographe de $\mathrm{PGL}_2(\mathbf{C})$ vérifiant cette condition. D'où

$$[a,b,c,d]_{\mathbf{C}} = f(d) = [a,b,c,d]_{\mathbf{R}}.$$

□

COROLLAIRE 3.30. Le birapport de quatre points de $\mathbf{C}$ alignés sur une droite affine réelle est un nombre réel ou l'infini.

DÉFINITION 3.31. On dit que n points de $\mathbf{C}$ sont *cocyclique* lorsqu'il existe un cercle qui les contient.

PROPOSITION 3.32 (avatar du théorème de l'angle inscrit). Soient $a,b,c \in \mathbf{C}$ trois points non alignés et $d \in \mathbf{C}$ un point différent de ces trois premiers. Alors les assertions suivantes sont équivalentes :

(i) le point d est sur le cercle passant par a, b et c ;

(ii) les angles de droites (ca, cb) et (da, db) sont égaux à π près ;

(iii) les angles de vecteurs $2(\overrightarrow{ca}, \overrightarrow{cb})$ et $2(\overrightarrow{da}, \overrightarrow{db})$ sont égaux à 2π près.

COROLLAIRE 3.33. Le birapport de quatre points de $\mathbf{C}$ est réel ou infini si et seulement si ces quatre points sont alignés ou cocyclique.

Preuve On peut supposer que les quatre points a, b, c et d sont distincts car sinon ils sont alignés ou cocyclique. On rappel que

$$(\overrightarrow{ca}, \overrightarrow{cb}) \equiv \mathrm{Arg}\left(\frac{c-b}{c-a}\right) \mod 2\pi.$$

Avec la proposition précédente, on obtient

$$\begin{aligned}
a, b, c \text{ et } d \text{ sont alignés} &\iff 2\,\mathrm{Arg}\left(\frac{c-b}{c-a}\right) \equiv 2\,\mathrm{Arg}\left(\frac{d-b}{d-a}\right) \mod 2\pi \\
&\iff 2\,\mathrm{Arg}\left(\frac{(d-b)(c-a)}{(d-a)(c-b)}\right) \equiv 0 \mod 2\pi \\
&\iff \mathrm{Arg}[a,b,c,d] \equiv 0 \mod \pi \\
&\iff [a,b,c,d] \in \mathbf{R}.
\end{aligned}$$

□

COROLLAIRE 3.34. Toute homographie de $\mathrm{PGL}_2(\mathbf{C})$ envoie une droite ou un cercle sur une droite ou un cercle.

◇ REMARQUE. Il est important de penser à une droite comme à un cercle passant par l'infini. Notons que c'est cohérent avec la vision de la compactification d'ALEXANDROV.

3.7.2 Construction du quatrième point harmonique dans $\mathbf{P}^1(\mathbf{C})$

PROPOSITION 3.35. Soient $a,b,c \in \mathbf{C}$ trois points non alignés. Alors la construction indique dans la figure 3.2 construit l'unique point $d \in \mathbf{C}$ tel que le quadruplet (a,b,c,d) soit harmonique.

LEMME 3.36 (puissance d'un point par rapport à un cercle). Soient M un point et Γ un cercle. Soit d un droite contenant M et rencontrant Γ en des points A et B. Alors la quantité $\overrightarrow{MA} \cdot \overrightarrow{MB}$ est indépendante de d, on l'appelle la *puissance* de M par rapport à Γ et on la note $P_\Gamma(M)$. En notant O le centre de Γ et R son rayon, on a

$$P_\Gamma(M) = OM^2 - R^2.$$

Preuve On note $H := \frac{1}{2}(A+B)$ le milieu du segment $[AB]$. Remarquons qu'alors la droite (OH) est la médiatrice de ce segment. Avec le théorème de PYTHAGORE dans les triangles OAH et MOH, on a

$$\overrightarrow{MA} \cdot \overrightarrow{MB} = (\overrightarrow{MA} + \overrightarrow{HA}) \cdot (\overrightarrow{MH} + \overrightarrow{HB})$$

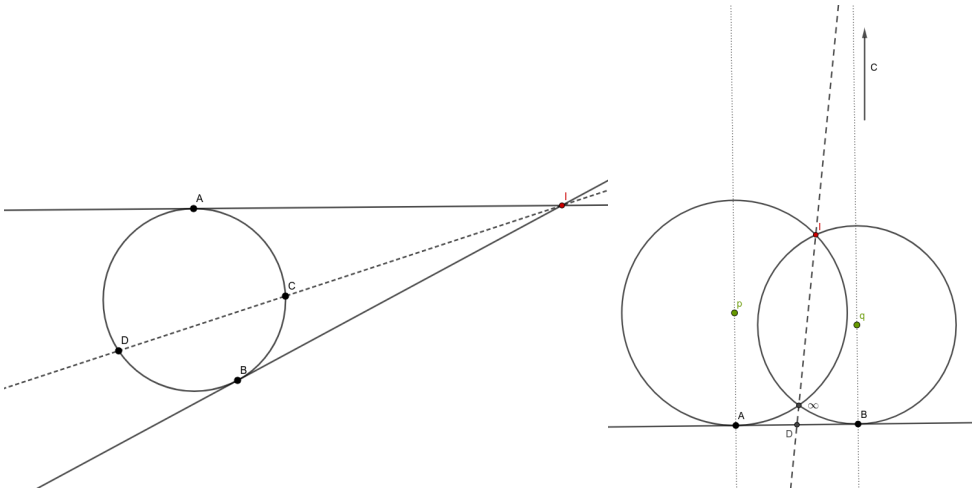


FIGURE 3.2 – Construction du quatrième point d dans $\mathbf{P}^1(\mathbf{C})$

$$\begin{aligned} &= MH^2 - HA^2 \\ &= MH^2 - (OA^2 - OH^2) \\ &= MO^2 - R^2. \end{aligned}$$

