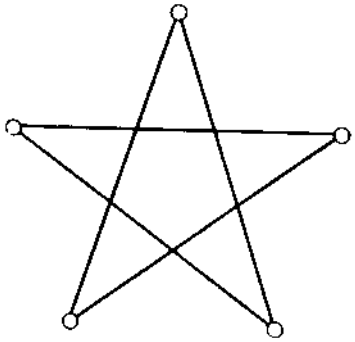
Nils-Peter Skoruppa

GROUPES et GEOMETRIE



Polycopié

Licence de Mathématiques Pures — Université Bordeaux 1

Version: Id: L2-poly.tex,v 1.3 2003/11/21 00:39:05 fenrir Exp

Table des Matières

Avertissement

Ce polycopié [1] est une version un peu élaborée de mes notes aux cours du même nom que j'ai assurés plusieurs fois pendant les années passées.

Ici les défauts principaux du polycopié. Comme les mots "peu élaborée" indiquent déjà le lecteur ne doit pas s'attendre à avoir un véritable livre entre ses mains : la présentation est plutôt courte et sèche et le français et l'orthographie sont un peu spécial. En plus, le titre de ce polycopié (ou du module) est maladroitement choisi, il me semble même assez vantard : les sujets traités dans ce module sont beaucoup plus modestes que suggérés par son titre, et malheureusement assez souvent très loin des mathématiques 2300 milles ans après Euclide. (L'explication est naturellement que en vérité le L2 ne sert à rien que à une première préparation à de concours dont les sujets suivent une certaine tradition.)

Néanmoins, le polycopié sera utile aux étudiants : les sujets traités suivent en gros littéralement le programme prescrit pour le "Module M2" de la licence de Math. Pures, leur présentation est cohérente et complète, les raisonnements peuvent servir comme bon exemple pour des déductions logiques "comme il faut" dans les mathématiques.

Dans le texte et à la fin de plusieurs chapitres l'étudiant va trouver plusieurs exercices.

Talence, le 24 décembre 1997

Notations

Il sera supposé une certaine familiarité avec le vocabulaire de base de la théorie des ensembles : $\in$, $\cup$, $\cap$, application, injectif, surjectif etc. Pour un ensemble fini X le symbole $|X|$ indique le nombre d'éléments de X. Par $\mathbb{Z}$, $\mathbb{R}$ et $\mathbb{C}$ on note l'ensemble des nombres entiers, réels et complexes respectivement.

Finalement, nous utilisons dans le texte de temps en temps la notion d'un corps. Des exemples sont : $\mathbb{R}$, $\mathbb{C}$ et les corps finis $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ (p un nombre premier). Si cette notion est inconnue au lecteur il peut considérer le mot "corps" comme synonyme pour $\mathbb{R}$ ou $\mathbb{C}$ (en retenant qu'il existe autres corps !). Le symbole K^n indique le K-espace vectoriel des vecteurs à *colonne*.

[1] Le pentacle sur la couverture était le symbole du club des Pythagoriciens.

Chapitre 1

Groupes

1.1 Définitions de base

Définition. Un ensemble G muni d'une opération binaire "$\cdot$", i.e. d'une application

$$\cdot : G \times G \to G,$$

est appelé un groupe si l'opération satisfait aux propriétés suivantes :

1. Pour tout $a, b, c \in G$ on a $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

2. Il existe un $n \in G$ tel que

i) $a \cdot n = n \cdot a = a$ pour tout $a \in G$, et

ii) pour tout $a \in G$ il existe un $b \in G$ avec $a \cdot b = b \cdot a = n$.

Remarque. Si il est convenable ou plus naturel on utilise autres symboles pour l'opération binaire d'un groupe donné, par exemple "+" ou "$*$". Souvent on supprime le point de l'opération et écrit ab pour $a \cdot b$.

Exemple. Ils sont des groupes : $\mathbb{Z}$ muni de l'addition usuelle comme opération binaire, $\mathbb{C}^* := \mathbb{C}\backslash\{0\}$ muni de la multiplication usuelle de nombres complexes, l'ensemble $\{0, 1\}$ avec l'opération "+" donnée par

$$0 + 0 := 0 \quad 1 + 0 := 1 \quad 1 + 0 := 1 \quad 1 + 1 := 0,$$

l'ensemble $\mathrm{GL}(n, K)$ des matrices carrées inversibles à n lignes et à éléments dans un corps K muni de la multiplication usuelle de matrices, l'ensemble $\mathrm{GL}(V)$ des applications linéaires et bijectives $V \to V$ muni de la composition d'applications, où V est un espace vectoriel sur un corps K.

Exercice. Si on a n éléments $a_1, \ldots, a_n$ d'un groupe G dans un ordre fixé il existe a priori plusieurs façons de "mettre des parenthèses" pour les multiplier et en calculer un élément de G. Montrer par récurrence sur n que tout tel produit est égal au produit de "référence"

$$(\ldots(((a_1a_2)a_3)a_4)\ldots a_n).$$

D'après cet exercice le produit de n éléments de G ne dépend pas de l'ordre des parenthèses mises pour évaluer le produit. En conséquence on supprime désormais les parenthèses dans les calculs dans un groupe.

Par contre, un produit dans un groupe arbitraire dépend en générale de l'ordre des éléments multipliés.

Exercice. Déterminer trois matrices A, B, C telles que leurs produits matriciels $(AB)C$ et $A(BC)$ sont différents.

Définition. Un groupe est dit abélien (ou commutatif) si $ab = ba$ pour tout $a, b \in G$.

Théorème 1.1. *L'élément neutre est unique.*

Démonstration. Soient n est n' neutres, alors $n = n \cdot n' = n'$. □

Théorème 1.2. *L'élément inverse associé à un $a \in G$ est unique.*

Démonstration. Soient b et b' des éléments inverse de a, alors $b = bn = bab' = nb' = b'$. □

Désormais on écrit 1 (ou 0, si l'opération est noté additive, i.e. par "+") pour l'élément neutre d'un groupe, et A^{-1} (ou $-A$ dans le cas de notation additive) pour l'inverse de a.

Théorème 1.3. $(ab)^{-1} = b^{-1}a^{-1}$

Démonstration. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$ et de même $(b^{-1}a^{-1})(ab) = 1$. □

Théorème 1.4. *Soit $a, b \in G$, alors il existe un et un seul $x \in G$ ($y \in G$) tel que $ax = b$ ($ya = b$).*

Remarque. Une formulation équivalente est : les deux applications "multiplication à gauche" et "multiplication à droite"

$$g_a \colon G \to G,\ x \mapsto ax, \quad d_a \colon G \to G,\ x \mapsto xa$$

sont bijectives.

Pour un groupe fini G, i.e. si G ne possède qu'un nombre fini d'éléments $a_1, \ldots, a_n$, on peut formuler la dernière remarque encore plus suggestif en regardant le tableau de multiplication de G :

	a_1	a_2	$\ldots$	a_n
a_1	a_1a_1	a_1a_2	$\ldots$	a_1a_n
a_2	a_2a_1	a_2a_2	$\ldots$	a_2a_n
$\vdots$				
a_n	a_na_1	a_na_2	$\ldots$	a_na_n

Le fait que g_a et d_a sont bijectifs pour tout a est équivalente à dire que tout $a \in G$ se manifeste une et une seule fois dans chaque colonne et une et une seule fois dans chaque ligne du tableau. En effet, cette propriété est presque équivalente à dire qu'une opération définie par un telle tableau satisfait aux axiomes d'un groupe. Plus précisément on a

Théorème 1.5. *Soit $\cdot \colon G \times G \to G$ une opération associative sur un ensemble $G \neq \emptyset$ (i.e. on a $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ pour tout $a, b, c \in G$). Si les applications*

$$g_a, d_a : G \to G, \quad g_a(x) = ax,\ d_a(x) = xa$$

sont bijectives, alors l'ensemble G muni de "$\cdot$" est un groupe.

Démonstration. On fixe $a_0 \in G$. Car g_{a_0} est surjective il existe un n tel que $g_{a_0}(n) = a_0$, i.e. $a_0 n = a_0$.

Avec ce n on a $na = a$ pour tout $a \in G$. En effet, $a_0 n = a_0$ entraîne $a_0 na = a_0 a$, i.e. $g_{a_0}(na) = g_{a_0}(a)$; d'après l'injectivité de g_{a_0} donc $na = a$.

En particulier on a $na_0 = a_0$, ce qui implique $an = a$ pour tout a : Encore $na_0 = a_0$ entraîne $ana_0 = a_0 a$, donc $d_{a_0}(an) = d_{a_0}(a)$, et car d_{a_0} est injective donc $an = a$.

Finalement, il existe pour tout a un b tel que $g_a(b) = n$, i.e. $ab = n$. On a $aba = a$, i.e. $g_a(ba) = g_a(n)$, donc aussi $ba = n$ car g_a est injective. □

Définition. Une application

$$f : G \to H$$

d'un groupe G dans un groupe H est dite morphisme de groupe (ou homomorphisme) si

$$f(ab) = f(a)f(b)$$

pour tout $a, b \in G$. Un isomorphisme est un morphisme qui est bijectif, On dit que G est isomorphe à H (avec des symboles :$G \approx H$) si il existe un isomorphisme $G \to H$.

Exemple. Soit G un groupe, $a \in G$. Pour $x \in \mathbb{Z}$ on pose

$$a^x = \begin{cases} a \cdots a \ (x - \text{fois}) & \text{si } x > 0 \\ 1 & \text{si } x = 0 \\ a^{-1} \cdots a^{-1} \ ((-x) - \text{fois}) & \text{si } x < 0 \end{cases}.$$

Alors $p_a \colon \mathbb{Z} \to G$, $\mathbb{Z} \ni n \mapsto a^n$ est un morphisme de groupes.

Exemple. Soit V un espace vectoriel sur $\mathbb{R}$ de dimension finie. Pour $L \in \mathrm{GL}(V)$ soit $M(L) \in \mathrm{GL}(n, K)$ la matrice associée à L par rapport à une base donnée. Alors $M \colon \mathrm{GL}(V) \to \mathrm{GL}(n, \mathbb{R})$, $L \mapsto M(L)$ est un isomorphisme de groupes.

Théorème 1.6. *Soit f un morphisme. Alors $f(1) = 1$ et $f(a)^{-1} = f(a^{-1})$ pour tout a.*

Démonstration. De $f(1) = f(1 \cdot 1) = f(1)f(1)$ la première identité, et de $f(a^{-1})f(a) = f(a^{-1}a) = f(1) = 1$ et $f(a)f(a^{-1} = f(aa^{-1}) = f(1) = 1$ la deuxième. □

Théorème 1.7. *Si f est un isomorphisme, alors f^{-1} est isomorphisme. Le composé $f \circ g$ de deux homomorphismes f et g est un homomorphisme.*

Démonstration. Exercice. □

Remarque. Le théorème entraîne que la relation $G \approx H$ est une relation d'équivalence sur la classe des groupes.

Définition. Un sous-ensemble $S \subset G$, $S \neq \emptyset$ est dit sous-groupe (de G) si

1. $ab \in S$ pour tout $a, b \in S$,

2. $a^{-1} \in S$ pour tous $a \in S$.

Exemple. Tout groupe G contient les deux sous-groupes "triviaux" $\{1\}$ et G.

Exercice. Montrer : Pour tout $a \in G$ l'ensemble $\langle a \rangle := \{a^x \mid x \in \mathbb{Z}\}$ est un sous-groupe.

Exercice. Montrer que les conditions 1. et 2. sont équivalente à la seule condition

$$ab^{-1} \in S \quad \text{pour tout } ab \in S.$$

Théorème 1.8. *Soit S un sous-groupe de G. Alors la restriction de la multiplication dans G à une application $S \times S \to S$ définit une structure de groupe sur S.*

Démonstration. Exercice. □

Théorème 1.9. *Tout sous-groupe de $\mathbb{Z}$ est de la forme $p\mathbb{Z}$ avec un $p \geq 0$.*

Démonstration. Soit S un sous-groupe de $\mathbb{Z}$. Cas 1 : $S = \{0\}$. Alors $\mathbb{Z} = 0 \cdot \mathbb{Z}$. Cas 2 : Il existe $0 \neq x \in S$. Alors $x, -x \in S$, donc S contient des éléments strictement positive. Soit p le plus petit de tels éléments. Il est clair que $p\mathbb{Z} \subset S$. Réciproquement soit $a \in S$. D'après la division euclidienne on a $a = bp + r$ avec des entiers b, r convenable et $0 \leq r < p$. Car $r = a - bp$ on a $r \in S$, donc $r = 0$ d'après la minimalité de p. □

Définition. Pour un morphisme $f : G \to H$ on pose

$$\ker(f) := \{a \in G : f(a) = 1\}.$$

Théorème 1.10. *Soit $f \colon G \to H$ un morphisme de groupes. Alors :*

1. $\ker(f)$ *est un sous-groupe.*
2. *Pour tout sous-groupe S l'image $f(S)$ est un sous-groupe.*
3. *Pour tout sous-groupe T de H l'image réciproque $f^{-1}(T)$ est sous-groupe.*

Démonstration. Exercice. □

Théorème 1.11. *Soit $f\colon G \to H$ un morphisme et $a, b \in G$. Alors on a $f(a) = f(b)$ si et seulement si $a = bk$ avec un $k \in \ker(f)$.*

Remarque. En particulier on a : f est injectif si et seulement si $\ker(f) = \{1\}$.

Démonstration. Si $f(a) = f(b)$, alors $1 = f(b)^{-1}f(a) = f(b^{-1}a)$, donc $k := b^{-1}a \in \ker(f)$ et $a = bk$. Réciproquement, si $a = bk$ et $f(k) = 1$, alors $f(a) = f(bk) = f(b)f(k) = f(b)$. □

Exemple. L'application

$$\det\colon \mathrm{GL}(n, K) \to K^*, A \mapsto \det(A)$$

(K un corps) est un morphisme de groupes. Son noyau est le sous-groupe $\mathrm{SL}(n\mathbb{R})$ de matrices à déterminant 1.

Exercice. Montrer que det est surjectif.

Exercice. L'ensemble des "automorphisme" de G

$$\mathrm{Aut}(G) := \{f : G \to G : f \text{ ismorphisme}\}.$$

muni de la composition d'applications est un groupe. Montrer que l'application

$$c\colon G \to \mathrm{Aut}(G), \quad a \mapsto c(a) \text{ où } \big(c(a)\big)(x) = axa^{-1}$$

est un homomorphisme. On appelle $\mathrm{Z}(G) := \ker(c)$ le centre de G. Montrer que

$$\mathrm{Z}(G) = \{a \in G : ax = xa \text{ pour tout} x \in G\}.$$

Les éléments dans l'image de G sous c sont appelés les automorphismes intérieurs, les autres extérieurs.

Exemple. On pose

$$\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}.$$

C'est un sous-groupe de $\mathbb{C}^*$. On définit

$$\phi : \mathbb{R} \to \mathbb{S}^1, \quad t \mapsto \exp(it)(= \cos t + i \sin t).$$

L'application ϕ est un morphisme de groupe; elle est surjective et

$$\ker \phi = 2\pi\mathbb{Z}.$$

Définition. Pour un sous-ensemble E d'un groupe G on pose

$$\langle E\rangle := \bigcap_S S,$$

où S parcourt les sous-groupes de G qui contiennent E. On appelle $\langle E\rangle$ le sous-groupe engendré par E.

Exercice. Montrer : L'intersection de sous-groupes d'un groupe G est un sous-groupe. En déduire que $\langle E\rangle$ est un sous-groupe. Montrer aussi que $\langle E\rangle$ est égal à l'ensemble "des mots sur l'alphabète a, a^{-1} avec $a \in G$".

Définition. L'ordre d'un élément a d'un groupe, noté $\mathrm{ord}(a)$, est le plus petit entier $p \geq 1$ tel que $a^p = 1$, si il existe un tel entier.

On écrit $\mathrm{ord}(a) = \infty$ pour indiquer que $a^p \neq 1$ pour tout entier $p \geq 1$.

Théorème 1.12. *Soit a un élément d'un groupe G. Si $\mathrm{ord}(a) = \infty$, alors $\langle a\rangle$ est isomorphe à $\mathbb{Z}$. Si $p := \mathrm{ord}(a)$ est fini, alors pour tout $x, y \in \mathbb{Z}$ on a $a^x = a^y$ si et seulement si $x \equiv y \bmod p$; en particulier, $\langle a\rangle = \{1 = a^0, a, \ldots, a^{p-1}\}$ et $\mathrm{ord}(a) = |\langle a\rangle|$*

Démonstration. On considère le morphisme

$$p_a : \mathbb{Z} \to \langle a\rangle, \quad x \mapsto a^x.$$

Il est évidemment surjectif. Si $\mathrm{ord}(a) = \infty$, alors son noyau se réduit à $\{0\}$, et donc il est injectif, donc bijectif. Sinon on vérifie $\ker p_a = p\mathbb{Z}$, et le théorème est une conséquence du fait que $p_a(x) = p_a(y)$ si et seulement si $x = y + k$ avec un $k \in \ker p_a$ convenable (voir théorème 1.11). □

1.2 Exemples de groupes finis

1.2.1 Le groupe $\mathrm{Perm}(X)$

Définition. Pour un ensemble X on note $\mathrm{Perm}(X)$ le groupe des applications bijectives $X \to X$ muni de la composition d'applications.

Théorème 1.13. *Tout groupe G est isomorphe à un sous-groupe du groupe $\mathrm{Perm}(G)$*

Démonstration. L'application

$$G \to \mathrm{Perm}(G), \quad a \mapsto g_a \quad (g_a(x) = ax)$$

est un morphisme injectif de groupes. □

1.2.2 Le groupe symétrique $\S_n$

Définition. Le groupe symétrique d'ordre n est le groupe

$$S_n := \mathrm{Perm}(\{1, 2, \ldots, n\}).$$

Remarque. Parfois on appelle le nombre d'éléments d'un groupe fini l'ordre de G. Dans ce sens l'ordre d'un élément $a \in G$ est égal à l'ordre du sous-groupe engendré par a (voir théorème 1.12). Malheureusement on parle du groupe symétrique d'ordre n, tandis que son ordre est différent de n (pour $n \geq 3$).

Théorème 1.14. *Si X est un ensemble fini avec n éléments, alors le groupe* $\mathrm{Perm}(X)$ *est isomorphe à S_n.*

Démonstration. Exercice. □

Théorème 1.15. *Tout groupe fini G est isomorphe à un sous-groupe de S_n, où $n = |G|$.*

Démonstration. C'est une conséquence des deux théorèmes précédents. □

Théorème 1.16. $|S_n| = n!$.

Démonstration. Pour définir une application bijective de $\{1, 2, \ldots, n\}$ sur soi-même, on a n images possibles pour 1, puis il reste $n-1$ images possibles pour 2, puis $n-2$ images pour 3 etc. Donc on a $n!$ possibilités de définir une telle application. □

On peut décrire les $\pi \in S_n$ par leurs "tables de valeurs"

$$\pi \approx \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}.$$

Exercice. Vérifier que l'on a dans S_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Définition. Pour des nombres naturels $1 \leq l_1, l_2, \ldots, l_r \leq n$ deux à deux différents on note $(l_1 l_2 \ldots l_r)$ la permutation π de S_n définie par

$$\pi(x) = \begin{cases} x & \text{si } x \notin \{l_1, \ldots, l_r\} \\ l_{j+1} & \text{si } x = l_j \text{ pour un } 1 \leq j < r \\ l_1 & \text{si } x = l_r \end{cases}.$$

Les permutations que l'on peut écrire sous cette forme sont appelée cycles.

Exercice. Vérifier que

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 3 & 5 & 1 & 7 & 8 \end{pmatrix} = (12436)$$

et

$$(1257)\,(256) = (127)(56).$$

Nous remarquons qu'une cycle de S_n peut être interprétée aussi comme cycle dans S_m pour tout $m \geq n$. Cette observation s'explique par le fait suivant :

Exercice. Soit $m \geq n$. Pour un $\pi \in S_n$ on définie $\tilde{\pi} \in S_m$ par $\tilde{\pi}(l) = \pi(l)$ si $l \leq n$, et $\tilde{\pi}(l) = l$ si $l > n$. Montrer que l'application

$$S_n \to S_m,\ \pi \mapsto \tilde{\pi}$$

est un morphisme injectif.

Théorème 1.17. *Soit $(l_1 l_2 \ldots l_r)$ un cycle dans S_n. On a*

1. $\operatorname{ord}\big((l_1 l_2 \ldots l_r)\big) = r$
2. $(l_1 l_2 \ldots l_{r-1} l_r)^{-1} = (l_r l_{r-1} \ldots l_2 l_1)$
3. $\pi(l_1 l_2 \ldots l_r)\pi^{-1} = (\pi(l_1)\pi(l_2)\ldots\pi(l_r))$ *pour tout* $\pi \in S_n$.

Démonstration. Exercice. □

L'importance des cycles est due au théorème suivant :

Théorème 1.18. *Toute permutation π s'écrit sous la forme*

$$\pi = c_1 \cdots c_s$$

avec des cycles c_j deux à deux disjoints. Les c_j différent de 1 sont uniques à l'ordre près.

Démonstration. Plus tard (voir la section 1.6.1). □

Définition. Une transposition est un cycle de la forme (kl).

Corollaire 1.18.1. *Toute permutation est un produit de transpositions.*

Démonstration. Par induction sur la longueur d'un cycle en utilisant

$$(l_1 l_2 \dots l_r) = (l_2 \dots l_r)(l_1 l_r).$$

□

1.2.3 Le groupe alterné A_n

Définition. Pour un $\pi \in S_n$ on pose

$$\operatorname{sign}(\pi) = \prod_{\{i,j\} \in I} \frac{\pi(i) - \pi(j)}{i - j}.$$

où I est l'ensemble des parties de $\{1, 2, \dots, n\}$ avec exactement 2 éléments.

Remarque. On remarque que

$$\frac{\pi(i) - \pi(j)}{i - j} = \frac{\pi(j) - \pi(i)}{j - i}.$$

Donc le facteur associé à un sous-ensemble $S = \{i, j\}$ dans la définition de $\operatorname{sign}(\pi)$ ne dépend que du S, mais pas de l'ordre de i et j.

Théorème 1.19. $\operatorname{sign}\colon S_n \to \{\pm 1\}$ *est un morphisme de groupes.*

Démonstration. Soit π et σ deux permutations de $\{1, 2, \dots, n\}$. Si $\{i, j\}$ parcourt les éléments de I, alors $\{\pi(i), \pi(j)\}$ les parcourt également. Donc on peut écrire

$$\operatorname{sign}(\pi) = \prod_{\{i,j\} \in I} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{\sigma(i) - \sigma(j)}.$$

On obtient ainsi

$$\begin{aligned}\operatorname{sign}(\pi)\operatorname{sign}(\sigma) &= \Big(\prod_{\{i,j\}\in I}\frac{\pi(\sigma(i))-\pi(\sigma(j))}{\sigma(i)-\sigma(j)}\Big)\Big(\prod_{\{i,j\}\in I}\frac{\sigma(i)-\sigma(j)}{i-j}\Big)\\ &= \prod_{\{i,j\}\in I}\Big(\frac{\pi(\sigma(i))-\pi(\sigma(j))}{\sigma(i)-\sigma(j)}\,\frac{\sigma(i)-\sigma(j)}{i-j}\Big) = \operatorname{sign}(\pi\sigma).\end{aligned}$$

□

Lemme. *La signature d'une transposition est égale à* -1.

Démonstration. Exercice. □

Définition. On pose

$$A_n := \{\sigma \in S_n : \operatorname{sign}(\sigma) = -1\}.$$

Remarque. Autrement dit $A_n = \ker(\operatorname{sign})$, ce qui montre que A_n en tant que noyau est un sous-groupe de S_n.

Théorème 1.20. *Soit* $\pi \in S_n$, *on suppose* $\pi = t_1 t_2 \cdots t_r$ *avec des transpositions* t_j. *Alors* $\operatorname{sign}(\pi) = (-1)^r$

Remarque. Donc la parité de r dans une écriture d'une permutation comme produit de r cycle est unique.

Démonstration. Evident en utilisant que sign est un morphisme et qu'une transposition a signature -1. □

Corollaire 1.20.1. A_n = *est égal à l'ensemble des permutations que l'on peut écrire comme produit d'un nombre pair de transpositions.*

Théorème 1.21. $|A_n| = n!/2$ *pour* $n \geq 2$.

Démonstration. D'après le corollaire on a, si $n \geq 1$,

$$S_n = A_n \cup tA_n \quad \text{(réunion disjointe)}$$

avec une transposition quelconque. D'où $|S_n| = 2|A_n|$. □

1.2.4 Groupes cycliques

Définition. Un groupe G est dit cyclique si $G =< a >$ pour un $a \in G$ convenable.

Remarque. Tous groupes cycliques de mêmes ordres sont isomorphes (voir théorème 1.12).

Définition. Pour un entier $n \geq 1$ on pose

$$\mu_n := \{z \in \mathbb{C} \,|\, z^n = 1\}$$

Théorème 1.22. *On a :*

1. *μ_n est sous-groupe de $\mathbb{S}^1$ et cyclique d'ordre n.*

2. *Tout sous-groupe fini de $\mathbb{S}^1$ est égal à μ_n.*

Démonstration. Pour 1. il suffit à remarquer

$$\mu_n = \{\exp(2\pi i \frac{k}{n} : 0 \leq k \leq n-1\},$$

ce qui est facilement à montrer en utilisant que $t \mapsto \exp(it)$ définit un morphisme surjectif $\mathbb{R} \to \mathbb{S}^1$ avec noyau $2\pi\mathbb{Z}$. 2. est un Exercice. Indication : Soit S un sous-groupe fini, soit $\alpha > 0$ minimal tel que $z_0 := \mathrm{e}(i\alpha) \in S$. Similaire à la preuve de théorème 1.9 on montre que S est engendré par z_0. □

Nous remarquons que dans la représentation graphiques usuelles des nombres complexes $\mathbb{S}^1$ correspond au cercle de rayon 1 à centre 0, et, d'après le théorème précédent, μ_n est l'ensembles des sommets d'un polygone régulier à n côtés, qui sont situés sur le cercle $\mathbb{S}^1$.

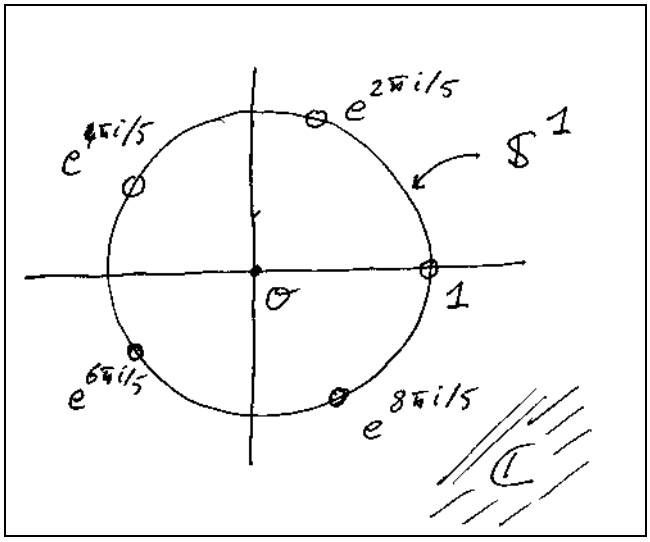


Figure 1.1: Le groupe μ_5

1.2.5 Groupes diédraux

Définition. Un groupe G est dit diédral d'ordre $2n$ si $G =< a > \cup (c < a >)$ (réunion disjointe) avec un a d'ordre n et un c d'ordre 2 tel que $cac = a^{-1}$.

Exercice. Tous groupes diédraux d'ordre $2n$ sont isomorphes.

