UNIVERSITÉ TOULOUSE III PAUL SABATIER Université de Toulouse

Sur le troisième problème de Hilbert

Anthony SAINT-CRIQ

Encadré par Joseph TAPIA

Sommaire

Introduction

Lors du deuxième congrès international de mathématiques, tenu à Paris en 1900, David Hilbert présenta une sélection de vingt-trois problèmes, dans le but de diriger la recherche et d'occuper les mathématiques pour le siècle à venir. Une sorte de problèmes du millénaire de l'époque.

Celui dont il sera question ici est le troisième de cette liste. Il fut par ailleurs le premier à être résolu, en 1902, mais fut l'objet de plusieurs poursuites. Il a été formulé de la manière suivante par Hilbert :

Étant donnés deux polyèdres de même volume, est-il possible de découper le premier polyèdre en des polyèdres et de les rassembler pour former le second polyèdre ?

En effet, le résultat est connu comme étant vrai dans le cas des polygones, et ce depuis 1807 (théorème de Wallace-Bolyai-Gerwien). La réponse est alors offerte par Max Dehn, élève de Hilbert, en 1902, et confirme la conjecture de ce dernier, en exhibant un contre-exemple pour lequel cela ne fonctionne pas.

Pour ce faire, il a construit une application appelée *invariant*, c'est-à-dire une application vérifiant une propriété d'additivité, et donc en particulier, invariante par découpage. Par la contraposée, cette application, appelée *invariant de Dehn*, diffère pour un tétraèdre régulier et un cube de même volume, donc il ne sera pas possible de découper l'un pour se ramener sur l'autre.

Nous tâcherons de donner un sens à la notion de découpage, et même à la notion de polyèdre, puis nous définirons, à l'aide des outils de l'algèbre, le concept d'*invariant*. Par des détours d'algèbre et d'algèbre linéaire, nous en viendrons à observer la construction de Dehn, en s'appuyant sur les angles dièdres, pour exhiber le contre-exemple.

1 Formalisme des polytopes

Dans cette partie, on s'efforce de construire formellement la notion de polyèdre (et plus généralement de polytope de $\mathbb{R}^n$, la construction ne coûtant pas plus à mettre en évidence), ainsi que de définir convenablement ce que l'on entend par *découpages* de polyèdres. Ces notions, conjuguées à la définition de volume, nous mèneront à définir ce qu'est un invariant sur le $\mathbb{Z}$-module des polytopes.

1.1 Complexes simpliciaux, polytopes

Fixons $n \in \mathbb{N}$, $n \geqslant 2$, et travaillons dans $\mathbb{R}^n$.

On prendra la convention que si $k = 0$, alors $\dim \mathrm{Vect}(v_1 - v_0, ..., v_k - v_0) = 0$.

Définition :

Un k-**simplexe**, $k \in [\![0, n]\!]$, est une partie $\mathbf{T} \subset \mathbb{R}^n$ donnée par :

$$\mathbf{T} = co(u_0, ..., u_k)$$

où $u_0, ..., u_k$ sont $k+1$ vecteurs de $\mathbb{R}^n$ tels que $\dim \mathrm{Vect}(u_1 - u_0, ..., u_k - u_0) = k$, et où $co(X)$ désigne l'enveloppe convexe de $X \subset \mathbb{R}^n$. L'entier k est appelé **rang** du simplexe $\mathbf{T}$, et on note alors $\mathrm{rg}(\mathbf{T}) = k$.

On rappelle que pour une partie $X \subset \mathbb{R}^n$, on note

$$co(X) = \left\{ \sum_{i=1}^{r} \lambda_i x_i,\ r \in \mathbb{N}^\star,\ \lambda_i \in [0,1] \text{ tels que } \lambda_1 + ... + \lambda_r = 1,\ x_i \in X \right\}$$

l'enveloppe convexe de X, formée de l'ensemble des combinaisons convexes de vecteurs de X. Si X est fini, on note alors $co(x_1, ..., x_{|X|})$ cette enveloppe convexe. Dans ce cas, on peut, quitte à demander à certains λ_i d'être nuls, prendre $r = |X|$ constamment dans la définition de $co(X)$.

On a, pour $X \subset \mathbb{R}^n$ quelconque :

$$X \text{ convexe } \iff X = co(X)$$

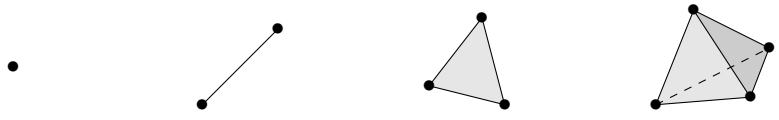
En particulier, toutes les enveloppes convexes sont elles-même convexes.

Dans le cas $X \subset \mathbb{R}^n$ infini, on a en réalité :

$$co(X) = \left\{ \sum_{i=1}^{n+1} \lambda_i x_i,\ \lambda_i \in [0,1] \text{ tels que } \lambda_1 + ... + \lambda_{n+1} = 1,\ x_i \in X \right\}$$

Ce résultat ne nous servant pas, il ne sera pas démontré.

Voici quelques prototypes de simplexes pour $k \in [\![0, 3]\!]$:



$\mathrm{rg}(\mathbf{T}) = 0$ $\mathrm{rg}(\mathbf{T}) = 1$ $\mathrm{rg}(\mathbf{T}) = 2$ $\mathrm{rg}(\mathbf{T}) = 3$

Afin de parler de complexes simpliciaux (*ie* les objets qui donneront naissance à la notion de polytope), il nous faut parler des faces d'un simplexe :

Définition :

Une **face** du simplexe $\mathbf{T}$ est une partie $F \subset \mathbf{T}$ donnée par :

$$F = co\left((u_i)_{i\in I}\right)$$

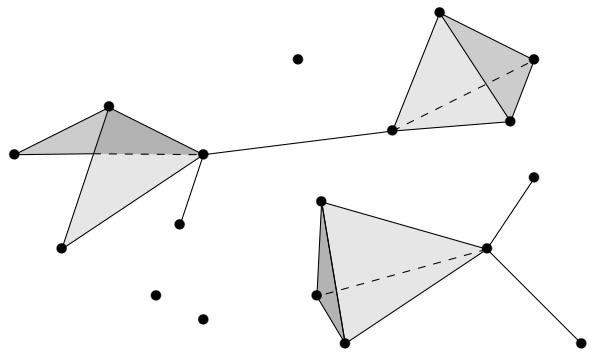
où I est une partie stricte et non vide de $[\![0, k]\!]$. On note $\mathcal{F}(\mathbf{T})$ l'ensemble des faces du simplexe $\mathbf{T}$. On notera $\mathcal{F}_\ell(\mathbf{T})$ l'ensemble des faces de rang ℓ de $\mathbf{T}$, $\ell \in [\![0, k-1]\!]$.

Ainsi, on peut enfin en venir à la définition de complexes simpliciaux, à savoir ce que l'on entend formellement par polytope :

Définition :

Un **complexe simplicial** est une famille **finie** $\mathcal{K}$ de simplexes telle que :
- si $\mathbf{T} \in \mathcal{K}$, alors $\mathcal{F}(\mathbf{T}) \subset \mathcal{K}$
- si $\mathbf{T}_1 \in \mathcal{K}$ et $\mathbf{T}_2 \in \mathcal{K}$ sont deux simplexes tels que $\mathbf{T}_1 \cap \mathbf{T}_2 \neq \varnothing$, alors $\mathbf{T}_1 \cap \mathbf{T}_2 \in \mathcal{K}$

Ces deux propriétés permettent d'assurer que l'on obtient une collection d'objets polytopiaux ne se touchant qu'en des sommets, arêtes, faces, etc... Voici un exemple dans $\mathbb{R}^3$:



Les complexes simpliciaux auront la propriété de générer des polytopes s'ils ont certaines "bonnes" propriétés.

- On dit que le complexe $\mathcal{K}$ est **non dégénéré** si pour tout simplexe $\mathbf{T} \in \mathcal{K}$, soit $\mathrm{rg}(\mathbf{T}) = n$, soit $\mathbf{T}$ est une face d'un simplexe de rang n, *ie* : $\exists \mathbf{T}' \in \mathcal{K}$ / $\mathrm{rg}(\mathbf{T}') = n$ et $\mathbf{T} \in \mathcal{F}(\mathbf{T}')$.

  C'est dire que l'on a des *vrais* simplexes, et non pas des choses "plates", *ie* de dimension strictement inférieure.

- Un complexe simplicial $\mathcal{K}$ est dit **polytopial** s'il est non dégénéré, et si $\bigcup_{\mathbf{T}\in\mathcal{K}} \mathbf{T}$ est d'intérieur connexe.

  Cette fois-ci, c'est dire que les simplexes se touchent réellement, et non pas par des objets de dimension trop petite (*ie* dans $\mathbb{R}^3$, des sommets ou des arêtes). Outre le fait d'obtenir des polytopes "en un seul morceau", on évite le cas dégénéré des polygones croisés (le nœud papillon) et leurs analogues polytopiaux.

Étant donné un complexe polytopial $\mathcal{K}$, on notera, pour $\ell \in [\![0, n]\!]$:

$$\mathcal{K}_\ell := \{\mathbf{T} \in \mathcal{K} \ / \ \mathrm{rg}(\mathbf{T}) = \ell\} \subset \mathcal{K}$$

l'ensemble des simplexes de rang ℓ de $\mathcal{K}$.

On peut à présent définir les polytopes de $\mathbb{R}^n$:

Définition :

Définissons deux familles de parties de $\mathbb{R}^n$:

- On appelle **polytope** toute partie $\mathbf{P} \subset \mathbb{R}^n$ telle que $\mathbf{P} = \bigcup_{\mathbf{T}\in\mathcal{K}} \mathbf{T} = \biguplus_{\mathbf{T}\in\mathcal{K}_n} \mathbf{T}$ pour $\mathcal{K}$ un complexe polytopial.
- On appelle **polytope dégénéré** toute partie $\mathbf{X}$ de $\mathbb{R}^n$ telle que $\mathbf{X} = \bigcup_{\mathbf{T}\in\mathcal{L}} \mathbf{T}$ pour $\mathcal{K}$ un complexe polytopial et $\mathcal{L} \subset \mathcal{K} \setminus \mathcal{K}_n$ une sous-famille de celle des faces dégénérées de $\mathcal{K}$.

On notera $\wp_n$ l'ensemble de toutes les parties de $\mathbb{R}^n$ de l'un de ces deux sortes.

Les polytopes ont donc la bonne propriété d'être des parties compactes de $\mathbb{R}^n$, et d'intérieur connexe et non vide. En revanche, si $\mathbf{X}$ est un polytope dégénéré, en particulier, $\mathbf{X}$ n'est **pas** un polytope, puisque $\mathbf{X}$ est alors d'intérieur vide (car inclus dans une réunion **finie** de parties toutes incluses dans des hyperplans affines). En outre, les "faces" d'un polytope (pourvu que l'on les définisse) sont des polytopes dégénérés.

$\wp_n$ possède la propriété d'être stable par unions et intersections finies, ainsi que par différences finies. On commettra cependant l'abus d'appeler "polytope" tout élément de $\wp_n$, et de préciser "dégénéré" ou "non dégénéré" le cas échéant.