□

Preuve de la proposition Envoyons le point c à l'infini. Alors le cercle passant par les points a, b et c devient une droite (ab) et les droites (ma) et (mb) deviennent des cercles Γ et Γ' tangents à la droite (ab) au points a et b respectivement. De plus, ces deux droites s'intersectent en m et ∞. Il faut à présent montrer que le point $(m\infty) \cap (ab)$ est le milieu du segment $[ab]$. Pour cela, on remarque que $P_\Gamma(d) = P_\Gamma(d')$ puisque $\Gamma \cap \Gamma' = \{m, \infty\}$ et $d \in (m\infty)$. Mais on a $P_\Gamma(d) = da^2$ et $P_\Gamma(d) = db^2$, donc le point d est bien le milieu du segment $[ab]$. □

3.7.3 Le groupe circulaire

DÉFINITION 3.37. Le *groupe circulaire* est le sous-groupes de homéomorphismes de $\mathbf{P}^1(\mathbf{C})$ engendré par le groupe $\mathrm{PGL}_2(\mathbf{C})$ et la conjugaison complexe.

THÉORÈME 3.38. Une bijection de $\mathbf{P}^1(\mathbf{C})$ préservant l'ensemble des droites et des cercles est une transformation du groupe linéaire.

Preuve Soit f une telle bijection. Quitte à la composer par une homographie, on peut supposer $f(\infty) = \infty$. Ainsi elle envoie une droite sur une droite et un cercle sur un cercle. La construction du quatrième pont harmonique dans $\mathbf{C}$ se fait unique à l'aide de droites ou de cercles. On obtient que, pour tout quadruplet harmonique (a, b, c, d), son image $(f(a), f(b), f(c), f(d))$ par f est aussi harmonique. On dit alors que la bijection f préservent les divisions harmoniques.

Quitte à composer f par une similitude, on peut supposer $f(0) = 0$ et $f(1) = 1$. Le lemme suivant montre alors que c'est un automorphisme du corps $\mathbf{C}$. De plus, elle préserve l'axe réel. Par conséquent, c'est l'identité ou la conjugaison complexe. □

LEMME 3.39. Une bijection $f\colon \mathbf{C} \longrightarrow \mathbf{C}$ fixant les points 0 et 1 et préservant les divisions harmoniques est un automorphisme de $\mathbf{C}$.

Preuve Commençons par montrer que l'application f est additive. Comme $[a, b, c, \infty] = -1 \Leftrightarrow c = \frac{1}{2}(a+b)$, on en déduit qu'elle préserve les milieux, c'est-à-dire

$$f\left(\frac{a+b}{2}\right) = \frac{f(a)+f(b)}{2}, \quad a, b \in \mathbf{C}.$$

En particulier, en prenant $b = 0$, on obtient $2f(a/2) = f(a)$ pour tout $a \in \mathbf{C}$. Pour tous $a, b \in \mathbf{C}$, on en déduit

$$f(a+b) = 2f\left(\frac{a+b}{2}\right) = f(a) + f(b).$$

Montrons maintenant qu'elle préserve les carrés. Soient $a, b \in \mathbf{C}$. Comme $[u, -u, u^2, 1] = -1$ pour tout $u \in \mathbf{C}$, on obtient

$$\begin{cases} -1 = [f(a), -f(a), f(a)^2, 1], \\ -1 = [a, -a, a^2, 1] = [f(a), f(-a), f(a^2), f(1)] = [f(a), -f(a), f(a^2), 1] \end{cases}$$

ce qui donne $f(a^2) = f(a)^2$. Maintenant, on a

$$\begin{aligned} 4f(ab) = f(4ab) &= f((a+b)^2 - (a-b)^2) \\ &= f((a+b)^2) - f((a-b)^2) \\ &= f(a+b)^2 - f(a-b)^2. \\ &= 4\left(f\left(\frac{a+b}{2}\right)\right)^2 - 4\left(f\left(\frac{a-b}{2}\right)\right)^2 \\ &= 4\left(\frac{f(a)+f(b)}{2}\right)^2 - 4\left(\frac{f(a)-f(b)}{2}\right)^2 \\ &= (f(a)+f(b))^2 - (f(a)-f(b))^2 \\ &= 4(f(a)f(b)) \end{aligned}$$

ce qui montre qu'elle est multiplicative. □

Chapitre 4

LE GROUPE LINÉAIRE : SIMPLICITÉ

4.1 DÉTERMINANT ET GROUPE SPÉCIAL LINÉAIRE

Soit E un k-espace vectoriel. L'application $\det\colon \mathrm{GL}(E) \longrightarrow k^\times$ est un morphisme surjective. Son noyau est le *groupe spécial linéaire* et se donne $\mathrm{SL}(E)$.

PROPOSITION 4.1. La suite exacte

$$1 \longrightarrow \mathrm{SL}(E) \longrightarrow \mathrm{GL}(E) \longrightarrow k^\times \longrightarrow 1$$

est scindé. Par conséquent, le groupe $\mathrm{GL}(E)$ est le produit semi-direct de $\mathrm{SL}(E)$ par $k^\times$.