Soit $\mathbb{C}_R$ le $\mathbb{R}$-espace vectoriel $\mathbb{C}$, i.e. l'ensemble des nombres complexes considéré comme espace vectoriel sur $\mathbb{R}$. Pour $a \in \mathbb{C}^*$ soit m_a l'élément de $\mathrm{GL}(\mathbb{C}_\mathbb{R})$ défini par $m_a(z) = az$, et soit c la conjugaison complexe $c(z) = \overline{z}$ (qui est aussi dans $\mathrm{GL}(\mathbb{C}_\mathbb{R})$).

Exercice. Montrer

$$cm_a c = m_a^{-1}$$

pour tout $a \in \mathbb{S}^1$.

Théorème 1.23. *Le sous-groupe G_n de $\mathrm{GL}(\mathbb{C}_\mathbb{R})$ engendré par c et les m_a avec $a \in \mu_n$ est un groupe diédral d'ordre $2n$. On a*

$$G_n = \langle m_a : a \in \mu_n \rangle \cup c\langle m_a : a \in \mu_n \rangle.$$

Démonstration. Exercice. □

Théorème 1.24. *Avec le groupe G_n du théorème précédent on a :*

$$G_n = \{f \in \mathrm{GL}(\mathbb{C}_{\mathbb{R}}) \,|\, f(\mu_n) = \mu_n\}.$$

si $n \geq 3$.

Démonstration. Plus tard (voir section 1.6.2). □

1.2.6 Le groupe quaternionien H_8

On pose

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \,|\, a, b \in \mathbb{C} \right\}.$$

Cet ensemble de matrices est stable sous l'addition et multiplication usuelle de matrices. En plus, toute matrice $x \in \mathbb{H}$ différente de 0 est inversible. On peut résumer ces faits en disant que "$\mathbb{H}$ est un est un corps non-commutatif", et c'est pour ça qu'on appelle $\mathbb{H}$ le corps des quaternions de Hamilton. En particulier, $\mathbb{H}^* := \mathbb{H} \setminus \{0\}$ est un groupe (par rapport
'a la multiplication de matrices).

$\mathbb{H}$ est aussi un espace vectoriel sur $\mathbb{R}$ (mais pas sur $\mathbb{C}$). La dimension est 4. Comme base on peut prendre

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

On vérifie que

$$I^2 = J^2 = K^2 = -1, \; IJ = -JI = K.$$

En utilisant ces formules on peut calculer le produit de deux quaternions $q = x + yI + uJ + vK$ et $q' = x' + y'I + \cdots$ (avec $x, x', y, \cdots \in \mathbb{R}$) sans faire de rapport à des matrices. On pose

$$\mathbb{H}_1 := \{q \in \mathbb{H} : \det q = 1\}.$$

Il est clair que S^3 est un sous-groupe de $\mathbb{H}^*$.

D'après la définition on a

$$\mathbb{H}_1 = \{x + Iy + uJ + vK : x^2 + y^2 + u^2 + v^2 = 1\}.$$

En générale on appelle

$$S^{n-1} := \{(x_1, \ldots, x_n)^t \in \mathbb{R}^n : x_1^2 + \cdots + x_n^2 = 1\}$$

la sphère de dimension $n-1$. On a vu que S^1 (identifié avec ensemble des nombres complexes de valeur absolue 1 via la bijection $(x,y) \mapsto x+iy$) est un groupe. Et dans cette section on obtient que S^3 (identifié avec $\mathbb{H}_1$ via $(x,y,u,v) \mapsto x1 + yI + uJ + vK$) est également un groupe. On est donc tenté à demander : pour quels n est-ce qu'on peut définir une opération 'naturelle' de groupe sur S^n ? Si on précise 'naturelle' par la condition que la multiplication est l'application $x \mapsto x^{-1}$ soient continues, alors la réponse est (difficile mais) connue : "seulement pour $n = 1$ et $n = 3$."

Théorème 1.25. *Soit H_8 l'ensemble des quaternions $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ dans $\mathbb{H}_1$ tels que les parties réelles et imaginaires de a et b sont des nombres entiers. Alors H_8 est un sous-groupe d'ordre 8 de $\mathbb{H}_1$ (le groupe quaternionien d'ordre 8). On a*

$$H_8 = \{\pm 1, \pm I, \pm J, \ \pm K\}.$$

Démonstration. Exercice. □

1.3 Quotients de groupes

Pour des sous-ensembles $E, E_1, \ldots$ et un élément a d'un groupe G on pose

$$aE := \{ab : b \in E\}, \quad Ea := \{ba : b \in E\},$$
$$E_1 \cdot E_2 = \{bc : b \in E_1, \ c \in E_2\}, \quad E^{-1} = \{b^{-1} : b \in E\}.$$

Exercice. Vérifier les règles de calcul suivant :

1. $(ab)E = a(bE)$, $(aE_1)E_2 = a(E_1E_2)$ et $E_1(E_2E_3) = (E_1E_2)E_3$.
2. $(aE)^{-1} = E^{-1}a^{-1}$ et $(E_1E_2)^{-1} = E_2^{-1}E_1^{-1}$.
3. $S \subseteq G$ est un sous-groupe si et seulement si $S \cdot S = S$ et $S^{-1} = S$.

Désormais dans cette section S désigne un sous-groupe de G.

Définition. Une classe à gauche par rapport à S est une partie de G de la forme aS avec un $a \in G$ convenable. On note G/S l'ensemble de toutes les classes à gauche par rapport à S, et on pose

$$[G : S] = |G/S|$$

("indice de S dans G").

Exercice. Vérifier :

1. $aS = S$ si et seulement si $a \in S$.
2. $aS = bS$ si et seulement si $a \in bS$ si et seulement si $b \in aS$ si et seulement si $b^{-1}a \in S$.

Exemple. Soit $G = \mathbb{Z}$, $S = p\mathbb{Z}$ $(p > 0)$, alors $a + p\mathbb{Z} = b + p\mathbb{Z}$ si et seulement si a et b laissent le même reste sous division par p Donc :

$$\mathbb{Z}/p\mathbb{Z} = \{\mathbb{Z}, 1 + \mathbb{Z}, 2 + \mathbb{Z}, \ldots, (p-1) + p\mathbb{Z}\}, \qquad [\mathbb{Z} : p\mathbb{Z}] = p.$$

Exemple. Soit $G = \mathbb{R}$ et $S = 2\pi\mathbb{Z}$. Alors

$$\mathbb{R}/2\pi\mathbb{Z} = \{a + 2\pi\mathbb{Z} : a \in [0, 2\pi[\}.$$

Théorème 1.26. *Tout élément de G appartient à une et une seule classe à gauche.*

Remarque. Une formulation équivalente est :

$$G = \dot{\bigcup_{\mathcal{C} \in G/S}} \mathcal{C}. \quad \text{(réunion disjointe)}$$

Une autre formulation équivalente est : La relation

$$a \equiv_g b \mod S :\Longleftrightarrow b^{-1}a \in S$$

est une relation d'équivalence. Les classes d'équivalence sont les classes à gauches par rapport à S.

Démonstration. "une" : $a \in aS$. "une seule" : Si $aS \cap bS \neq \emptyset$, alors $as = bs'$ pour des $s, s' \in S$ convenables, et donc $a = bs's^{-1}$, donc $aS = bs's^{-1}S = bS$. □

Comme conséquence immédiate on obtient :

Théorème 1.27. *Si $|G|$ est fini, alors $[G : S] = |G|/|S|$.*

Démonstration. En effet, en utilisant la décomposition de G en classes à gauches disjointes on obtient

$$|G| = \sum_{\mathcal{C} \in G/S} |\mathcal{C}|.$$

Mais $\mathcal{C} = |S|$ car la multiplication par un élément fixé est injective. D'où la formule. □

Corollaire 1.27.1. *Si $|G|$ est fini, alors $|S|$ divise $|G|$*

Corollaire 1.27.2. *Si G est fini, $a \in G$, alors l'ordre de a divise $|G|$.*

Démonstration. Car $\mathrm{ord}(a) = |\langle a \rangle|$. □

Corollaire 1.27.3. *Si $|G|$ est un nombre premier, alors G est un groupe cyclique.*

Démonstration. Soit $a \in G$ tel que $a \neq 1$. Alors $T := \langle a \rangle$ satisfait $|T| > 1$ et $|T|$ divise $|G|$, un nombre premier. Donc $|T| = |G|$, d'où $G = T$. □

Au lieu de classes à gauches on peut considérer également des classes à droites Sa et l'ensemble $S\backslash G$ des classes à droite. Les deux théories que l'on obtiens ainsi sont équivalentes dans le sens :

Théorème 1.28. *L'application $\mathcal{C} \mapsto \mathcal{C}^{-1}$ définit une bijection $G/S \to S\backslash G$.*

Démonstration. Exercice. □

On particulier on a $|G/S| = |S\backslash G \to S|$, i.e. une seule notion d'indice de S dans G.

Définition. Le sous-groupe S est dit distingué si si toute classe à gauche par rapport à S est aussi une classe à droite par rapport à S et vice versa.

Remarque. Les propriétés suivantes sont équivalentes :

1. S est distingué.
2. $aS = Sa$ pour tout $a \in G$.
3. $aSa^{-1} = S$ pour tout $a \in G$ (i.e. le groupe S est invariant sous tout automorphisme intérieur de G).

Exemple. Montrer :

1. Tout sous-groupe d'un groupe abélien est distingué.
2. Le noyau d'un homomorphisme est distingué (pas toujours l'image !)
3. $\langle(12)\rangle \subset S_3$ n'est pas distingué (Considérer la conjugaison avec (13) par exemple).

Lemme. *Soit S distingué dans G. Alors*

$$\mathcal{C}_1 \cdot \mathcal{C}_2 \ (= \{c_1 c_2 \,|\, c_1 \in \mathcal{C}_1,\, c_2 \in \mathcal{C}2\} \ )$$

est une classe à gauche.

Démonstration. Soit $\mathcal{C}_1 = aS, \mathcal{C}_2 = bS$, alors $\mathcal{C}_1 \cdot \mathcal{C}_2 = aSbS = abSS = abS$. □

Théorème 1.29. *Soit S distingué dans G. Alors G/S muni de l'opération $(\mathcal{C}_1, \mathcal{C}_2) \mapsto \mathcal{C}_1 \cdot \mathcal{C}_2$ est un groupe. L'application canonique $p : G \to G/S$, $a \mapsto aS$ est un morphisme.*

Démonstration. Exercice. □

Exemple. $G/G = \{G\}$, $G/\{1\} \approx G$.

Exercice. Montrer $\mathbb{Z}/p\mathbb{Z} = \langle 1 + p\mathbb{Z}\rangle$.

Théorème 1.30. *(***Théorème de Factorisation***) Soit $f : G \to H$ un morphisme de groupes et $p : G \to G/\ker(f)$ l'application canonique. Alors il existe un et un seul morphisme $\underline{f} : G/\ker(f) \to H$ tel que $\underline{f} \circ p = f$. Le morphisme $\underline{f}$ est injectif.*

Remarque. Si f est surjectif, alors $\underline{f}$ définit un isomorphisme entre $G/\ker(f)$ et H.

Démonstration. Si un tel $\underline{f}$ existe, alors $\underline{f}(aS) = \underline{f} \circ p(a) = f(a)$ pour tout $a \in G$, donc est unique. Réciproquement, l'application $\underline{f}(aS) := f(a)$ est bien-définie est possède toutes les propriétés annoncées dans le théorème. □

Exemple. $\mathbb{R} \to \mathbb{S}^1$, $t \mapsto \exp(it)$ induit un isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \approx \mathbb{S}^1$.

Exemple. Si $G =< a >$ avec un a d'ordre n, alors $p_a : \mathbb{Z} \to G$, $x \mapsto a^x$ induit un isomorphisme $\mathbb{Z}/n\mathbb{Z} \approx G$. Donc :

Théorème 1.31. *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

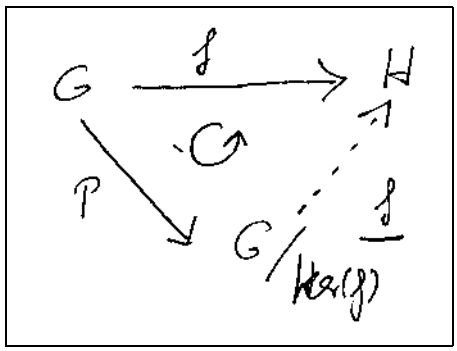


Figure 1.2: Le Théorème de Factorisation

1.4 Produit direct et semi-direct

Soient G, H deux groupes, $\alpha : G \to \mathrm{Aut}(H)$ un morphisme. On définit sur $H \times G$ une opération par

$$(h, g) \cdot (\tilde{h}, \tilde{g}) = (h\,\alpha(g)(\tilde{h}), g\tilde{g}). \qquad (*)$$

Théorème 1.32. *$H \times G$ muni de l'opération $(*)$ est un groupe (noté $H \rtimes_\alpha G$ ou $H \rtimes G$, si α est clair du contexte, et appelé produit semi-direct de H et G). La suite de morphismes*

$$1 \to H \xrightarrow{i} H \rtimes G \xrightarrow{\pi} G \to 1,$$

où la deuxième flèche est l'application $h \mapsto (h, 1)$ et la troisième l'application $(h, g) \mapsto g$, est exacte.

Remarque. Le mot "exacte" signifie que pour toute flèche de la suite son image est égale au noyau de la flèche suivante. La lettre 1 indique le groupe trivial ne contenant qu'un seule élément (son élément neutre). Évidemment on un et un seule morphisme $1 \to G$ et $G \to 1$ pour tout groupe G. Que la suite c-dessus est exacte signifie donc : i est injectif, $\mathrm{im}(i) = \ker(\pi)$, et π et surjectif.

Démonstration. Exercice. □

Exemple. Soit $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ le morphisme tel que

$$[\alpha(1 + 2\mathbb{Z})](b + n\mathbb{Z}) = -b + n\mathbb{Z}.$$

Alors $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est un groupe diédral d'ordre $2n$.

Théorème 1.33. *Tout groupes diédral d'ordre $2n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.*

Démonstration. Soit G diédral, engendré par a et c avec $a^n = 1$ et $c^2 = 1$ et $cac = a^{-1}$. Alors

$$\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \to G, \quad (x + n\mathbb{Z}, y + 2\mathbb{Z}) \to a^x c^y$$

est bien-défini et est un isomorphisme. □

Définition. Si $\alpha(g) = 1$ pour tout $g \in G$ on appelle $H \rtimes_\alpha G$ le produit direct (extérieur) de H et G, noté $H \times G$.

Remarque. Dans le cas $\alpha \equiv 1$, i.e. dans le cas d'un produit direct, l'opération $(*)$ est plus simple :

$$(h, g) \cdot (\tilde{h}, \tilde{g}) = (h\tilde{h}, g\tilde{g}).$$

Exercice. $V := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe d'ordre 4. Montrer que V n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$, et que tout groupe d'ordre 4 est isomorphes à soit V, soit $\mathbb{Z}/4\mathbb{Z}$.

Théorème 1.34. *Soient H, K sous-groupes d'un groupes G. On suppose que*

1. *$G = HK$ et $H \cap K = \{1\}$,*
2. *H distingué dans G.*

Alors l'application $H \rtimes_\alpha K \to G$, $(h, k) \mapsto hk$ est un isomorphisme, où $\alpha(k)(h) = khk^{-1}$.

Démonstration. Exercice. □

Remarque. Si supplémentaire aux hypothèses du théorème les éléments du sous-groupe K commutent avec les éléments de H, alors $\alpha = 1$. Dans ce cas on dit que G est le produit direct intérieur de H et K. D'après le théorème les notions produit intérieur et extérieur coïncident à isomorphisme près.

1.5 Actions de groupe

Définition. Une action d'un groupe G sur un ensemble X est une application

$$\cdot : G \times X \to X$$

telle que

1. $1 \cdot x = x$ pour tout $x \in X$,

2. $(a \cdot (b \cdot x)) = (ab) \cdot x$ pour tout $a, b \in G$ et $x \in G$.

Remarque. A cause de 2. on peut écrire sans ambiguïté simplement $ab \cdot x$ au lieu de $(a(b \cdot x))$ ou $(ab) \cdot x$. En plus on supprime dans les formules souvent le point dans $a \cdot x$.

Théorème 1.35. *Soit '$\cdot$' une action de G sur X. Pour $a \in G$ on pose $T_a : X \to X$, $T_a(x) = a \cdot x$. Alors T_a est une bijection, et l'application $G \to \mathrm{Perm}(X)$, est un morphisme de groupes.*

Réciproquement, si $\alpha \colon G \to \mathrm{Perm}(X)$ est un homomorphisme, alors $(a, x) \mapsto \alpha(a)(x)$ définit une action de G sur X.

Démonstration. Exercice. □

Exemple. 1. Tout groupe G agit sur $X = G$ par $(a, x) \mapsto ax$ et 2. aussi par $(a, x) \mapsto axa^{-1}$. 3. $\mathrm{GL}(n, \mathbb{R})$ agit sur $\mathbb{R}^n$ (vecteurs à colonnes) par $(A, x) \mapsto A \cdot x$ où le point signifie le produit matriciel.

Exercice. Montrer que $\mathbb{S}^1$ agit sur $\mathbb{R}^2$ par

$$(s, (x, y)) = (ax - by, ay + bx) \qquad (s = a + ib,\ a, b \in \mathbb{R}).$$

Définition. Une opération de G sur X est dite

1. Fidèle si seulement $a = 1$ satisfait à $a \cdot x = x$ pour tout $x \in X$,

2. Transitive si pour tout x et y dans X il existe un $a \in G$ tel que $y = a \cdot x$.

3. Simplement transitive si pour tout x et y dans X il existe un *et un seul* $a \in G$ tel que $y = a \cdot x$.

Théorème 1.36. *Toute opération transitive et fidèle d'un groupe abélien est simplement transitive.*

Démonstration. Soit $x, y \in X$, $a, b \in G$ et $y = ax = bx$. A montrer : $a = b$. D'abord nous remarquons $x = a^{-1}bx$. Soit $z \in X$. Alors il existe un $c \in G$ tel que $z = cx$. Donc

$$a^{-1}bz = a^{-1}bcx = ca^{-1}bx = cx = z.$$

Pour la deuxième identité nous avons utilisé que G est abélien. Or l'action est fidèle, donc $a^{-1}bz = z$ pour tout $z \in X$ implique $a^{-1}b = 1$, i.e. $a = b$. □

Définition. Une orbite dans X par rapport à l'action de G est une partie $\mathcal{O}$ de X de la forme

$$\mathcal{O} = G \cdot x := \{ax \,|\, a \in G\}..$$

On note

$$G\backslash X$$

l'ensemble des orbites. Pour $x \in X$ on pose

$$G_x = \{a \in G : a \cdot x = x\},$$

et on l'appelle stabilisateur de x.

Théorème 1.37. *L'application*

$$G/G_x \to Gx, \quad aG_x \mapsto ax$$

est bien-définie et est une bijection.

Démonstration. Exercice. □

Théorème 1.38. *Tout élément de X appartient à une et une seule orbite.*

Remarque. Une formulation équivalente est

$$X = \dot{\bigcup_{\mathcal{O} \in G\backslash X}} \mathcal{O} \qquad \text{(réunion disjointe)}.$$

Démonstration. Tout $x \in X$ appartient à Gx. Si $Gx \cap Gy \neq \emptyset$, alors $ax = by$ pour $a, b \in G$ convenable. Donc $y = b^{-1}ax$ et $Gy = G = b^{-1}ax = Gx$. □

Théorème 1.39. *(***Formule d'Orbite***) Soit X fini, alors on a*

$$|X| = \sum_{\mathcal{O} = Gx \in G\backslash X} [G : G_x].$$

Démonstration. D'après le théorème précédent on a

$$|X| = \sum_{\mathcal{O}\in G\backslash X} |\mathcal{O}|.$$

Si $\mathcal{O} = Gx$ on a la bijection $G/G_x \to \mathcal{O}$, en particulier $|\mathcal{O}| = [G : G_x]$. □

1.6 Application des actions de groupes

1.6.1 Toute permutation est un produit de cycle disjoint.

Soit $\pi \in S_n$. Le groupe $G := \langle\pi\rangle$ agit sur $X := \{1, 2, \ldots, n\}$ par $\pi \cdot j = \pi(j)$. A une orbite $\mathcal{O} \subset X$, disons $\mathcal{O} = Gl$ et $t = |\mathcal{O}|$ on associe le cycle

$$c_{\mathcal{O}} = (l\, \pi(l)\, \pi^2(l)\, \ldots\, \pi^{t-1}(l)).$$

C'est un cycle car $\pi^r(l) \neq \pi^s(l)$ pour $0 \leq r < s \leq t-1$ (exercice). En utilisant que $\{1, 2, \ldots, n\}$ est la réunion disjointe d'orbites sous G on vérifie facilement que

$$\pi = \prod_{\mathcal{O}\in G\backslash X} c_{\mathcal{O}}.$$

C'est la décomposition de π en produit de cycles disjoints.

Réciproquement, si on a une décomposition de π en cycles disjoints, alors les ensembles formés par les nombres, qui appartiennent aux cycles différent de 1 respectivement, sont exactement les orbites de $\{1, 2, \ldots, n\}$ sous $\langle\pi\rangle$ qui possède plus qu'un seul élément (exercice), et chaque cycle est égal à $c_{\mathcal{O}}$ avec son orbite associé (exercice). D'où l'unicité de la décomposition.

1.6.2 Les symétries de μ_n

Nous utilisons les notations de section 1.2.5 pour montrer ici le théorème 1.24. Nous posons

$$H = \{f \in \mathrm{GL}(\mathbb{C}_{\mathbb{R}}) : f(\mu_n) = \mu_n\}.$$

Pour montrer $H = G_n$ il suffit à montrer $|H| = 2n$.

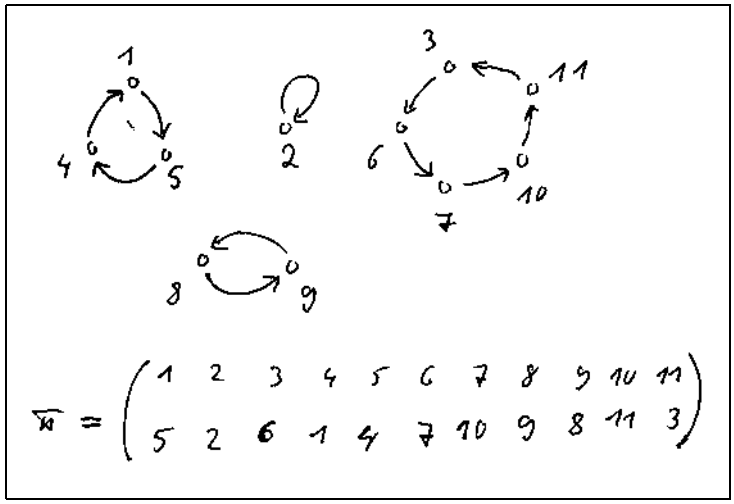


Figure 1.3: Cycles et orbites

D'abord nous remarquons que l'action de H sur μ_n, définit par $(f, z) \mapsto f(z)$, est transitive. D'après la formule d'orbite on a donc

$$n = |\mu_n| = [H : H_1],$$

où H_1 est le stabilisateur du nombre $1 \in \mu_n$. Il est clair que $H_1 \supset \{1, c\}$. Nous allons montrer que l'on a ici en effet égalité. En conséquence $|H_1| = 2$, H est fini et $n = |H|/|H_1| = |H|/2$.

Soit donc $f \in H_1$. Car $n > 3$ il existe un $z \in \mu_n$ différent de 1 et -1, en particulier 1 et z forment une $\mathbb{R}$-base de $\mathbb{C}_{\mathbb{R}}$. Il suffit donc à montrer que $f(z) = z$ ou $f(z) = \overline{z}$ pour en déduire que $f = 1$ ou $f = c$ respectivement. Si $n = 4$ il est clair que $f(z) \in \{z, \overline{z}\}$. Sinon il existe un $u \in \mu_n$ différent de $1, -1, z, -z$. Donc $u = a + bz$ avec $a, b \neq 0$. Or $1 = |u|^2 = a^2 + 2ab\,\mathrm{Re}(z) + b^2$ et $1 = |f(u)^2| = |a + bf(z)|^2 = a^2 + 2ab\,\mathrm{Re}(f(z)) + b^2$, et car $ab \neq 0$ donc $\mathrm{Re}(z) = \mathrm{Re}(f(z))$, et d'où $f(z) = z$ ou $= \overline{z}$.

1.6.3 Les théorèmes de Sylow

Lemme. *Soit G un groupe abélien fini et p un nombre premier divisant l'ordre de G. Alors G possède un élément d'ordre p.*

Démonstration. Soit e l'exponent de G, i.e. le p.g.c.d. des ordres des éléments de G. Nous montrons par récurrence sur l'ordre de G que $|G|$ divise une

puissance de e. Soit $a \neq 1$ un élément de G, H le sous-groupe engendré par a. Il est clair que l'ordre de tout élément de H et de G/H divise e. Par hypothèse de récurrence $|H|$ et $|G/H|$ divisent une puissance de e. Mais donc

$$|G| = [G : H] \cdot |H|$$

divise une puissance de e.

En particulier p divise e, donc il existe un b dans G d'ordre pn avec un n convenable. Évidemment b^n est d'ordre p. □

Théorème 1.40. *(**Sylow I**) Si une puissance p^n d'un nombre premier divise l'ordre du groupe fini G, alors G possède un sous-groupe d'ordre p^n.*

Démonstration. Le groupe G agit sur G par conjugaison :

$$(a, x) \mapsto axa^{-1}.$$

Une orbite contient un seul élément x si et seulement si x appartient au centre $\mathrm{Z}(G)$. Donc la formule de classes s'écrit sous la forme

$$|G| = |\,\mathrm{Z}(G)| + \sum [G : G_a].$$

Nous montrons le théorème par récurrence sur $|G|$. Supposons il est vrai pour tout groupe d'un ordre strictement petit de $|G|$.

Cas 1 : il existe un a tel que $[G : G_a]$ n'est pas divisible par p. Alors p^n divise $|G_a|$, et par hypothèse de récurrence G_a possède donc un sous-groupe d'ordre p^n.

Cas 2 : Tout $[G : G_a]$ est divisible par p. Alors p divise l'ordre du groupe abélien $\mathrm{Z}(G)$. Donc il existe un élément a d'ordre p dans le centre de G. Le sous-groupe H engendré par a est distingué dans G en tant que sous- groupe du centre. Donc on peut considérer le groupe G/H. Soit $p : G \to G/H$ l'application canonique. Or p^{n-1} divise $[G : H]$, donc d'après l'hypothèse de récurrence il existe un sous-groupe K' d'ordre p^{n-1} dans G/H. Soit $K = \pi^{-1}(K')$. Alors $K \supset H = \ker(\pi)$ et $K' = K/H$. Donc

$$p^{n-1} = |K'| = |K|/|H| = |K|/p,$$

i.e. K est d'ordre p^n. □

Corollaire 1.40.1. *(**Cauchy**) Si le nombre p premier divise l'ordre d'un groupe fini G, alors G possède un élément d'ordre p.*

Démonstration. G possède un sous-groupe d'ordre p. Mais un tel sous-groupe est cyclique. □

Pour un nombre premier p on appelle p-Sylow sous-groupe de G tout sous-groupe d'ordre p^n ou p^n est la puissance maximale divisant $|G|$. D'après le théorème précédent il existe toujours un p- Sylow sous-groupe.

Théorème 1.41. *(***Sylow II***) Soit G un groupe fini et P un p-Sylow sous-groupe. Alors pour chaque sous-groupe H de G d'ordre p^n il existe un $a \in G$ tel que $aHa^{-1} \subset P$. En particulier, tous p-Sylow de G sont conjugués.*

Démonstration. Soit S l'ensemble de tous p-Sylow sous-groupes de G. G agit sur S par conjugaison. Alors le stabilisateur G_P contient P, et donc l'ordre de l'orbite S_0 de P divise $[G : P]$, et est donc premier à p.