1.2 Équivalence par congruence, équivalence par adjonction, théorème de Zylev

Étant donné deux polytopes $\mathbf{P}, \mathbf{Q} \in \wp_n$ non dégénérés, on dit que $\mathbf{P}$ et $\mathbf{Q}$ sont **congrus**, que l'on note $\mathbf{P} \cong \mathbf{Q}$, s'il est possible de ramener l'un sur l'autre par découpages et déplacements successifs. Plus formellement :

Définition :

On dit que deux polytopes $\mathbf{P}, \mathbf{Q} \in \wp_n$ non dégénérés sont **congrus** s'il existe :

- $\mathcal{K}$ et $\mathcal{K}'$ deux complexes polytopiaux tels que $\mathbf{P} = \bigcup_{\mathbf{T}\in\mathcal{K}_n} \mathbf{T}$ et $\mathbf{Q} = \bigcup_{\mathbf{T}'\in\mathcal{K}'_n} \mathbf{T}'$.
- $\Phi : \mathcal{K}_n \to \mathcal{K}'_n$ bijective telle que pour tout $\mathbf{T} \in \mathcal{K}_n$, il existe $\varphi_{\mathbf{T}} : \mathbb{R}^n \to \mathbb{R}^n$ isométrie affine telle que $\varphi_{\mathbf{T}}(\mathbf{T}) = \Phi(\mathbf{T})$ et telle que $\det\varphi_{\mathbf{T}} > 0$.

On rappelle qu'une application $f : E \to F$ entre deux espaces vectoriels est **affine** s'il existe un vecteur $u \in F$ (alors unique) et une application linéaire $\ell : E \to F$ (alors unique aussi) de sorte que $f(x) = \ell(x) + u$ pour tout $x \in E$. On définit alors son rang, son déterminant, etc... comme le rang, le déterminant etc... de l'application linéaire ℓ. En particulier, une isométrie affine est la composée d'une translation avec une isométrie linéaire.

Cela définit alors une relation d'équivalence sur l'ensemble des polytopes. Moins formellement cette fois, c'est dire que l'on peut décomposer $\mathbf{P}$ et $\mathbf{Q}$ en réunion de simplexes tous superposables deux à deux. La condition $\det\varphi_{\mathbf{T}} > 0$ signifie que l'isométrie ne renverse pas l'orientation, *ie* qu'on ne symétrise pas les simplexes.

Cependant, cette condition est superflue, comme le montre la proposition suivante :

Proposition :

Si $\mathbf{T}, \mathbf{T}' \in \wp_n$ sont deux simplexes (non dégénérés) isométriques, *ie* $\mathbf{T} = \varphi(\mathbf{T}')$ avec $\varphi : \mathbf{T} \to \mathbf{T}'$ isométrie, alors $\mathbf{T} \cong \mathbf{T}'$, en le sens précédemment défini.

Preuve : soient donc $\mathbf{T}, \mathbf{T}' \in \wp_n$ deux simplexes, et soit $\varphi : \mathbf{T} \to \mathbf{T}'$ une isométrie. Supposons que $\det\varphi < 0$, autrement le problème est déjà résolu. Alors soit $s : \mathbb{R}^n \to \mathbb{R}^n$ une symétrie vectorielle hyperplane. Il existe donc $\psi : s(\mathbf{T}) \to \mathbf{T}'$ isométrie telle que $\det\psi > 0$.

Ainsi, il faut et il suffit de démontrer que tout simplexe $\mathbf{T}$ est congru à son symétrique $s(\mathbf{T})$.

- Prouvons pour commencer l'existence d'une (en fait, de l'unique) hypersphère inscrite d'un simplexe. Soit $\mathbf{T} = co(u_0, ..., u_n)$ un simplexe de $\mathbb{R}^n$, et posons pour $i \in [\![0, n]\!]$:

$$F_i = co(u_0, ..., u_{i-1}, u_{i+1}, ..., u_n)$$

  la $(n-1)$-face de $\mathbf{T}$ qui ne contient pas u_i. On cherche à montrer l'existence d'un point $m \in \overset{\circ}{\mathbf{T}}$ tel que $d(m, F_0) = ... = d(m, F_n) = r$ une constante. On peut, sans perte de généralité, supposer $u_0 = 0$, quitte à translater $\mathbf{T}$ et à re-numéroter les sommets.

  Si $i \neq 0$, alors $u_0 = 0 \in F_i$. On considère $H_i = \mathrm{Vect}(F_i)$ l'hyperplan vectoriel qui contient la face F_i. On pose $b_0 = \dfrac{u_1 + ... + u_n}{n}$ l'isobarycentre de $u_1, ..., u_n$. On a alors $b_0 \in F_0$; on peut considérer $H_0 = \mathrm{Vect}(F_0 - b_0)$ l'hyperplan vectoriel parallèle à la face F_0. Ces deux derniers sont strictement parallèles (*ie* ne s'intersectent pas), car $0 \notin F_0$, puisque $\mathbf{T}$ est un simplexe.

  Chaque H_i est donc un hyperplan vectoriel ($i \in [\![0, n]\!]$), donc les supplémentaires $H_i^\perp$ sont des droites. Il existe donc deux vecteurs $k_i \in H_i^\perp$ tels que $\|k_i\| = 1$ qui sont tels que $H_i = \{x \in \mathbb{R}^n \ / \ \langle k_i | x \rangle = 0\}$. Choisissons un des deux k_i pour chaque $i \in [\![0, n]\!]$:

  * Si $i = 0$, alors $u_1 - b_0, ..., u_n - b_0 \in H_0$, donc $\langle k_0 | u_1 - b_0 \rangle = ... = \langle k_0 | u_n - b_0 \rangle = 0$. Ainsi, on a :

$$\langle k_0 | u_1 \rangle = ... = \langle k_0 | u_n \rangle = \langle k_0 | b_0 \rangle$$

    Choisissons donc l'unique k_0 tel que $\langle k_0 | b_0 \rangle \geqslant 0$. Or $b_0 \notin H_0$, donc $\langle k_0 | b_0 \rangle \neq 0$, *ie* : $\langle k_0 | b_0 \rangle > 0$.

  * Si $i \in [\![1, n]\!]$, alors : $\langle k_i | u_0 \rangle = ... = \langle k_i | u_{i-1} \rangle = \langle k_i | u_{i+1} \rangle = ... = \langle k_i | u_, \rangle = 0$. Or $u_i \notin F_i$, donc $u_i \notin H_i$, et donc $\langle k_i | u_i \rangle \neq 0$. On peut alors choisir de manière unique k_i tel que $\langle k_i | u_i \rangle > 0$.

Posons alors :

$$r := \frac{\langle k_0|b_0\rangle}{1+\sum_{j=1}^{n}\frac{\langle k_0|b_0\rangle}{\langle k_j|u_j\rangle}} > 0$$

et posons, pour $i \neq 0$:

$$\theta_i := \frac{r}{\langle k_i|u_i\rangle} > 0$$

En particulier, on a : $\theta_1 + ... + \theta_n = \dfrac{\sum_{j=1}^{n}\frac{\langle k_0|b_0\rangle}{\langle k_j|u_j\rangle}}{1+\sum_{j=1}^{n}\frac{\langle k_0|b_0\rangle}{\langle k_j|u_j\rangle}} < 1$. On pose alors : $\theta_0 := 1 - (\theta_1 + ... + \theta_n)$. En particulier, on a donc : $\theta_0 + ... + \theta_n = 1$. Posons enfin :

$$m := \sum_{j=0}^{n}\theta_j u_j$$

Puisque m est défini en coordonnées barycentriques avec des coordonnées **toutes** non nulles, m est dans l'intérieur de l'enveloppe convexe des u_i, à savoir $m \in \overset{\circ}{\mathbf{T}}$.

On déduit de plus que pour tout $i \in [\![0, n]\!]$, le projeté orthogonal $p_{F_i}(m)$ de m sur l'hyperplan affine contenant la face F_i est en réalité **sur** la face F_i. Si $i \neq 0$ cette fois, on a de plus : $p_{F_i}(m) = p_{H_i}(m)$.

Ensuite, on a : $d(m, F_i) = \|m - p_{F_i}(m)\|$ par le théorème de projection sur un convexe fermé. Finalement, puisque les applications p_{H_i} sont des projections orthogonales linéaires (et non affines), on a : $m - p_{H_i}(m) = p_{H_i^\perp}(m) = \langle k_i|m\rangle k_i$.

Passons aux vérifications :

* Pour $i \neq 0$, on a :

  $$d(m, F_i) = \|m - p_{F_i}(m)\| = \|p_{F_i^\perp}(m)\| = \|\langle k_i|m\rangle k_i\| = |\langle k_i|m\rangle| \qquad \text{car } \|k_i\| = 1$$

  Et on a :

  $$\begin{aligned}\langle k_i|m\rangle &= \left\langle k_i \middle| \sum_{j=0}^{n}\theta_j u_j \right\rangle = \sum_{j=0}^{n}\theta_j u\langle k_i|u_j\rangle \\ &= \theta_i\langle k_i|u_i\rangle \qquad \text{car } \langle k_i|u_j\rangle = 0 \text{ si } i \neq j \\ &= \frac{r}{\langle k_i|u_j\rangle}\langle k_i|u_j\rangle = r\end{aligned}$$

* Cette fois, si $i = 0$, on a :

  $$\begin{aligned}d(m, F_0) &= d(m - b_0, F_0 - b_0) = d(m - b_0, H_0) = \|(m - b_0) - p_{H_0}(m - b_0)\| \\ &= \|p_{H_0^\perp}(m - b_0)\| = \|\langle k_0|m - b_0\rangle k_0\| = |\langle k_0|m - b_0\rangle|\end{aligned}$$

Et d'un autre côté, on a :

$$\begin{aligned}
\langle k_0|m-b_0\rangle &= \langle k_0|m\rangle - \langle k_0|b_0\rangle \\
&= \left\langle k_0 \middle| \sum_{j=0}^{n} \theta_j u_j \right\rangle - \langle k_0|b_0\rangle \\
&= \sum_{j=0}^{n} \theta_j u \langle k_0|u_j\rangle - \langle k_0|b_0\rangle \\
&= (\theta_1 + ... + \theta_n - 1)\langle k_0|b_0\rangle \\
&\qquad\qquad \text{car } u_0 = 0 \implies \langle k_0|u_0\rangle = 0 \text{ et car } \langle k_0|u_1\rangle = ... = \langle k_0|u_1\rangle = \langle k_0|b_0\rangle \\
&= \left[\frac{\displaystyle\sum_{j=1}^{n} \frac{\langle k_0|b_0\rangle}{\langle k_j|u_j\rangle}}{\displaystyle 1 + \sum_{j=1}^{n} \frac{\langle k_0|b_0\rangle}{\langle k_j|u_j\rangle}} - 1 \right] \langle k_0|b_0\rangle = \left[\frac{-1}{\displaystyle 1 + \sum_{j=1}^{n} \frac{\langle k_0|b_0\rangle}{\langle k_j|u_j\rangle}} \right] \langle k_0|b_0\rangle = -r
\end{aligned}$$

Donc on obtient finalement : $d(m, F_0) = |-r| = r$.

On a donc bien vérifié :

$$m \in \overset{\circ}{\mathbf{T}} \qquad \text{et} \qquad d(m, F_0) = ... = d(m, F_n) = r$$

autrement dit, m est le centre de l'hypersphère inscrite à $\mathbf{T}$, et r et le rayon de cette hypersphère inscrite.

- Montrons maintenant que tout simplexe est congru à son symétrique.