4.2 TRANSVECTION ET DILATATION

4.2.1 Définition

Soit $g \in \mathrm{GL}(E)$. Le théorème du rang assure $\dim\mathrm{Ker}(g-\mathrm{Id}_E) + \dim\mathrm{Im}(g-\mathrm{Id}_E) = \dim E$. On va s'intéresser aux automorphismes linéaires $g \in \mathrm{GL}(E)$ vérifiant $\dim\mathrm{Ker}(g-\mathrm{Id}_E) = \dim E$ car ce sont eux qui ont le plus de points fixes et ce sont donc les transformations les plus simples de E. Ils vont jouer le rôle que jouaient les transpositions et les 3-cycles dans le groupe symétrique.

DÉFINITION-PROPOSITION 4.2. Soient $g \in \mathrm{GL}(E) \setminus \{\mathrm{Id}_E\}$ tel que le noyau $H := \mathrm{Ker}(g-\mathrm{Id}_E)$ soit un hyperplan. Alors les assertions suivantes sont équivalentes :

(i) on a $\lambda := \det g \neq 1$;
(ii) l'isomorphisme g admet λ comme valeur propre et est diagonalisable ;
(iii) on a $\mathrm{Im}(g-\mathrm{Id}_E) \not\subset \mathrm{Ker}(g-\mathrm{Id}_E)$;
(iv) dans une base convenable, sa matrice est $\mathrm{diag}(\lambda, 1, \ldots, 1)$.

Dans ces cas, on dit que l'isomorphisme g est la *dilatation* d'hyperplan H, de droite $D := \mathrm{Im}(g-\mathrm{Id}_E)$ et de rapport λ. De plus, les assertions suivantes sont équivalentes :

(i) on a $\det g = 1$;
(ii) l'isomorphisme g est diagonalisable ;
(iii) on a $\mathrm{Im}(g-\mathrm{Id}_E) \subset \mathrm{Ker}(g-\mathrm{Id}_E)$;
(iv) il existe $f \in E'$ et $a \in \mathrm{Ker}\, f$ tels que $g = \mathrm{Id}_E + fa := \tau_{f,a}$.
(v) dans une base convenable, sa matrice est

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

Dans ces cas, on dit que l'isomorphisme g est la *transvection* d'hyperplan H et de droite D.

◇ REMARQUES. – Dans la carte affine d'hyperplan à l'infini H, une transvection est une translation. Réciproquement, toute translation d'un espace affine se prolonge en une transvection de sa complétion projective.
– Le triplet (H, D, λ) caractérise la dilatation. Cependant, le couple (H, D) ne caractérise pas la transvections, on peut considérer les transvections

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

qui ont les mêmes espaces H et D. Par contre, le couple (f,a) caractérise la transvection, mais la réciproque est fausse.

4.2.2 Conjugaison des dilations et des transvections

COROLLAIRE 4.3. 1. Deux dilatations sont conjuguées dans $\mathrm{GL}(E)$ si et seulement si elles ont le même rapport.
2. Les transvections sont conjuguées dans $\mathrm{GL}(E)$.

Preuve Il suffit d'utiliser les réduites de JORDAN donnée par la définition précédente. □

NOTATION. Pour $\lambda \in k$ et $n \geqslant 2$, on pose

$$J_\lambda := \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad J_\lambda^n := \mathrm{diag}(J_\lambda, I_{n-2}) \in \mathrm{GL}_n(k).$$

PROPOSITION 4.4. 1. Pour tout entier $n \geqslant 3$, les transvections sont conjuguées dans $\mathrm{SL}_n(k)$.
2. Tout transvection est conjuguée dans $\mathrm{SL}_2(k)$ à une matrice J_λ pour un certain $\lambda \in k^\times$.
3. Pour tous $\lambda, \mu \in k^\times$, les matrices J_λ et J_μ sont conjuguées dans $\mathrm{SL}_2(k)$ si et seulement si le quotient λ/μ est un carré.

◇ REMARQUE. On note $k^{\times 2} \subset k^\times$ l'ensemble des carrés du groupe $k^\times$. Alors la proposition affirme les classes de conjugaisons des transvections dans $\mathrm{SL}_2(k)$ sont en bijection avec le groupe quotient $k^\times/k^{\times 2}$. On peut montre que

$$\mathbf{C}^\times/\mathbf{C}^{\times 2} = \{1\}, \quad \mathbf{R}^\times/\mathbf{R}^{\times 2} = \{\pm 1\}, \quad |\mathbf{F}_q^\times/\mathbf{F}_q^{\times 2}| = 2 \quad \text{et} \quad |\mathbf{Q}^\times/\mathbf{Q}^{\times 2}| = +\infty.$$

Preuve 1. Soient $n \geqslant 3$ un entier et $u \in \mathrm{GL}(E)$ une transvection. Alors il existe $g \in \mathrm{GL}_n(k)$ telle que $gug^{-1} = J_1^n$. Posons $\lambda := \det g \in k^\times$ et $\gamma := \mathrm{diag}(\lambda^{-1}, \lambda^{-1}, \lambda, 1, \ldots, 1) \in \mathrm{GL}_n(k)$. Alors

$$\gamma J_1^n \gamma^{-1} = J_1^n \quad \text{et} \quad \det \gamma g = 1,$$

donc

$$(\gamma g) u (\gamma g)^{-1} = J_1^n \quad \text{et} \quad \gamma g \in \mathrm{SL}_n(k)$$

ce qui montre que la transvection u est conjuguées à la matrice J_1^n. On en déduit le résultat.
2. Soit $u \in \mathrm{GL}(E)$ une transvection. Alors il existe une base $(\varepsilon_1, \varepsilon_2)$ dans laquelle la matrice de u est J_1. Ainsi pour tout $a \in k^\times$, dans la base $(a\varepsilon_1, \varepsilon_2)$, la matrice de u est de la forme J_λ. En posant $a := \det(\varepsilon_1, \varepsilon_2)^{-1}$, la matrice de u dans la base $(a\varepsilon_1, \varepsilon_2)$ est alors de déterminant 1 ce qui montre le point 2.
3. $\Leftarrow$ On suppose qu'il existe $g \in \mathrm{SL}_2(k)$ telle que $gJ_\lambda = J_\mu g$. Notons