Or H agit sur S_0 par conjugaison. Chaque orbite est d'ordre divisant $|H|$, donc d'ordre une puissance de p. Car l'ordre de S_0 est premier à p il existe d'après la formule e classes pour S_0 modulo l'action de H une orbite avec un seul élément P'. Car $aP' = P'a$ pour tout $a \in H$ l'ensemble HP' est un sous-groupe de G et P' distingué dans HP' (exercice). Car

$$HP'/P' \approx H/(H \cap P')$$

l'ordre de HP' est une puissance de p. Car P' est maximal d'ordre une puissance de p on conclut $P' = HP'$, i.e. $H \subset P'$. Car P' est conjugué à P le théorème est prouvé. □

1.7 Exercices

1. Soit X un ensemble et $\mathcal{P}(X)$ l'ensemble de toutes les parties de X. Pour $A, B \subseteq X$ on pose $A * B := (A \cup B) \setminus (A \cap B)$. Montrer que $\mathcal{P}(X)$ muni de l'opération $*$ est un groupe.

2. Faire la table d'opération pour $V := \mathcal{P}(\{1, 2, \})$ (groupe de Klein à 4 éléments). Montrer que V est isomorphe à un produit directe de deux groupes d'ordre 2.

3. Montrer directement, en considérant les tables d'opération, que tout groupe d'ordre 4 est soit cyclique, soit isomorphe au groupe V.

4. Montrer que $\mathrm{Aut}(V) \approx S_3$ (Indication : $\mathrm{Aut}(V)$ agit sur l'ensemble des éléments différents de 1 de V.)

5. Pour $\pi \in S_n$ soit $M(\pi) \in \mathrm{GL}(n, \mathbb{R})$ la matrice telle que $e_{\pi(j)} = M(\pi)e_j$ pour $1 \leq j \leq n$, où $e_1, \ldots, e_n$ est la base canonique de $\mathbb{R}^n$. Montrer que $\pi \to M(\pi)$ est un morphisme de groupes, et que $\mathrm{sign}(\pi) = \det(M(\pi))$.

6. Montrer que le sous-groupe $\mathrm{Aut}_{\mathrm{int.}}(G)$ des automorphisme intérieurs d'un groupe G est distingué dans $\mathrm{Aut}(G)$.

7. Soit t une transposition dans S_n. On définit un morphisme $\alpha : \langle t \rangle \to \mathrm{Aut}(A_n)$ par $\alpha(t)(\pi) = t\pi t^{-1}$. Montrer que $S_n \approx A_n \rtimes_\alpha \langle t \rangle$.

8. Montrer que tout sous-groupe d'indice 2 dans un groupe G est distingué dans G. Montrer que A_n est le seul sous-groupe d'indice 2 dans A_n.

9. Soit p le diviseur premier le plus petit de l'ordre du groupe fini G. Montrer que tout sous-groupe d'indice p est distingué dans G. (Attention : ce n'est pas évident.)

10. Montrer, en vérifiant directement la définition, que $\mathrm{GL}(2, \mathbb{F}_2)$ est un groupe diédral.

11. Déterminer l'ordre de $\mathrm{GL}(2, \mathbb{F}_p)$ pour un nombre premier p arbitraire. (Indication : Montrer que l'action naturelle de $\mathrm{GL}(2, \mathbb{F}_p)$ sur $\mathbb{F}_p^2 \setminus \{0\}$ est transitive. Déterminer le stabilisateur de $(1, 0)^t$, et appliquer la formule d'orbite.)

12. Montrer que le groupe quaternionien H_8 n'est pas isomorphe à un produit direct de groupes non-triviaux. (Indication : faire une liste des sous-groupes de H_8.)

13. Soit H un sous-groupe d'un groupe G. L'action de G sur G/H par multiplication à gauche définit un morphisme $\phi : G \to \mathrm{Perm}(G/H)$. Déterminer le noyau de ϕ en fonction de H.

Chapitre 2

Géométrie affine

2.1 Notions de base

Toujours dans cette chapitre K désigne un corps fixé, par exemple $K = \mathbb{R}$ ou $K = \mathbb{C}$ ou $K = \mathbb{F}_n := \mathbb{Z}/p\mathbb{Z}$ avec un nombre premier p. Les mots "espace vectoriel" signifient toujours un espace vectoriel sur K, pas nécessairement de dimension finie.

Définition. Un espace affine est un triplet $(E, V, +)$ où

E est un ensemble,

V est un espace vectoriel,

et "+" est une action fidèle et transitive de V_+ sur E.

Ici V_+ signifie l'espace vectoriel V considéré comme un groupe abélien par rapport à l'addition dans V.

Le résultat de l'action d'un $v \in V$ sur un $p \in E$ est noté $p + v$, i.e. le v est mis à droite.

Exemple. 1. $E = \{p\}$, $V = \{0\}$, $+ \colon (0, p) \mapsto p$. 2. $E = V =$ un espace vectoriel, $+ \colon V \times E \to E$ est l'addition dans V.

Théorème 2.1. *Pour tout $p, q \in E$ il existe un et un seul vecteur, noté $\overrightarrow{pq}$, tel que $p + \overrightarrow{pq} = q$.*

Démonstration. Car une action fidèle et transitive d'un groupe abélien est simplement transitive. □

Remarque. Une formulation équivalente du théorème est à dire : Pour tout $p \in E$ l'application

$$V \to E, v \mapsto p + v$$

est une bijection.

Corollaire 2.1.1. *Si V est de dimension finie, disons avec base $a_1, \ldots, a_n$, et si o est un point de E, alors tout p de E s'écrit uniquement sous la forme*

$$p = o + \sum_{j=1}^{n} \lambda_j a_j$$

avec des scalaires λ_j. (On appelle $(0, a_1, \ldots, a_n)$ un repère cartésien de E.)

Définition. Soit $o \in E$. La vectorialisation E_0 de E en o est l'espace vectoriel $(E, +, \cdot)$, où l'addition et multiplication scalaire sont définies par

$$p + q := o + \overrightarrow{op} + \overrightarrow{oq}, \quad \lambda \cdot p := o + \lambda \overrightarrow{op}.$$

Théorème 2.2. *L'application $V \mapsto E_o$, $v \mapsto o + v$ est un isomorphisme d'espaces vectoriels.*

Démonstration. Exercice. □

Théorème 2.3. *Pour tout $p, q, r \in E$, $v \in V$ on a :*

1. $\overrightarrow{pp} = 0$.
2. $\overrightarrow{pq} = \overrightarrow{qp}$.
3. $\overrightarrow{pq} + \overrightarrow{qr} = \overrightarrow{pr}$ *(Relation de Chasles).*
4. $\overrightarrow{(p+v)\,(q+v)} = \overrightarrow{pq}$

Démonstration. Car

$$p + 0 = p, \quad p = q + \overrightarrow{qp} \Longrightarrow p + (-\overrightarrow{qp}) = q,$$

car "+" est une action de groupe, et car

$$q + v = p + v + \overrightarrow{(p+v)\,(q+v)} \Longrightarrow q = p + \overrightarrow{(p+v)\,(q+v)}.$$

respectivement. □

Théorème 2.4. *Soit S un sous-espace vectoriel de V. Alors l'ensemble des orbites E/S est un espace affine par rapport à l'action de l'espace vectoriel de quotient V/S donnée par $(p+S, v+S) \mapsto (p+v)+S$.*

Démonstration. Exercice. □

On considère des triplets $(X, G, \cdot)$ où G est un groupe, X un ensemble et $\cdot$ une action de G sur X. Pour comparer deux tels triplets, disons $(X, G, \cdot)$ et $(Y, H, \cdot)$, on considère un morphisme de groupes $f : G \to H$ et une application $g : X \to Y$ tels que $g(a \cdot x) = f(a) \cdot g(x)$ pour tout $a \in G$ et $x \in X$. Les applications affines forment un cas spécial de cette idée.

Définition. Une application $f\colon E \to E'$ est dite affine si il existe une application linéaire $F : V \to V'$ tels que

$$f(p+v) = f(p) + F(v)$$

pour tout $p \in E$ et $v \in V$.

Remarque. L'application F associée à une application affine est unique. En effet, on a

$$F(\overrightarrow{pq}) = \overrightarrow{f(p)\, f(q)},$$

i.e.

$$F(v) = \overrightarrow{f(p)\ f(p+v)}$$

pour tout $p, q \in E$ et $v \in V$. Elle est noté $\overrightarrow{f}$.

Théorème 2.5. *Soit $o \in E$, $o' \in E'$, et $F\colon V \to V'$ linéaire. Alors l'application $f : E \to E'$, $f(o+v) := o' + F(v)$ est affine.*

Remarque. En particulier en peut associer à tout $o \in E$ et $F \in \mathrm{GL}(V)$ l'application affine

$$F_o : E \to E, \quad F_o(o+v) = o + F(v).$$

Démonstration. On calcule

$$\begin{aligned} f(p+v) = f(o+\overrightarrow{op}+v) &= o' + F(\overrightarrow{op}+v) \\ &= o' + F(\overrightarrow{op}) + F(v) = f(o+\overrightarrow{op}) + F(v) = f(p) + F(v). \end{aligned}$$

□

Théorème 2.6. *Tout espace affine E avec $\dim V = n$ est isomorphe à l'espace affine K^n, i.e. il existe une application affine $f : K^n \to E$ qui est bijective.*

Démonstration. Soit $(o, a_1, \ldots, a_n)$ un repère cartésien. Alors l'application affine

$$f(\lambda_1, \cdots, \lambda_n) := o + \sum_j \lambda_j \, a_j$$

est un isomorphisme d'espaces affines entre K^n et E. □

Exemple. Les applications suivantes sont affines :

1. Les application constantes.
2. La homothétie $H = H_{o,\lambda} : E \to E$ avec centre $p \in E$ et rapport $\lambda \in K$, qui est définie par $H(o + v) = o + \lambda v$
3. La translation $T = T_t : E \to E$ par un $t \in V$, définie par $T_t(p) = p + t$. Ici $\overrightarrow{T}_t = 1$.
4. Les dilatations, i.e. les composés d'une translation avec une homothétie.
5. L'application canonique $\pi \colon E \to E/S$ avec $S \subset V$ un sous-espace vectoriel.

Théorème 2.7. *Soient $f \colon E \to F$ et $g \colon F \to G$ affines.*

1. *Alors $g \circ f$ est affine et $\overrightarrow{g \circ f} = \overrightarrow{g} \circ \overrightarrow{f}$.*
2. *Soit f bijective, alors f^{-1} est affine; plus précisément $\overrightarrow{f}$ est bijective et $\overrightarrow{(f^{-1})} = (\overrightarrow{f})^{-1}$.*

Démonstration. Exercice. □

Corollaire 2.7.1. *Les affinités de E, i.e. les applications affines et bijectives de $E \to E$, forment un groupe par rapport à la composition d'applications, noté* $\mathrm{GA}(E)$.

Théorème 2.8. *La suite de morphismes*

$$1 \to V_+ \to \mathrm{GA}(E) \to \mathrm{GL}(V) \to 1,$$

où la deuxième et troisième application sont définies par $t \mapsto T_t$ et $F \mapsto \overrightarrow{f}$ respectivement, est exacte.

Démonstration. Il est clair que $t \mapsto T_t$ est injectif, et nous avons déjà montré que $f \mapsto \overrightarrow{f}$ est surjectif. Nous avons également déjà montré que $\overrightarrow{T_t} = 1$. Donc il reste à montrer que $\overrightarrow{f} = 1$ implique $f = T_t$ pou un t. Pour cela on pose $t = \overrightarrow{o\, f(o)}$. Alors on calcule

$$f(p) = f(o + \overrightarrow{op}) = f(o) + \overrightarrow{op} = o + \overrightarrow{o\, f(o)} + \overrightarrow{op} = p + t.$$

□

Théorème 2.9. *Pour tout $o \in E$ fixé, l'application*

$$V_+ \rtimes \mathrm{GL}(V) \to \mathrm{GA}(E), \quad (t, F) \mapsto T_t \circ F_o$$

est un isomorphisme de groupe. Ici le produit semi-direct est par rapport à l'action naturelle de $\mathrm{GL}(V)$ sur V, (i.e. la multiplication dans $V_+ \rtimes \mathrm{GL}(V)$ est donnée par $(t, F)(t', F') = (t + F(t'), F \circ F')$.)

Démonstration. Excellente exercice. □

2.2 Sous-espaces affines et dimension

Définition. Une partie non-vide A de E est dite sous-espace affine de E si il existe un sous-espace vectoriel S de V et un $p \in A$ tel que

$$A = p + S.$$

Exemple. Un sous-ensemble ne contenant qu'un seul point et E lui-même sont des sous-espaces de E.

Théorème 2.10. *Avec les notations comme dans la définition on a pour tout $q \in A$ l'identité $A = q + S$. En particulier, A est un espace affine sous l'action de S induite par l'action de V sur E.*

Démonstration. Exercice. □

Remarque. Le sous-espace S est donc uniquement déterminé par A : en effet,

$$S = \{\overrightarrow{pq} : p, q \in A\}.$$

Il est noté $\overrightarrow{A}$ et appelé direction de A.

Remarque. L'ensemble des sous-espace affines de E avec direction S donnée n'est rien d'autres que l'ensemble E/S des orbites de E sous l'action de S. Donc, l'ensemble des sous-espaces affines avec direction S porte une structure naturelle d'un espace affine.

Théorème 2.11. *Soient A_i ($i \in I$ = un ensemble d'indices) des sous-espaces affine de E. Si*

$$A := \bigcap_{i \in I} A_i \neq \emptyset,$$

alors A est un sous-espace affine avec direction

$$\overrightarrow{A} = \bigcap_{i \in I} \overrightarrow{A_i}$$

Démonstration. Exercice. □

Définition. Pour une partie $X \subset E$ le sous-espace affine engendré par X est défini comme

$$(X) = \bigcap_{X \subset A} A,$$

où A parcourt les sous-espaces affine de E contenant X.

Remarque. D'après la proposition précédente (X) est un sous-espace affine de E.

Exercice. Montrer que l'on a

$$(p_0\, p_1 \ldots p_n) = p_0 + \sum_{j=1}^{n} K \cdot \overrightarrow{p_0 p_j}.$$

Définition. Pour un sous-espace affine on pose $\dim A = \dim \overrightarrow{A}$. Un (sous-)espace affine A est dit droite si $\dim A = 1$, plan si $\dim A = 2$, et hyperplan dans E si $\dim A = \dim E - 1$.

Exemple. On a

$$\dim(p_0 p_1 \ldots p_n) \leq n.$$

Définition. On dit que $p_0, p_1, \ldots, p_n \in E$ sont en position générales (ou affinement indépendants) si $\dim(p_0\ p_1 \ldots p_n) = n$. Ils sont appelés alignés si $\dim(p_0\ p_1 \ldots p_n) \leq 2$.

Théorème 2.12. *Soient $p_0, p_1, \ldots, p_n \in E$. Les propriétés suivantes sont équivalentes :*

1. *$p_0, p_1, \ldots, p_n$ sont en position générale.*
2. *Pour tout p_i on a $p_i \notin (p_0\, p_1 \ldots p_{i-1}, p_{i+1}, \ldots\, p_n)$.*
3. *$\overrightarrow{p_0p_1}, \overrightarrow{p_0p_1}, \ldots, \overrightarrow{p_0p_n}$ sont linéairement indépendants.*

Démonstration. Il est évident que 1 entraîne 2 et 3 entraîne 1. Il reste à monter que non 3 implique non 2. Donc, supposons que les vecteurs $\overrightarrow{p_0p_j}$ sont dépendants, disons

$$\overrightarrow{p_0p_{j_0}} = \sum_{j \neq j_0} \lambda_j \overrightarrow{p_0p_j}.$$

Alors

$$p_{j_0} = p_0 + \sum_{j \neq j_0} \lambda_j \overrightarrow{p_0p_j},$$

et donc $p_{j_0} \in (p_0, \ldots, p_{j_0-1}, p_{j_0-1}, \ldots, p_n)$. □

Théorème 2.13. *Soit* $\dim E = n$.

1. *Tout système de $r > n+1$ points de E est affinement dépendent (i.e. pas en position générale).*
2. *Il existe $n+1$ points qui sont en position générales.*

Démonstration. Exercice. □

Théorème 2.14. *Soient $A \subseteq B \subseteq E$ des sous-espaces affines. Alors on a* $\dim A \leq \dim B$ *avec égalité si et seulement si $A = B$.*

Démonstration. Evident. □

Théorème 2.15. *Soient A, B sous-espaces affines de E, $A \cap B \neq \emptyset$. Alors on a*

$$\dim A \cap B = \dim A + \dim B - \dim\big(\overrightarrow{A} + \overrightarrow{B}\big).$$

En particulier $\dim A \cap B \leq \min(\dim A, \dim B)$.

Démonstration. Car

$$\dim \overrightarrow{A} \cap \overrightarrow{B} = \dim \overrightarrow{A} + \dim \overrightarrow{B} - \dim\big(\overrightarrow{A} + \overrightarrow{B}\big).$$

□

Théorème 2.16. *Soit E un espace affine de dimension finie n. Alors tout sous-espace affine de E de dimension k est intersection de $n-k$ hyperplans.*

Démonstration. Soit $a_1, \ldots, a_k$ une base de $\overrightarrow{A}$. Compléter avec des vecteurs $b_1, \ldots, b_{n-k}$ à une base de V. Pour $1 \leq i \leq n-k$ poser

$$H_i := p + \overrightarrow{A} + \sum_{\substack{=1 \\ j \neq i}}^{n-k} K \cdot b_j.$$

Alors $A = \cap_i H_i$. □

Théorème 2.17. *Soit $f\colon E \to F$ affine. Alors on a*

1. *Si $A \subset E$ et $B \subset F$ sont des sous-espaces affines, alors $f(A)$ et $f^{-1}(B)$, si non-vide, sont également des sous-espaces affine. avec direction $\overrightarrow{f}(\overrightarrow{A})$ et $\overrightarrow{f}^{-1}(\overrightarrow{B})$ respectivement.*

2. *En particulier, si $q = f(p)$, alors $f^{-1}(q) = p + \ker(\overrightarrow{f})$ et $\dim f(E) + \dim f^{-1}(q) = \dim E$.*

Démonstration. Exercice. □

2.3 Parallélisme

Définition. Soient $A, B \subset E$ des sous-espaces affines. Alors on dit :

A est faiblement parallèle à B (noté $A \triangle B$) si $\overrightarrow{A} \subseteq \overrightarrow{B}$.

A parallèle à B (noté $A \| B$) si $\overrightarrow{A} = \overrightarrow{B}$.

Remarque. Soient $A, B \subset E$ sous-espaces affines.

1. Si $A \triangle B$, alors on a soit $A \cap B = \emptyset$, soit $A \subset B$.

2. Si $A \| B$, alors on a soit $A \cap B = \emptyset$, soit $A = B$.

Théorème 2.18. *Soient $A, B \subset E$ des sous-espaces affines tels que $\overrightarrow{A} + \overrightarrow{B} = \overrightarrow{E}$. Alors $A \cap B \neq \emptyset$.*

Démonstration. En effet, soit $a \in A$ et $b \in B$. D'après l'hypothèse on a $\overrightarrow{ab} = v + w$ avec $v \in \overrightarrow{A}$ et $w \in \overrightarrow{B}$. Donc $a + v = b - w$ (car $b = a + \overrightarrow{ab} = a + v + w$), et $a + v \in A$ et $b - w \in B$. □

Corollaire 2.18.1. *Soit A un sous-espace affine et H un hyperplan de E tel que A n'est pas faiblement parallèle à H. Alors $A \cap H \neq \emptyset$ et* $\dim A \cap H = \dim A - 1$.

Exemple. Pour assurer que $A \cap B \neq \emptyset$, il ne suffit pas que $\dim A + \dim B \geq n$. Contre-exemple : $A = \{(*, *, *, 0, 1)\}$ et $B = \{(*, *, 0, *, 0)\}$ dans $E = K^5$. Or $\dim A + \dim B > 5$ (et A, B ne sont faiblement parallèles), mais $A \cap B = \emptyset$.

Théorème 2.19. *Soit A un sous-espace affine de E et S un sous-espace vectoriel de $\overrightarrow{E}$, tel que*

$$\overrightarrow{A} \oplus S = \overrightarrow{E}.$$

Alors pour tout $p \in E$ l'intersection $(p + S) \cap A$ contient exactement un seul point, appelé la projection de p sur A parallèle à S.

Démonstration. D'après le théorème $B := A \cap (p + S)$ n'est pas vide. Pour la dimension on trouve $\dim B \dim A + \dim(p + S) - \dim(\overrightarrow{A} + S) = 0$. □

Dans la situation décrite par le théorème on pose

$$\pi = \pi_{A,S} : E \to E,\ \pi(p) = \text{point d'intersection de } A \text{ et } p + S.$$

Théorème 2.20. *$\pi = \pi_{A,S}$ est une application affine. On a $\pi^2 = \pi$, et $\overrightarrow{\pi}_{A,S} = P_{\overrightarrow{A},S}$, où $P_{\overrightarrow{A},S}$ est la projection $\overrightarrow{E} \to \overrightarrow{A}$ par rapport à la décomposition $\overrightarrow{E} = \overrightarrow{A} \oplus S$.*

Démonstration. Exercice. □

Théorème 2.21. *Soit $\pi \colon E \to E$ affine, on suppose $\pi^2 = \pi$. Alors $\pi = \pi_{A,S}$ avec convenables A, S.*

Démonstration. On pose $A = \pi(E)$, donc $\overrightarrow{A} = \overrightarrow{\pi}(V)$, $\phi = \overrightarrow{\pi}$ et $S := \ker \phi$. On a $V = \overrightarrow{A} \oplus S$. En effet, $v = \phi(v) + (1 - \phi)(v)$ pour tout $v \in V$ et $(1 - \phi)(v) \in S$ car $\phi^2 = \phi$. En plus, si $w \in \overrightarrow{A} \cap S$, disons $w = \phi(v)$, alors $0 = \phi(w) = \phi^2(w) = \phi(w) = 0$.

Soit $q = \pi(p)$. Alors $q \in A$. D'autre part, $\pi(q) = \pi^2(p) = \pi(p)$, et donc $q \in p + S$. Donc $q \in A \cap (p + S)$. □

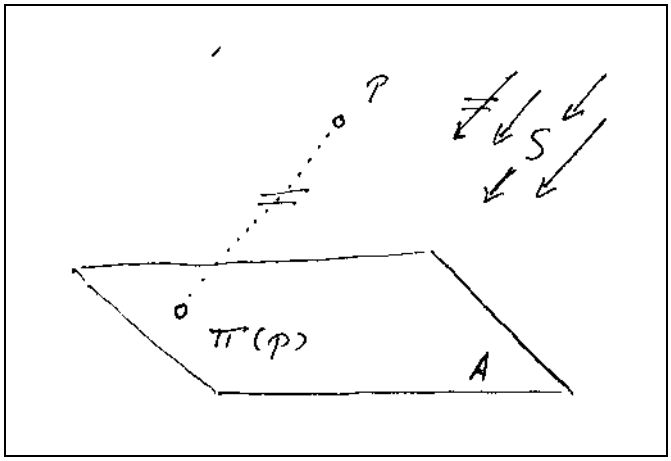


Figure 2.1: Projection sur A dans la direction S

Exercice. Pour $\lambda \in K$ soit

$$f_\lambda \colon E \to E,\ p \mapsto p + \lambda\overrightarrow{p\pi(p)}$$

($\pi = \pi_{A,S}$ comme ci-dessus). Montrer que f_λ est affine, que $\overrightarrow{f_\lambda} = (1-\lambda)\mathrm{id} + \lambda P_{\overrightarrow{A},S}$, est que f_λ est bijective si et seulement si $\lambda \neq 1$.

On appelle f_2 la symétrie par rapport à A parallèle à S.

Exercice. Soit $f : E \to E$ affine et $f^2 = \mathrm{id}$. Alors f est une symétrie.

2.4 Calcul barycentric

Si on fixe un $o \in R$ et vectorialise par rapport à o, alors l'expression

$$\sum_{i=0}^{k} \lambda_i p_i$$

a un sens comme somme de vecteurs, et sa valeur b est un point de E. En effet, selon la définition de la structure d'espace vectoriel sur E_o la somme peut être remplacé par

$$o + \sum_{i=0}^{k} \lambda_i \overrightarrow{op_i}.$$

En générale le point b dépend de o, sauf dans la situation décrite dans le

Théorème 2.22. *On suppose que* $\sum_{i=0}^{k} \lambda_i = 1$. *Alors le point*

$$b = o + \sum_{i=0}^{k} \lambda_i \overrightarrow{op_i}$$

ne dépend pas du choix de $o \in E$. *On l'appelle le barycentre des* p_i *par rapport aux masses* λ_i.

Démonstration. Soit $o' \in E$. Alors

$$o' + \sum_{i=0}^{k} \lambda_i \overrightarrow{o'p_i} = o' + \sum_{i=0}^{k} \lambda_i \big(\overrightarrow{o'o} + \overrightarrow{op_i}\big)$$
$$= o' + \overrightarrow{oo'}\big(\sum_{i=0}^{k} \lambda_i\big) + \sum_{i=0}^{k} \lambda_i \overrightarrow{o'p_i}\big) = o + \sum_{i=0}^{k} \lambda_i \overrightarrow{o'p_i}.$$

□

Remarque. Soit $b \in E$. Alors le point b du lemme est l'unique point de E tel que

$$\sum_{i=0}^{k} \lambda_i \overrightarrow{bp_i} = 0$$

(car, pour tout b, on a $\sum \lambda_i p_i = b + \sum \lambda_i \overrightarrow{bp_i}$). Comme déjà expliqué on l'écrit simplement comme

$$b = \sum_{i=0}^{k} \lambda_i p_i,$$

où la somme à droite doit être interprétée comme somme de vecteurs dans une vectorialisation de E par rapport à un point o quelconque.

Dans des livres on trouve parfois

$$\mathrm{baryc}(\{p_i\}_{i=0}^{k}; \{\lambda_i\}_{i=0}^{k})$$

ou des notations monstrueuses pareilles, évidemment comme renforcement de l'aspect pédagogique.

Le point b et appelé equibarycentre si $\lambda_0 = \cdots = \lambda_k = \frac{1}{k+1}$.

Définition. Soit E une droite, $p, q, r \in E$, $q \neq r$. Alors il existe un unique $\lambda \in K$ tel que

$$\overrightarrow{pq} = \lambda \overrightarrow{qr}.$$

On pose

$$R(p, q, r) = \lambda$$

et l'appelle le rapport de $\overrightarrow{pq}$ et $\overrightarrow{qr}$.

Remarque. Si $q = \alpha p + \beta r$ avec $\alpha + \beta = 1$, alors

$$R(p, q, r) = \frac{\beta}{\alpha} = \frac{1 - \alpha}{\alpha} = \frac{\beta}{1 - \beta}.$$

En effet, $q = \alpha p + \beta r$ entraîne $\overrightarrow{pq} = \beta pr$ et $\overrightarrow{rq} = \alpha \overrightarrow{rp}$.