  Soit $\mathbf{T}$ un simplexe, et soit $s(\mathbf{T})$ son symétrique pour s symétrie vectorielle hyperplane. On cherche à découper $\mathbf{T}$ et $s(\mathbf{T})$ en simplexes tous isométriques avec des isométries à déterminant positif. Plus précisément, on va découper $\mathbf{T}$ en plusieurs polytopes (et non des simplexes) qui seront tous symétriques à eux-même. Ce même découpage effectué sur $s(\mathbf{T})$ permettra de conclure à l'aide de la propriété suivante de la congruence :

$$\Big(\mathbf{P} = \mathbf{P}_1 \uplus ... \uplus \mathbf{P}_\ell,\ \mathbf{Q} = \mathbf{Q}_1 \uplus ... \uplus \mathbf{Q}_n \quad \text{et} \quad \mathbf{P}_i \cong \mathbf{Q}_i\Big) \implies \mathbf{P} \cong \mathbf{Q}$$

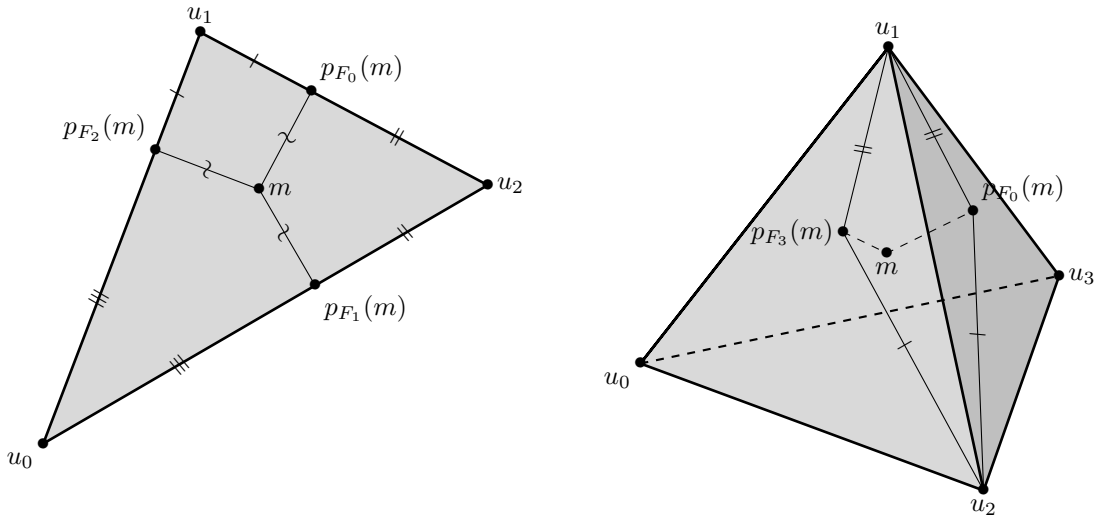
  On écrit donc $\mathbf{T} = co(u_0, ..., u_n)$, et on note m le centre de l'hypersphère inscrite à $\mathbf{T}$.

  En utilisant les notations précédentes, on va montrer que les projections orthogonales de m sur les faces sont équidistantes des sommets de la sous-face commune aux deux. Autrement dit, on cherche à montrer que si $i_0 \in [\![0, n]\!] \setminus \{i_1, i_2\}$ pour $i_1 \neq i_2$, alors $\|u_{i_0} - p_{F_{i_1}}(m)\| = \|u_{i_0} - p_{F_{i_2}}(m)\|$.

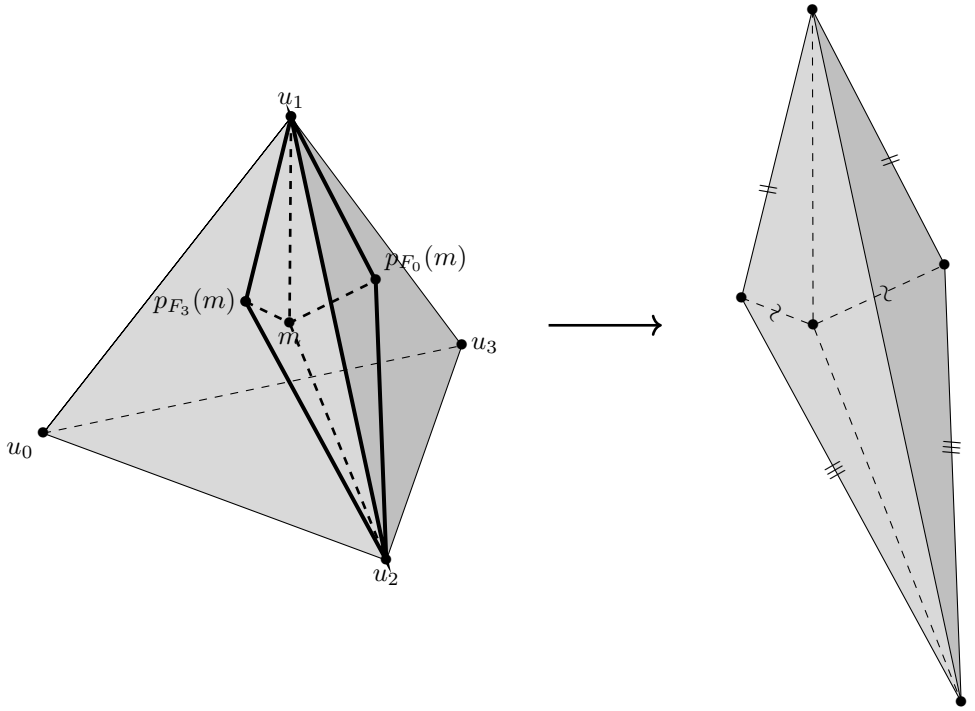
  En effet, on avait trouvé : $p_{F_i}(m) = m - p_{F_i^\perp}(m) = m - \langle k_i|m\rangle k_i$, et puisque $\langle k_i|m\rangle = r$, alors on a : $p_{F_i^\perp}(m) = rk_i$. De plus, on rappelle que $\langle k_i|u_j\rangle = 0$ si $i \neq j$. On peut alors effectuer un calcul direct :

$$\begin{aligned}
\|u_{i_0} - p_{F_{i_1}}(m)\|^2 &= \|u_{i_0} - m + rk_i\|^2 = \|u_{i_0} - m\|^2 + r^2 + 2r\langle u_{i_0} - m|k_{i_1}\rangle \\
&= \|u_{i_0} - m + rk_i\|^2 = \|u_{i_0} - m\|^2 + r^2 + 2r\underbrace{\langle u_{i_0}|k_{i_1}\rangle}_{=0} - 2r\underbrace{\langle m|k_{i_1}\rangle}_{=r} \\
&= \|u_{i_0} - m\|^2 - r^2 \\
&= \|u_{i_0} - p_{F_{i_2}}(m)\| \qquad \text{en remontant les calculs}
\end{aligned}$$

  Plus précisément, ce calcul nous permet de coder le dessin suivant avec les égalités de longueur (pour des raisons pratiques évidentes, on se contentera des dimensions 2 et 3) :



Il est donc possible de découper le simplexe en $\binom{n+1}{n-1} = \binom{n+1}{2}$ polytopes (autant qu'il y a d'arêtes ; une arête correspondant à un point dans $\mathbb{R}^2$, un segment dans $\mathbb{R}^3$, un triangle dans $\mathbb{R}^4$, *etc*...) de la manière suivante :



Finalement, par les égalités entre longueurs faites auparavant et par des considérations géométriques, il est rapide de voir que chacun de ces polytopes est symétrique avec lui-même, et que l'hyperplan affine de symétrie

(droite si $n = 2$, plan si $n = 3$, *etc...*) est donné par celui qui passe par le point m et l'arête de $\mathbf{T}$ contenue dans ce polytope. Par exemple, sur le dessin précédent, le plan affine de symétrie est celui qui contient $[u_1, u_2]$ et qui passe par m.

En conclusion, en utilisant cette décomposition en plusieurs polytopes symétriques, on obtient bien la propriété souhaitée.

Par conséquent, si on a un découpage de deux polytopes en des simplexes isométriques, quitte à re-découper ces simplexes en découpages plus fins, on peut toujours se ramener à des isométries positives. On a donc :

Proposition :

Si $\mathbf{P}, \mathbf{Q} \in \wp_n$ sont deux polytopes non dégénérés, alors $\mathbf{P} \cong \mathbf{Q} \iff \mathbf{P} = \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_k$, $\mathbf{Q} = \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_k$ avec $\mathbf{T}_i$ et $\mathbf{S}_i$ des simplexes isométriques pour tout $i \in [\![1, k]\!]$.

On définit maintenant la congruence **par adjonction**, notée $\mathbf{P} \cong_+ \mathbf{Q}$, par :

$$\mathbf{P} \cong_+ \mathbf{Q} \text{ s'il existe } \mathbf{A}, \mathbf{B} \text{ deux polytopes } \textbf{congrus} \text{ tels que } (\mathbf{P} \uplus \mathbf{A}) \cong (\mathbf{Q} \uplus \mathbf{B})$$

C'est dire que les polytopes sont congrus si on rajoute à chacun un morceau polytopial, et que ces deux morceaux sont semblables. Il est donc immédiat que si $\mathbf{P} \cong \mathbf{Q}$, alors $\mathbf{P} \cong_+ \mathbf{Q}$. En effet, il suffit de rajouter le même simplexe aux deux. En revanche, ce qui est moins évident est le résultat suivant, dû à Zylev (1965) :

Théorème de Zylev :

Si $\mathbf{P}, \mathbf{Q} \in \wp_n$ sont deux polytopes non dégénérés, alors :

$$\mathbf{P} \cong \mathbf{Q} \iff \mathbf{P} \cong_+ \mathbf{Q}$$

Preuve : démontrons une étape intermédiaire, et travaillons par récurrence.

- On suppose que $\mathbf{P} \uplus \mathbf{T} \cong \mathbf{Q} \uplus \mathbf{T}$ pour $\mathbf{P}, \mathbf{Q} \in \wp_n$ et $\mathbf{T}$ un simplexe. On veut obtenir $\mathbf{P} \cong \mathbf{Q}$. On écrit :

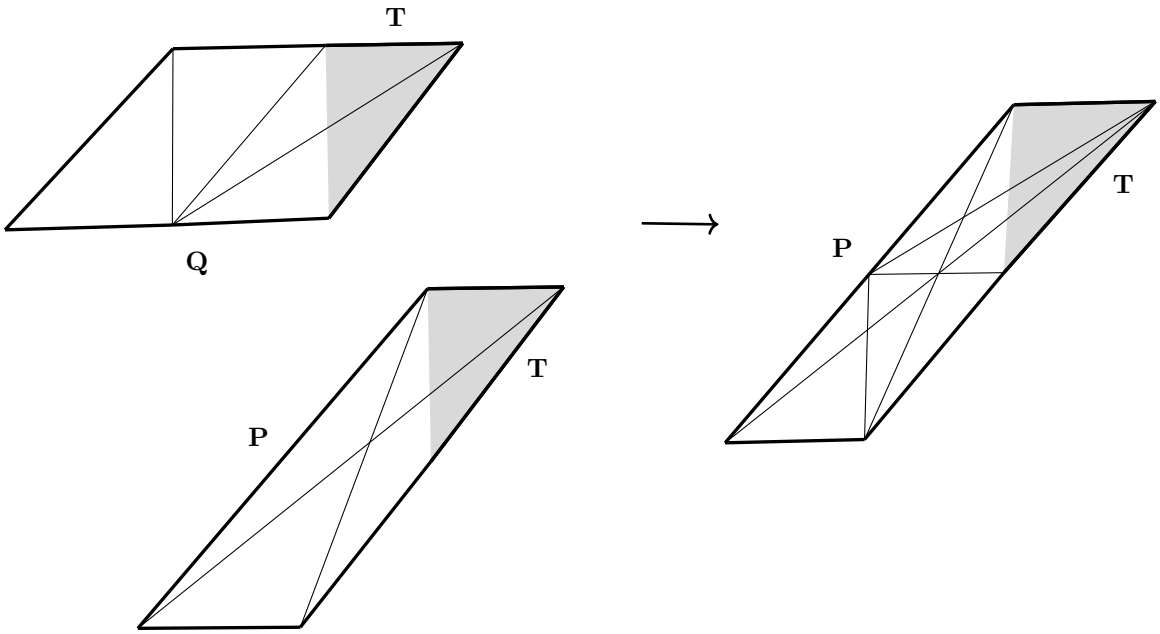
$$\begin{cases} \mathbf{P} \uplus \mathbf{T} = \mathbf{A}_1 \uplus ... \uplus \mathbf{A}_r \\ \mathbf{Q} \uplus \mathbf{T} = \mathbf{B}_1 \uplus ... \uplus \mathbf{B}_r \end{cases} \quad \text{où } \mathbf{A}_i, \mathbf{B}_j \text{ simplexes tels que } \mathbf{A}_i = \varphi_i(\mathbf{B}_i) \text{ pour } \varphi_i \text{ isométrie}$$

  En ramenant chaque $\mathbf{B}_j$ sur $\mathbf{P} \uplus \mathbf{T}$ *via* φ_j, on peut superposer la triangulation de $\mathbf{Q} \uplus \mathbf{T}$ sur celle de $\mathbf{P} \uplus \mathbf{T}$ en déplaçant chaque morceau à l'aide de l'isométrie correspondante.