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

En calculant les produits gJ_λ et $J_\mu g$, on obtient $\mu c = 0$, $a\lambda = \mu d$ et $c\lambda = 0$, donc $c = 0$, $ad = 1$ et $\lambda/\mu = d/a = d^2$.

Réciproquement, on suppose qu'il existe $\delta \in k$ tel que $\lambda/\mu = \delta^2$. Alors la matrice

$$g := \begin{pmatrix} \delta^{-1} & b \\ 0 & \delta \end{pmatrix}, \quad b \in k$$

convient. □

4.2.3 Centre des groupes linéaires et spécial linéaire

PROPOSITION 4.5. Soient $g \in \mathrm{GL}(E)$, $f \in E^*$ et $a \in \mathrm{Ker}\, f$. Alors en reprenant les notations de la définition 4.2, on a

$$g\tau_{f,a}g^{-1} = \tau_{f\circ g^{-1}, g(a)}.$$

Preuve Il s'agit d'un simple calcul. □

PROPOSITION 4.6. Le centre de $\mathrm{GL}(E)$ est le groupe des homothéties et le centre de $\mathrm{SL}(E)$ est le groupe des homothéties de déterminant 1. Ce dernier est isomorphe au groupe $\mu_n(k)$ des racines n-ième de l'unité de k.

Preuve Montrons la première affirmation, le reste s'en déduit facilement. Soit $g \in \mathrm{Z}(\mathrm{GL}(E))$. En particulier, il commute avec toutes les transvections. En particulier, pour tous $f \in E^* \setminus \{0\}$ et $a \in \mathrm{Ker}\, f$, la proposition précédent assure $\tau_{f\circ g^{-1}, g(a)} = \tau_{f,a}$, *i. e.* les vecteurs $g(a)$ et a sont colinéaires. Ceci étant vrai pour tout $a \in E$ car on peut trouver une forme linéaire $f \in E'$ tel que $f(a) = 0$, on en déduit que l'isomorphisme g est une homothétie. □

4.2.4 Génération

DÉFINITION 4.7. 1. Pour $i, j \in [\![1, n]\!]$, on note $E_{i,j} \in \mathscr{M}_n(k)$ la matrice qui ne contient que des zéros sauf un 1 en position (i, j). Ces matrices sont appelées les *matrices élémentaires*.
2. Pour $i, j \in [\![1, n]\!]$ tels que $i \neq j$ et $\lambda \in k$, on note $T_{i,j}(\lambda) := I_n + \lambda E_{i,j} \in \mathrm{SL}_n(k)$. Ces matrices sont appelées les *transvections élémentaires*.
3. Les matrices $I_n + (\lambda - 1)E_{i,i} \in \mathrm{GL}_n(k)$ sont appelées les *dilatations élémentaires*.

PROPOSITION 4.8. Les transvections élémentaires engendrent $\mathrm{SL}_n(k)$.

Preuve On procède par récurrence sur la dimension n et on utilise l'algorithme du pivot de GAUSS. □

COROLLAIRE 4.9. Les transvections élémentaires et les dilatations élémentaires engendrent $\mathrm{GL}_n(k)$.

4.3 GROUPE DÉRIVÉ

PROPOSITION 4.10. Soient $n \geqslant 2$ un entier et k un corps tels que $(n, k) \notin \{(2, \mathbf{F}_2), (2, \mathbf{F}_3)\}$. Alors toute transvection élémentaire est un commutateur de $\mathrm{SL}_n(k)$.

Preuve On suppose d'abord $n \geqslant 3$. Pour tout $x \in k$, on a

$$\left[\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

c'est-à-dire $[T_{1,2}(x), T_{2,3}(x)] = T_{1,3}(x)$. De manière général, pour tous $i, j, k \in [\![1, n]\!]$ tels que $i \neq j \neq k$, on a

$$[T_{i,j}(x), T_{j,k}(x)] = T_{i,k}(x)$$

ce qui montre le résultat. On suppose désormais $n = 2$. Pour tous $x \in k^\times$ et $y \in k$, on a

$$\left[\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}\right] = \begin{pmatrix} 1 & y(1-x^2) \\ 0 & 1 \end{pmatrix}.$$

Comme l'équation $x^2 = 1$ possède au plus deux solutions et comme $|k| \geqslant 4$, on peut trouver un élément $x \in k^\times$ tel que $x^2 \neq 1$. Dans ce cas, le calcul précédent montre que toutes les transvections élémentaires sont des transvections ce qui montre aussi le résultat dans le cas $n = 2$. □

COROLLAIRE 4.11. Avec les mêmes hypothèses que la proposition précédente, le groupe $\mathrm{SL}_n(k)$ est parfait.

EXERCICE 4.1. Montrer que tout quotient d'un groupe parfait est encore parfait.