Le rapport $R(p, q, r)$ est parfois noté suggestivement $\frac{\overrightarrow{pq}}{\overrightarrow{qr}}$

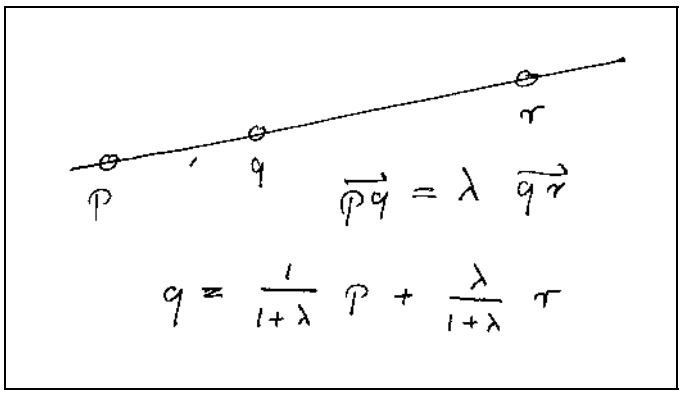


Figure 2.2: Le rapport de trois point alignés

Théorème 2.23. *Soient p_i et q_j des points de E et λ_i, μ_j des scalaires $(0 \leq i \leq p,\ 0 \leq j \leq q)$ tel que $\lambda = \sum_{i=0}^{p} \lambda_i \neq 0$, $\mu = \sum_{j=0}^{q} \mu_j \neq 0$, $\lambda + \mu = 1$. Alors le barycentre des p_i et q_j par rapport aux masses λ_i, μ_j est égal au barycentre $\lambda b_1 + \mu b_2$, où $b_1 = \sum_{i=0}^{p} \frac{\lambda_i}{\lambda} p_i$ et $b_2 = \sum_{j=0}^{q} \frac{\mu_j}{\mu} q_j$. Bref :*

$$\sum_i \lambda_i p_i + \sum_j \mu_j q_j = \lambda\Big(\sum_i \frac{\lambda_i}{\lambda} p_i\Big) + \mu\Big(\sum_j \frac{\mu_j}{\mu} q_j\Big).$$

Démonstration. Vectorialiser et lire l'identité comme une identité pour des vecteurs. □

Définition. Un ensemble $\{p_0, \ldots, p_i\} \subset E$ est dit n-simplex si les p_i sont en position générale. Un 2-simplex est aussi appelé triangle.

Théorème 2.24. *Soient* $1+1, 1+1+1 \neq 0$ *dans* K*, soit* $\{p, q, r\}$ *un triangle, et soit*

$$p' = \frac{1}{2}q + \frac{1}{2}r,\ q' = \frac{1}{2}p + \frac{1}{2}r,\ r' = \frac{1}{2}p + \frac{1}{2}q.$$

Alors les droites (pp')*,* (qq') *et* (rr') *se coupent en exactement un point* c*. Ce point est égal à* $c = \frac{1}{3}p + \frac{1}{3}q + \frac{1}{3}r$*.*

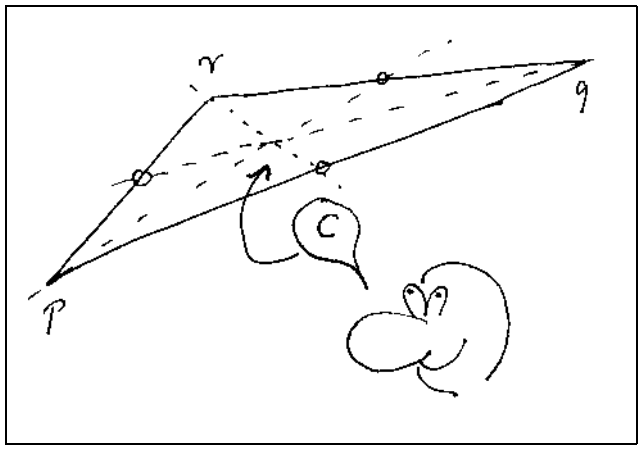


Figure 2.3: L'équibarycentre de trois points

Démonstration. Le point c est sur (pp') car

$$c = \frac{1}{3}p + \frac{2}{3}(\frac{1}{2}q + \frac{1}{2}r)$$

d'après le théorème précédent. Analogue on montre que c est sur les deux autres droites en question. Car (pp') et (qq') ne sont pas parallèles, leur intersection est de dimension 1. □

Exercice. Soit $\{p, q, r, s\}$ un parallélogramme (i.e. $(pq)\|(rs)$ et $(pr)\|(qs)$ et les quatre points sont deux à deux différents). Alors les diagonales (ps) et (qr) se coupent en exactement un point c. On a $c = \frac{1}{2}p + \frac{1}{2}s = \frac{1}{2}q + \frac{1}{2}r$.

Lemme. *Soient $p_0, \ldots, p_k \in E$ et $\lambda_1, \ldots, \lambda_k \in K$. Alors, pour tout $b \in E$ on a*

$$b = p_0 + \sum_{i=1}^{k} \lambda_i \overrightarrow{p_0 p_i}$$

si et seulement si

$$b = \big(1 - \sum_{i=1}^{k} \lambda_i\big) p_0 + \sum_{i=1}^{k} \lambda_i p_i.$$

Démonstration. Evident de la définition du barycentre. □

Théorème 2.25. *Soit A un sous-espace affine engendré par des points p_i $(0 \leq i \leq k)$. Alors $b \in A$ si et seulement si il existe λ_i avec $sum\lambda_i = 1$ tel que $b = \sum_{i=0}^{k} \lambda_i p_i$.*

Démonstration. Conséquence immédiat du lemme. □

Théorème 2.26. *Soient $p_0, \ldots, p_n \in E$ en position générale, λ_i, μ_i des scalaires tels que $\sum_{i=0}^{n} \lambda_i = \sum_{i=0}^{n} \mu_i = 1$. Alors*

$$\sum_{i=0}^{n} \lambda_i p_i = \sum_{i=0}^{n} \mu_i p_i$$

si et seulement si $\lambda_i = \mu_i$ pour tout i.

Démonstration. Encore une conséquence immédiat du lemme en utilisant que les vecteurs $\overrightarrow{p_0 p_1}, \ldots, \overrightarrow{p_0 p_n}$ sont linéairement indépendant. □

Définition. Soit $\dim E = n$. Un repère affine de E est un $(n+1)$-uplet $(p_0, p_1, \ldots, p_n)$ de points de E en position générale.

Remarque. La famille $(p_0, p_1, \ldots, p_n)$ est un repère affine de E si et seulement si $(p_0, \overrightarrow{p_0 p_1}, \ldots, \overrightarrow{p_0 p_n})$ est un repère cartésien.

Remarque. Soit $(p_0, p_1, \ldots, p_n)$ un repère affine de E. Alors tout $p \in E$ s'écrit uniquement sous la forme $b = \sum_{i=0}^{n} \lambda_i p_i$ avec des λ_i tels que $\sum \lambda_i = 1$. (Coordonnées affines).

$(p_0, p_1, \ldots, p_n)$ est un repère affine si et seulement si $(p_0, \overrightarrow{p_0p_1}, \ldots, \overrightarrow{p_0p_n})$ est un repère cartésien.

Théorème 2.27. *Soient $p_0, \ldots, p_n \in E$ en position générale. Supposons que pour $0 \leq j \leq n$*

$$q_j = \sum_{i=0}^{n} \lambda_{i,j} p_i, \quad (\sum_i \lambda_{i,j} = 1).$$

Alors les $q_0, \ldots, q_n$ sont en position générale si et seulement si le déterminant $\det(\lambda_{i,j})_{1 \leq i,j \leq n}$ est différent de 0.

Démonstration. Supposons que les q_j sont en position générale, i.e. que l'on a $\dim(q_0, \ldots, q_n) = n$. Car $(q_0, \ldots, q_n) \subseteq (p_0, \ldots, p_n)$ (d'après l'hypothèse) on a donc égalité. Il existe donc une matrice $\check{\Lambda}$ dont les colonnes ont somme égale à 1, telle que

$$(p_0, \ldots, p_n) = (q_0, \ldots, q_n)\check{\Lambda}.$$

En utilisant

$$(q_0, \ldots, q_n) = (p_0, \ldots, p_n)\Lambda$$

(avec $\Lambda := \big(\lambda_{i,j}\big)$) et l'unicité des coordonnées barycentriques on déduit

$$\Lambda\check{\Lambda} = 1,$$

et d'où $\det \Lambda \neq 0$.

La direction réciproque est laissé comme exercice. On utilise que les matrices inversibles telles que la somme des éléments dans chaque colonne est égal à 1 forment un sous-groupe de $\mathrm{GL}(n+1, K)$ (voir l'exercice ci-dessus) □

Exercice. Montrer que les matrices dans $\mathrm{GL}(n+1, K)$ dont la somme éléments dans chaque ligne est égale à 1 forment un sous-groupe. (Indication : c'est le stabilisateur d'un certain vecteur sous l'action naturelle sur $\mathbb{R}^{n+1}$). En déduire que les matrices de $\mathrm{GL}(n+1, K)$ avec sommes des colonnes égales à 1 forment également un sous-groupe.

Théorème 2.28. *Pour une application $f\colon E \to F$ les 2 propriétés suivantes sont équivalentes :*

1. *f est affine.*

2. Pour tous $p_0, \dots, p_k \in E$ et tous $\lambda_i \in K$ tels que $1 = \sum_i \lambda_i$ on a

$$f\big(\sum_i \lambda_i p_i\big) = \sum_i \lambda_i f(p_i).$$

Démonstration. Exercice. □

Corollaire 2.28.1. *Soient E, F des espaces affines, $\dim E = n$, et soit $(p_0, p_1, \dots, p_n)$ un repère affine de E, et $q_0, \dots, q_n$ des points de F. Alors il existe une et une seule application affine $f\colon E \to F$ telle que $f(p_i) = q_i$ pour tout $0 \le i \le n$.*

Démonstration. Clair d'après le théorème précédent. □

Remarque. Soit $(p_0, \dots, p_n)$ un repère affine de E. Alors d'après le théorème l'application

$$\Phi\colon \mathrm{A}(E, F) \to F^n, \quad \Phi(f) = (f(p_0), \dots, f(p_n))$$

est une bijection.

2.5 Trois célèbres théorèmes ou des mathématiques d'un monde perdu

Rappel : Pour trois points p, q, r, deux à deux différents, on a posé

$$R(p, q, r) = \frac{\beta}{\alpha}$$

où $q = \alpha p + \beta r$.

Lemme. *Soit f une application affine. Alors pour tous les trois points alignés et deux à deux différents p, q, r tel que $f(p), f(q), f(r)$ sont deux à deux différents, on a*

$$R(p, q, r) = R(f(p), f(q), f(r)).$$

Démonstration. L'identité $q = \alpha p + \beta r$ entraîne $f(q) = \alpha f(p) + \beta f(r)$. □

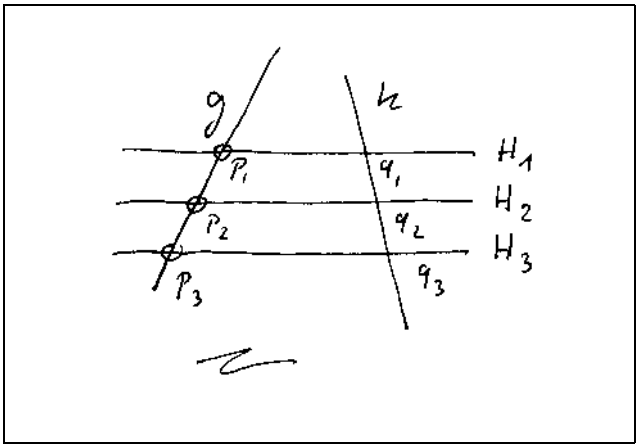


Figure 2.4: Le théorème de Thalès

Théorème 2.29. *(de Thalès : Thales de Milet, -625 – -547(?)) Soient H_1, H_2, H_3 trois hyperplans parallèles et distincts, soient g, h deux droites dont n'aucune est faiblement parallèle aux H_j. Soit $\{p_i\} = g \cap H_i$ et $\{q_i\} = h \cap H_i$. Alors*

$$R(p_1, p_2, p_3) = R(q_1, q_2, q_3)$$

Démonstration. Soit $\pi\colon E \to E/S$ la projection canonique, où $S = \overrightarrow{H_1}$. On a $\pi(p_i) = p_i + S = H_i = q_i + S = \pi(q_i)$, et donc, d'après le lemme précédent,

$$R(p_1, p_2, p_3) = R(H_1, H_2, H_3) = R(q_1, q_2, q_3).$$

Au lieu de π on peut considérer alternativement la projection π' sur h le long de S. Car $\pi'(p_i) = q_i$ le théorème est également une conséquence du lemme précédent. □

Théorème 2.30. *(Ménelaüs d'Alexandre : vivait vers 100 à Rome) Soit (p_0, p_1, p_2) un repère affine d'un plan E, soit $q_i \in (p_i p_{i+1})$, $q_i \neq p_i, p_{i+1}$ (où on pose $p_{n+1} := p_0$). Alors les q_i sont alignés si et seulement si*

$$\prod_{i=0}^{2} R(p_i, q_i, p_{i+1}) = \frac{\overrightarrow{p_0 q_0}}{\overrightarrow{q_0 p_1}} \cdot \frac{\overrightarrow{p_1 q_1}}{\overrightarrow{q_1 p_2}} \cdot \frac{\overrightarrow{p_2 q_2}}{\overrightarrow{q_2 p_0}} = -1.$$

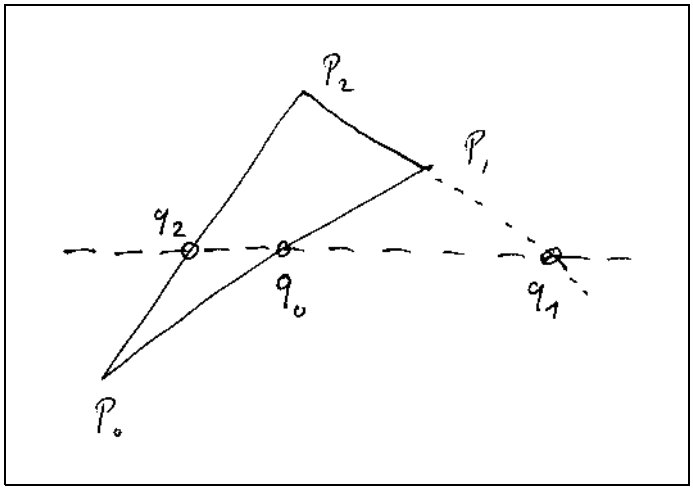


Figure 2.5: Le théorème de Ménelaüs

Démonstration. Les q_i sont alignés si et seulement si $\Delta = 0$, où Δ désigne le déterminant des coordonnées barycentriques des q_j par rapport au repère (p_0, p_1, p_2).

Soit $q_i = \alpha_i p_i + \beta_i p_{i+1}$ avec $\alpha_i + \beta_i = 1$ convenables. On trouve

$$\Delta = \begin{vmatrix} \alpha_0 & \beta_0 & 0 \\ 0 & \alpha_1 & \beta_1 \\ \beta_2 & 0 & \alpha_2 \end{vmatrix} = \alpha_0\alpha_1\alpha_2 + \beta_0\beta_1\beta_2.$$

Donc

$$\Delta = 0 \Longleftrightarrow \prod \frac{\beta_i}{\alpha_i} = -1$$

D'autre part, on a

$$R(p_i, q_i, p_{i+1}) = \frac{\beta_i}{\alpha_i},$$

et d'où le théorème. □

Théorème 2.31. *(Céva : Giovanni Ceva, 1647(?8) – 1743, né à Milan, frère du mathématicien et poète Tomasso Ceva) Mêmes données que dans Ménelaüs. Soit $D_i = (q_i p_{i'})$, où i' est l'indice tel que $i' \neq i, i+1$. Alors les D_i sont concourantes ou parallèles si et seulement si*

$$\prod_{i=0}^{2} R(p_i, q_i, p_{i+1}) = +1.$$

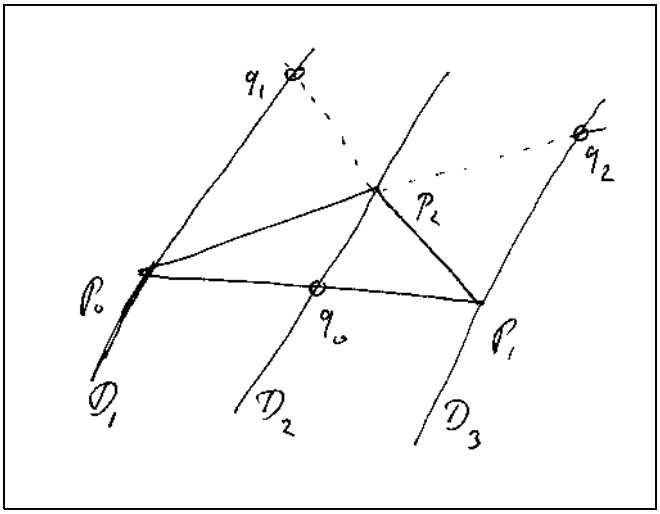


Figure 2.6: Le théorème de Ceva

Démonstration. Soit π_i projection sur (p_i, p_{i+1}) le long de $\overrightarrow{D_i}$. Donc $D_i = \pi_i^{-1}(q_i)$. En conséquence, pour tout $c \in E$ on a :

$$c \in A := \bigcap D_i \Longleftrightarrow \forall i \ \pi_i(c) = q_i.$$

Soit $q_i = \alpha_i p_i + \beta_i p_{i+1}$ et $c = \sum \lambda_i p_i$ avec $\sum \lambda_i = 1$. Alors, par un petit calcul (en utilisant $\pi_i(p_{i'}) = q_i$ et que π conserve les barycentre)

$$\begin{aligned}\pi_i(c) &= \lambda_i p_i + \lambda_{i+1} p_{i+1} + \lambda_{i'} q_i = \lambda_i p_i + \lambda_{i+1} p_{i+1} + (1 - \lambda_i - \lambda_{i+1}) q_i \\ &= \lambda_i p_i + \lambda_{i+1} p_{i+1} + (1 - \lambda_i - \lambda_{i+1})(\alpha_i p_i + \beta_i p_{i+1}) \\ &= [\beta_i \lambda_i - \alpha_i \lambda_{i+1} + \alpha_i] p_i + [\alpha_i \lambda_{i+1} - \beta_i \lambda_i + \beta_i] p_{i+1}.\end{aligned}$$

Donc l'existence d'un $c \in A$ se réduit à la question d'une solution $(\lambda_0, \lambda_1, \lambda_2)$ de $\beta_i \lambda_i - \alpha_i \lambda_{i+1} = 0$ $(0 \leq i \leq 2)$ avec $\sum \lambda_i = 1$.

Analogue on trouve que les trois droites D_i sont parallèles si et seulement si il existe un vecteur $v \neq 0$ tel que $\overrightarrow{\pi}_i(v) = 0$ pour tout i. (Le vecteur v sera la direction des D_i.) En écrivant $v = \sum \lambda_i \overrightarrow{op_i}$ avec un o n'importe lequel et $\sum \lambda_i = 0$ les équations $\overrightarrow{\pi}_i(v) = 0$ deviennent $\beta_i \lambda_i - \alpha_i \lambda_{i+1} = 0$ avec $\sum \lambda_i = 0$ (et $(\lambda_0, \lambda_1, \lambda_2) \neq 0$).

Donc les D_i sont concourantes ou parallèles si et seulement si le déterminant Δ de la matrice

$$\begin{pmatrix} \beta_0 & -\alpha_0 & 0 \\ 0 & \beta_1 & -\alpha_1 \\ -\alpha_2 & 0 & \beta_2 \end{pmatrix}$$

associée au système d'équation linéaire en question est 0. Mais $\Delta = \prod_i \beta_i - \prod_i \alpha_i$. Donc $\Delta \neq 0$ si et seulement si $\prod \beta_i/\alpha_i = +1$. Avec $\beta_i/\alpha_i = R(p_i, q_i, q_{i+1})$, on déduit le théorème. □

2.6 Exercices

1. Soit A un sous-ensemble de l'espace affine E sur le corps K qui satisfait à la propriété suivante : Si $p, q \in A$ alors $(pq) \subseteq A$. Montrer : Si $1 + 1 \neq 0$ dans K, alors A est un sous-espace affine.

2. Montrer que le A de l'exercice précédent est non nécessairement un sous-espace affine si $1 + 1 = 0$. (Considérer le plan affine sur $\mathbb{F}_2$.)

3. Soient p, q, r des points en position générales dans un plan affine E. Montrer que $\{f \in \mathrm{GA}(E) \mid f(\{p, q, r\}) = f(\{p, q, r\})\}$ est isomorphe à S_3.

4. Dans le notations de l'exercice précédent soit $s = \alpha p + \beta q + (1 - \alpha - \beta)r$ avec des scalaires α, β. Déterminer

$$H_{\alpha,\beta} := \{\{f \in \mathrm{GA}(E) \mid f(\{p, q, r, s\}) = f(\{p, q, r, s\}\}$$

en fonction de α, β. (Cet exercice montre comment les groupes mesurent des symétries.)

Chapitre 3

Espaces vectoriels euclidiens et groupes orthogonaux

3.1 Notions de base

Définition. Un espace vectoriels euclidien est un couple $(V, (\ ,\ ))$ où

V est un espace vectoriel sur $\mathbb{R}$ de dimension finie.

$(\ ,\ )$ est un produit scalaire défini positif sur V.

Remarque. Un produit scalaire est une application $V \times V \to V$ qui est bilinéaire et symétrique. Il est défini positif si $(x, x) > 0$ pour tout $0 \neq x \in V$.

Exemple. Des exemples de base sont :

1. $\mathbb{R}^n$ et $(x, y) = x^t \cdot y = \sum_{i=1}^n x_i y_i$ ($x = (x_1, \ldots, x_n)^t$, $y = (y_1, \ldots, y_n)^t$).
2. $\mathbb{C}$ et $(x, y) = \mathrm{Re}(x\overline{y})$.
3. $\mathbb{H}$ = quaternions de Hamilton et $(x, y) = \frac{1}{2}(x\overline{y} + \overline{x}y)$ ($\overline{x} = x_0 - x_1 I - x_2 J - x_3 K$ si $x = x_0 + x_1 I + x_2 J + x_3 K$).
4. L'espace P_k des polynômes de degré $\leq k$ à coefficients réels et $(p, q) = \int_0^1 p(x)q(x)\,dx$.

Théorème 3.1. *Le produit scalaire $(\ ,\ )$ d'un espace vectoriel euclidien est non-dégénéré, i.e. $(x, V) = 0$ seulement pour $x = 0$ et $(V, y) = 0$ seulement pour $y = 0$.*

Démonstration. Si $(x, V) = 0$, alors $(x, x) = 0$, donc $x = 0$. □

Remarque. L'espace vectoriel dual de V, noté V^* est l'espace des applications linéaires $V \to \mathbb{R}$. On a $\dim V^* = \dim V$. L'application

$$(x, \cdot)\colon V \to \mathbb{R}, \quad y \mapsto (x, y)$$

est un élément de V^*. Le théorème précédent est équivalent à dire que l'application

$$V \to V^*, \quad x \mapsto (\cdot, x)$$

est un isomorphisme d'espaces vectoriels.

Pour $x \in V$ on pose $|x| = \sqrt{(x, x)}$ (longueur ou valeur absolue de x).

Remarque. La formule de clef pour la longueur des vecteurs est : $|x + y|^2 = |x|^2 + 2(x, y) + |y|^2$.

Théorème 3.2. *$V \to \mathbb{R}$, $x \mapsto |x|$ est une norme sur V, i.e.*

1. *$|x| \geq 0$, et $|x| = 0$ si et seulement si $x = 0$.*
2. *$|\lambda x| = |\lambda| \cdot |x|$.*
3. *Inégalité de triangle : $|x + y| \leq |x| + |y|$.*

Pour la démonstration on utilise

Théorème 3.3. *(Inégalité de Cauchy-Schwartz) Pour tout $x, y \in V$ on a*

$$|(x, y)| \leq |x| \cdot |y|,$$

avec égalité si et seulement si x, y sont linéairement dépendants.

Démonstration. Si x, y sont linéairement dépendants, alors pour tout $t \in \mathbb{R}$ on a

$$f(t) := |x + ty| = t^2|y|^2 + 2t(x, y) + |x|^2 > 0,$$

i.e. le polynôme quadratique $f(t)$ n'a pas de racines réelles. Donc son discriminant D est < 0. Or

$$D = 4(x, y)^2 - 4|x|^2 \cdot |y|^2,$$

et d'où le théorème. □

Démonstration de théorème 3.2. D'après Cauchy-Schwartz :

$$|x+y|^2 = |x|^2 + 2(x,y) + |y|^2 \leq |x|^2 + 2|x||y| + |y|^2 = (|x| + |y|)^2.$$

□

Remarque. $d(x,y) := |x-y|$ définit une métrique sur V, i.e. $d(x,y) \geq 0$, $d(x,y) = d(y,x)$, $d(x,y) = 0$ si et seulement si $x = y$, et $d(x,y) \leq d(x,z) + d(z,y)$.

Définition. La matrice de Gram associée à une base a_i est

$$G(a_1, \ldots, a_n) := \big((a_i, a_j)\big)_{1 \leq i,j \leq n}.$$

Exercice. On a

$$(x,y) = (x_1, \ldots, x_n) G(y_1, \ldots, y_n)^t = \sum_{i,j} x_i (a_i, a_j) y_j$$

$$(x = \sum x_i a_i, y = \sum_j y_j a_j).$$

Définition. On dit qu'un vecteur x est orthogonal à un vecteur y, noté $x \perp y$, si $(x,y) = 0$. Pour des sous-espace Set T de V on écrit $x \perp S$ si $x \perp y$ pour tout $y \in S$, et $S \perp T$ si $x \perp y$ pour tout $x \in S$ et $y \in T$. Une base orthonormale de V (base ON) est une base $e_1, \ldots, e_n$ de V telle que

$$(e_i, e_j) = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}$$

pour tout i, j.

Remarque. On vérifie facilement

1. Si les vecteurs $a_1, \ldots, a_k$ sont deux à deux orthogonaux et $\neq 0$, alors ils sont linéairement indépendants.
2. Si $x \perp y$, alors $|x+y|^2 = |x|^2 + |y|^2$.
3. Pour une base ON $e_1, \ldots, e_n$ on a
   (a) $G(e_1, \ldots, e_n) = 1$,

(b) $x = \sum_{i=1}^{n}(x, e_i)e_i$.
(c) $|x|^2 = \sum_{i=1}^{n}(x, e_i)^2$ (Identité de Parceval).

Théorème 3.4. *(Orthonormalisation à la Schmidt) Soit $a_1, \ldots, a_n$ une base de V. Alors il existe une unique base orthonormale $e_1, \ldots, e_n$ telle que*

$$\langle a_1, \ldots, a_k \rangle = \langle e_1, \ldots, e_k \rangle$$

pour tout $1 \leq k \leq n$. Ici $\langle a_1, \ldots, a_k \rangle$ indique le sous-espace engendré par $a_1, \ldots, a_n$).

Démonstration. On pose

$$e_1 = a_1/|a_1|$$

$$e_{k+1} = e'_{k+1}/|e'_{k+1}|,\ e'_{k+1} = a_{k+1} - \sum_{j=0}^{k}(a_{k+1}, e_j)e_j \quad (k \geq 0).$$

L'unicité de la base e_i est laissé comme exercice. □

Corollaire 3.4.1. *Tout espace euclidien possède une base ON.*

Définition. Une somme de sous-espaces $S_1 \ldots, S_p$ est orthogonale, notée

$$S_1 \widehat{\oplus} S_2 \widehat{\oplus} \cdots \widehat{\oplus} S_p,$$

si $S_i \perp S_j$ pour $i \neq j$.

Théorème 3.5. *Une somme orthogonale est directe, i.e. $\sum_{j=0}^{p} s_j = 0$, $s_j \in S_j$ entraîne $s_j = 0$ pour tout j.*

Démonstration. Exercice. □

Définition. Le complément orthogonal d'un sous-espace $S \subset V$ est

$$S^{\perp} = \{y \in V \mid (y, S) = 0\}.$$

Remarque. $S^{\perp}$ est un sous-espace.

Théorème 3.6. $V = S \oplus S^{\perp}$.