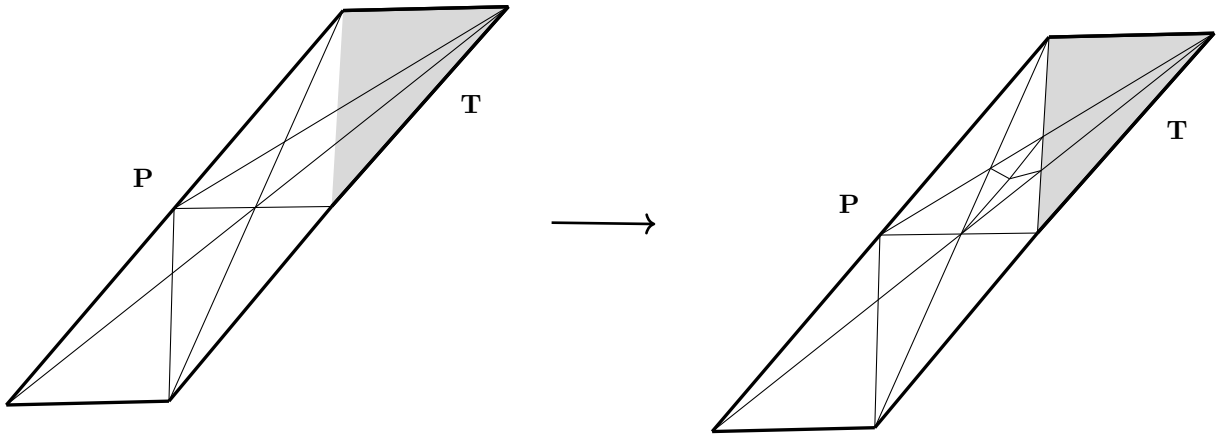
  On peut alors construire une nouvelle triangulation de $\mathbf{P} \uplus \mathbf{T}$ comme sous-triangulation de son originale, ainsi que comme sous-triangulation de celle de $\mathbf{Q} \uplus \mathbf{T}$. Il convient d'observer que l'on doit trianguler les nouveaux polytopes qui ne sont pas simpliciaux (on fixe un point intérieur au polytope que l'on relie aux sommets, puisque le polytope est convexe). De plus, on peut aussi distinguer les éléments de la triangulation en deux parties : ceux inclus dans $\mathbf{P}$, et ceux inclus dans $\mathbf{T}$.

  En ramenant tous ces morceaux sur $\mathbf{Q} \uplus \mathbf{T}$ à l'aide des φ_j^{-1}, on obtient deux nouvelles triangulations.

  On décompose le procédé en trois étapes :



Étape 1 - Superposition



Étape 2 - Triangulation compatible

Étape 3 - Report de la triangulation

On utilise les φ_j^{-1} pour ramener tous les morceaux inclus dans $\mathbf{B}_j$ sur $\mathbf{Q} \uplus \mathbf{T}$. Par ce biais, on peut alors séparer tous les morceaux de la nouvelle triangulation en deux catégories : ceux inclus dans $\mathbf{P}$ (resp. dans $\mathbf{Q}$) et ceux inclus dans $\mathbf{T}$. En les notant $\mathbf{X}_1, ..., \mathbf{X}_s$ (resp. $\mathbf{Y}_1, ..., \mathbf{Y}_s$) et $\mathbf{X}'_1, ..., \mathbf{X}'_t$ et $\mathbf{Y}'_1, ..., \mathbf{Y}'_t$, on obtient finalement :

$$\begin{cases} \mathbf{P} \uplus \mathbf{T} = \mathbf{X}_1 \uplus ... \uplus \mathbf{X}_s \uplus \mathbf{X}'_1 \uplus ... \uplus \mathbf{X}'_t \\ \mathbf{Q} \uplus \mathbf{T} = \mathbf{Y}_1 \uplus ... \uplus \mathbf{Y}_s \uplus \mathbf{Y}'_1 \uplus ... \uplus \mathbf{Y}'_t \end{cases} \quad \text{où } \mathbf{X}_i \subset \mathbf{P}, \mathbf{Y}_j \subset \mathbf{Q} \text{ et } \mathbf{X}'_i, \mathbf{Y}'_j \subset \mathbf{T}, \text{ avec } \mathbf{X}_i \cong \mathbf{Y}_i \text{ et } \mathbf{X}'_i \cong \mathbf{Y}'_i$$

où l'isométrie entre $\mathbf{X}_i$ et $\mathbf{Y}_i$ est l'isométrie φ_j en écrivant $\mathbf{X}_i \subset \mathbf{A}_i$ et $\mathbf{Y}_i \subset \mathbf{B}_j$, et de même pour $\mathbf{X}'_i$ et $\mathbf{Y}'_i$.

En particulier, on est parvenu à décomposer :

$$\begin{cases} \mathbf{P} = \mathbf{X}_1 \uplus ... \uplus \mathbf{X}_s \uplus \mathbf{T} \\ \mathbf{Q} = \mathbf{Y}_1 \uplus ... \uplus \mathbf{Y}_s \uplus \mathbf{T} \end{cases} \quad \text{et } \mathbf{X}_i \cong \mathbf{Y}_i$$

En omettant alors la partie en $\mathbf{T}$, on obtient bien $\mathbf{P} \cong \mathbf{Q}$.

- Traitons maintenant le cas général, à savoir $\mathbf{P} \cong_+ \mathbf{Q} \implies \mathbf{P} \cong \mathbf{Q}$. On suppose que $\mathbf{P} \cong_+ \mathbf{Q}$, c'est-à-dire on suppose qu'il existe $\mathbf{A} \cong \mathbf{B}$ tels que $\mathbf{P} \uplus \mathbf{A} \cong \mathbf{Q} \uplus \mathbf{B}$. Par congruence de $\mathbf{A}$ avec $\mathbf{B}$, écrivons :

$$\begin{cases} \mathbf{A} = \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_r \\ \mathbf{B} = \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_r \end{cases} \quad \text{où } \mathbf{T}_i, \mathbf{S}_j \text{ sont des simplexes tels que } \mathbf{T}_i = \varphi_i(\mathbf{S}_i) \text{ avec } \varphi_i \text{ isométrie}$$

  Procédons par récurrence sur $r \in \mathbb{N}^\star$.

  * Traitons le cas $r = 1$, et supprimons temporairement tous les indices pour plus de clarté.

    Alors $\mathbf{P} \uplus \mathbf{T} \cong \mathbf{Q} \uplus \mathbf{S}$, donc $\mathbf{P} \uplus \mathbf{T} \cong \varphi(\mathbf{Q} \uplus \mathbf{S}) = \varphi(\mathbf{Q}) \uplus \varphi(\mathbf{S}) = \varphi(\mathbf{Q}) \uplus \mathbf{T}$ car l'union est à intersection dégénérée, et car φ est bijective puisque isométrique.

    Ainsi, par le point précédent, on a $\mathbf{P} \cong \varphi(\mathbf{Q})$, et donc $\mathbf{P} \cong \mathbf{Q}$ car φ est une isométrie.

  * Supposons que le résultat soit vrai au rang r fixé (qui apparaîtra à la ligne marquée $(*)$ dans le calcul suivant). On veut le montrer au rang $r+1$. On développe le même argument qu'à l'initialisation (utilisé à la ligne marquée $(\ddagger)$ dans le calcul), en utilisant aux lignes marquées $(**)$ le fait que φ_{r+1} est isométrique et à la ligne $(\dagger)$ que φ_{r+1} est bijective et que l'union est d'intersection dégénérée :

$$\begin{aligned}
& \left(\mathbf{P} \uplus \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_r\right) \uplus \mathbf{T}_{r+1} \cong \left(\mathbf{Q} \uplus \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_r\right) \uplus \mathbf{S}_{r+1} \\
(**) \quad \implies & \left(\mathbf{P} \uplus \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_r\right) \uplus \mathbf{T}_{r+1} \cong \varphi_{r+1}\left[\left(\mathbf{Q} \uplus \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_r\right) \uplus \mathbf{S}_{r+1}\right] \\
(\dagger) \quad \iff & \left(\mathbf{P} \uplus \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_r\right) \uplus \mathbf{T}_{r+1} \cong \varphi_{r+1}\left(\mathbf{Q} \uplus \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_r\right) \uplus \varphi_{r+1}(\mathbf{S}_{r+1}) \\
\iff & \left(\mathbf{P} \uplus \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_r\right) \uplus \mathbf{T}_{r+1} \cong \varphi_{r+1}\left(\mathbf{Q} \uplus \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_r\right) \uplus \mathbf{T}_{r+1} \\
(\ddagger) \quad \implies & \mathbf{P} \uplus \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_r \cong \varphi_{r+1}\left(\mathbf{Q} \uplus \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_r\right) \\
(**) \quad \iff & \mathbf{P} \uplus \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_r \cong \mathbf{Q} \uplus \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_r \\
(*) \quad \implies & \mathbf{P} \cong \mathbf{Q}
\end{aligned}$$

    Ceci achève la preuve du théorème de Zylev.

1.3 Volume et définition d'invariant

Étant donné un polytope $\mathbf{P} \in \wp_n$, on définit son **volume** par la quantité :

$$\mathrm{vol}(\mathbf{P}) = \lambda^{\otimes n}(\mathbf{P})$$

où $\lambda^{\otimes n}$ désigne la mesure de Lebesgue dans $\mathbb{R}^n$. Cette quantité existe et est finie, car les polytopes (dégénérés ou non) sont des parties compactes de $\mathbb{R}^n$, donc boréliennes (*a fortiori* Lebesgue-mesurables) et de mesure finie. En particulier, il est immédiat de voir que $\mathbf{P}$ est dégénéré si et seulement si $\mathrm{vol}(\mathbf{P}) = 0$.