COROLLAIRE 4.12. Avec les mêmes hypothèses que la proposition précédente, le groupe $\mathrm{PSL}_n(k)$ est parfait.

◇ REMARQUE. L'énoncé précédent est optimal puisque $\mathrm{PSL}_2(\mathbf{F}_2) \simeq \mathfrak{S}_3$ et $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathfrak{A}_4$.

4.4 LE LEMME D'IWASAWA

4.4.1 Le lemme

THÉORÈME 4.13 (lemme d'IWASAWA). Soit G un groupe parfait agissant sur un ensemble X. On suppose que

– l'action est fidèle et 2-transitive ;
– le stabilisateur G_x d'un point $x \in X$ possède une sous-groupe distingué de A tels que les éléments conjugués de A dans G engendre G.

Alors le groupe G est simple.

LEMME 4.14. Soit G un groupe agissant 2-transitivement sur un ensemble X. Soient $x \in X$ et H un groupe tel que $G_x < H \leqslant G$. Alors $H = G$, *i. e.* le stabilisateur d'un point est un sous-groupe maximal de G.

Preuve Soit $g \in G$. Si $g \cdot x = x$, alors $g \in H$. On suppose donc $y := g \cdot x \neq x$. Comme $G_x \subsetneq H$, il existe $h \in H$ tel que $z := h \cdot x \neq x$. Comme l'action est 2-transitive, il existe $k \in G_x$ tel que $ky = z$. On obtient alors $h^{-1}kg \cdot x = x$, donc $h^{-1}kg \in H$, donc $g \in H$. □

Preuve du théorème Soient $x \in X$ et $N \lhd G$. Distinguons deux cas. On suppose $N \leqslant G_x$. Pour tout $g \in G$, comme le sous-groupe N est distingué dans G, on a $N = gNg^{-1} \leqslant gG_xg^{-1} = G_{g\cdot x}$ et la la transitivité puis la fidélité de l'action impliquent

$$N \leqslant \bigcap_{y\in X} G_y = \mathrm{Ker}(G \curvearrowright X) = \{1\},$$

donc $N = \{1\}$. Le groupe G est bien parfait.

On suppose désormais $N \not\leqslant G_x$. Le lemme précédent assure alors $NG_x = G$. Montrons alors $G = AN$. Pour tout $g \in G$, il existe alors $n \in N$ et $k \in G_x$ tels que $g = nk$, donc

$$gAg^{-1} = nkAk^{-1}n^{-1} = nAn^{-1} \leqslant AN.$$

Or le groupe G est engendré par les conjugués de A dans G, donc $G \leqslant AN$. L'inclusion réciproque étant évidente, on obtient $G = AN$. Par conséquent, le quotient

$$\frac{G}{N} = \frac{AN}{N} = \frac{A}{A\cap N}$$

est abélien, donc $\mathrm{D}(G) \leqslant N$. Comme G est parfait, on en déduit $G \leqslant N$ et donc $N = G$. □

4.4.2 Application au groupe projectif spécial linéaire

Soit V un k-espace vectoriel de dimension finie $n \geqslant 1$. Appliquons le lemme d'IWASAWA au groupe $\mathrm{PSL}(V)$. L'action de $\mathrm{PSL}(V)$ sur $\mathbf{P}(V)$ est bien 2-transitive et fidèle et le groupe $\mathrm{PSL}(V)$ est parfait. Il reste à trouver un sous-groupe distingué A vérifiant les hypothèses. Par dualité, le stabilisateur P du point $[e_n]$ pour cette action est

$$\begin{aligned} P &= \left\{ g \in \mathrm{PSL}_n(k) \;\middle|\; g \sim \begin{pmatrix} A & 0 \\ 0 & \lambda \end{pmatrix}, A \in \mathrm{GL}_{n-1}(k), \lambda \in k^\times, \lambda \det A = 1 \right\} \\ &\simeq \left\{ \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix} \in \mathrm{SL}_n(k) \;\middle|\; A \in \mathrm{SL}_{n-1}(k), b \in k^n \right\} \\ &\simeq \left\{ \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_n(k) \;\middle|\; A \in \mathrm{SL}_{n-1}(k), b \in k^n \right\} := \mathrm{SAff}_{n-1}(k). \end{aligned}$$

Cela veut dire que le stabilisateur P du point $[e_n]$ pour cette action $\mathrm{PSL}(V) \curvearrowright \mathbf{P}(V)$ est isomorphe au stabilisateur de l'hyperplan $\{x_n = 0\}$ qui est lui-même isomorphe au groupe spécial affine sur k^{n-1}.

Le groupe spécial affine sur k^{n-1} possède une sous-groupe abélien distingué : le sous-groupe des translations. Autrement dit, on prend

$$\begin{aligned} A :&= \left\{ g \in \mathrm{PSL}_n(k) \;\middle|\; g \sim \begin{pmatrix} I_{n-1} & 0 \\ b & \lambda \end{pmatrix}, b \in k^n, \lambda \in k^\times, \lambda \det A = 1 \right\} \\ &\simeq \left\{ \begin{pmatrix} I_{n-1} & 0 \\ b & 1 \end{pmatrix} \in \mathrm{SL}_n(k) \;\middle|\; b \in k^n \right\} \simeq k^n. \end{aligned}$$

C'est le groupe des transvections de droite $[e_n]$. Le groupe $\mathrm{PSL}(V)$ étant engendré par les transvections, on obtient le résultat souhaité.