Démonstration. Soit $x \in V$. Car $S \to S^*$, $s \mapsto (\cdot, s)$ est un isomorphisme, il existe donc un $s \in S$ tel que $(t, x) = (x, s)$ pour tout $t \in S$, i.e. tel que $s^{\perp} := x - s \in S^{\perp}$. □

Définition. Soit $S \subset V$ un sous-espace. La projection orthogonale sur S, notée P_S, est l'application linéaire

$$P_S \colon V \to V, \quad x \mapsto s, \qquad (x = s + s^\perp,\ s \in S,\ s^\perp \in S^\perp).$$

Remarque. Soit $e_1, \ldots, e_p$ une base orthonormale de S, alors

$$P_S(x) = \sum_{j=1}^{p} (x, e_j) e_j$$

pour tout $x \in V$. En effet, $e_k \perp x - \sum_{j=1}^{p} (x, e_j) e_j$ pour tout k.

Définition. (Distance de x à S) Pour un sous-espace S de V et un $x \in V$ on pose

$$d(x, S) = \inf_{y \in S} |x - y|.$$

Théorème 3.7. *Il existe un et un seul $y_0 \in S$ tel que $d(x, S) = |x - y_0|$. On a $y_0 = P_S(x)$.*

Remarque. Si $e_1, \ldots, e_p$ est une base orthonormale de $S^\perp$, on a donc la formule

$$d(x, S) = \big(|x|^2 - \sum_{j=1}^{p} (x, e_j)^2\big)^{1/2}.$$

Démonstration. Soit $x = s + s^\perp$. Pour $y \in S$ on a

$$|x - y|^2 = |s - y|^2 + |s^\perp|^2.$$

Cette expression est minimale pour $y = s$. □

Définition. Une isométrie de deux espaces euclidiens V et W est un isomorphisme d'espaces vectoriels $f \colon V \to W$ tel que

$$\forall x \in V : |f(x)| = |x|.$$

Exercice. Montrer :

1. Pour une isométrie f on a

$$(f(x), f(y)) = \frac{1}{2}(|f(x) - f(y)|^2 - |f(x)|^2 - |f(y)|^2)$$
$$= \frac{1}{2}(|x - y)|^2 - |x|^2 - |y|^2) = (x, y).$$

2. f isométrie, alors f^{-1} isométrie.

3. Soit $f\colon V \to W$ linéaire et $|f(x)| = |x|$ pour tout $x \in V$. Alors f est injectif. (En particulier, l'existence d'une telle application entraîne $\dim V \leq \dim W$.)

4. $\mathbb{R}^m$ est isométrique à $\mathbb{R}^n$ si et seulement si $m = n$.

5. Soit $h\colon V \to W$ une application ensembliste entre des espaces vectoriels euclidiens V et W telle que $(f(x), f(y))_W = (x, y)_V$ pour tout $x, y \in V$. Alors f est linéaire.

Théorème 3.8. *Tout espace euclidien de dimension n est isométrique à $\mathbb{R}^n$.*

Démonstration. Soit $e_1, \ldots, e_n$ une base ON de V. L'application $\mathbb{R}^n \to V$, $(x_1, \ldots, x_n)^t \mapsto \sum x_j e_j$ est une isométrie. □

Définition. L'ensemble

$$\mathrm{O}(V) = \{g\colon V \to V \mid g \text{ linéaire}, \forall x, y \in V\colon (g(x), g(y)) = (x, y)\}$$

est appelé le groupe orthogonal de V, ses éléments les isométries de V. On pose

$$\mathrm{SO}(V) = \{g \in \mathrm{O}(V) \mid \det(g) = +1\}.$$

Les éléments de $\mathrm{SO}(V)$ sont appelés les rotations de V.

Remarque. Let déterminant $\det(g)$ est définie comme déterminant de la matrice de g sur une base n'importe laquelle. Cette définition ne dépend de la base choisie.

Théorème 3.9. $\mathrm{O}(V)$ *et* $\mathrm{SO}(V)$ *sont des sous-groupes de* $\mathrm{GL}(V)$.

Démonstration. Clair. □

Théorème 3.10. *On a* $\det(g) = \pm 1$ *pour tout* $g \in \mathrm{O}(V)$. *Le groupe* $\mathrm{SO}(V)$ *est distingué dans* $\mathrm{O}(V)$ *d'indice 2.*

Démonstration. On va montrer plus tard que $\det(g) = \pm 1$ (voir la section ci-dessous). Or l'application $\mathrm{O}(V) \to \{\pm 1\}$, $g \mapsto \det(g)$ et un morphisme de groupe avec noyau $\mathrm{SO}(V)$. Il est surjectif : soit $e_1, \ldots, e_n$ une base ON de V, alors l'application linéaire g telle que $g(e_1) = -e_1$ et $g(e_j) = e_j$ $(2 \leq j \leq n)$ est une isométrie à déterminant -1. D'après le théorème de factorisation on conclut $\mathrm{O}(V)/SO(V) \approx \{\pm 1\}$. □

Remarque. Dans ce qui suit on utilise souvent les propriétés suivantes d'un $g \in \mathrm{O}(V)$:

1. Soit S un sous-espace de V qui est invariant sous g. Alors $g(S^\perp) = S^\perp$ et $g|_S \in \mathrm{O}(S)$.

2. $\mathrm{Fix}(g) := \{x \in V \mid g(x) = x\}$ est un sous-espace vectoriel de V.

3.2 Description géométrique de $\mathrm{O}(V)$

Définition. Pour un sous-espace vectoriel U de V la symétrie par rapport à U est l'application linéaire $\sigma_U : V \to V$ telle que

$$\sigma_U(x) = \begin{cases} x & \text{pour } x \in U \\ -x & \text{pour } x \perp U \end{cases}.$$

Une symétrie hyperplane est une application σ_U avec $\operatorname{codim} U = 1$.

Une symétrie g est dite renversement ou, dans le cas $\dim V = 3$, aussi retournement ou demi-tour, si $\operatorname{codim} \mathrm{Fix}(g) = 2$.

Exercice. Montrer :

1. Pour tout U on a $\sigma_U \in \mathrm{O}(V)$, $\sigma_U^2 = 1$ et $\det(\sigma_U) = (-1)^q$ où $q = \operatorname{codim} U$. En particulier, $\det(g) = -1$ pour une symétrie hyperplane g.

2. Soit $\operatorname{codim} U = 1$ et $a \perp H$, $a \neq 0$, alors $\sigma_U(x) = x - 2\frac{(x,a)}{(a,a)}a$.

3. Si $g \in O(V)$ et $\operatorname{codim} \mathrm{Fix}(g) = 1$, alors g est une symétrie hyperplane.

Théorème 3.11. *Soit $g \in \mathrm{O}(V)$, $g \neq 1$ et $g^2 = 1$. Alors g est une symétrie (i.e. $g = \sigma_U$ pour un sous-espace U convenable).*

Démonstration. Soit $U = \{x \,|\, g(x) = x\}$. A montrer : Si $x \perp U$, alors $g(x) = -x$.

Pour tout x on a $x = x_+ + x_-$, où $x_\pm = \frac{1}{2}(x \pm g(x))$. On a $x_+ \in U$ et $g(x_-) = -x_-$. La dernière identité entraîne $x_- \perp U$: en effet, en utilisant $g^2 = 1$, pour tout $y \in U = \mathrm{Fix}(g)$ on trouve $(x_-, y) = (x_-, g(y)) = (g^{-1}(x_-), y) = -(x_-, y)$, d'où $(x_-, y) = 0$.

Donc, si $x \perp U$, alors $x = x_-$ et puis $g(x) = -x$. □

Théorème 3.12. *(***Représentation géométrique***) Le groupe $\mathrm{O}(V)$ est engendré par les symétries hyperplanes. Plus précisément, soit $g \in \mathrm{O}(V)$ et $q = \operatorname{codim} \mathrm{Fix}(g)$. Alors il existe q symétries hyperplanes σ_j telles que*

$$g = \sigma_1 \cdots \sigma_q.$$

Remarque. La décomposition $g = \sigma_1 \cdots \sigma_q$ n'est pas unique (on peut par exemple trivialement prolonger en joignant des carrés de symétries). Par contre, si $g = \tau_1 \cdots \tau_s$ avec des symétries hyperplanes τ_j, alors la parité de s est unique (car $(-1)^q = \det(g)$), et $s \geq q$. En effet, si $\tau_j = \sigma_{H_j}$, alors $U := H_1 \cap \cdots \cap H_s \subseteq \mathrm{Fix}(g)$, donc $n - s \leq \dim U \leq \dim \mathrm{Fix}(g) = n - q$.

Démonstration. On fait une récurrence sur $\dim V$. Soit $U := \mathrm{Fix}(g)$ et $W := U^\perp$.

Cas 1 : $\dim U > 0$**.** On considère $g|_W \in \mathrm{O}(W)$. D'après l'hypothèse de récurrence et avec $q = \operatorname{codim} \mathrm{Fix}(g|_W)$ on a $g|_W = \sigma_1 \cdots \sigma_q$ avec des symétries hyperplanes de W. On peut prolonger σ_j à une symétrie hyperplane $\widetilde{\sigma}_j$ de V en posant

$$\widetilde{\sigma}_j(x) = \begin{cases} \sigma_j(x) & \text{si } x \in W = U^\perp \\ x & \text{si } x \in U \end{cases}.$$

Evidemment on a $g = \widetilde{\sigma}_1 \cdots \widetilde{\sigma}_q$.

Cas 2 : $\dim U = 0$**.** Fixons un $x \in V, x \neq 0$ et posons $y = g(x)$. On a $x \neq y$, mais $|x| = |y|$, et donc $x - y \perp x + y$. Soit $H = \langle x - y \rangle^\perp$. On a

$$\sigma_H(x) = \sigma_H[\frac{1}{2}(x - y) + \frac{1}{2}(x + y)] = -\frac{1}{2}(x - y) + \frac{1}{2}(x + y) = y.$$

Donc $x \in \mathrm{Fix}(\sigma_H^{-1} g)$, d'où $\dim \mathrm{Fix}(\sigma_H^{-1} g) > 0$. D'après cas 1 on a $\sigma_H^{-1} g = \sigma_1 \cdots \sigma_r$ avec des symétries hyperplanes σ_j convenables, où r est la codimension de $\mathrm{Fix}(\sigma_H^{-1} g)$. Mais

$$0 = \mathrm{Fix}(g) \supseteq \mathrm{Fix}(\sigma_H^{-1} g) \cap \mathrm{Fix}(\sigma_H),$$

donc $\dim \mathrm{Fix}(\sigma_H^{-1}) = 1$ (exercice), i.e. $r = n - 1$. □

Corollaire 3.12.1. $\det(g) = \pm 1$ *pour toute isométrie* g.

3.3 Description matricielle de $\mathrm{O}(V)$

On sait que toute endomorphisme de $V = \mathbb{R}^n$ est de la forme $x \mapsto Ax$ avec une matrice $A \in \mathbb{R}^{n \times n}$ (l'ensemble des matrices carrées avec n lignes et n colonnes).

Définition. On pose

$$\mathrm{O}(n) := \{A \in \mathbb{R}^{n \times n} \mid (Ax)^t (Ay) = x^t y\}$$
$$\mathrm{SO}(n) := \{A \in \mathrm{O}(n) \mid \det(A) = +1\}.$$

Théorème 3.13. $\mathrm{O}(n)$ *et* $\mathrm{SO}(n)$ *sont des sous-groupes de* $\mathrm{GL}(n, \mathbb{R})$. *On a*

$$\mathrm{O}(n) = \{A \in \mathbb{R}^{n \times n} \mid A^t A = 1_n\}.$$

Démonstration. Exercice. □

Remarque. On vérifie facilement :

1. Soient $c_1, \ldots c_n$ les colonnes d'une matrice $A \in \mathbb{R}^{n \times n}$. Alors $A \in \mathrm{O}(n)$ si et seulement si $c_1, \ldots, c_n$ est une base orthonormale de $\mathbb{R}^n$.

2. Soit $A \in \mathrm{GL}(n, \mathbb{R})$: on a $A \in \mathrm{O}(n)$ si et seulement si $A^{-1} = A^t$.

3. Pour tout $A \in \mathrm{O}(n)$ on a $\det(A) = \pm 1$.

Théorème 3.14. *Soit* $e_1, \cdots e_n$ *une base orthogonale de* V. *Pour* $g \in \mathrm{O}(V)$ *on désigne par* $M(g)$ *la matrice de* g *par rapport à* $e_1, \ldots, e_n$. *Alors l'application* $g \to M(g)$ *définit un isomorphisme de groupes* $\mathrm{O}(V) \to \mathrm{O}(n)$.

Démonstration. Soit $L : V \to \mathbb{R}^n$ la isométrie $L(x) = \big((x, e_1), \ldots, (x, e_n)\big)^t$. On a $L(g(x)) = M(g)L(x)$.

Pour montrer $M(g) \in \mathrm{O}(n)$ on observe

$$L(x)^t L(y) = (x, y) = (g(x), g(y)) = \big(M(g)L(x)\big)^t \big(M(g)L(y)\big) = L(x)^t \big(M(g)^t M(g)\big) L(y).$$

Car $L(x)$ et $L(y)$ parcourent tous les vecteurs de $\mathbb{R}^n$ on en déduit l'identité $M(g)^t M(g) = 1$.

L'application $g \mapsto M(g)$ est surjective : si $A \in \mathrm{O}(n)$, alors $A = M(g)$ où $g(x) := AL(x)$.

Que l'application $g \mapsto M(g)$ est injective et un morphisme de groupes est bien connu. □

En utilisant remarque 1. ci-dessus on vérifie les deux théorèmes suivants :

Théorème 3.15. $\mathrm{O}(1) = \{\pm 1\}$.

Théorème 3.16. $\mathrm{SO}(2) = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a^2 + b^2 = 1\}$.

Et donc on a aussi $\mathrm{O}(2) \setminus \mathrm{SO}(2) = \mathrm{SO}(2) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \{\begin{pmatrix} a & -b \\ b & -a \end{pmatrix} \mid a^2 + b^2 = 1\}$.

Remarque. Un élément de SO(2) (comme dans le théorème) donne la base canonique $(0, 1)^t, (1, 0)^t$ de $\mathbb{R}^2$ sur $(a, b)^t$ et $(-b, a)^t$ respectivement. Donc pour tout vecteur $x \in \mathbb{R}^2$ on obtient Ax en faisant une rotation de x par l'angle entre $(0, 1)^t$ et $(a, b)^t$.

Lemme. *Soit X un espace vectoriel réel de dimension finie et $f : X \to X$ linéaire. Alors il existe un sous-espace $S \subset X$ de dimension 1 ou 2 et tel que $f(S) \subset S$.*

Démonstration. Soit $p(X) \neq 0$ un polynôme à coefficients réels tel que $p(f) = 0$ (Existence : $1, f, f^2, \ldots, f^{n^2}$ en tant que vecteurs de l'espace $\mathrm{End}(X)$ de dimension n^2 sont linéairement dépendants.) On peut décomposer $p = p_1 \cdots p_r$ avec de polynômes p_i à coefficients réels et de degré ≤ 2. Pour un de ces polynômes, disons p_1, l'application $p_1(f)$ n'est pas inversible (sinon, $p(f) = 0$ serait inversible). Soit $v \in \ker(p_1(f))$, $v \neq 0$. On vérifie facilement que $S := \langle v, f(v) \rangle$ est invariant sous f (exercice). □

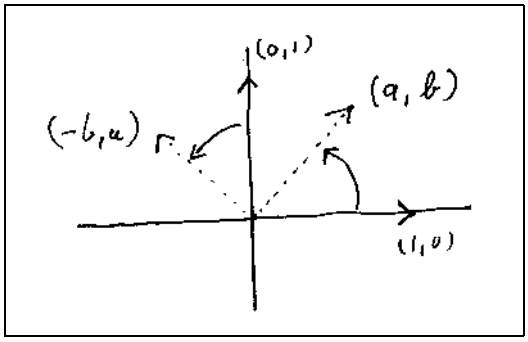


Figure 3.1: La rotation du plan induite par une matrice de SO(2)

Théorème 3.17. *(***Forme normale d'une isométrie***) Soit $g \in \mathrm{O}(V)$. Alors il existe une décomposition*

$$V = S_1 \widehat{\oplus} S_2 \widehat{\oplus} \cdots \widehat{\oplus} S_k$$

telle que $\dim S_j \leq 2$, *$g(S_j) = S_j$ et telle que S_j est irréductible sous g. Si* $\dim S_j = 2$, *alors* $g|_{S_j} \in \mathrm{SO}(S_j)$.

Remarque. On dit qu'un sous-espace S est irréductible sous g si il n'existe pas des sous-espaces non-triviaux de S qui sont invariants sous g.

Démonstration. Récurrence sur $\dim V$. Soit $V_0 \neq 0$ un sous-espace stable par g et de dimension minimale. D'après le lemme $\dim V_1 \leq 2$. On a $V = V_1 \widehat{\oplus} V_1^\perp$ et $g(V_1^\perp) = V_1^\perp$. L'hypothèse de récurrence appliqué à $g|_{V_1^\perp}$ implique la décomposition en question.

Si $\dim S_j = 2$, alors $h := g|_{S_j}$ a déterminant $+1$. Sinon h serait une symétrie hyperplane, donc $h(x) = x$ avec un vecteur $x \in S_j$, $x \neq 0$, qui est en contradiction à la irréductibilité de S_j. □

Théorème 3.18. *(***Description algébrique : forme normale***) Pour tout $g \in \mathrm{O}(V)$ il existe une base orthonormale de V telle que la matrice $M(g)$ de g par rapport à cette base est de la forme*

$$(FN) \qquad M(g) = \begin{pmatrix} A_1 & & & & \\ & \ddots & & & \\ & & A_p & & \\ & & & 1_q & \\ & & & & -1_r \end{pmatrix} \qquad (p, q, r \geq 0,\ 2p+q+r = n)$$

avec $A_j \in \mathrm{SO}(2)$, $A_j \neq \pm 1$ *pour* $1 \leq j \leq p$.

Démonstration. C'est la traduction matricielle du théorème précédent. □

Remarque. En considérant le cas $V = \mathbb{R}^n$ on obtient : Tout $A \in \mathrm{O}(n)$ est conjugué (dans $\mathrm{O}(n)$) à une matrice de la forme (FN).

3.4 Classification suivant $\dim \mathrm{Fix}(g)$

Lemme. *Soit* $\dim V = 2$, $g \in \mathrm{O}(V)$, $g \neq 0$. *Si* $\det(g) = +1$, *alors* g *et un produit de deux symétries hyperplanes différentes. Si* $\det(g) = -1$, *alors* g *est une symétrie hyperplane (i.e. il existe une base orthonormale* e_1, e_2 *de* V *telle que* $g(e_1) = e_1$ *et* $g(e_2) = -e_2$*).*

Démonstration. Voir le théorème 3.12 sur la "représentation géométrique". □

Théorème 3.19. *Dans le cas* $\dim V = 2$ *on a la classification suivante pour les* $g \in \mathrm{O}(V)$ *:*

$\dim \mathrm{Fix}(g)$	*0*	*1*	*2*
g	*rotation* $\neq 1$	*sym.hyp.*	*identité*

Démonstration. On utilise le lemme précédent : Si $\dim \mathrm{Fix}(g) = 0$, alors g n'est pas une symétrie hyperplane (qui laisse invariante une droite), donc $\det(g) = +1$. Si $\dim \mathrm{Fix}(g) = 1$, alors g n'est pas produit de deux symétries hyperplanes différentes (car un tel produit n'a pas de vecteurs fixes non nuls. □

Lemme. *Soit* $\dim V = 3$, $g \in \mathrm{O}(V)$. *Alors il existe une base orthonormale* e_1, e_2, e_3 *de* V *telle que la matrice de* g *est de la forme*

$$M(g) = \begin{pmatrix} A & \\ & \det(g) \end{pmatrix}$$

avec un $A \in \mathrm{SO}(V)$ *(possiblement* $A = \pm 1$*).*

Démonstration. C'est une conséquence de "la forme normale" (voir théorème 3.18). □

Théorème 3.20. *Dans le cas* $\dim(V) = 3$, $g \in \mathrm{SO}(V)$, $g \neq 1$, *on a* $\dim \mathrm{Fix}(g) = 1$.

Démonstration. C'est une conséquence du lemme précédent (où pour un tel g on a nécessairement $A \neq 1$ et $\det(g) = +1$). □

Remarque. Pour $g \in \mathrm{SO}(V)$, $g \neq 1$, on appelle $\mathrm{Fix}(g)$ l'axe fixe de g. Donc toute est $g \in \mathrm{SO}(V)$ est "une rotation autour de son axe fixe" dans le sens naturel.

Théorème 3.21. *Dans le cas* $\dim V = 3$ *on a la classification suivante pour les* $g \in \mathrm{O}(V)$ *:*

$\dim \mathrm{Fix}(g)$	*0*	*1*	*2*	*3*
g	$r \circ \sigma$ *avec* $r\sigma = \sigma r$	$r \neq 1$	σ	*1*

Ici r *indique une rotation et* σ *une symétrie hyperplane.*

Démonstration. Clair du lemme précédent. □

3.5 Description analytique de $\mathrm{O}(V)$

Lemme. *L'application*

$$\mathbb{S}^1 \to \mathrm{SO}(2),\ \zeta = a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

est un isomorphisme de groupes.

Démonstration. Par calcul direct. □

Exercice. Montrer que toute isométrie g de l'espace euclidien $V = \mathbb{C}$ (avec produit scalaire $(z, w) = \mathrm{Re}(z\overline{w})$) est de la forme $g : z \mapsto \xi z$ avec un $\xi \in \mathbb{C}$, $|\xi| = 1$.

Donc l'application dans le théorème n'est rien d'autres que $\xi \mapsto M(g)$ où $M(g)$ est la matrice de g sur la base $1, i = \sqrt{-1}$.

Théorème 3.22. *L'application*

$$\mathbb{R} \to \mathrm{SO}(2),\ s \mapsto r(s) = \begin{pmatrix} \cos s & -\sin s \\ \cos s & \sin s \end{pmatrix}$$

est un morphisme de groupes surjectif avec noyau $2\pi\mathbb{Z}$.

Démonstration. l'application en question est le composé de l'isomorphisme du lemme est de l'application $s \mapsto \exp(is)$ qui est surjective et a le noyau $2\pi\mathbb{Z}$ (voir le deuxième exemple après théorème 1.11). □

Nous allons généraliser cette description à de dimensions arbitraires.

Définition. Pour une matrice $A \in \mathbb{R}^{n\times n}$ on pose

$$\exp(A) = \sum_{k=0}^{\infty} \frac{A^k}{k!} = \Big(\sum_{k=0}^{\infty} \frac{(A^k)_{ij}}{k!}\Big)_{1\le i,j\le n}.$$

Ici, pour une matrice B, on utilise B_{ij} pour l'élément dans la $i$ème ligne et $j$ème colonne.

Cette définition a un sens car on a :

Lemme. *Pour tout i, j la suite (s_n) avec $s_n = \sum_{k=0}^{\infty} \frac{(A^k)_{ij}}{k!}$ converge.*

Démonstration. Pour une matrice A on pose $|A| := \max |a_{i,j}|$. On a $|AB| \le n|A| \cdot |B|$. En particulier $|A^k| \le n^k |A|^k$. Donc la suite $|s_n|$ est majoré par $\exp(n|A|)$. □

Exercice. Montrer $\exp\left(s \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} \cos s & -\sin s \\ \sin s & \cos s \end{pmatrix}$

Nous citons sans preuve (la démonstration n'est pas difficile, mais appartient plutôt à l'analyse) :

Théorème 3.23. *Si $AB = BA$, alors $\exp(A+B) = \exp(A)\exp(B)$. En plus, $\det(\exp(A)) = \exp(\mathrm{tr}(A))$.*

Remarque. O En particulier, pour toute matrice $A \in \mathbb{R}^{n\times n}$ fixé, l'application $t \mapsto \exp(tA)$ est un morphisme de groupes $\mathbb{R} \to \mathrm{GL}(n, \mathbb{R})$. On a donc par exemple $\exp(A)^{-1} = \exp -A$.

Définition. On pose

$$\mathrm{so}(n) = \{X \in \mathbb{R}^{n\times n} \mid X^t + X = 0\}.$$

Exercice. $\mathrm{so}(n)$ est un sous-espace de dimension $\frac{n(n-1)}{2}$ de $\mathbb{R}^{n\times n}$.

Théorème 3.24. *(***Représentation paramétrique***) L'association $X \mapsto \exp(X)$ définit une application surjective $\mathrm{so}(n) \to \mathrm{SO}(n)$. Pour tout $X \in \mathrm{so}(n)$ l'application $s \mapsto \exp(sX)$ définit un morphisme de groupes $\mathbb{R} \to \mathrm{SO}(n)$.*

Démonstration. Soit $X \in \mathrm{so}(n)$. Alors

$$\exp(X)^{-1} = \exp(-X) = \exp(X^t) = \exp(X)^t,$$

et car $\mathrm{tr}(X) = 0$ on a $\det(\exp(X)) = \exp(\mathrm{tr}(X)) = 1$. Donc $\exp(X)$ est bien un élément de $\mathrm{SO}(n)$.

Si $A \in \mathrm{SO}(n)$, alors

$$A = T \begin{pmatrix} r(s_1) & & & \\ & \ddots & & \\ & & r(s_p) & \\ & & & 1_q \end{pmatrix} T^{-1}$$

avec une matrice inversible T (voir le théorème 3.18 sur la forme normale). Donc

$$A = T \exp \begin{pmatrix} s_1 \begin{pmatrix} 0, -1 \\ 1, 0 \end{pmatrix} & & & \\ & \ddots & & \\ & & s_p \begin{pmatrix} 0, -1 \\ 1, 0 \end{pmatrix} & \\ & & & 0_q \end{pmatrix} T^{-1} = \exp(TXT^{-1}),$$

où X est la matrice au milieu. Il est clair que X, et donc TXT^{-1} sont dans $\mathrm{so}(n)$.

Que $t \mapsto \exp(tX)$ pour $X \in \mathrm{so}(n)$ est un morphisme est clair d'après la remarque suivant théorème 3.23. □

3.6 L'action de O(V) sur V

3.6.1 Orientation

Nous fixons un espace vectoriel euclidien et nous posons

$$\mathrm{BON} = \{(e_1, \ldots, e_n) \in V^n \,|\, e_1, \ldots, e_n \text{ est une base orthonormale de } V\}.$$

Le groupe $\mathrm{O}(V)$ agit sur BON via

$$(g, (e_1, \ldots, e_n)) \mapsto (g(e_1), \ldots, g(e_n)).$$

Si on fixe une base $e := (e_1, \ldots, e_n)$, alors l'application

$$\mathrm{BON} \ni e' \mapsto \text{ l'applic. linéaire telle que } g(e) = e'$$

définit une bijection

$$\phi : \mathrm{BON} \to \mathrm{O}(V).$$

On a

$$\phi(g \cdot e') = g\phi(e')$$

pour tout $e' \in \mathrm{BON}$ et $g \in \mathrm{O}(V)$. En particulier, les orbites de BON sous $\mathrm{SO}(V)$ correspondent aux classes à gauches de $\mathrm{O}(V)$ par rapport à $\mathrm{SO}(V)$. Plus précisément :

Théorème 3.25. *On a* $|\,\mathrm{BON} \,/\, \mathrm{SO}(V)| = 2$. *Si* e *est une base orthonormale fixé, alors* $\{ge \,|\, g \in \mathrm{SO}(V)\}$ *et* $\{ge \,|\, g \in \mathrm{O}(V),\ \det(g) = -1\}$ *sont les deux orbites de* BON *par rapport à* $\mathrm{SO}(V)$.

Définition. Une espace vectoriel euclidien orienté est un couple $(V, \mathcal{O})$ où V est un espace vectoriel euclidien et où $\mathcal{O}$ est une des deux orbites de $\mathrm{BON} \,/\, \mathrm{SO}(V)$. L'orbite $\mathcal{O}$ est appelée l'orientation de V. Une base ON e est appelée directe si $e \in \mathcal{O}$.