Rappelons maintenant une propriété importante de la mesure de Lebesgue :

$$\lambda^{\otimes n}(A \cup B) = \lambda^{\otimes n}(A) + \lambda^{\otimes n}(B) - \lambda^{\otimes n}(A \cap B)$$

En effet, cela provient des relations (valables pour des ensembles de mesure finie ; en particulier, $\lambda^{\otimes n}$ est finie sur les compacts, et les polytopes sont compacts) :

$$\begin{cases} \lambda^{\otimes n}(A \cup B) = \lambda^{\otimes n}(A) + \lambda^{\otimes n}(B) & \text{si } A \cap B = \varnothing \\ \lambda^{\otimes n}(A \setminus B) = \lambda^{\otimes n}(A) - \lambda^{\otimes n}(B) & \text{si } B \subset A \end{cases}$$

En effet, on a :

$$\begin{aligned} \lambda^{\otimes n}(A \cup B) &= \lambda^{\otimes n}(A \setminus B) + \lambda^{\otimes n}(B \setminus A) + \lambda^{\otimes n}(A \cap B) \\ &= \Big(\lambda^{\otimes n}(A) - \lambda^{\otimes n}(A \cap B)\Big) + \Big(\lambda^{\otimes n}(B) - \lambda^{\otimes n}(A \cap B)\Big) + \lambda^{\otimes n}(A \cap B) \\ &= \lambda^{\otimes n}(A) + \lambda^{\otimes n}(B) - \lambda^{\otimes n}(A \cap B) \end{aligned}$$

Ainsi, l'application $\mathrm{vol}_n : \wp_{\mathcal{O}_n} \to \mathbb{R}$ est telle que $\mathrm{vol}(\mathbf{P}) + \mathrm{vol}(\mathbf{Q}) = \mathrm{vol}(\mathbf{P} \cup \mathbf{Q}) + \mathrm{vol}(\mathbf{P} \cap \mathbf{Q})$. De manière plus générale, on définit les invariants par :

Définition :

Un invariant est une application $I : \wp_{\mathcal{O}_n} \to \Gamma$, où Γ est une groupe abélien, telle que :

$$I(\mathbf{P}) + I(\mathbf{Q}) = I(\mathbf{P} \cup \mathbf{Q}) + I(\mathbf{P} \cap \mathbf{Q})$$

La condition demandant que I soit à valeurs dans un groupe abélien permet justement de pouvoir faire ces sommes. Cependant, nous verrons par la suite les groupes abéliens comme des $\mathbb{Z}$-modules.

Si on considère $M = \mathbb{Z}^{(\wp_{\mathcal{O}_n})}$ le $\mathbb{Z}$-module des $\mathbb{Z}$-combinaisons linéaires formelles des polytopes (*ie* de manière équivalente, les applications $f : \wp_{\mathcal{O}_n} \to \mathbb{Z}$ à support fini), et si on considère X le sous-module de M engendré par les éléments de la forme :

$$\begin{cases} \mathbf{P} - \mathbf{Q}_1 - \mathbf{Q}_2 & \text{si } \mathbf{P} = \mathbf{Q}_1 \cup \mathbf{Q}_2 \\ \mathbf{P} - \varphi(\mathbf{P}) & \text{si } \varphi \text{ isométrie} \end{cases}$$

alors on peut considérer $\mathfrak{p}_n := M/X$ le module quotient. On note $[\mathbf{P}]$ la classe d'un polytope $\mathbf{P}$ dans $\mathfrak{p}_n$. Ce module $\mathfrak{p}_n$ est utile, car on a le résultat suivant :

Proposition :

Si $\mathbf{P}, \mathbf{Q} \in \wp_{\mathcal{O}_n}$ sont deux polytopes non dégénérés, alors :

$$\mathbf{P} \cong \mathbf{Q} \iff [\mathbf{P}] = [\mathbf{Q}] \text{ dans } \mathfrak{p}_n$$

Preuve :

- Supposons que $\mathbf{P} \cong \mathbf{Q}$. Décomposons-les en $\mathbf{P} = \mathbf{T}_1 \uplus ... \uplus \mathbf{T}_r$ et $\mathbf{Q} = \mathbf{S}_1 \uplus ... \uplus \mathbf{S}_r$ avec $\mathbf{T}_i = \Phi_i(\mathbf{S}_i)$ pour Φ_i isométrie. En particulier, on a $[\mathbf{T}_i] = [\Phi_i(\mathbf{S}_i)] \overset{\text{déf.}}{=} [\mathbf{S}_i]$, et donc :

$$[\mathbf{P}] \overset{\text{déf.}}{=} [\mathbf{T}_1] + ... + [\mathbf{T}_r] = [\mathbf{S}_1] + ... + [\mathbf{S}_r] \overset{\text{déf.}}{=} [\mathbf{Q}]$$

- Inversement, supposons que $[\mathbf{P}] = [\mathbf{Q}]$ dans $\mathfrak{p}_n$. On a :

$$\begin{cases} \mathbf{P} = (\mathbf{P} \setminus \mathbf{Q}) \uplus (\mathbf{P} \cap \mathbf{Q}) \\ \mathbf{Q} = (\mathbf{Q} \setminus \mathbf{P}) \uplus (\mathbf{P} \cap \mathbf{Q}) \end{cases} \qquad \text{donc} \qquad \begin{cases} [\mathbf{P}] = [\mathbf{P} \setminus \mathbf{Q}] + [\mathbf{P} \cap \mathbf{Q}] \\ [\mathbf{Q}] = [\mathbf{Q} \setminus \mathbf{P}] + [\mathbf{P} \cap \mathbf{Q}] \end{cases}$$

  Ainsi on a obtenu : $[\mathbf{P} \setminus \mathbf{Q}] = [\mathbf{Q} \setminus \mathbf{P}]$, et comme les deux sont disjoints, on a nécessairement $\mathbf{P} \setminus \mathbf{Q} = \varphi(\mathbf{Q} \setminus \mathbf{P})$, *ie* : $\mathbf{P} \setminus \mathbf{Q} \cong \mathbf{Q} \setminus \mathbf{P}$.

  On en déduit alors :

$$\mathbf{P} = (\mathbf{P} \setminus \mathbf{Q}) \uplus (\mathbf{P} \cap \mathbf{Q}) \cong_+ (\mathbf{Q} \setminus \mathbf{P}) \uplus (\mathbf{P} \cap \mathbf{Q}) = \mathbf{Q}$$

  car $\mathbf{P} \cap \mathbf{Q}$ est congru à lui-même, et en vertu du théorème de Zylev, on obtient finalement : $\mathbf{P} \cong \mathbf{Q}$.

Par ce biais, une manière strictement équivalente de voir un invariant $I : \wp_n \to \Gamma$ est de le lire comme une application $\mathbb{Z}$-linéaire induite sur les classes $\hat{I} : \mathfrak{p}_n \to \Gamma$.

En particulier, on a, pour I invariant :

$$\mathbf{P} \cong \mathbf{Q} \implies I(\mathbf{P}) = I(\mathbf{Q})$$

2 Constructions d'ordre théorique

2.1 Produit tensoriel de modules

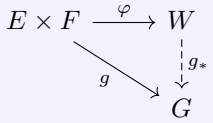
Dans le cas vectoriel, la somme directe correspond à la construction d'un espace de dimension la somme des dimensions de départ. De manière analogue, le produit tensoriel construirait dans le cas vectoriel (qui est un cas particulier de module) un espace de dimension produit.

Il faut garder à l'esprit que l'artefact des applications bilinéaires ne sert qu'à travailler de manière pertinente sur le produit des modules, qui quant à lui, ne possède pas de bonnes propriétés.

[La] présentait une construction à l'aide des catégories, tandis que **[Se]** détaille de manière plus pratique la construction. Nous en présenterons ici un mélange. L'objectif est de prouver la définition-proposition suivante :

Définition, proposition :

Soit A un anneau commutatif, soient E et F deux A-modules. Alors il existe un **unique** couple (W, φ), où W est un A-module et $\varphi : E \times F \to W$ une application bilinéaire, tel que pour tout A-module G et toute application bilinéaire $g : E \times F \to G$, il existe une **unique** application linéaire $g_* : W \to G$ tel que $g = g_* \circ \varphi$, *ie* g_* est l'application qui rend le diagramme suivant commutatif :

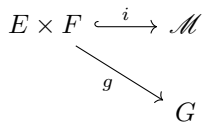


Le A-module W sera noté $E \otimes_A F$ et appelé **produit tensoriel** des deux modules E et F, et pour $(x, y) \in E \times F$, on notera $\varphi(x, y) = x \otimes_A y$ le produit tensoriel de x et y. De plus, $E \otimes_A F$ est engendré par les tenseurs $x \otimes_A y$.

2.1.1 Existence

Considérons $\mathscr{M} = A^{(E \times F)}$ le A-module libre des combinaisons linéaires formelles d'éléments de $E \times F$. Il est donc engendré par $E \times F$, qui s'y injecte canoniquement.

Étant donné un bilinéaire $g : E \times F \to G$, il paraîtrait *naturel* que si l'on veuille factoriser g pour rendre ce diagramme commutatif :



il faille identifier les éléments de la forme $(x + x', y)$ à ceux de la forme $(x, y) + (x', y)$, ainsi que les analogues décrits ci-après. Considérons les parties de $\mathscr{M}$ suivantes :

$$\begin{cases} X_1 = \{(x + x', y) - (x, y) - (x', y),\ (x, x', y) \in E^2 \times F\} \\ Y_1 = \{(x, y + y') - (x, y) - (x, y'),\ (x, y, y') \in E \times F^2\} \\ X_2 = \{(ax, y) - a(x, y),\ (a, x, y) \in A \times E \times F\} \\ Y_2 = \{(x, ay) - a(x, y),\ (a, x, y) \in A \times E \times F\} \end{cases}$$

On considère alors $\mathscr{N}$ le A-sous module de $\mathscr{M}$ engendré par ces parties :

$$\mathscr{N} = < X_1,\, X_2,\, Y_1,\, Y_2 >$$

Posons $W = \mathscr{M}/\mathscr{N}$ le quotient au sens des A-modules. Ce quotient est le produit recherché. Il identifie donc les éléments désirés au sein des classes d'équivalence. On a (la suite n'étant pas nécessairement exacte) :

$$E \times F \xhookrightarrow{\ i\ } \mathscr{M} \xrightarrow{\ \pi\ } \mathscr{M}/\mathscr{N}$$

où i désigne l'injection de $E \times F$ dans $\mathscr{M}$, et π la projection d'un élément dans sa classe.

Posons finalement :

$$\varphi(x, y) = \pi \circ i(x, y) = \overline{(x, y)} \qquad (\text{mod } \mathscr{N})$$

Si l'on pourrait croire que ne considérer que $\mathscr{M}$ en place de W suffise, en fait, l'injection i n'est pas bilinéaire, justement parce que $E \times F$ est une famille **libre** de $\mathscr{M}$! En revanche, φ est bilinéaire.

Il faut et il suffit de montrer la linéarité en chacun des deux variables de φ. Les raisonnements effectués à gauche se transportent à droite de manière strictement analogue. On a :

$$\begin{aligned}
\varphi(x + x', y) - \varphi(x, y) - \varphi(x', y) &= \overline{(x + x', y)} - \overline{(x, y)} - \overline{(x', y)} \\
&= \overline{(x + x', y) - (x, y) - (x', y)} && \text{par la structure que } \mathscr{M} \text{ induit sur le quotient} \\
&= 0 && \text{par définition de } \mathscr{N}
\end{aligned}$$

On fait de même pour obtenir $\varphi(ax, y) - a\varphi(x, y) = 0$.

Considérons maintenant $g : E \times F \to G$ un bilinéaire. On en est donc à ce diagramme :

$$\begin{array}{ccc}
E \times F & \xrightarrow{\ \varphi\ } & \mathscr{M}/\mathscr{N} \\
& \searrow^{g} & \\
& & G
\end{array}$$

On cherche maintenant à factoriser g pour faire commuter le diagramme à droite.