Chapitre 5
GROUPES ORTHOGONAUX EUCLIDIENS

Soit $n \geqslant 1$ un entier. On munit l'espace $\mathbf{R}^n$ de son produit scalaire canonique. On va considérer le groupe orthogonal euclidien $\mathrm{O}_n(\mathbf{R}) \leqslant \mathrm{GL}_n(\mathbf{R})$ et le groupe spécial orthogonal euclidien $\mathrm{SO}_n(\mathbf{R}) \leqslant \mathrm{GL}_n(\mathbf{R})$. On rappel que, pour tout sous-espace vectoriel V de $\mathbf{R}^n$, on peut écrire la somme direct $\mathbf{R}^n = V \oplus V^\perp$.

5.1 GÉNÉRATEURS

Une *réflexion* est une isométrie $g \in \mathscr{L}(\mathbf{R}^n)$ telle que $\dim \mathrm{Ker}(g - \mathrm{Id}_{\mathbf{R}^n}) = n-1$, on dit que cette réflexion est d'hyperplan $H := \mathrm{Ker}(g - \mathrm{Id}_{\mathbf{R}^n})$ et on la notera σ_H. Dans une bonne base orthonormée, sa matrice vaut

$$\mathrm{diag}(-1, 1, \dots, 1). \tag{5.1}$$

Remarquons que, en notant $v \in \mathbf{R}^n$ un vecteur unitaire dirigeant la droite $H^\perp$, on a

$$\sigma_H(x) = x - \langle x, v\rangle v, \quad x \in \mathbf{R}^n.$$

Un *retournement* est une isométrie $g \in \mathscr{L}(\mathbf{R}^n)$ telle que $\dim \mathrm{Ker}(g - \mathrm{Id}_{\mathbf{R}^n}) = n-2$ et $\dim \mathrm{Ker}(g + \mathrm{Id}_{\mathbf{R}^n}) = 2$, on dit que ce retournement est de plan $\Pi := \mathrm{Ker}(g + \mathrm{Id}_{\mathbf{R}^n})$ et on le note τ_Π qui vérifie donc $\Pi^\perp = \mathrm{Ker}(\tau_\Pi - \mathrm{Id}_{\mathbf{R}^n})$. Dans une bonne base orthonormée, sa matrice vaut

$$\mathrm{diag}(-1, -1, 1, \dots, 1). \tag{5.2}$$

PROPOSITION 5.1. Le groupe $\mathrm{O}_n(\mathbf{R})$ est engendré par les réflexions.

Preuve Procédons par récurrence sur l'entier n. La proposition est évidente pour $n = 1$. Soit $n \geqslant 2$ un entier. On suppose que la proposition tient en dimension $n-1$. Soient $g \in \mathrm{O}_n(\mathbf{R})$ et $v \in \mathbf{R}^n \setminus \{0\}$. Distinguons deux cas. On suppose d'abord $g(v) = v$. Alors $g(v^\perp) = v^\perp$ où l'orthogonal $v^\perp \subset \mathbf{R}^n$ est un hyperplan. En appliquant l'hypothèse de récurrence, la restriction $g|_{v^\perp}$ est un produit de réflexions de l'espace $v^\perp$ que l'on peut prolonger par l'identité à tout l'espace $\mathbf{R}^n$. Donc l'application g est bien un produit de réflexions.

On suppose désormais $g(v) \neq v$. Alors il existe une réflexion $\sigma \in \mathrm{GL}(\mathbf{R}^n)$ telle que $\sigma(v) = g(v)$. Ainsi la composée $\sigma \circ g$ fixe le vecteur v, donc cette dernière est un produit de réflexions d'après le premier paragrapge. Il en va donc de même pour l'application g ce qui termine la récurrence. □

PROPOSITION 5.2. Le groupe $\mathrm{SO}_n(\mathbf{R})$ est engendré par les retournements.

Preuve Comme toute élément du groupe $\mathrm{SO}_n(\mathbf{R})$ s'écrit comme un produit d'un nombre pair de réflexions, il suffit de tout montrer que tout produit de deux réflexions est un produit de retournements. Soient $\sigma_1, \sigma_2 \in \mathrm{GL}(\mathbf{R}^n)$ deux réflexions.

On suppose d'abord $n = 3$. Alors les écritures matricielles (5.1) et (5.2) montre que les opposés $-\sigma_i$ sont des retournements ce qui permet d'écrire $\sigma_1 \circ \sigma_2 = (-\sigma_1) \circ (-\sigma_2)$ et on a gagné.

On suppose désormais $n \geqslant 4$. On note H_1 et H_2 les hyperplans associés aux réflexions σ_1 et σ_2. Soit $V \subset \mathbf{R}^n$ un sous-espace vectoriel de co-dimension 3 inclus dans $H_1 \cap H_2$. Ainsi son orthogonal $V^\perp$, de dimension 3, est préservé par les réflexions σ_1 et σ_2. Pour $i \in \{1,2\}$, on note $\tau_i \in \mathrm{GL}(\mathbf{R}^n)$ l'isométrie valant $-\sigma_i$ sur $V^\perp$ et l'identité sur V. Ces deux isométries τ_i sont des retournements vérifiant $\sigma_1 \circ \sigma_2 = \tau_1 \circ \tau_2$. □

5.2 ACTION TRANSITIVE ET CONSÉQUENCES

PROPOSITION 5.3. Le groupe $\mathrm{SO}_n(\mathbf{R})$ agit simplement et transitivement sur les bases orthonormées directes.