Remarque. D'après le théorème précédent tout V possède exactement deux orientations possible.

Si $V = \mathbb{R}^n$, alors

$$\{e = (e_1, \ldots, e_n) \,|\, e \text{ base ON},\ \det(e_1 \ldots e_n) = +1\}$$

est une orientation de $\mathbb{R}^n$ (l'orientation canonique). C'est l'orbite i.e. l'orbite de la base canonique de V sous $\mathrm{SO}(n)$.

Soit $\dim V = 2$. Si a, b est une base ON, alors les deux bases (a, b) et $(a, -b)$ représentent les deux orientations possibles de V.

Exercice. Montrer : Soit V un espace euclidien orienté, $e_1, \ldots, e_n$ une base ON directe de V, et $\sigma \in S_n$. Alors $e_{\sigma(1)}, \ldots, e_{\sigma(n)}$ est directe si et seulement si $\mathrm{sign}(\sigma) = +1$.

Définition. La sphère de rayon r et centre 0 dans un espace euclidien V est définie par

$$S_r(V) = \{x \in V \mid |x| = r\}.$$

Théorème 3.26. *Soit* $\dim V \geq 2$. *Alors* $(g, x) \mapsto g(x)$ *définit une opération transitive de* $\mathrm{SO}(V)$ *sur* $S_r(V)$.

Remarque. Si $\dim V = 1$, disons $V = \mathbb{R} \cdot e$, $|e| = 1$, alors $S_r(V) = \{\pm re\}$ et $\mathrm{SO}(V)$ laisse re et $-re$ invariant.

Démonstration. Soient $x, y \in V$. On peut compléter x et y à des bases ON $x = e_1, \ldots, e_n$ et $y = e'_1, \ldots, e'_n$. L'application linéaire telle que $g(e_i) = e'_i$ $(1 \leq i < n)$ et $g(e_n) = \epsilon e_n$ est dans $\mathrm{SO}(V)$ avec un choix convenable de $\epsilon = \pm 1$, et $g(x) = y$. □

Corollaire 3.26.1. *L'ensembles ensemble des orbites* $V/\mathrm{SO}(V)$ *est égal à l'ensemble des sphères* $S_r(V)$ *(*$r \geq 0$*).*

3.6.2 Angles

Dans cette section on suppose que V est un espace vectoriel euclidien orienté de dimension 2. La sphère de rayon 1 dans V est notée $S(V)$.

Théorème 3.27. *Soit* a, b *une base directe de* V.

1. *Alors l'application*

$$(A, \alpha a + \beta b) \mapsto (a, b) A \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

   définit une action de $\mathrm{SO}(2)$ *sur* $S(V)$.

2. *Cette action ne dépend du choix de la base directe* a, b.

3. *Elle est simplement transitive, i.e. pour tout* $x, y \in S(V)$ *il existe un unique* $A \in SO(2)$ *tel que* $y = A \cdot x$.

Démonstration. (1) et (3) sont clair. Pour montrer (2) soit a', b' une base directe. Soit T la matrice telle que $(a', b') = (a, b)T$. Alors $T \in \mathrm{SO}(2)$. Soit $x = \alpha a + \beta b = \alpha' a' + \beta' b' \in S(V)$. Alors pour tout $A \in \mathrm{SO}(2)$ on a

$$(a', b') A \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = (a, b) T A T^{-1} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = (a, b) A \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

car $\mathrm{SO}(2)$ est abélien et donc $TAT^{-1} = A$. □

Exercice. Soit (a, b) une base directe de V. Montrer que $b = r(\frac{\pi}{2})a$, et que par rapport à l'autre orientation de V, qui est représenté par $(a, \overline{b}) = (a, -b)$ on a $\overline{b} = -b = r(\frac{\pi}{2})a$.

Donc une orientation commun avec l'opération de SO(2) donne "un sens positif de rotation"

Nous avons vu (théorème 3.22 que

$$\theta = s + 2\pi\mathbb{Z} \mapsto r(\theta) := r(s) = \begin{pmatrix} \cos s & -\sin s \\ \sin s & \cos s \end{pmatrix}$$

est un isomorphisme de groupes

$$\mathbb{R}/2\pi\mathbb{Z} \to \mathrm{SO}(2).$$

Définition. Pour $x, y \in V$, $x, y \neq 0$ on pose $\widehat{xy}$ = l'unique $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ telle que

$$\frac{y}{|y|} = r(\theta)\left(\frac{x}{|x|}\right)$$

(angle orienté de x et y).

Théorème 3.28. *Pour $x \in S(V)$ soit $\wedge x$ l'unique vecteur de $S(V)$ tel que $x, \wedge x$ est une base directe de V. Alors pour tout $x, y \in S(V)$ on a $\widehat{xy}$ = l'unique $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ telle que*

$$(y, \wedge y) = (x, \wedge x)r(\theta)$$

Démonstration. Exercice. □

Remarque. Dans $V = \mathbb{R}^2$ avec l'orientation telle que $(1, 0)$ et $(0, 1)$ est une base directe on a $\wedge(a, b) = (-b, a)$.

Corollaire 3.28.1. *Pour tout $x, y \in V$, $x, y \neq 0$ on a*

$$\cos(\widehat{xy}) = \frac{(x, y)}{|x| \cdot |y|}$$

Démonstration. On peut supposer $|x| = |y| = 1$. Alors

$$(y, \wedge y) = (x, \wedge x)\begin{pmatrix} (y, x) & (\wedge y, x) \\ (y, \wedge x) & (\wedge y, \wedge x) \end{pmatrix},$$

et d'où le corollaire. □

Théorème 3.29. *Pour tout $x, y, z \in V$, $x, y, z \neq 0$, on a*

1. $\widehat{xx} = 0$,
2. $\widehat{xy} = -\widehat{yx}$,
3. $\widehat{xy} = \widehat{xz} + \widehat{zy}$. *(Relation de Chasles).*
4. *Si $g \in \mathrm{O}(V)$, alors* $\widehat{g(x)\, g(y)} = \det(g)\widehat{xy}$.
5. $\widehat{x, -y} = \pi + \widehat{xy}$.

Démonstration. (1) et (2) sont clairs.

Pour (3) on suppose $x, y, z \in S(V)$. Soient $\theta_1 = \widehat{xz}$ et $\theta_2 = \widehat{zy}$, i.e.

$$z = r(\theta_1)x, \quad y = r(\theta_2)z.$$

Alors

$$y = r(\theta_2)r(\theta_1)x = r(\theta_1 + \theta_2)x,$$

donc $\theta_1 + \theta_2 = \widehat{xy}$.

Pour (4) soit $\theta = \widehat{xy}$, et soit h la rotation de V donné par $h(t) = r(\theta)t$ pour tout $t \in V$. Alors

$$y = h(x) \Longrightarrow g(y) = ghg^{-1}(g(x)) = h^{\epsilon}(g(x)) = r(\theta)^{\epsilon} g(x) = r(\epsilon\theta)g(x),$$

où $\epsilon = \det(g)$.

Pour (5) on utilise $\widehat{y, -y} = \pi$ et puis la relation de Chasles : $\widehat{x, -y} = \widehat{x, y} + \widehat{y, -y}$. □

3.6.3 Angles de droites

Toujours V est un espace vectoriel euclidien orienté de dimension 2. Soit $\mathcal{D}$ l'ensemble des droites dans V passant 0.

Théorème 3.30. *Soient $D, D' \in \mathcal{D}$, disons $D = \mathbb{R}x$, $D' = \mathbb{R}y$ avec $x, y \in S(V)$. Soit $s_0 \in \mathbb{R}$ tel que $y = r(s_0)x$. Alors la classe de s_0 modulo $\pi\mathbb{Z}$ ne dépend du choix de x, y. Elle est appelée angle orienté de D et D' et noté $\widehat{DD'}$.*

Démonstration. Les choix possibles pour des bases ON de D et D' sont x, y, $-x, y$, $x, -y$ et $-x, -y$. L'ensemble des s tels que $r(s)$ donne le premier sur le deuxième vecteur sont respectivement $s_0+2\pi\mathbb{Z}$, $s_0+\pi+2\pi\mathbb{Z}$, $s_0+\pi+2\pi\mathbb{Z}$, $s_0+2\pi\mathbb{Z}$. □

Exercice. Montrer : Le groupe $\mathrm{SO}(2)/\{\pm 1\}$ agit simplement transitive sur $\mathcal{D}$ via

$$(\{\pm A\}, D = \mathbb{R}x) \mapsto \mathbb{R}Ax.$$

On a que $\widehat{DD'}$ est l'unique $s + \pi\mathbb{Z} \in \mathbb{R}/\pi\mathbb{Z}$ tel que $D' = \{\pm r(s)\}D$.

3.6.4 Angles non orientés

Ici V est toujours un espace vectoriel euclidien de dimension 2, mais non nécessairement orienté.

Définition. Soient $x, y \in V$, $x, y \neq 0$. On appelle

$$\arccos\left(\frac{(x,y)}{|x|\cdot|y|}\right) \in [0, \pi]$$

l'angle non-orienté des vecteurs x et y.

Remarque. C'est bien défini, car

$$-1 \leq \frac{(x,y)}{|x|\cdot|y|} \leq 1$$

d'après l'inégalité de Schwartz.

Théorème 3.31. *Soit V orienté, $x, y \in V$, $x, y \neq 0$ et $s \in]-\pi, +\pi]$ l'unique représentant de la classe de $\widehat{xy}$ dans $\mathbb{R}/2\pi\mathbb{Z}$. Alors l'angle non-orienté de x et y est égal à $|s|$.*

Démonstration. On suppose que $|x| = |y| = 1$. Alors $\cos s = (x, y)$ d'après corollaire 3.28.1, et donc $\arccos(x, y) = \arccos(\cos s) = |s|$. □

Remarque. On peut définir l'angle non-orienté de droites D et d' avec bases ON x et y comme

$$\arccos\left(\frac{|(x,y)|}{|x|\cdot|y|}\right) \in [0, \frac{\pi}{2}],$$

et on une relation analogue entre l'angle orienté et l'angle non-orienté de droites comme dans le théorème précédent.

3.6.5 Volume

Soit $\dim V = n$. L'espace vectoriel $\bigwedge^n V^*$ des formes multilinéaires et alternées $d\colon V^n \to \mathbb{R}$ est de dimension 1. En plus, on a pour tout $g \in \mathrm{GL}(V)$ et $d \in \bigwedge^n V^*$ l'identité

$$d(g(x_1, \dots, x_n)) = \det(g) d(x_1, \dots, x_n).$$

Comme conséquences de ces deux faits il existe exactement deux formes $v_i \in \bigwedge^n V^*$ $(i = 1, 2)$ telles que pour toute base orthonormale $e = (e_1, \dots, e_n)$ on a

$$|v_1(e)| = |v_2(e)| = 1.$$

Les ensembles

$$\mathcal{N}(v_i) = \{e \,|\, e \text{ base ON et } v_i(e) = +1\} \quad (i = 1, 2)$$

sont les deux orientations possible de V. Réciproquement, si V est orienté par $\mathcal{O}$, le $d = v_i$ tel que $\mathcal{O} = \mathcal{N}(v)$ est appelle le volume euclidien (ou produit mixte) de V.

Désormais soit V orienté avec volume euclidien d. Pour $x_1, \dots, x_{n-1} \in V$ l'application

$$V \to \mathbb{R}, \quad x \to d(x_1, \dots, x_{n-1}, x)$$

est linéaire. Donc il existe un unique vecteur, noté

$$x_1 \wedge x_2 \wedge \cdots \wedge x_{n-1}$$

et appelé produit vectoriel de $x_1, \dots, x_{n-1}$, tel que

$$d(x_1, \dots, x_{n-1}, x) = (x_1 \wedge x_2 \wedge \cdots \wedge x_{n-1}, x)$$

pour tout $x \in V$.

Théorème 3.32. *On a*

1. *L'application $V^{n-1} \to V$, $(x_1, \dots, x_{n-1}) \mapsto x_1 \wedge \cdots \wedge x_{n-1}$ est multilinéaire est alternée.*
2. $x_1 \wedge \cdots \wedge x_{n-1} \perp \langle x_1, \dots, x_{n-1} \rangle$.
3. $\det(x_1, \dots, x_{n-1}, x_1 \wedge x_2 \wedge \cdots \wedge x_{n-1}) = |x_1 \wedge x_2 \wedge \cdots \wedge x_{n-1}|^2$, *en particulier : Si les $x_1, \dots, x_{n-1}$ sont deux à deux orthogonaux, alors $x_1, \dots, x_{n-1}, x_1 \wedge x_2 \wedge \cdots \wedge x_{n-1}$ est une base orthogonale directe.*

Démonstration. Immédiat de la définition du produit vectoriel. □

Exercice. Soit V égal à $\mathbb{R}^n$, orienté tel que la base canonique est directe. Montrer $d = \det$, et déduire une formule explicite pour $x_1 \wedge \cdots \wedge x_{n-1}$ en fonction des composants des x_i.

3.7 Exercices

1. Soit S un sous-espace de l'espace vectoriel euclidien V, soit P_S la projection orthogonale sur S, i.e. $P_S(x) = x_1$ si $x = x_1 + x_2$ avec $x_1 \in S$ et $x_2 \perp S$. Soit $a_1, \ldots, a_k$ une base quelconque de S et G la matrice de Gram associée. Montrer :

$$P_S(x) = (a_1, \ldots, a_k) G^{-1} \begin{pmatrix} (x, a_1) \\ \vdots \\ (x, a_k) \end{pmatrix}.$$

(Indication : Considérer d'abord le cas $k = 1$.)

2. Avec les notations de l'exercice précédent montrer que $P_{S^\perp} = 1 - P_S$ et déduire deux formules explicites pour $d(x, S)$ pour $x \in X$.

3. Soit σ_S la symétrie par rapport au sous-espace S de l'espace euclidien V. Montrer (notation comme dans le premier exercice) que

$$\sigma_S = 2P_S - 1 = 1 - 2P_{S^\perp}.$$

En déduire deux formules explicites pour σ_S en fonction de bases de S et $S^\perp$ respectivement.

4. Pour $x, y \in \mathbb{R}^2$, on pose $v(x, y) = |x|\,|y| \sin(\widehat{x, y})$, i.e. $v(x, y)$ est l'aire naive du parallélogramme engendré par x et y, multiplié par $\operatorname{sign}(\widehat{x, y})$. Ici l'angle est par rapport à l'orientation canonique de $\mathbb{R}^2$, et il est considéré comme élément de $]-\pi, +\pi]$. Montrer directement, avec des dessins, que v est multilinéaire et alterné. En déduire que $v(x, y) = \det(x, y)$.

5. Soient A, B, C des matrices orthogonales dans $\mathrm{O}(3)$ avec polynômes caractéristiques $\chi_A(x) := \det(x - A) = (x - 1)(x^2 + x + 1)$, $\chi_B(x) =$

$(x-1)^2(x+1)$, $\chi_C(x) = (x+1)(x^2 - \sqrt{2}x + 1)$. Qu'est-ce que l'on peut dire sur $X = A, B, C$? ($\dim \mathrm{Fix}(X)$? X est rotation, symétrie hyperplane, ...? Les angles des rotations?)

Chapitre 4

Espaces affines euclidiens

4.1 Notions de base

Définition. Un espace (affine) euclidien est un espace affine $(E, V, +)$ tel que V est un espace vectoriel euclidien.

Exemple. L'exemple fondamental est $E = \mathbb{R}^n$ et $\overrightarrow{E} = \mathbb{R}^n$ muni du produit scalaire usuel.

Définition. Pour $p, q \in E$ on pose

$$pq = d(p, q) := |\overrightarrow{pq}|.$$

Une isométrie d'espaces euclidiens E et E' est une application affine bijective $f\colon E \to E'$ tel que

$$\forall\, p, q \in E : f(p)f(q) = pq.$$

Exercice. Montrer qu'une application affine $f : E \to E'$ est une isométrie si et seulement si $\overrightarrow{f}$ est une isométrie.

Théorème 4.1. *(***Pythagore***) Soient $p, q, r \in E$. Avec les notations $a = qr$, $\overrightarrow{a} = \overrightarrow{qr}$, $b = rp$, $\overrightarrow{b} = \overrightarrow{rp}$, $c = pq$ et $\overrightarrow{c} = \overrightarrow{pq}$ on a*

1. *$a^2 + b^2 = c^2 - 2(\overrightarrow{a}, \overrightarrow{b})$.*
2. *Si $(\overrightarrow{a}, \overrightarrow{b}) = 0$, alors $a^2 + b^2 = c^2$.*

Démonstration. $c^2 = |\overrightarrow{c}|^2 = |\overrightarrow{a} + \overrightarrow{b}|^2 = a^2 + 2(\overrightarrow{a}, \overrightarrow{b}) + b^2$. □

Théorème 4.2. *L'application $d\colon E \times E \to \mathbb{R}$ est une métrique. En particulier on a $d(p,q) \leq d(p,r) + d(r,q)$ pour tout $p,q,r \in E$.*

Démonstration. C'est rien que l'inégalité de triangle dans l'espace vectoriel euclidien $\overrightarrow{E}$. □

Théorème 4.3. *Il existe toujours un repère orthonormale (ON) de E, i.e. un repère affine $p_0,\dots,p_n$ tel que les vecteurs $\overrightarrow{p_0p_1},\dots,\overrightarrow{p_0p_n}$ forment une base orthonormale.*

Démonstration. C'est clair car $\overrightarrow{E}$ possède des base ON. □

Exemple. Les points $0, c_1, \dots, c_n$ (où c_i est la base canonique) est un repère ON de $\mathbb{R}^n$.

Théorème 4.4. *Tout espace affine euclidien est isométrique à $\mathbb{R}^n$.*

Démonstration. Soit $p_0,\dots,p_n$ un repère ON de E. Alors l'application affine $f : E \to \mathbb{R}^n$ telle que $f(p_0) = O$ et $f(p_j) = c_j$ (où c_j est la base canonique de $\mathbb{R}^n$) est une isométrie. □

4.2 Distances de sous-espaces

Définition. Pour un point $p \in E$ et des sous-espaces affines $S, T \subset E$ on pose

$$d(p,S) = \inf\{pq\,|, q \in S\}, \qquad d(S,T) = \inf\{pq\,|, p \in S,\ q \in T\}.$$

Dans cette partie on déduit des formules variées pour ces distances.

Définition. Soient S et T des sous-espaces affines de E.

1. On pose $S \perp T$ (S orthogonale ou perpendiculaire à T) si $\overrightarrow{S} \perp \overrightarrow{T}$.
2. La projection sur S parallèle à $\overrightarrow{S}^{\perp}$ est notée $\hat{\pi}_S$, et appelée projection orthogonal sur S.

Remarque. D'après la définition de la projection parallèle à un sous-espace $\hat{\pi}_S(p)$ est l'unique point d'intersection de S et $p + \overrightarrow{S}^{\perp}$, ou bien, l'unique $q \in S$ tel que $\overrightarrow{pq} \perp S$.

Théorème 4.5. *Soit $p \in E$ et $S \subset E$ un sous-espace affine. Alors il existe un et un seul $q \in S$ tel que $d(p,S) = pq$. On a $q = \hat{\pi}_S(p)$.*

Démonstration. Soit $q = \hat{\pi}_S(p)$. Alors pour $r \in S$ on a d'après Pythagore

$$pr^2 = pq^2 + qr^2 \geq pq^2,$$

et donc pr^2 est minimal si et seulement si $r = q$. □

Théorème 4.6. *Soit V un espace vectoriel euclidien. Pour $a_1, \ldots, a_k \in V$ on pose*

$$\Delta(a_1, \ldots, a_k) = \det\big((a_i, a_j)\big)_{1 \leq i,j \leq k}$$

(déterminant de Gram des a_i). Alors on a:

1. *$\Delta(a_1, \ldots, a_k) \neq 0$ si et seulement si les a_i sont linéairement indépendants.*
2. *$\Delta(x, a_1, \ldots, a_k) = \Delta(y, a_1, \ldots, a_k)$ si $x - y \in \langle a_1, \ldots, a_k \rangle$.*
3. *$\Delta(x, a_1, \ldots, a_k) = |x|^2 \cdot \Delta(a_1, \ldots, a_k)$ si $x \perp \langle a_1, \ldots, a_k \rangle$.*

Démonstration. Propriété 3 est évidente. Les autres sont un exercice dans l'algèbre multilinéaire. On utilise que

$$\Gamma(a_1, \ldots, a_k; b_1, \ldots, b_k) := \det\left((a_i, b_j)\right)_{1 \leq i,j \leq k}.$$

est multilinéaire est alternée dans les a_j et les b_j respectivement. □

Exercice. L'interprétation géométrique de Δ est la suite : Soit X le sous-espace de V engendré par les a_j. C'est un espace vectoriel euclidien (avec le produit scalaire provenant de V). Montrer : Si d est un des deux volumes possibles de X et si les a_j sont linéairement indépendants, alors

$$\Delta(a_1, \ldots, a_k) = d(a_1, \ldots, a_k)^2.$$

Théorème 4.7. *Soit $(O, a_1, \ldots, a_k)$ un repère cartésien du sous-espace S de E, et soit $p \in E$. Alors*

$$d(p,S)^2 = \frac{\Delta(\overrightarrow{Op}, a_1, \ldots, a_k)}{\Delta(a_1, \ldots, a_k)}.$$

Démonstration. Soit $q = \hat{\pi}_S(p)$. Alors $\overrightarrow{Op} \in \overrightarrow{qp} + \overrightarrow{S}$, d'où et d'après le théorème sur les déterminants de Gram

$$\Delta(\overrightarrow{Op}, a_1, \ldots . a_k) = \Delta(\overrightarrow{qp}, a_1, \ldots . a_k) = |\overrightarrow{qp}|^2 \, \Delta(a_1, \ldots . a_k)$$

□

Théorème 4.8. *Soient S, T des sous-espaces affine de E. Alors :*

1. *Il existe $s \in S$ et $t \in T$ tels que $d(S,T) = st$.*
2. *Soient $s \in S$ et $t \in T$. Alors $st = d(S,T)$ si et seulement si $\overrightarrow{st} \in \overrightarrow{S}^{\perp} \cap \overrightarrow{T}^{\perp}$.*
3. *Le couple $(s,t) \in S \times T$ tel que $st = d(S,T)$ est unique si et seulement si $\overrightarrow{S} \cap \overrightarrow{T} = 0$.*

Démonstration. Exercice. □

Théorème 4.9. *Soient D, D' deux droites dans E, $a, b \in D$ et $a', b' \in D'$, $a \neq b$ et $a' \neq b'$. Alors*

$$d(D,D')^2 = \frac{\Delta(\overrightarrow{aa'}, \overrightarrow{ab}, \overrightarrow{a'b'})}{\Delta(\overrightarrow{ab}, \overrightarrow{a'b'})}.$$

Théorème 4.10. *Soient $s \in D$ et $t \in D'$ tel que $\overrightarrow{st} \perp \overrightarrow{D}, \overrightarrow{D'}$, i.e. et tel que $st = d(S,T)$. Alors d'après le théorème sur les déterminants de Gram*

$$\Delta(\overrightarrow{aa'}, \overrightarrow{ab}, \overrightarrow{a'b'}) = \Delta(\overrightarrow{st}, \overrightarrow{ab}, \overrightarrow{a'b'}) = |\overrightarrow{st}|^2 \cdot \Delta(\overrightarrow{ab}, \overrightarrow{a'b'}).$$

Une formule un peu différente des deux formules précédentes (qui ont utilisé le déterminant de Gram) est la suivante :

Théorème 4.11. *Soit $f \colon E \to \mathbb{R}$ affine et non constant, soit $u \in \overrightarrow{E}$ tel que $\overrightarrow{f}(x) = (x,u)$ pour tout $x \in \overrightarrow{E}$. Alors pour tout $p \in H$ et $c \in \mathbb{R}$ on a*

$$d(p, f^{-1}(c)) = \frac{|f(p) - c|}{|u|}.$$

Remarque. L'hypothèse que f est non-constant implique que $\overrightarrow{f} \neq 0$, f est surjectif et que $f^{-1}(c)$, pour tout c, est donc un hyperplan dans E.

Exemple. Comme exemple concret on considère un hyperplan

$$H = \{q \in \mathbb{R}^n \mid u^t \cdot q = c\}$$

dans $\mathbb{R}^n$ (où $0 \neq u \in \mathbb{R}^n$, $c \in \mathbb{R}$). Alors pour tout $p \in \mathbb{R}^n$ on a d'après le théorème (appliqué à $f(p) = u^t \cdot p$) que

$$d(p, H) = \frac{|u^t \cdot p - c|}{|u|}.$$

Démonstration du théorème. Soit $H = f^{-1}(c)$ et $q = \hat{\pi}_H(p)$. Alors $f(q) = c$, et d'où

$$|f(p) - c| = |\overrightarrow{f}(\overrightarrow{qp})| = |(\overrightarrow{qp}, u)| = |\overrightarrow{qp}| \cdot |u|.$$

La dernière identité car $\overrightarrow{qp}$ et u sont tous les deux dans $\overrightarrow{H}^{\perp}$, un espace vectoriel de dimension 1, et donc $\overrightarrow{qp}$ est un multiple de u. □

4.3 Ensembles définis par distance

On s'intéresse dans cette section pour des ensemble qu'on peut décrire en utilisant seulement la notion de distance. Autrement dit, on fixe des points $p_0, \ldots, p_n$ de E, et on veut étudier les images réciproques d'ensembles dans $\mathbb{R}^{n+1}$ sous l'application

$$\Lambda \colon E \to \mathbb{R}^{n+1}, \quad \Lambda(p) = \begin{pmatrix} pp_0^2 \\ pp_1^2 \\ \vdots \\ pp_n^2 \end{pmatrix}.$$

Dans cette section nous supposons toujours que *les $p_0, \ldots, p_n$ forment un repère affine de E*. Donc ils sont en position générale et $\dim R = n$.

Nous considérons d'abord l'application auxiliaire

$$\kappa \colon E \to \mathbb{R}^n, \quad \kappa(p) = \begin{pmatrix} pp_1^2 \\ \vdots \\ pp_n^2 \end{pmatrix} - pp_0^2 \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Théorème 4.12. *L'application κ est une application affine bijective.*

Démonstration. En effet

$$\kappa(p) = \begin{pmatrix} p_0p_1^2 \\ \vdots \\ p_0p_n^2 \end{pmatrix} + 2 \begin{pmatrix} (\overrightarrow{pp_0}, \overrightarrow{p_0p_1}) \\ \vdots \\ (\overrightarrow{pp_0}, \overrightarrow{p_0p_n}) \end{pmatrix} =: \kappa(p_0) + F(\overrightarrow{pp_0}).$$

L'application F est linéaire, et car le produit scalaire est non dégénéré, elle est bijective. □

Corollaire 4.12.1. *L'application Λ est injective, i.e. pour tout $p, q \in E$ on a $p = q$ si et seulement si $pp_i = qp_i$ $(0 \leq i \leq n)$*

Démonstration. On utilise que $\Lambda(p) = \Lambda(q)$ entraîne $\kappa(p) = \kappa(q)$, et que κ est bijective. □

Définition. Nous utilisons

$$C(r, c) = C_E(c, r) = \{p \in E \mid pc = r\}$$

pour la "sphère dans E de rayon r et avec centre c".

Corollaire 4.12.2. *L'intersection de $n + 1$ sphères avec centres en position générales est soit vide, soit contient un seul point.*

Démonstration. Cette intersection est l'image réciproque sous Λ d'un point dans $\mathbb{R}^{n+1}$, donc vide ou un seul point. □

Corollaire 4.12.3. *Pour tout k L'ensemble*

$$S := \{p \in E \mid pp_0 = pp_1 = \cdots = pp_k\}$$

est un sous-espace affine de E de dimension $n - k$ (appelé médiateur des p_i ou, si $k = 1$, aussi médiatrice des p_i).