On peut considérer l'application $h : \mathscr{M} \to G$ définie par :

$$h(\lambda_1 e_1 + ... + \lambda_r e_r) = \lambda_1 g(e_1) + ... + \lambda_r g(e_r)$$

où les e_i sont éléments de $E \times F$ la base de $\mathscr{M}$. La définition est donc correcte et non ambigüe, et on a :

$$\begin{array}{ccc}
E \times F & \xhookrightarrow{\ i\ } & \mathscr{M} \\
& \searrow^{g} & \downarrow{\scriptstyle h} \\
& & G
\end{array}$$

Le diagramme commute, car :

$$h \circ i(x,y) = h(1_A \times (x,y)) = 1_A \times g(x,y) = g(x,y)$$

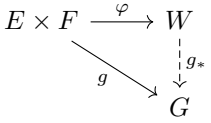
En revanche, i n'est pas bilinéaire. On a réussi à factoriser, mais il faut travailler un peu plus pour atteindre notre but. Il faut remarquer que h est linéaire, de par sa définition, et nulle sur $\mathscr{N}$ par bilinéarité de g, car (pour l'exemple de cet élément, les trois autres étant analogues) :

$$h(x+x',y) - h(x,y) - h(x',y) := g(x+x',y) - g(x,y) - g(x',y) = 0$$

Ainsi, $h : \mathscr{M} \to G$ induit une application linéaire $\overline{h} : \mathscr{M}/\mathscr{N} \to G$ donnée par :

$$\overline{h}\left(\overline{(x,y)}\right) = h(x,y)$$

Cette fois-ci, si l'on pose $g_* = \overline{h}$, on a accompli la factorisation, et le diagramme commute :



Il reste à montrer que cette factorisation est unique, *ie* si $g = h_1 \circ \varphi = h_2 \circ \varphi$, alors $h_1 = h_2$.

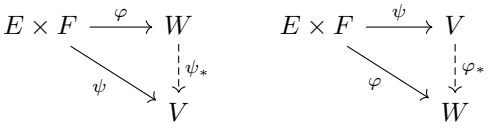
On rappelle que W est engendré par les $\varphi(x,y)$, puisque $\mathscr{M}$ lui-même est engendré par $E \times F$. Ainsi, supposons que $g = h_1 \circ \varphi = h_2 \circ \varphi$, alors $h_1 = h_2$. On a donc, en tout $(x,y) \in E \times F$:

$$g(x,y) = h_1(\varphi(x,y)) = h_2(\varphi(x,y))$$

ie h_1 et h_2 coïncident sur $\varphi(E \times F)$, qui engendre W, donc sont égales, d'où l'unicité.

2.1.2 Unicité

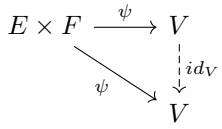
Reste à prouver l'unicité du couple (W, φ) précédemment construit. C'est une unicité *à isomorphisme canonique près* : supposons que (W, φ) et (v, ψ) soient convenables, on va montrer que W et V sont isomorphes *de façon naturelle*. On a les deux diagrammes commutatifs suivants, en appliquant la factorisation tantôt pour φ, tantôt pour ψ :



Ainsi, on a :

$$\psi = \psi_* \circ \varphi = (\varphi_* \circ \psi) = (\psi_* \circ \varphi_*) \circ \psi$$

De plus, on a, en factorisant ψ par ψ *via* le diagramme suivant :



donc $\psi = (\psi_* \circ \varphi_*) \circ \psi$ et $\psi = id_V \circ \psi$, *ie* $\psi_* \circ \varphi_* = id_V$ par unicité de la factorisation. De même, on a : $\varphi_* \circ \psi_* = id_W$, donc φ_* est un isomorphisme de V sur W, d'inverse ψ_*.

2.1.3 Propriétés du produit tensoriel

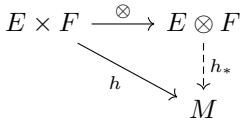
Si [**La**] présente les preuves sous l'angle des catégories et des foncteurs, nous les ferons ici de manière plus traditionnelle.

Comme énoncé précédemment, le A-module W est noté $E \otimes_A F$ (ou $E \otimes F$ s'il n'y a pas d'ambiguïté) et appelé **produit tensoriel** des modules. Les éléments $\varphi(x, y) = x \otimes y$ sont appelés **tenseurs purs**, et le tenseur $x \otimes y$ est appelé **produit tensoriel** de x et y.

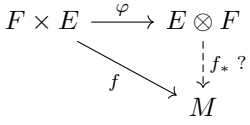
La bilinéarité du produit tensoriel permet d'obtenir les relations suivantes :

$$\begin{cases} (ax) \otimes y = x \otimes (ay) = a(x \otimes y) \\ (x + x') \otimes y = x \otimes y + x' \otimes y \\ x \otimes (y + y') = x \otimes y + x \otimes y' \end{cases}$$

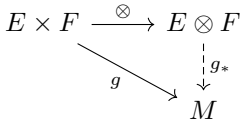
À la question "Quelle différence y a-t-il entre $E \otimes F$ et $F \otimes E$?", la réponse est : aucune, à isomorphisme près ; montrons que $F \otimes E \approx E \otimes F$. Considérons le produit tensoriel à gauche :



Soit $\varphi : F \times E \to E \otimes F$ définie par : $\varphi(y, x) = x \otimes y$. φ est bilinéaire, par bilinéarité de $\otimes$. Soit $f : F \times E \to M$ une application bilinéaire vers un module M quelconque. On cherche à la factoriser en $f_* : E \otimes F \xrightarrow{\text{lin.}} M$ telle que $f = f_* \circ \varphi$.



On définit l'application $g : E \times F \to M$ par : $g(x, y) = f(y, x)$. Alors g est factorisable pour le produit tensoriel à gauche :



On pose alors : $f_*(t) = g_*(t)$, qui est donc bien une application $E \otimes F \to M$ linéaire. Elle vérifie :

$$f_* \circ \varphi(y,x) = f_*(x \otimes y) = g_*(x \otimes y) = g(x,y) = f(y,x)$$

donc c'est bien une factorisation de f. Ainsi, par la propriété d'unicité, on a bien : $E \otimes F \approx F \otimes E$. En particulier, par la définition de φ, qui sera l'application produit tensoriel, il existe un isomorphisme $\Phi : E \otimes F \to F \otimes E$ tel que les tenseurs à gauche sont envoyés sur les tenseurs à droite, *ie* : $\Phi(x \otimes y) = y \otimes x$. Puisque ces tenseurs engendrent chacun des deux modules $E \otimes F$ et $F \otimes E$, cet isomorphisme Φ est même unique, et est en fait canonique.

Si les tenseurs engendrent le produit tensoriel, il n'est pas évident que la famille qu'ils forment soit libre. C'est même faux dans la plupart des cas. En revanche, démontrons le résultat suivant :

Théorème de décomposition des produits tensoriels :

Soit F un A-module. Si E est un A-module libre de base $(v_i)_{i\in I}$, alors pour tout tenseur $t \in E \otimes_A F$, il existe une **unique** famille $(x_i)_{i\in I} \in F^{(I)}$ à support fini (*ie* presque tous les x_i sont nuls) telle que :

$$t = \sum_{i\in I} v_i \otimes_A x_i$$

Preuve : montrons d'abord que $E \otimes F \approx F^{(I)}$.

- Supposons d'abord que $\text{rang}_A E = 1$, *ie* $E = Av_0 = \text{Vect}_A(v_0)$. Alors chaque $x \in E$ s'écrit de manière unique comme $x = \lambda_x v_0$. On va montrer que $E \otimes F \approx F$. Soit $\varphi : E \times F \to F$ définie par : $\varphi(x,y) = \lambda_x y$. Montrons que φ est un produit tensoriel (et donc *le* produit tensoriel) de E par F. Pour commencer, φ est bilinéaire :

$$\begin{aligned}\varphi(x+\mu x', y) &= \varphi(\lambda_x v_0 + \mu\lambda_{x'} v_0, y) = \varphi\left((\lambda_x + \mu\lambda_{x'})v_0, y\right) = (\lambda_x + \mu\lambda_{x'})y \\ &= \lambda_x y + \mu\lambda_{x'} y = \varphi(\lambda_x v_0, y) + \mu\varphi(\lambda_{x'} v_0, y) = \varphi(x,y) + \mu\varphi(x',y)\end{aligned}$$

$$\varphi(x, y+\mu y') = \lambda_x(y+\mu y') = \lambda_x y + \mu\lambda_x y' = \varphi(x,y) + \mu\varphi(x,y')$$

  Il reste à montrer que φ factorise les applications bilinéaires. Soit $f : E \times F \to M$ une application bilinéaire vers un A-module M quelconque. Posons $f_*(y) = f(v_0, y)$ pour $y \in F$. On a donc : $f_* = f(v_0, \cdot)$, ce qui montre sa linéarité. On a de plus :

$$f_* \circ \varphi(x,y) = f_*(\lambda_x y) = \lambda_x f_*(y) = \lambda_x f(v_0, y) = f(\lambda_x v_0, y) = f(x,y)$$

  Ainsi, on a factorisé f comme souhaité. On a donc bien obtenu : $E \otimes_A F \approx F$.

- Traitons le cas fini. Supposons que E soit de rang n, et soit alors $(v_1, ..., v_n)$ une A-base de E. On a la décomposition :

$$E = \bigoplus_{i=1}^{n} E_i$$

  où $E_i = \text{Vect}_A(v_i)$. Ainsi, chaque $x \in E$ se décompose de manière unique comme $x = \lambda_1 v_1 + ... + \lambda_n v_n$. On définit alors $v_i^*(x) = \lambda_i$ la i-ème forme linéaire duale associée à v_i : $v_i^\star : E \to A$. De manière analogue à précédemment, définissions $\varphi : E \times F \to F^n$ par :

$$\varphi(x,y) = (v_1^*(x)y, ..., v_n^*(x)y)$$

Vérifions la bilinéarité de φ :

$$\begin{aligned}\varphi(x, y+\mu y') &= \Big(v_1^*(x)(y+\mu y'), ..., v_n^*(x)(y+\mu y')\Big) \\ &= (v_1^*(x)y, ..., v_n^*(x)y) + \mu(v_1^*(x)y', ..., v_n^*(x)y') \\ &= \varphi(x,y) + \mu\varphi(x,y')\end{aligned}$$

Et de même, par linéarité des v_i^*, on a la linéarité à gauche. Finalement, φ factorise les applications bilinéaires, de la même manière que précédemment. Soit $f : E \times F \to M$ une application bilinéaire.

On définit $f_* : F^n \to M$ par :

$$f_*(y_1, ..., y_n) := f(v_1, y_1) + ... + f(v_n, y_n)$$

Cette application est linéaire, en utilisant la linéarité à droite de f dans $(*)$:

$$\begin{aligned}f_*(\mathbf{y}+\mu\mathbf{y}') &= f_*\Big((y_1, ..., y_n) + \mu(y_1', ..., y_n')\Big) \\ &= f\Big((y_1+\mu y_1', ..., y_n+\mu y_n')\Big) \\ &= f(v_1, y_1+\mu y_1') + ... + f(v_n, y_n+\mu y_n') \\ &= f(v_1,y_1) + \mu f(v_1,y_1') + ... + f(v_n,y_n) + \mu f(v_n,y_n') \qquad (*) \\ &= \Big[f(v_1,y_1) + ... + f(v_n,y_n)\Big] + \mu\Big[f(v_1,y_1') + ... + f(v_n,y_n')\Big] \\ &= f_*(\mathbf{y}) + \mu f_*(\mathbf{y}')\end{aligned}$$

De plus, elle vérifie, par bilinéarité de f aux endroits marqués $(**)$:

$$\begin{aligned}f_* \circ \varphi(x,y) &= f_*\Big((v_1^*(x)y, ..., v_n^*(x)y)\Big) \\ &= f\Big(v_1, v_1^*(x)y\Big) + ... + f\Big(v_n, v_n^*(x)y\Big) \\ &= v_1^*(x)f(v_1,y) + ... + v_n^*(x)f(v_n,y) \qquad (**) \\ &= f(v_1^*(x)v_1, y) + ... + f(v_n^*(x)v_n, y) \qquad (**) \\ &= f(v_1^*(x)v_1 + ... + v_n^*(x)v_n, y) \qquad (**) \\ &= f(x,y)\end{aligned}$$

Ainsi, φ est bien une factorisation de f. On a donc obtenu : $E \otimes F \approx F^n$.