Preuve Il suffit de remarque qu'une matrice est dans $\mathrm{SO}_n(\mathbf{R})$ si et seulement si la famille de ses vecteurs colonnes forment une base orthonormée directe. □

PROPOSITION 5.4. Soit $k \in [\![1, n]\!]$. Le groupe $\mathrm{SO}_n(\mathbf{R})$ agit transitivement sur les espaces de dimension k.

Preuve On utilise le procédé de GRAM-SCHMIDT et la proposition précédente. □

PROPOSITION 5.5 (principe de conjugaison). Soit $g \in \mathrm{O}_n(\mathbf{R})$. Soient H un hyperplan de $\mathbf{R}^n$ et Π un plan de $\mathbf{R}^n$. Alors

$$g \circ \sigma_H \circ g^{-1} = \sigma_{g(H)} \quad \text{et} \quad g \circ \tau_\Pi \circ g^{-1} = \tau_{g(\Pi)}.$$

COROLLAIRE 5.6. Les réflexions sont conjuguées dans $\mathrm{O}_n(\mathbf{R})$ et les retournements sont conjugués dans $\mathrm{SO}_n(\mathbf{R})$.

Preuve Il suffit d'appliquer la proposition précédente et le fait que le groupe $\mathrm{SO}_n(\mathbf{R})$ agit transitivement sur les hyperplans et les plans. □

PROPOSITION 5.7. Le tableau suivant résume les centres des groupes $\mathrm{O}_n(\mathbf{R})$ et $\mathrm{SO}_n(\mathbf{R})$.

	$n = 2$	$n \in 2\mathbf{N}$	$n \in 2\mathbf{N}+1$
$\mathrm{O}_n(\mathbf{R})$	$\{\pm \mathrm{Id}_{\mathbf{R}^n}\}$	$\{\pm \mathrm{Id}_{\mathbf{R}^n}\}$	$\{\pm \mathrm{Id}_{\mathbf{R}^n}\}$
$\mathrm{SO}_n(\mathbf{R})$	$\mathrm{SO}_2(\mathbf{R})$	$\{\pm \mathrm{Id}_{\mathbf{R}^n}\}$	$\{+\mathrm{Id}_{\mathbf{R}^n}\}$

5.3 TOPOLOGIE

PROPOSITION 5.8. Le groupe $\mathrm{SO}_n(\mathbf{R})$ est connexe et compact.

Preuve Ce groupe est une partie fermée et bornée de $\mathbf{R}^n$ qui en fait un compact. De plus, il est connexe par arcs et donc connexe. En effet, tout élément de $\mathrm{SO}_n(\mathbf{R})$ peut s'écrire sous la forme

$$\mathrm{diag}(1, \dots, 1, R(\theta_1), \dots, R(\theta_r))$$

où les matrices $R(\theta_k)$ sont des matrices de rotations. À partir de là, on peut construit un chemin continue entre deux matrices de $\mathrm{SO}_n(\mathbf{R})$ et à valeurs dans $\mathrm{SO}_n(\mathbf{R})$. □

5.4 SIMPLICITÉ

PROPOSITION 5.9. On suppose $n \notin \{1, 2, 4\}$. Alors le groupe $\mathrm{PSO}_n(\mathbf{R})$ est simple. Autrement dit,

– si $n \geqslant 3$ est impair, alors le groupe $\mathrm{SO}_n(\mathbf{R})$ est simple ;
– si $n \geqslant 6$ est pair, alors le groupe $\mathrm{SO}_n(\mathbf{R})/\{\mathrm{Id}_{\mathbf{R}^n}\}$ est simple.

Preuve Montrons la proposition uniquement dans le cas $n = 3$. Soit N un sous-groupe distingué de $\mathrm{SO}_3(\mathbf{R})$. Montrons que ce sous-groupe N contient un retournement ou est central. Soit $n \in N$. On considère l'application continue

$$\varphi_n : \left| \begin{array}{l} \mathrm{SO}_3(\mathbf{R}) \longrightarrow [0, \pi], \\ \qquad g \longmapsto \mathrm{Arccos}\left(\dfrac{\mathrm{tr}[g, n] - 1}{2}\right). \end{array} \right.$$

Comme le groupe $\mathrm{SO}_3(\mathbf{R})$ est compact et connexe, l'image $I_n := \mathrm{Im}\,\varphi$ est un segment de la forme $[0, a_n]$. Distinguons deux cas.

Premier cas On suppose que les images I_n sont réduites au singleton $\{0\}$. Or pour tout $n \in N$ et $g \in \mathrm{SO}_3(\mathbf{R})$, on a l'équivalence $\varphi_n(g) = 0 \Leftrightarrow [g, n] = 1$. Ceci montre $N \leqslant \mathrm{Z}(\mathrm{SO}_3(\mathbf{R})) = \{\mathrm{Id}_{\mathbf{R}^n}\}$, donc le sous-groupe N est trivial.

Second cas On suppose qu'il existe $\varepsilon > 0$ et $n \in N$ tels que $I_n \supset [0, \varepsilon]$. Cela assure l'existence d'un entier $k \in \mathbf{N}$ et d'un élément $g \in \mathrm{SO}_3(\mathbf{R})$ tels que le commutateur $[g, n] \in N$ soit une rotation d'angle π/k. Ainsi l'application $[g, n]^k$ est une rotation d'angle π, *i. e.* un retournement. Or les retournements sont conjugués dans $\mathrm{SO}_3(\mathbf{R})$ et le sous-groupe N est distingué, donc ce dernier contient tous les retournements. Or les retournements engendrent $\mathrm{SO}_3(\mathbf{R})$. D'où $N = \mathrm{SO}_3(\mathbf{R})$. □

5.5 DÉCOMPOSITION DANS LES GROUPES LINÉAIRES

NOTATION. On note $\mathrm{Sym}_n^{++}(\mathbf{R}) \subset \mathscr{M}_n(\mathbf{R})$ l'ensemble des matrices symétriques définies positives.