Démonstration. Car

$$S = \kappa^{-1}\left(\begin{pmatrix} 0_k \\ \mathbb{R}^{n-k} \end{pmatrix}\right).$$

□

Exercice. Montrer dans le notations du théorème que $\overrightarrow{p_ip_j} \perp S$.

Corollaire 4.12.4. *Il existe une et une seule sphère circonscrite S du n-simplex $\{p_0, \ldots, p_n\}$, i.e. une et une seule sphère S telle que $p_i \in S$ pour tout i.*

Démonstration. C'est le corollaire précédent dans le cas $k = n$ (et donc c comme l'unique point de S. □

Il est un exercice intéressant à déterminer l'image de Λ.

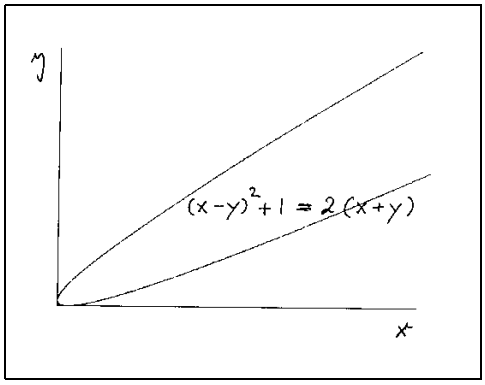


Figure 4.1: L'image de $\Lambda : E = \mathbb{R} \to \mathbb{R}^2$ où $p_0 = 0$, $p_1 = 1$.

La nature des images réciproque sous Λ de hyperplans dans $\mathbb{R}^{n+1}$ sont expliquées par la formule d'Apollonius :

Théorème 4.13. *(***Formule d'Apollonius***) Soient $q_0, \ldots, q_k \in E$, et soit $b = \sum_{i=1}^k \lambda_i q_i$ avec des $\lambda_i \in \mathbb{R}$, $\sum_{i=0}^k \lambda_i = 1$. Alors pour tout p on a*

$$\sum_{i=1}^{k} \lambda_i p q_i^2 = pb^2 + \sum_{i=1}^{k} \lambda_i b q_i^2.$$

Démonstration. On écrit

$$pq_i^2 = pb^2 + 2(\overrightarrow{pb}, \overrightarrow{bp_i}) + bq_i^2$$

et fait la somme sur i en observant que $\sum_i \lambda_{i=0}^k \overrightarrow{bp_i} = 0$. □

Corollaire 4.13.1. *Soient $\lambda_0, \cdots, \lambda_n, c \in \mathbb{R}$ tels que $\sum_{i=0}^n \lambda_i \neq 0$. Alors*

$$\{p \in E \mid \sum_{i=0}^{n} \lambda_i pp_i^2 = c\}$$

est soit vide soit une sphère.

Remarque. L'ensemble dans le corollaire n'est rien d'autre que $\Lambda^{-1}(H)$ où H est le hyperplan $H = \{x \in \mathbb{R}^{n+1} \mid \sum \lambda_i x_i = c\}$ de $\mathbb{R}^{n+1}$. On remarque que tout hyperplan de $\mathbb{R}^{n+1}$ est de cette forme, mais pas avec la somme des λ_i nécessairement différente de 0.

Démonstration. Soit $\lambda = \sum_i \lambda_i$, $\mu_i = \lambda_i/\lambda$ et $b = \sum_i \mu_i p_i$. D'après la formule d'Appolonius, appliquée aux p_i et μ_i, on a donc $\Lambda(p) \in H$ si et seulement si

$$pb^2 = c - \sum_{i=0}^{n} \mu_i bp_i^2.$$

D'où le corollaire. □

On prend les notations comme dans la formule d'Appolonius. Si $\sum \lambda_i = 0$ on peut vérifier que

$$v = \sum_{i=0}^{k} \lambda_i \overrightarrow{Oq_i}$$

ne dépend pas de $O \in E$. On appelle ce v le barycentre des q_i affectés des masses λ_i (avec somme des masse égale à 0). En plus on vérifie dans ce cas la "formule généralisée d'Apollonius" : Pour tout $p, q \in E$ on a

$$\sum_{i=0}^{n} \lambda_i pq_i^2 = \sum \lambda_i qq_i^2 + 2(\overrightarrow{pq}, v).$$

Comme conséquence on trouve

Corollaire 4.13.2. *Avec le notations du corollaire précédent, mais maintenant avec $\sum_{i=0}^k \lambda_i = 0$, soit $v = \sum_{i=0}^k \lambda_i p_i$. Alors pour tout $c \in \mathbb{R}$ l'ensemble p*

$$\{p \in E \mid \sum_{i=0}^{n} \lambda_i pp_i^2 = c\}$$

est soit vide, soit un hyperplan.

Démonstration. Supposons l'ensemble contient un point q. Alors il est égal à

$$q + \{x \in E \,|\, (x, v) = 0\}.$$

d'après la formule d'Appolonius généralisée. □

Exemple. L'ensemble $\{p \in E \,|\, pp_0^2 + pp_1^2 = c\}$ est soit vide, soit une sphère, et l'ensemble $\{p \in E \,|\, pp_0^2 - pp_1^2 = c\}$ est soit vide, soit un hyperplan.

Une conséquence intéressante de la formule de l'Appolonius est la suivante

Corollaire 4.13.3. *Soient les notations comme dans la formule d'Appolonius. Alors le barycentre $g = \sum_{j=0}^{k} \lambda_j q_j$ est l'unique minimum de la fonction*

$$p \mapsto \sum_{j=0}^{n} \lambda_j p q_j^2.$$

4.4 Le groupe des isométries de E

Les isométries $f : E \to E$ forment un sous-groupe Isom de $\mathrm{GA}(E)$. L'application

$$\mathrm{Isom}(E) \to \mathrm{O}(\overrightarrow{E})$$

et surjective et a comme noyau le sous-groupe des translations. Analogue à $\mathrm{GA}(E)$ (voir théorème 2.9) on a la description suivante :

Théorème 4.14. *Soit $o \in E$. Pour $F \in \mathrm{O}(\overrightarrow{E})$ soit F_o l'isométrie de E telle que $F_o(o + x) = o + F(x)$ pour tout $x \in \overrightarrow{E}$. Alors l'application*

$$V \rtimes \mathrm{O}(\overrightarrow{E}) \to \mathrm{Isom}(E), \quad (t, F) \mapsto T_t \circ F_o$$

est un isomorphisme de groupes.

La décomposition d'une isométrie comme produit d'une translation et d'une isométrie avec point fixe n'est pas unique. Mais parmi toutes ces décompositions il en existe exactement une qui est distinguée dans un sens à préciser. Nous la décrivons dans ce qui suit.

Définition. Soit S un sous-espace affine de E. Soit $r \in \mathrm{O}(\overrightarrow{S}^{\perp})$. On pose

$$\rho_S(r) : E \to E, \quad \rho_S(r)(p + v) = p + r(v) \quad \text{pour } p \in S,\ v \perp S..$$

Ici est dans le suivant on utilise : Si v est un vecteur, X un sous-espace vectoriel de $\overrightarrow{E}$ et A, S des sous-espaces affines, alors $v \perp S$, $X \perp S$, $A \perp S$ indique que $v \perp \overrightarrow{S}$, $X \perp \overrightarrow{S}$ ou $\overrightarrow{A} \perp \overrightarrow{S}$.

Théorème 4.15. *L'application $\rho_S(r)$ est une isométrie. L'application*

$$\mathrm{O}(\overrightarrow{S}^{\perp}) \to \mathrm{Isom}(E),\ r \mapsto \rho_S(r)$$

est un morphisme injectif de groupes.

Démonstration. Evident. □

Un exemple important est $r = -1$. Ici $\rho_S(-1)$ est appelé symétrie orthogonale par rapport à S et noté simplement

$$\sigma_S (= \rho_S(-1)).$$

Lemme. *Soit $f : E \to E$ affine. Alors f possède un et un seul point fixe si et seulement si* $\mathrm{Fix}(\overrightarrow{f}) = 0$.

Démonstration. On fixe $o \in E$. Alors

$$f(o+x) = f(o) + \overrightarrow{f}(x) = o + x \Longleftrightarrow (\overrightarrow{f} - 1)(x) = \overrightarrow{f(o)\,o}.$$

□

Lemme. *Soit $k = \dim \mathrm{Fix}(\overrightarrow{g})$. Alors il existe un et un seul sous-espace S de dimension k tel que $g(S) = S$ et tel que $g|_S$ est une translation. Ce sous-espace est noté $I(g)$.*

Démonstration. La restriction de g sur un sous-espace S de dimension k est une translation si et seulement si $\overrightarrow{(g|_S)} = 1$, i.e. si et seulement si $S = \mathrm{Fix}(\overrightarrow{g})$. Posons $X := \mathrm{Fix}(\overrightarrow{g})$. Il est donc à montrer que l'application

$$G : E/X \to E/X, \quad p + X \mapsto g(p + X)$$

a un et un seul point fixe. Or cette application est affine avec $\overrightarrow{G}(x + X) = \overrightarrow{g}(x) + X$. D'après le lemme nous avons donc à montrer que $\mathrm{Fix}(\overrightarrow{G}) = 0$. Or pour tout $x \in X$ on a $\overrightarrow{G}(x+X) = x+X$ si et seulement si $\overrightarrow{g}(x) - x \in X$. Ecrivons $x = x' + x''$ avec $x' \in X$ et $x'' \perp X$. Alors $\overrightarrow{g}(x) - x = \overrightarrow{g}(x'') - x'' \in X^{\perp}$. Donc $\overrightarrow{g}(x) - x \in X$ si et seulement si $\overrightarrow{g}(x'') - x'' = 0$, i.e. $x'' \in X$, i.e. $x'' = 0$. D'où le théorème. □

Comme conséquence on peut dire

Théorème 4.16. *Soit $g \in \mathrm{Isom}(E)$ et $k = \dim \mathrm{Fix}(\overrightarrow{g})$. Alors il existe un sous-espace affine $S \subset E$ de dimension k, un vecteur $t \| S$ et un $r \in \mathrm{O}(\overrightarrow{S}^{\perp})$ tel que $g = T_t \circ \rho_S(r)$. Le triplet (S, t, r) est unique.*

Remarque. On remarque que T_t et $\rho_S(r)$ commutent. En plus, g possède de points fixes si et seulement si $t = 0$. Dans ce cas on a $\mathrm{Fix}(g) = S$.

Démonstration. Unicité : $g = T_t \circ \rho_S(r)$ et $t \| S$ entraîne que $g(S) = S$ et que $g|_S$ est la translation par t. Donc $S = I(g)$ et t sont unique. Car $r = \overrightarrow{g}|_{\overrightarrow{S}^{\perp}}$ il l'est aussi.

Existence : on prend $S := I(g)$, t tel que $T_t|_S = g|_S$ et $r = \overrightarrow{g}|_Y$ où $Y = \mathrm{Fix}(\overrightarrow{g})^{\perp}$. Pour $p \in S$ et $y =\in Y$ on a donc

$$g(p + y) = g(p) + \overrightarrow{g}(y) = T_t(p) + r(y) = \rho_S(r)(T_t(p + y)).$$

□

On applique ce théorème pour en tirer — en commun avec la classification de O(2) et O(3) (voir section 3.4) — la classification des isométries g d'un espace euclidien de dimension 2 ou 3 selon la dimension de $I(g)$ ou $\mathrm{Fix}(\overrightarrow{g})$.

Théorème 4.17. *Soit E un plan euclidien. Alors tout $g \in \mathrm{Isom}(E)$ est égal à un des 3 types suivantes :*

$\dim \mathrm{Fix}(\overrightarrow{g})$	0	1	2
$I(g)$	$\{O\}$	D	E
g	$\rho_O(r)$	$\sigma_D \circ T_t \quad (t \| D)$	T_t
$\overrightarrow{g}$	$\det = +1$	$\det = -1$	id
type	*rotation*	*symétrie glissée*	*translation*

Ici D est une droite, $r \in \mathrm{SO}(\overrightarrow{E})$, $r \neq 1$.

Théorème 4.18. *Soit $\dim E = 3$. Alors tout $g \in \mathrm{Isom}(E)$ est égal à un des 4 types suivantes :*

$\dim \mathrm{Fix}(\overrightarrow{g})$	0	1	2	3
$I(g)$	$D \cap P$	D	P	E
g	$\sigma_P \circ \rho_D(r)$ $D \perp P$	$g = T_t \circ \rho_D(r)$ $t \| D$	$T_t \circ \sigma_P$ $t \| P$	T_t
$\overrightarrow{g}$	$\det = -1$	$\det = +1$	$\det = -1$	id
nom	*symétrie-rotation*	*vissage*	*sym. glissée*	*transl.*

Ici D indique une droite, P un plan, et $r \in \mathrm{SO}(\overrightarrow{D}^{\perp})$, $r \neq 1$.

Les isométries g avec $\det(\overrightarrow{g}) = +1$ sont aussi appelées déplacements, les autres anti-déplacements. Les déplacements forment un sous-groupe des isométries de E.

4.5 Un théorème fondamental

Théorème 4.19. *Soient $p_0, \ldots, p_k$ et $q_0, \ldots, q_k$ des points dans E. Alors il existe une $g \in \mathrm{Isom}(E)$ tel que $g(P_i) = q_i$ $(0 \leq i \leq k)$ si et seulement si $p_i p_j = q_i q_j$ pour tout $0 \leq i, j \leq k$.*

Remarque. Donc une "figure" à $k+1$ sommets $p_0, \ldots, p_k$ dans E est uniquement déterminée (à isométries près) par les longueurs $p_i p_j$ de ses $\frac{k(k+1)}{2}$ arrêts.

Corollaire 4.19.1. *Soit $\dim E = n$ et soient $A = p_0, \ldots, p_n$ et $q_0, \ldots, q_n$ deux n-simplex avec des côtés égaux (i.e. $p_i p_j = q_i q_j$ pour tout i, j). Alors il existe une et une seule isométrie g (à multiplication à droite avec des symétries de A, i.e. des éléments de $\{h \in \mathrm{Isom}(E) \mid h(A) = A\}$ près) telle que $g(p_i) = q_i$ $(0 \leq i \leq n)$.*

Remarque. Cas particulier : E un plan. Si A et B sont 2 triangles congruents (i.e. avec mêmes côtés), alors il existe une isométrie g tell e que $g(A) = B$.

Démonstration du corollaire. D'après le théorème il existe un tel g. Elle est uniquement déterminée par ses valeurs sur le repère affine formé par les p_i. □

Lemme. *Soient $rq_i = sq_i$ pour $0 \leq i < k$, $T := \langle q_0, \ldots, q_{k-1} \rangle$. Alors on a $r = \rho_T(u)(s)$ avec un $u \in \mathrm{O}(\overrightarrow{T}^{\perp})$ convenable.*

Démonstration. On observe que (avec $a_i = \overrightarrow{q_0 q_i}$) :

$$rq_i^2 = rq_0^2 + q_0 q_i^2 + 2(\overrightarrow{rq_0}, a_i),$$

et donc

$$2(\overrightarrow{q_0 r}, a_i) = rq_0^2 + q_0 q_i^2 - rq_i^2 = sq_0^2 + q_0 q_i^2 - sq_i^2 = 2(\overrightarrow{q_0 s}, a_i).$$

On en déduit, en écrivant $\overrightarrow{q_0 r} = x + y$ et $\overrightarrow{q_0 s} = x' + y'$ avec $x, x' \in \overrightarrow{T}$ et $y, y' \perp \overrightarrow{T}$, que $x = x'$ (car x est uniquement déterminé par les équations $(\overrightarrow{q_0 r}, a_i) = (x, a_i)$ $(0 \leq i < k)$, et pareil pour x'), et $|y|^2 = q_0 r^2 - |x|^2 = q_0 s^2 - |x'|^2 = |y'|^2$. Soit $u \in \mathrm{O}(\overrightarrow{T})$ tel que $u(y) = y'$, alors $s = \rho_T(r)(u)$. □

Preuve du théorème. Le "seulement si" clair. Le "si" est démontré par récurrence sur k. Pour $k = 0$ le théorème est évident : $T_{\overrightarrow{p_0q_0}}(p_0) = q_0$. Supposons qu'il existe une isométrie g telle que $g(p_i) = q_i$ pour $0 \leq i \leq k-1$. Posons $r = g(p_k)$. On a pour $i < k$: $rq_i = rg(p_i) = p_kp_i = q_kq_i$. D'après le lemme

$$q_k = \rho_T(u)(r)$$

avec u convenable, et donc $\rho_T(u) \circ g$ donne p_i sur q_i pour tout $i \leq k$. □

Remarque. On peut formuler le théorème en disant que l'application

$$\iota_k : E^k/\operatorname{Isom}(E) \to \mathbb{R}^{\frac{k(k+1)}{2}}, \quad (p_0, \ldots, p_k) \mapsto (p_ip_j)_{0\leq i<j\leq k}$$

est injective. Autrement dit, les figures dans E à $k+1$ sommets modulo les isométries possède une description paramétrique. Pour compléter cette description il faut encore déterminer l'image de ι_k, i.e. répondre à la question : Pour quelles systèmes de nombres d_{ij} existe-t-il une figure à $k+1$ points dans E telle que les distances entres les sommets sont égales aux $d_{i,j}$? C'est un exercice intéressant.

Dans le cas $k = 2$ cet exercice est le problème de déterminer tous triplets (a, b, c) de nombres réels tels qu'il existe un triangle avec côtés a, b et c. La réponse est donné par le théorème suivant :

Théorème 4.20. *On suppose* $\dim E \geq 2$. *Soient* $a, b, c \geq 0$ *des nombres réels. Pour qu'il existe* $p, q, r \in E$ *tels que* $qr = a$, $rp = b$ *et* $pq = c$ *il faut et il suffit que*

$$a \leq b + c,\ b \leq c + a,\ c \leq a + b.$$

Démonstration. le "faut" est clair. Pour le "suffit" on remarque que les trois inégalités entraînent (en effet sont équivalentes à)

$$-1 \leq l := \frac{b^2 + c^2 - a^2}{2bc} \leq +1.$$

Donc $\alpha := \arccos l$ est réel. On choisit $\overrightarrow{b}, \overrightarrow{c} \in \overrightarrow{E}$ tel que

$$|\overrightarrow{b}| = b,\ |\overrightarrow{c}| = c,\ \frac{(\overrightarrow{b}, \overrightarrow{c})}{bc} = \alpha.$$

On fixe un $p \in E$ et pose $q = p + \overrightarrow{c}$ et $r = p + \overrightarrow{b}$. On vérifie que p, q, r sont comme il faut. □

Chapitre 5

Géométrie à l'ancien

5.1 Remarques historiques

La géométrie d'Euclide se trouvent dans les 6 premiers livres d'une série de 13 intitulée "Les éléments". Livre 7 - 10 concerne la théorie des nombres et les trois derniers la géométrie en trois dimensions : En particulier on y trouve une discussion des célèbre cinq corps de Platon. Euclide fait (en suivant Platon) des liens mystiques entre cube, tetraèdre, octaèdre, icosaèdre et les quatre éléments terre, feu, air et eau D'après Euclide l'étude de ces liens est le but de son discours en 13 livres, donc le nom 'éléments' pour son œuvre. Le dodécaèdre, le cinquième corps, représente l'univers qui contient les quatre éléments. Ici des patrons des 5 corps de Platon, les seules polyèdres convexes et réguliers en 3 dimension ('Régulier' indique que le groupe des isométries qui conserve le polyèdre agit transitivement sur les sommets, arrêts et faces.) :

Il est vivement conseillé à l'étudiant de fabriquer et étudier ces corps de Platon.

On observe par exemple que l'on a toujours :

$$\text{sommets} - \text{côtés} + \text{faces} = 2.$$

Un célèbre découverte d'Euler (formule d'Euler 1750) qui a eu une immense influence sur le développement de la mathématique, en particulier dans notre siècle. En effet cette formule et toujours vraie pour n'importe laquelle 'subdivision' de la sphère par des polygones. Très lié est la formule

$$\text{pics} - \text{cols} + \text{vaux} = 2,$$

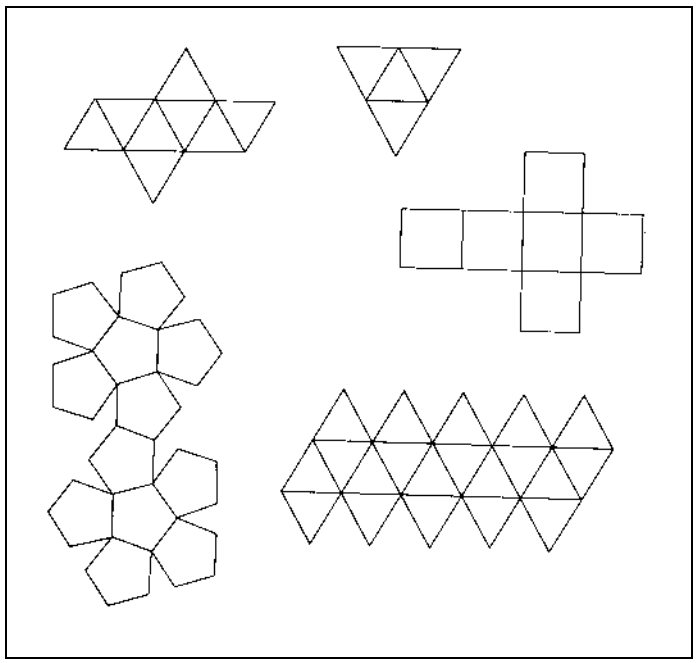


Figure 5.1: Patrons des 5 corps de Platon

par exemple sur toute planète comme Terre, Mars et Venus. Sur un île

le 2 est à remplacer par 1, sur un tore par 0. Bien sûr, dans la précision mathématique on parle des maxima, minima et points de selle des fonctions dérivables sur la sphère (Théorie de Marston Morse).

Euclide écrivait ses livres 300 a.D. On ne sait beaucoup de lui, sauf quelques anecdotes. Très célèbre la suivante : Ptolemaios (un roi célèbre) lui demandait s'il n'y a pas un chemin plus court que ses 'éléments'. Euclide répondait : "Il n'existe pas un chemin royal pour la géométrie." Les éléments étaient le centre de toute la recherche en mathématiques pendant 15 siècles et ont eu une immense influence sur le développement de la mathématique.

5.2 Arc capable

Dans cette section E désigne un plan affine euclidien orienté, i.e. nous supposons que $\overrightarrow{E}$ soit orienté. En particulier on a la notion des angles orientés

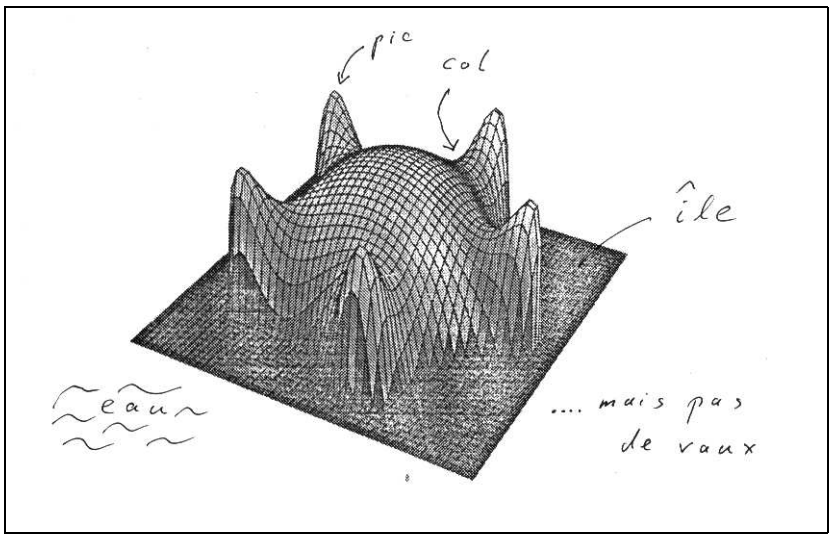


Figure 5.2: pics − cols + vaux = 1

dans $\overrightarrow{E}$.

Définition. Pour $a, b, c \in E$, $a, c \neq b$, on pose

$$\widehat{abc} := \widehat{\overrightarrow{ba}\,\overrightarrow{bc}} \qquad \text{(angle orienté)},$$
$$\angle abc := \arccos\Big[\frac{(\overrightarrow{ba}\,\overrightarrow{bc})}{ba \cdot bc}\Big] \qquad \text{(angle non-orienté)}.$$

Si on considère un angles orienté comme nombres dans $]-\pi, +\pi]$, on a

$$\angle abc = |\widehat{abc}|,$$

ce qui admets souvent de passer facilement d'un théorème concernant des angles orientés à la version non-orientée. Le mot angle sans supplément indique toujours un angle non-orienté.

On peut traduire les règles de calcul pour les angles orientés dans nos nouvelles notations. Par exemple la règle de Chasles devient :

$$\widehat{abc} = \widehat{abx} + \widehat{xbc}.$$

Une grande partie du raisonnement de la géométrie d'Euclide consiste de la comparaison des angles dans des figures comme triangle, parallélogramme etc. en utilisant le fait que les isométries (ou plus générale : les similitudes, voir section 6.1) conservent les angles non-orientés ou orientés (à signes près) :

$$\widehat{g(a)\,g(b)\,g(c)} = \det(\overrightarrow{g}) \cdot \widehat{abc}, \quad \angle g(a)\,g(b)\,g(c) = \angle abc$$

pour tout $a, b, c \in E$ et $g \in \mathrm{Isom}(E)$.

Un autre rôle important dans ce genre d'arguments est joué par les bissectrices.

Définition. La bissectrice de $\angle abc$ est l'unique droite D passant b tel que la symétrie orthogonale par rapport à D échange les rayons $b + \mathbb{R}_{\geq 0}\overrightarrow{ba}$ et $b + \mathbb{R}_{\geq 0}\overrightarrow{bc}$.

Théorème 5.1. *La bissectrice D d'un angle $\angle abc$ existe et est unique. On a $bp = b\sigma_D(p)$ pour tout p sur la droite (ba).*

Démonstration. On peut supposer que $ba = bc = 1$. On pose $D := b + \mathbb{R} \cdot \frac{\overrightarrow{ba}+\overrightarrow{bc}}{2}$, et on observe que $\overrightarrow{ca} \perp D$. Donc

$$\sigma_D(b + \lambda\overrightarrow{ba}) = \sigma_D\big(b + \lambda[\frac{\overrightarrow{ba} + \overrightarrow{bc}}{2} + \frac{\overrightarrow{ca}}{2}]\big) = b + \lambda[\frac{\overrightarrow{ba} + \overrightarrow{bc}}{2} - \frac{\overrightarrow{ca}}{2}] = b + \lambda\overrightarrow{bc}.$$

D'où l'existence et la formule de distance. Unicité : exercice. □

Un théorème de base de la géométrie d'Euclide est

Théorème 5.2. *(**Pons asinorum**) Les angles de bases dans un triangle isocèle a, b, c sont égaux. (Version orienté : $\widehat{bac} = -\widehat{bca}$.)*

Démonstration. La symétrie par rapport à la bissectrice (bb') de l'angle $\angle abc$ échange a et c car $ba = bc$ (lemme précédent). Donc $\angle bac = \angle bca$, ou bien $\widehat{bac} = -\widehat{bca}$. □

Comme illustration de cette géométrie à l'ancien nous allons montrer le théorème de l'Arc Capable.