- En fait, le cas général se traite exactement de la même manière − le cas fini nous permettait juste de comprendre ce qui se passe. On suppose que E est libre de base $(v_i)_{i\in I}$. Un élément de $F^{(I)}$ est une famille $(y_i)_{i\in I} \in F^I$ d'éléments de F indexée par I telle que seul un nombre fini de y_i sont non nuls.

  Puisque $E = \bigoplus_{i=1} E_i$ où $E_i = \mathrm{Vect}_A(v_i)$, alors chaque $x \in E$ se décompose de manière **unique** en :

$$x = \lambda_{i_1} v_{i_1} + ... + \lambda_{i_r} v_{i_r}$$

  On peut alors définir $v_i^*(x) = \lambda_i$ de manière unique sans ambiguïté, et on a :

$$x = \sum_{i\in I} v_i^*(x) v_i$$

car la somme est à support fini. En adoptant les notations précédentes, posons $\varphi(x,y) = (v_i^*(x)y)_{i\in I}$ et $f_*\left((y_i)_{i\in i}\right) = \sum_{i\in I} f(v_i,y_i)$, où la somme est bien définie car à support fini, puisque f_* est définie sur l'ensemble des familles à support fini. On obtient alors exactement le résultat escompté, à savoir la bilinéarité de φ, la linéarité de f_* et la factorisation.

On a donc obtenu que si $(v_i)_{i\in I}$ est une base de E, alors $E\otimes F \approx F^{(I)}$. On a de plus : $F^{(I)} = \bigoplus_{i\in I} F \approx \bigoplus_{i\in I} E_i\otimes F$ où $E_i = \mathrm{Vect}_A(v_i)$. Ainsi, on a :

$$E\otimes F = \left(\bigoplus_{i\in I} E_i\right)\otimes F \approx F^{(I)} \approx \bigoplus_{i\in I} E_i\otimes F$$

Autrement dit, le produit tensoriel est en quelque sorte distributif sur la somme directe.

En particulier, l'isomorphisme naturel $E\otimes F\approx F^{(I)}$ permet d'identifier chaque tenseur pur $x\otimes y\in E\otimes F$ à une unique famille $(z_i)_{i\in I}\in F^{(I)}$. Cet isomorphisme est donné par :

$$\Phi : \mathbf{y}\in F^{(I)} \mapsto \sum_{i\in I} v_i\otimes y_i \quad \text{et} \quad \Phi^{-1}(x\otimes y) = \left(v_i^*(x)y\right)_{i\in I}$$

De cet isomorphisme, on déduit le résultat souhaité, à savoir l'existence et l'unicité de la décomposition, par :

$$x\otimes y = \sum_{i\in I} v_i\otimes\left(v_i^*(x)y\right)$$

Un cas particulier est lorsque E et F sont libres, de bases respectives $(v_i)_{i\in I}$ et $(w_j)_{j\in J}$. Alors $E\otimes F$ est libre de base $(v_i\otimes w_j)_{(i,j)\in I\times J}$. De plus, si $\mathrm{rang}_A E < +\infty$ et $\mathrm{rang}_A F < +\infty$, alors $\mathrm{rang}_A E\otimes F = \mathrm{rang}_A E\times\mathrm{rang}_A F$.

2.2 Angles dièdres

Sans transition, nous aurons besoin de considérer certains angles au sein des polyèdres, à savoir les **angles dièdres**. Travaillons dans $\mathbb{R}^3$ (*ie* $n=3$) muni de sa structure euclidienne canonique.

Étant donné un tétraèdre, *ie* un simplexe de $\mathbb{R}^3$, $\mathbf{T} = co(u_0,u_1,u_2,u_3)$, soit $a\in\mathcal{F}_1(\mathbf{T})$ une arête, que l'on écrit sous la forme :

$$a = co(u_{i_0},u_{i_1}) \text{ pour } i_0\neq i_1\in[\![0,3]\!]$$

On note $[\![0,3]\!]\setminus\{i_0,i_1\} = \{i_2,i_3\}$.

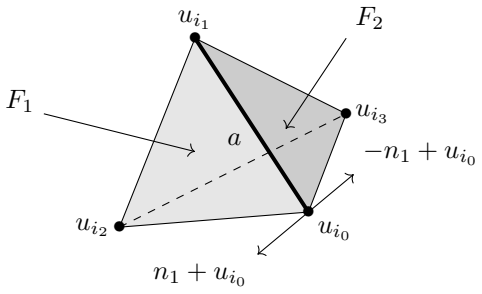
Posons $F_1 = co(u_{i_0},u_{i_1},u_{i_2})$ et $F_2 = co(u_{i_0},u_{i_1},u_{i_3})$ les deux faces de $\mathcal{F}_2(\mathbf{T})$ telles que $F_1\cap F_2 = a$.

En particulier, on considère les plans **vectoriels**, et non affines, $H_1 = \mathrm{Vect}(F_1-u_{i_0})$ et $H_2 = \mathrm{Vect}(F_2-u_{i_0})$, parallèles respectivement à F_1 et F_2.

On a : $\dim H_1 = \dim H_2 = 2$, donc $\dim H_1^\perp = \dim H_2^\perp = 1$, *ie* soit $n_1\in\mathbb{R}^3$ tel que $\|n_1\| = 1$ et $H_1^\perp = \mathrm{Vect}(n_1)$, et de même pour n_2.

En vertu de l'inégalité de Cauchy-Schwartz, on a : $|\langle n_1|n_2\rangle|\leqslant 1$. Comme $\cos : [0,\pi]\to[-1,1]$ est bijective, on serait tenté d'écrire directement $\theta = \arccos(\langle n_1|n_2\rangle)$. Cependant, il existe deux choix possibles pour n_1 ($\pm n_1$), et de même pour n_2. Cela pourrait donner lieu à 4 valeurs de produits scalaires différentes, mais en réalité, opposer deux fois les vecteurs ne contribue pas à changer le produit scalaire. Ainsi, il y a deux valeurs possibles de produit scalaire.

Puisque c'est l'angle **dièdre** qui nous intéresse, il faut choisir "les bons" vecteurs normaux, *ie* ceux qui sont dirigés *vers* le tétraèdre.



Soit Φ_1 une forme linéaire sur $\mathbb{R}^3$ telle que $H_1 = \ker \Phi_1$, et de même pour Φ_2. Alors $\mathbf{T}$ est inclus soit dans $u_{i_0} + \{v \in \mathbb{R}^3 \,/\, \Phi_1(v) \geqslant 0\}$, soit dans $u_{i_0} + \{v \in \mathbb{R}^3 \,/\, \Phi_1(v) \leqslant 0\}$, mais uniquement dans l'un des deux, de par sa convexité. Soit alors $\varepsilon_1 \in \{-1, 1\}$ tel que $\mathbf{T} \subset u_{i_0} + \{v \in \mathbb{R}^3 \,/\, \varepsilon_1\Phi_1(v) \geqslant 0\}$.

De même, il existe un unique $\varepsilon_2 = \pm 1$ tel que $\mathbf{T} \subset \{v \in \mathbb{R}^3 \,/\, \varepsilon_2\Phi_2(v) \geqslant 0\}$. On peut à présent considérer les formes linéaires $\Psi_1 \equiv \varepsilon_1\Phi_1$ et $\Psi_2 \equiv \varepsilon_2\Phi_2$, qui vérifient :

$$\begin{cases} H_1 = \ker \Psi_1 \quad \text{et} \quad H_2 = \ker \Psi_2 \\ \mathbf{T} \subset \Psi_1^{-1}(\mathbb{R}_+) \quad \text{et} \quad \mathbf{T} \subset \Psi_2^{-1}(\mathbb{R}_+) \end{cases}$$

Soit alors n_1 l'unique vecteur de $H_1^\perp$ tel que $\Psi_1(n_1) = 1$, et soit n_2 de même tel que $\Psi_2(n_2) = 1$. On n'a pas nécessairement $\|n_1\| = 1$, ni $\|n_2\| = 1$, mais on peut désormais considérer :

$$\theta := \arccos\left(\frac{-\langle n_1 | n_2\rangle}{\|n_1\| \times \|n_2\|}\right)$$

En effet, les deux vecteurs normaux sont bien "dirigés" vers $\mathbf{T}$, par la construction considérée.

Par la suite, on considèrera plutôt le $\mathbb{Z}$-module $\Delta = \mathbb{R}/\pi\mathbb{Z}$, à savoir le groupe des angles modulo π. Ainsi, on définira : $\theta_{\mathbf{T}}(a) = \theta + \pi\mathbb{Z} \in \Delta$. On commettra cependant l'abus de confondre la classe $\overline{\theta} \in \Delta$ d'un angle avec une de ses mesures $\theta \in \mathbb{R}$.

2.3 Extensions cyclotomiques

Le but de cette partie est de démontrer, à l'aide des prémices de la théorie de Galois, que l'extension cyclotomique est d'ordre l'indicatrice d'Euler.

2.3.1 L'indicatrice d'Euler

Rappelons la définition de l'indicatrice d'Euler, ainsi que ses propriétés fondamentales.

Définition : (indicatrice d'Euler)

On appelle **indicatrice d'Euler** la fonction φ définie sur $\mathbb{N}^\star$ par :

$$\varphi(n) = \operatorname{card}\{k \in [\![1, n]\!] \,/\, k \wedge n = 1\}$$

ie $\varphi(n)$ est le nombre d'entiers premiers avec n et inférieurs à n.

On notera que cette définition donne $\varphi(1) = 1$.

En particulier, en vertu du théorème de Bézout ($u \wedge v = 1 \iff \exists p, q \in \mathbb{Z}$ tels que $pu + qv = 1$), le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^\times$ des inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est d'ordre $\varphi(n)$. De cela, on déduit que si $p \in \mathbb{P}$ est un nombre premier, alors $\varphi(p) = p - 1$. Plus généralement, on a :

Proposition :

Si $p \in \mathbb{P}$ et $k \in \mathbb{N}$, alors $\varphi(p^k) = (p-1)p^{k-1}$.