THÉORÈME 5.10 (décomposition polaire). L'application

$$\varphi : \left| \begin{array}{c} \mathrm{O}_n(\mathbf{R}) \times \mathrm{Sym}_n^{++}(\mathbf{R}) \longrightarrow \mathrm{GL}_n(\mathbf{R}), \\ (Q,S) \longmapsto QS \end{array} \right.$$

est un homéomorphisme.

◇ REMARQUE. On peut également remplacer cette application par $(Q,S) \longmapsto SQ$. De plus, le théorème est encore valable sur le corps $\mathbf{C}$: l'application

$$\varphi' : \left| \begin{array}{c} \mathrm{U}_n(\mathbf{C}) \times \mathrm{H}_n^{++}(\mathbf{C}) \longrightarrow \mathrm{GL}_n(\mathbf{C}), \\ (Q,S) \longmapsto QS \end{array} \right.$$

est encore un homéomorphisme. Dans les deux cas, on a le même énoncé dans le cas des groupes spéciaux en changeant les ensembles de manière adéquate.

COROLLAIRE 5.11. Les groupes $\mathrm{GL}_n(\mathbf{R})$ et $\mathrm{O}_n(\mathbf{R}) \times \mathbf{R}^{n(n+1)/2}$ sont homéomorphes.

LEMME 5.12. L'application

$$\left| \begin{array}{c} \mathrm{Sym}_n^{++}(\mathbf{R}) \longrightarrow \mathrm{Sym}_n^{++}(\mathbf{R}), \\ M \longmapsto M^2 \end{array} \right.$$

est un homéomorphisme dont on note $\sqrt{\cdot}$ la réciproque.

Preuve On a déjà vu que cette application est continue et bijective. Montrons que sa réciproque est continue. Soit $(M_n)_{n\in\mathbf{N}}$ une suite de $\mathrm{Sym}_n^{++}(\mathbf{R})$ et $N \in \mathrm{Sym}_n^{++}(\mathbf{R})$ telles que $M_n^2 \longrightarrow N$. Pour tout $n \in \mathbf{N}$, d'après le théorème spectrale, il existe une matrice $k_n \in \mathrm{O}_n(\mathbf{R})$ et une matrice diagonale $\alpha_n \in \mathrm{GL}_n(\mathbf{R})$, dont la diagonale est strictement positive, telles que

$$M_n = k_n \alpha_n k_n^{-1}.$$

La suite $(\alpha_n^2)_{n\in\mathbf{N}}$ converge et ses termes sont strictement positifs, donc la suite $(\alpha_n)_{n\in\mathbf{N}}$ converge dans $\mathrm{GL}_n(\mathbf{R})$. De plus, la suite $(k_n)_{n\in\mathbf{N}}$ est une suite du compact $\mathrm{O}_n(\mathbf{R})$. Donc la suite $(M_n)_{n\in\mathbf{N}}$ est à valeurs dans un compact. De plus, comme tout valeur d'adhérence de celle-ci est une racine carrée de la matrice N, elle possède une unique valeur d'adhérence $\sqrt{N}$. Donc la suite $(M_n)_{n\in\mathbf{N}}$ converge vers son unique valeur d'adhérence $\sqrt{N}$. Ceci montre la continuité de l'application $M \longmapsto \sqrt{M}$. □

Preuve du théorème Montrons la surjectivité de l'application φ. Soit $g \in \mathrm{GL}_n(\mathbf{R})$. Comme ${}^t g g \in \mathrm{Sym}_n^{++}(\mathbf{R})$, on considère la matrice $S := \sqrt{{}^t g g} \in \mathrm{Sym}_n^{++}(\mathbf{R})$ et on pose $Q := gS^{-1}$. Alors $g = QS$ et $Q \in \mathrm{O}_n(\mathbf{R})$ puisque

$${}^t Q Q = {}^t(gS^{-1}) g S^{-1} = S^{-1}\,{}^t g g S^{-1} = S^{-1} S^2 S^{-1} = I_n.$$

D'où la surjectivité. Montrons qu'elle est injective. Soient $(Q,S),(Q',S') \in \mathrm{O}_n(\mathbf{R}) \times \mathrm{Sym}_n^{++}(\mathbf{R})$ tels que $QS = Q'S'$. Alors

$${}^t(QS) QS = {}^t S\,{}^t Q Q S = S^2$$

et, en refaisant le même calcul avec le couple (Q',S'), on obtient $S^2 = S'^2$. Par le lemme, on en déduit $S = S'$. Il s'ensuit $Q = Q'$. D'où l'injectivité.

Ainsi l'application φ est bijective et continue. Il reste à montrer que sa réciproque est continue. Mais grâce à ce qui précède, sa réciproque est

$$\varphi^{-1} : \left| \begin{array}{c} \mathrm{GL}_n(\mathbf{R}) \longrightarrow \mathrm{O}_n(\mathbf{R}) \times \mathrm{Sym}_n^{++}(\mathbf{R}), \\ g \longmapsto (g({}^t g g)^{-1/2}, ({}^t g g)^{-1/2}) \end{array} \right.$$

qui est clairement continue puisque l'application $S \in \mathrm{Sym}_n^{++}(\mathbf{R}) \longmapsto \sqrt{S}$ l'est. □