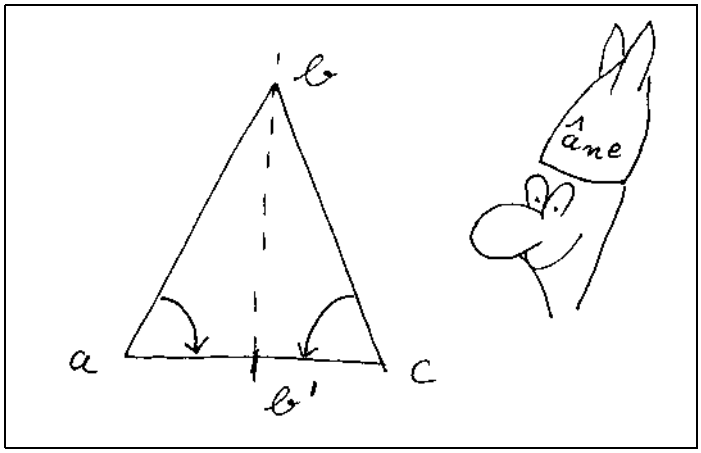


Figure 5.3: Pons asinorum

Lemme. *Soit C un cercle de centre ω dans E, $a, x \in C$, $a \neq x$, et soit y est le point sur C diamétralement opposé à x (i.e. $y = x - \overrightarrow{\omega a}$). Alors*

$$\angle a\omega y = 2\angle axy.$$

(Version orienté : $\widehat{a\omega y} = 2\widehat{axy}$.)

Démonstration.

$$\begin{aligned}
\widehat{a\omega y} &= T\widehat{(a)aT}(y) && (T = \text{translation} : \omega \mapsto a)\\
&= T\widehat{(a)a\sigma}(x) + \sigma\widehat{(x)aT}(y) && (\text{Chasles et } \sigma = \sigma_{\{a\}})\\
&= \widehat{\omega ax} + \sigma\widehat{(x)aT}(y) && (\sigma \text{ au 1er terme})\\
&= \widehat{\omega ax} + \widehat{ax\omega} && (U\text{translation} : \sigma(x) \mapsto a)\\
&= 2\widehat{ax\omega} && (\text{Pons asinorum})
\end{aligned}$$

□

Théorème 5.3. *(**Arc capable**) Soient $a, b \in C$. Alors pour tout $x \in C$, différent de a et b*

$$\angle a\omega b = 2\angle axb,$$

si les angles sont sur le même arc. (Version non orientée : Sans restriction on a pour tout $x \in C$ l'identité $\widehat{a\omega b} = 2\widehat{axb}$)

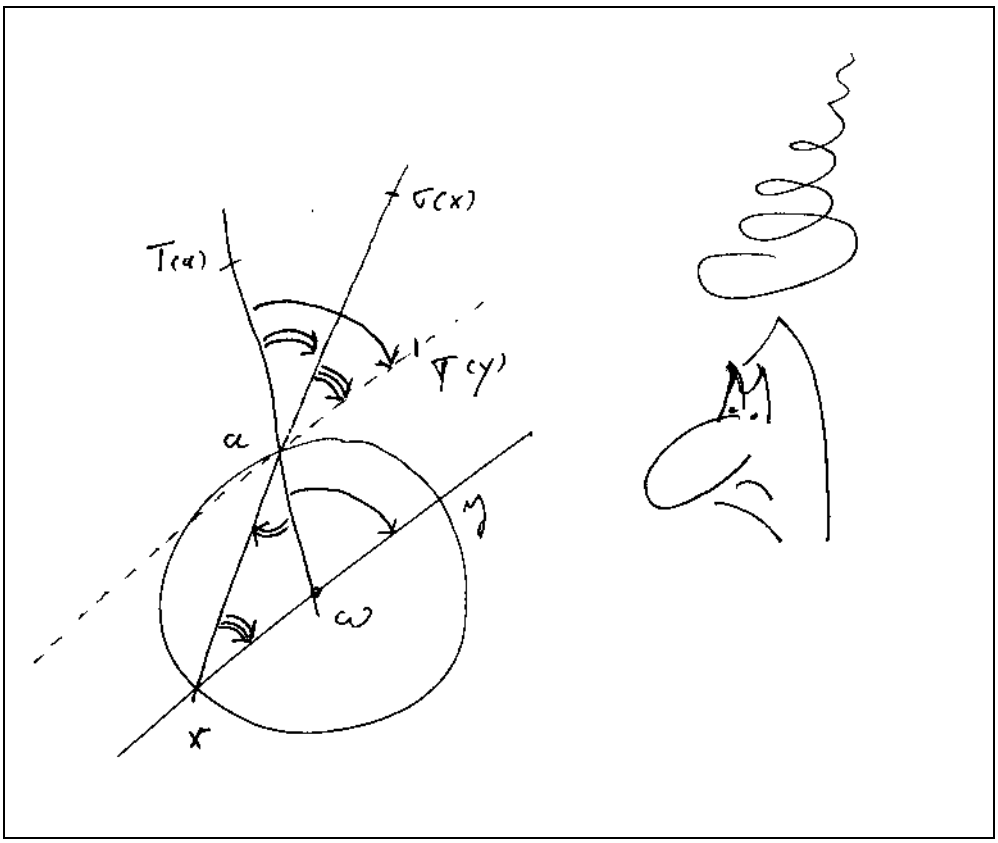


Figure 5.4: Un demi arc capable

Démonstration. Soit y le point diamétralement opposé de x. Alors, d'après le lemme, on a

$$\widehat{a\omega b} = \widehat{a\omega y} + \widehat{y\omega b} = 2\widehat{axy} + 2\widehat{yxb} = 2\widehat{axb}.$$

□

Corollaire 5.3.1. *Soient $a, b \in C$ diamétralement opposés (i.e. le centre ω et a, b sont alignés), alors pour tout $x \in C$, différent de a, b, on a*

$$\angle axb = \frac{\pi}{2}.$$

Démonstration. Clair. □

Corollaire 5.3.2. *Soient $a, b \in E$, $a \neq b$, α un angle $\neq 0$. Alors l'ensemble*

$$C = \{x \in E \,|\, 2\widehat{axb} = \alpha\}$$

est un cercle.

Remarque. Dans le cas $\alpha = 0$ on vérifie facilement que

$$\{x \,|\, 2\widehat{axb} = 0\} = (ab).$$

Lemme. *Soit D la médiatrice de a, b. Alors l'application*

$$D \ni \omega \mapsto \widehat{a\omega b} \in (-\frac{\pi}{2}, +\frac{\pi}{2}]$$

est une bijection.

Démonstration. Exercice. □

Preuve du corollaire. Chercher ω sur la médiatrice de a et b tel que $\widehat{a\omega b} = \alpha$. Poser $C' := C(\omega, \omega a)$. D'après l'arc capable on a $C' \subseteq C$. Soit réciproquement $x \in C$, $x \neq a, b$. Car $2\widehat{axb} = \alpha \neq 0$ les points a, x, b ne sont pas alignés (voir la remarque ci-dessus). Si ω' est le centre du cercle circonscrit de x, a, b, alors d'après l'arc capable

$$\widehat{a\omega' b} = 2\widehat{axb} = \widehat{a\omega b},$$

d'où $\omega' = \omega$. □

Corollaire 5.3.3. *Quatre points a, b, c, d deux à deux différents de E sont alignés ou cocycliques si et seulement si*

$$2\widehat{acb} = 2\widehat{adb}$$

Remarque. On n'est pas autorisé à supprimer le "2" ici. Il faut lire l'identité $2\widehat{acb} = 2\widehat{adb}$ comme identité dans le groupe abélien $\mathbb{R}/2\pi\mathbb{Z}$, dans lequel le morphisme "multiplication par 2" n'est pas injectif.

Démonstration. Si a, b, c sont alignés, alors d est sur la droite (a, b) si et seulement si $\widehat{adb} = 0, \pi$, i.e. si et seulement si $2\widehat{adb} = 0 = 2\widehat{acb}$.

Si a, b, c ne sont pas alignés, soit C le cercle circonscrit de a, b, c. D'après le corollaire précédent c'est l'ensemble des points x tel que $2\widehat{axb} = 2\widehat{acb}$. Donc a, b, c, d sont cocycliques si et seulement si $d \in C$, i.e. si et seulement si $2\widehat{adb} = 2\widehat{acb}$. □

Chapitre 6

Suppléments

6.1 Similitudes

Définition. Une similitude d'un espace vectoriel euclidien V (de rapport $k > 0$) est une application linéaire telle que

$$|f(x)| = k|x|$$

pour tout $x \in V$. L'ensemble des similitudes est noté $\mathrm{Sim}(V)$.

Théorème 6.1. *L'application*

$$\mathbb{R}_{>0} \times \mathrm{O}(V) \to \mathrm{Sim}(V), \quad (k, f) \mapsto k \cdot f$$

est un isomorphisme.

Démonstration. Evident. □

Remarque. L'image de $\mathbb{R}_{>0} \times \{1\}$ sous l'application du théorème est le groupe des homothéties de V avec un rapport positif, i.e. le groupe des applications de la forme $\lambda \cdot \mathrm{id}$ avec un $\lambda > 0$.

Soit maintenant E un espace affine euclidien.

Définition. On note $\mathrm{Sim}(E)$ les affinités g de E pour lesquelles il existe un $k > 0$ tel que

$$g(p)g(q) = k\,pq$$

pour tout $p, q \in E$. Les éléments de $\mathrm{Sim}(E)$ sont appelés similitude de E.

Remarque. Soit $f \in \mathrm{GA}(E)$. Alors $g \in \mathrm{Sim}(E)$ si et seulement si $\overrightarrow{g} \in \mathrm{Sim}(\overrightarrow{E})$. Les homothéties de E sont des similitudes.

Analogue aux théorèmes 2.9 et 4.14 on a

Théorème 6.2. *Soit $o \in E$. Alors*

$$V \rtimes \mathrm{Sim}(\overrightarrow{E}) \to \mathrm{Sim}(E),\ (v, F) \mapsto T_v \circ F_o).$$

est un isomorphisme de groupes.

Exercice. Soit $g\colon E \to E$ une bijection (ensembliste). Alors g est une similitude si et seulement si

$$\frac{g(p')g(q')}{g(p)g(q)} = \frac{p'q'}{pq}$$

pour tout $p, p', q, q' \in E$ tels que $p \neq q$.

Exercice. Montrer : Soit g une similitude de E, $g(p)g(q) = k\,pq$ avec un $k \neq 1$. Alors g possède un et un seul point fixe o et il existe un $\lambda \in \mathbb{R}$ ($\lambda^2 = k$) et $r \in \mathrm{O}(\overrightarrow{E})$ tel que

$$g(o + x) = o + \lambda r(x)$$

6.2 Le triangle

On fixe un triangle $T = \{p, q, r\}$ dans un plan euclidien, i.e. on fixe trois points p, q, r en position générale. On pose

$$\begin{array}{lll} A = \overrightarrow{qr}, & B = \overrightarrow{rp}, & C = \overrightarrow{pq}, \\ a = qr, & b = rp, & c = pq, \\ \alpha = \angle rpq, & \beta = \angle pqr, & \gamma = \angle qrp, \\ \overrightarrow{\alpha} = \widehat{rpq}, & \overrightarrow{\beta} = \widehat{pqr}, & \overrightarrow{\gamma} = \widehat{qrp}. \end{array}$$

Ici la notation est choisie telle que l'on a le principe universel suivant : Toute

formule qui fait un raccord des quantités ci-dessus et qui est valable pour tout

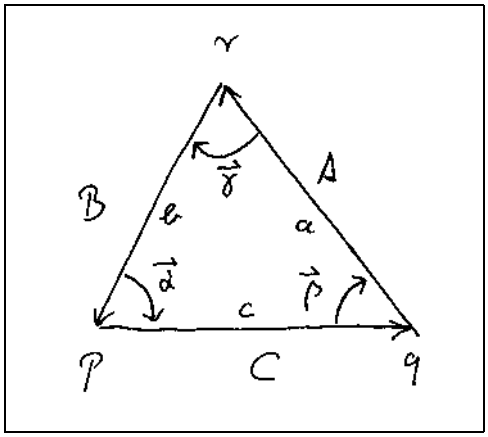


Figure 6.1: Les noms des choses

triangle reste valable si on fait une permutation cyclique des quantités dans cette formule.

Soit $T' = \{p', q', r'\}$ un autre triangle. Nous avons vu qu'il existe un $g \in \mathrm{Isom}(E)$ tel que $g(p) = p'$, $g(q) = q'$, $g(r) = r'$ si et seulement si $a = a'$, $b = b'$, $c = c'$. Ici $a' = q'r'$, $b' = r'p'$, $c' = p'q'$.

Exercice. Montrer qu'il existe un $g \in \mathrm{Sim}(E)$ tel que $g(p) = p'$, $g(q) = q'$, $g(r) = r'$ si et seulement si

$$\frac{a}{a'} = \frac{b}{b'} = \frac{c}{c'}.$$

Tous ce qu'on peut dire en générale sur les triangles euclidiens est une conséquence du fait (évident) suivant :

$$A + B + C = 0.$$

Comme exemple :

Théorème 6.3. *$\alpha + \beta + \gamma = \pi$ (Version orientée : $\overrightarrow{\alpha} + \overrightarrow{\beta} + \overrightarrow{\gamma} = \pi$).*

Démonstration.

$$\begin{aligned}\overrightarrow{\alpha} + \overrightarrow{\beta} + \overrightarrow{\gamma} &= \widehat{-B\,C} + \widehat{-C\,A} + \widehat{-A\,B} \\ &= \widehat{B\,-C} + \widehat{-C\,A} + \widehat{-A\,B} = \widehat{B\,A} + \widehat{-A\,B} = \widehat{-A\,A} = \pi.\end{aligned}$$

□

Théorème 6.4. $\cos\alpha = \dfrac{-a^2+b^2+c^2}{2bc}$.

Démonstration. C'est équivalent à $(-B,C) = -|A|^2+|B|^2+|C|^2$, i.e. $|A|^2 = |B+C|^2$, ce-qui est évident. □

Soit ω le médiateur de p,q,r. Donc ω est le point d'intersection des trois médiatrices de p,q, de q,r et de r,p, et ω est le centre du cercle circonscrit de $\{p,q,r\}$. Soit R son rayon.

Théorème 6.5. $2R = \dfrac{a}{\sin\alpha} = \dfrac{b}{\sin\beta} = \dfrac{c}{\sin\gamma}$.

Lemme. *Si* $\gamma = \frac{\pi}{2}$, *alors* $\frac{a}{c} = \sin\alpha, \quad \frac{b}{c} = \cos\alpha$.

Démonstration.

$$\cos\alpha = \frac{(-B,C)}{bc} = \frac{(B,A+B)}{bc} = \frac{b}{c},$$

$$\sin\alpha = \sqrt{1-\cos^2\alpha} = \sqrt{1-\frac{b^2}{c^2}} = \frac{a}{c},$$

où on utilise $a^2+b^2=c^2$ (Pythagore) pour la dernière identité. □

Démonstration du théorème. D'après l'arc capable $\angle r\omega q = 2\angle rpq$. Soit s le point d'intersection de la médiatrice de q,r et (qr). Car il existe une isométrie $g : \omega,q,s \mapsto \omega,r,s$ on a $\angle\omega rs = \alpha$. Car la médiatrice est perpendiculaire à (qr) le lemme implique la première formule. □

Exercice. (**Le cercle de Feuerbach ou cercle de neuf points.**) Soient p_1,q_1,r_1 les milieux des côtés A,B,C respectivement, soient p_2,q_2,r_2 les pieds des hauteurs (droites passant p,q,r et perpendiculaires sur les côtés A,B,C resp.), o l'orthocentre (points d'intersection des hauteurs), et p_3,q_3,r_3 les milieux des segments $[o,p]$, $[o,q]$ et $[o,r]$ resp. Alors les 9 points p_i,q_i,r_i $(i=1,2,3)$ sont cocycliques.

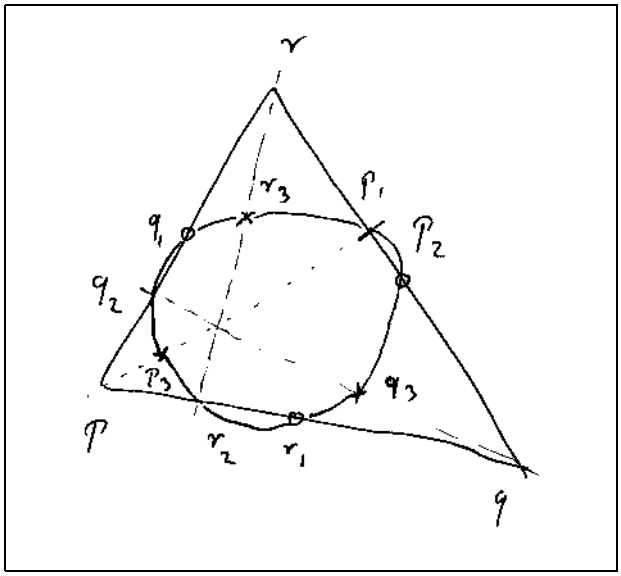


Figure 6.2: Le cercle de Feuerbach

6.3 Intersections

6.3.1 Intersection sphère — sous-espace affine

Dans un espace affine euclidien E on considère :

$$C = C_E(p, r) \text{ uen sphère}, \qquad S \subset E \text{ un sous-espace affine.}$$

Soit $p' = \hat{\pi}_S(p)$ la projection orthogonale de p sur T et $d = d(p, S) = pp'$. Alors on a :

Théorème 6.6. $C \cap S = \begin{cases} C_S\big(p', \sqrt{r^2 - d^2}\big) & si\ r \geq d \\ \emptyset & sinon \end{cases}$.

Démonstration. Exercice. □

6.3.2 Intersection sphère — sphère

Ici on considère deux sphères :

$$C_0 = C_E(p_0, r_0), \qquad C_1 = C_E(p_1, r_1)$$

telles que $p_0 \neq p_1$. On pose

$$g = \frac{1}{2}\Big(1 - \frac{r_0^2 - r_1^2}{p_0p_1^2}\Big)p_0 + \frac{1}{2}\Big(1 + \frac{r_0^2 - r_1^2}{p_0p_1^2}\Big)p_1, \quad H := \{p \in E \,|\, (\overrightarrow{gp}, \overrightarrow{p_0p_1}) = 0\}.$$

Donc H est un hyperplan orthogonal à $\overrightarrow{p_0p_1}$. On vérifie

$$r_0^2 - gp_0^2 = r_1^2 - gp_1^2,$$

en particulier

$$C_0 \cap C_1 = C_0 \cap H = C_1 \cap H$$

(car $C_0 \ni p$ si et seulement si $gp^2 + gp_0^2 - 2(\overrightarrow{gp}, \overrightarrow{gp_0}) = r_0^2$). Donc :

Théorème 6.7.

$$C_0 \cap C_1 = \begin{cases} C_H\Big(g, \sqrt{r_0^2 - gp_0^2}\Big) & \textit{si } r_0 \geq gp_0 \\ \emptyset & \textit{sinon} \end{cases}.$$

Remarque. La condition $r_0 \geq gp_0$ (ou équiv. $r_1 \geq gp_1$) est équivalent à

$$|r_0 - r_1| \leq p_0p_1 \leq r_0 + r_1.$$

6.4 Géométrie conforme

D'après l'arc capable l'application $x \mapsto 2\widehat{axb}$, où a, b sont des points différents d'un cercle et x parcours le même cercle, est constante. la vraie explication de ce phénomène (ainsi que des corollaires de la section précédente) est donné par une extension de la géométrie euclidien du plan, la géométrie conforme (ou géométrie de Moebius ou géométrie inverse; 19ème siècle) : Comme modèle pour le plan euclidien on prend $\mathbb{C}$. On peut facilement vérifier

$$\begin{aligned} \mathrm{Isom}(\mathbb{C})^+ &= \{z \mapsto az + b \,|\, a \in \mathbb{C}^*,\ |a| = 1,\ b \in \mathbb{C}\}, \\ \mathrm{Sim}(\mathbb{C})^+ &= \{z \mapsto az + b \,|\, a \in \mathbb{C}^*,\ b \in \mathbb{C}\}, \end{aligned}$$

où le "+" indique le sous-groupe des isométries respectivement similitudes g avec $\det(\overrightarrow{g}) = +1$. On obtient tout $\mathrm{Isom}(\mathbb{C})$ et $\mathrm{Sim}(\mathbb{C})$ on admettant aussi les transformations $z \mapsto a\overline{z} + b$.

Pour trois points a, b, x (deux à deux différents) on a

$$\widehat{axb} = \mathrm{Arg}\,(\frac{b-x}{a-x}),$$

où $\mathrm{Arg}(w)$, pour un nombre complexe w est l'unique classe $s + 2\pi\mathbb{Z}$ dans $\mathbb{R}/2\pi\mathbb{Z}$ tel que $w = |w| \exp(is)$.

On pose $\overline{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ avec un symbole ∞. Le résultat est appelé plan conforme. Un cercle de $\overline{C}$ est un cercle de $\mathbb{C}$, et une droite de $\overline{\mathbb{C}}$ et la réunion d'une droite de $\mathbb{C}$ avec ∞. On peut regarder les droites comme cercles passant ∞. Cette idée obtient un sens très précis si on identifie le plan conforme avec la sphère via la projection steréographique :

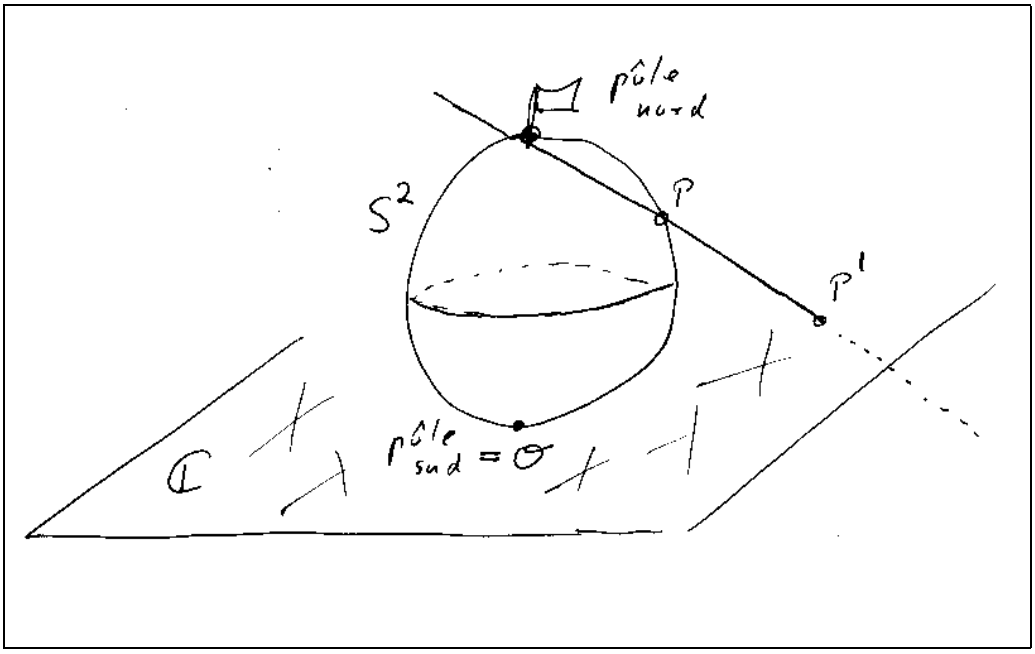


Figure 6.3: Projection stéreographique

Ici cercles sur la sphère correspond à cercles ou droites dans le plan conforme.

Toute application bijective $\overline{C} \mapsto \overline{\mathbb{C}}$ qui donne cercles et droites sur cercles ou droites et de la forme

$$z \mapsto \frac{az+b}{cz+d} \quad \text{ou} \quad z \mapsto \frac{a\overline{z}+b}{c\overline{z}+d}$$

avec $a, b, c, d \in \mathbb{C}$, $ad - bc \neq 0$. (Ici ∞ est donné sur $\frac{a}{c}$ et $-\frac{d}{c}$ et donné sur ∞, si $c \neq 0$, et sinon ∞ et donné sur ∞.) Les transformations qui fixent ∞, i.e. ceux qui ont $c = 0$ sont exactement les similitudes de $\mathbb{C}$.

Soit maintenant C un cercle à centre ω, et soient $a, b \in C$, $a \neq b$. Or

$$g : x \mapsto \frac{b-x}{a-x}$$

donne $a \mapsto 0$ et $b \mapsto \infty$. Donc $g(C)$ est une droite passant 0, donc un ensemble de la forme

$$\{y \in \mathbb{C} \mid 2 \operatorname{Arg} y = \text{const.}\} \cup \{\infty\}.$$

En particulier on obtient que donc

$$2\widehat{axb} = 2 \operatorname{Arg}\left(\frac{b-x}{a-x}\right)$$

est constant. C'est en gros le théorème de l'Arc Capable.

Les corollaires à l"arc Capable deviennent également naturels si on passe à la géométrie conforme (exercice).

6.5 Les symétries des corps de Platon

Soit C un des corps de Platon dans un espace euclidien de dimension 3. Posons

$$\operatorname{Sym}(C) = \{g \in \operatorname{Isom}(E)^+ \mid g(C) = C\}.$$

Ces sont des sous-groupes de $\operatorname{Isom}(E)$.

Pour déterminer la structure de $G := \operatorname{Sym}(T)$ pour un tetraèdre T on considère l'action de G sur l'ensemble S des quatre sommets du tetraèdre. Cette action nous donne le morphisme

$$G \to \operatorname{Perm}(S) \approx S_4, \quad g \mapsto g|_S.$$

Car les sommets forme un repère affine de E ce morphisme est injectif. En particulier, G est fini. L'action de G sur T est transitive. D'après la formule de classes donc

$$4 = \frac{|G|}{|G_a|}$$

où a est un sommet et G_a le stabilisateur de a dans G, Chaque élément de G laisse invariant l'équibarycentre b de T. En particulier, tout élément de G_a laisse invariant point par point la droite (ab), et est donc une rotation autour de ce droite. Evidemment il en existe exactement 3 rotations autour de (ab) dans G. Donc : $|G_a| = 3$ et $|G| = 12$. Il en existe un seul sous-groupe d'ordre 12, i.e. d'indice 2, dans S_4; c'est A_4 (pour la démonstration utiliser qu'un tel sous-groupe, étant distingué, ne contient aucune transposition). Nous pouvons dire en conséquence :

Théorème 6.8. Sym(*tetraèdre*) $\approx A_4$.

Exercice. Montrer par un raisonnement analogue que Sym(cube) $\approx S_4$, Sym(octaèdre) $\approx S_4$, Sym(dodécaèdre) $\approx A_5$, Sym(icosaèdre) $\approx A_5$. Pour le cube, par exemple, laisser agir le groupe des symétries sur les quatre diagonales principales du cube.

Que les groupes du cube et du octaèdre sont égaux n'est pas accidentel : Les quatre milieux des faces du cube sont des sommets d'un octaèdre. C'est pareil pour l'icosaèdre et le dodécaèdre.

On peut montrer que tout sous-groupe fini de O(3) est soit cyclique, soit diédral, soit le groupe des symétries d'un corps de Platon dans $\mathbb{R}^3$ avec équibarycentre en 0.

Quelques livres

Ici une courte liste de livres qui m'étaient utiles quand j'ai préparé les cours.

Berger, Marcel Géométrie tome 1, nouvelle édition. — Fernand Nathan, 1990.

Berger, Marcel Géométrie tome 2, nouvelle édition. — Fernand Nathan, 1990.

Cohen, Henri Algèbre élémentaire, polycopié, Bordeaux 1994.

Coxeter, Harold S.M. Unvergängliche Geometrie. Birkhäuser, 1963.

Coxeter, Harold S.M. Introduction to geometry. 2nd edition. — John Wiley and Sons, 1969.

Fresnel, Jean Géométrie, 1993. Polycopié Université de Bordeaux 1, réédition d'un cours enseigné aux étudiants de la maîtrise de math. de Bordeaux pendant les années scolaires 1981-83. - Université de Bordeaux, 1993.

Lang, Serge Algebra. 3d edition. — Addison Wesley, 1994.

Index