Preuve : posons $q = p^k$. On a :

$$\begin{aligned}\varphi(q) &= \operatorname{card} \mathbb{Z}/q\mathbb{Z}^\times \\ &= \operatorname{card} \mathbb{Z}/q\mathbb{Z} - \operatorname{card} \{j \in [\![1, q]\!] \ / \ j \wedge q \neq 1\} \\ &= p^k - \operatorname{card} \{j \in [\![1, p^k]\!] \ / \ j \wedge p^k \neq 1\}\end{aligned}$$

Et on a : $j \wedge p^k \neq 1 \iff p|j$ car $p \in \mathbb{P}$, donc : $\{j \in [\![1, p^k]\!] \ / \ j \wedge p^k \neq 1\} = p\mathbb{Z} \cap [\![1, p^k]\!] = \{p \times r, \ r \in [\![1, p^{k-1}]\!]\}$, d'où :

$$\varphi(q) = p^k - p^{k-1} = (p-1)p^{k-1}$$

Tout cela nous permet de caractériser complètement l'indicatrice d'Euler. Pour ce faire, rappelons d'abord un résultat classique d'arithmétique :

Lemme des restes chinois :

Soient $a, b \in \mathbb{N}^\star$ deux entier. Alors les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes si et seulement si $a \wedge b = 1$, et l'isomorphisme d'anneaux est alors donné par :

$$\begin{array}{rccc}\Phi : & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} & \to & \mathbb{Z}/ab\mathbb{Z} \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{ab}\end{array}$$

Utilisons ce lemme pour démontrer le théorème suivant :

Théorème :

L'indicatrice d'Euler est une fonction multiplicative, *ie* si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$. En particulier, si $n = p_1^{\alpha_1} \times ... \times p_r^{\alpha_r}$ désigne la décomposition primaire de n, alors :

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \times ... \times (p_r - 1)p_r^{\alpha_r - 1}$$

Preuve : soient a et b deux entiers premiers entre eux. On note Φ l'isomorphisme d'anneaux donné par le lemme chinois. Montrons que $\mathbb{Z}/ab\mathbb{Z}^\times$ et $\mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times$ sont de même cardinal par double comparaison.

- Soit $(\overline{x}, \overline{y}) \in \mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times$. Alors il existe $(\overline{u}, \overline{v}) \in \mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times$ tel que $\overline{xu} = \overline{1}$ dans $\mathbb{Z}/a\mathbb{Z}$ et $\overline{yv} = \overline{1}$ dans $\mathbb{Z}/b\mathbb{Z}$.

Ob obtient donc $\Phi(\overline{x},\overline{y}) \times \Phi(\overline{u},\overline{v}) = \Phi(\overline{xu},\overline{yv}) = \Phi(\overline{1},\overline{1}) = \overline{1}$ dans $\mathbb{Z}/ab\mathbb{Z}$.

On a ainsi $\Phi(\overline{x},\overline{y}) \in \mathbb{Z}/ab\mathbb{Z}^\times$, et donc : $\Phi(\mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times) \subset \mathbb{Z}/ab\mathbb{Z}^\times$. Or, Φ étant bijective, on obtient :

$$\operatorname{card}(\mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times) = \operatorname{card}\Phi(\mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times) \leqslant \operatorname{card}(\mathbb{Z}/ab\mathbb{Z}^\times)$$

- Cette fois-ci, si $\overline{z} \in \mathbb{Z}/ab\mathbb{Z}^\times$, alors il existe $\overline{w} \in \mathbb{Z}/ab\mathbb{Z}^\times$ tel que $\overline{zw} = \overline{1}$ dans $\mathbb{Z}/ab\mathbb{Z}$. On écrit de même :

$$\begin{cases} \overline{z} = \Phi(\overline{x},\overline{y}) & (\overline{x},\overline{y}) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \overline{w} = \Phi(\overline{u},\overline{v}) & (\overline{u},\overline{v}) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \end{cases}$$

  On en déduit : $\Phi(\overline{1},\overline{1}) = \overline{1} = \overline{zw} = \Phi(\overline{x},\overline{y})\Phi(\overline{u},\overline{v}) = \Phi(\overline{xu},\overline{yv})$, et par injectivité de Φ, on obtient $\overline{xu} = \overline{1}$ dans $\mathbb{Z}/a\mathbb{Z}$ et $\overline{yv} = \overline{1}$ dans $\mathbb{Z}/b\mathbb{Z}$. Ainsi, $(\overline{x},\overline{y}) \in \mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times$, et donc $\overline{z} \in \mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times$. On obtient alors l'autre inclusion, et donc l'autre inégalité.

- On a naturellement :

$$\operatorname{card}(\mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}/b\mathbb{Z}^\times) = \operatorname{card}\mathbb{Z}/a\mathbb{Z}^\times \times \operatorname{card}\mathbb{Z}/b\mathbb{Z}^\times = \operatorname{card}\mathbb{Z}/ab\mathbb{Z}^\times$$

  On arrive alors à : $\varphi(ab) = \varphi(a)\varphi(b)$. L'expression de $\varphi(n)$ dans sa décomposition primaire est obtenue à l'aide de ce qui précède et de la proposition qui suivait la définition de φ.

2.3.2 Rudiments de théorie de Galois

Développons toutes les idées présentées par **[Ne]** : définissons le groupe de Galois d'une extension de corps, dans le cadre des extensions finies, et donnons-en quelques propriétés. On occultera cependant toute la partie sur les corps de décomposition, et on adaptera les résultats. Rappelons d'abord qu'une extension L/K est dite **finie** si le K-espace vectoriel L est de dimension finie. On note alors $[L : K] = \dim_K(L)$ sa dimension. On supposera que l'on travaille **en caractéristique nulle** pour simplifier tous les résultats (l'objectif que l'on vise ne requiert pas plus). Dans ce cadre-ci, on possède un théorème assez utile :

Théorème de l'élément primitif :

Soit L/K une extension finie. Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Ce théorème dit que les extensions finies sont engendrées (au sens des extensions de corps) par un élément, alors appelé **élément primitif**. Si $\mu_{\alpha,K}$ désigne son **polynôme minimal**, *ie* un polynôme de $K[X]$ qui admette α pour racine, alors $\deg(\mu_{\alpha,K}) = [L : K]$.

Ce résultat nous permet entre autres de donner la définition suivante :

Définition : (groupe d'automorphismes)

Soit L/K une extension finie. On note $\operatorname{Aut}_K(L)$ le groupe des automorphismes de L laissant K invariant, *ie* les applications K-linéaires $\sigma : L \to L$ telles que $\sigma(xy) = \sigma(x)\sigma(y)$.

En particulier, si $x \in K$, alors $\sigma(x) = \sigma(x \times 1_L) = x\sigma(1) = x$, *ie* $\sigma|_K \equiv id_K$. De plus, $\mathrm{Aut}_K(L)$ est bien un groupe, et son ordre est majoré par $[L : K]$.

En effet, par le théorème de l'élément primitif, on a $L = K(\alpha)$ pour $\alpha \in L$ primitif. De ce fait, tout $\sigma \in \mathrm{Aut}_K(L)$ est déterminé de manière unique par $\sigma(\alpha)$. Soit $\mu_{\alpha,K} \in K[X]$ son polynôme minimal. On a alors :

$$\mu_{\alpha,K}(\sigma(\alpha)) = \sigma(\mu_{\alpha,K}(\alpha))$$

par propriété de morphisme de corps de σ, et donc $\sigma(\alpha)$ est un zéro de $\mu_{\alpha,K}$. Ce nombre de zéros est majoré par le degré de ce polynôme, *ie* on a au plus $\deg(\mu_{\alpha,K}) = [L : K]$ choix pour $\sigma(\alpha)$. Il vient ainsi :

$$|\mathrm{Aut}_K(L)| \leqslant [L : K]$$

Quels sont les cas d'égalité ? Pour répondre à la question, observons le fait suivant :

Définition, proposition :

Soit H un sous-groupe du groupe d'automorphismes $\mathrm{Aut}_K(L)$ d'une extension finie L/K. Alors l'ensemble

$$L^H := \{x \in L \ / \ \forall \sigma \in H,\ \sigma(x) = x\}$$

est un corps, et il est tel que : $K \subset L^H \subset L$.

Preuve : la vérification est immédiate :

- Si $x, y \in L^H$, alors pour tout $\sigma \in \mathrm{Aut}_K(L)$, on a :
  - $\sigma(x + y) = \sigma(x) + \sigma(y) = x + y$
  - $\sigma(xy) = \sigma(x)\sigma(y) = xy$
  - $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}$
  - Si $\lambda \in K$, $\sigma(\lambda x) = \lambda\sigma(x) = \lambda x$

  Ainsi, on obtient : $x + y, xy, x^{-1}, \lambda x \in L^H$.
- Par définition de $\mathrm{Aut}_K(L)$, on a $\sigma(x) = x$ pour tout $x \in K$ et tout $\sigma \in \mathrm{Aut}_K(L)$, donc *a fortiori* pour tout $\sigma \in H$. Ainsi, on a bien : $K \subset L^H \subset L$.

Notons alors $\mathrm{gr}(L/K)$ l'ensemble des sous-groupes de $\mathrm{Aut}_K(L)$, et notons $\mathrm{ext}(L/K)$ l'ensemble de toutes les extensions de corps intermédiaires, *ie* les extensions de K contenues dans L. On a :

Proposition : (correspondance galoisienne)

Soit L/K une extension finie. Soit Γ l'application définie par :

$$\begin{array}{rccc} \Gamma : & \mathrm{gr}(L/K) & \to & \mathrm{ext}(L/K) \\ & H & \mapsto & L^H \end{array}$$

Alors l'application Γ est injectve, et est appelée **correspondance galoisienne**.

Preuve :

- On va d'abord démontrer le **lemme d'Artin**, à savoir :

$$\begin{cases} \mathrm{Aut}_{L^H}(L) = H \\ |H| = |\mathrm{Aut}_{L^H}(L)| = [L : L^H] \end{cases} \quad \text{pour tout } H \in \mathrm{gr}(L/K)$$

Par le théorème de l'élément primitif, soit $\alpha \in L$ un élément primitif de l'extension L/L^H, *ie* $L = L^H(\alpha)$. On considère μ_{α,L^H} le polynôme minimal de α sur L^H, qui est donc de degré $[L : L^H]$.

Posons :

$$P(X) = \prod_{\sigma \in H} (X - \sigma(\alpha)) = \sum_{k=0}^{|H|} a_k X^k \in L[X]$$

Si $\tau \in H$, alors :

$$\tau(P(X)) = \prod_{\sigma \in H} \tau(X - \sigma(\alpha)) = \prod_{\sigma \in H} (X - \tau\sigma(\alpha))$$

L'application $\Phi : \sigma \in H \mapsto \tau\sigma \in H$ est bijective, de réciprique $\Psi : \sigma \in H \mapsto \tau^{-1}\sigma$. On en déduit :

$$\tau(P(X)) = \prod_{\sigma \in H} (X - \sigma(\alpha)) = P(X)$$

Ainsi, on a : $\tau(a_k) = a_k$, car $\tau(P(X)) = \sum_{k=0}^{|H|} \tau(a_k) X^k = P(X) = \sum_{k=0}^{|H|} a_k X^k$. Les coefficients a_k de P sont donc tels que pour tout $\tau \in H$, $\tau(a_k) = a_k$, *ie* ce sont éléments de L^H. On a donc en réalité $P \in L^H[X]$.

En particulier, on a : $\mu_{\alpha,L^H} | P$, et donc $\deg \mu_{\alpha,L^H} \leqslant \deg P$. Il vient alors :

$$|H| = \deg P \geqslant \deg \mu_{\alpha,L^H} = [L : L^H] \qquad (*)$$

Inversement, on a évidemment $H \subset \mathrm{Aut}_{L^H}(L)$, car les automorphismes de H préservent L^H par définition. On a donc $|H| \leqslant |\mathrm{Aut}_{L^H}(L)|$. On savait de plus, avec la définition du groupe de Galois, que $|\mathrm{Aut}_{L^H}(L)| \leqslant [L : L^H]$. On a donc :

$$|H| \leqslant |\mathrm{Aut}_{L^H}(L)| \leqslant [L : L^H] \qquad (**)$$

Ainsi, en mettant en commun $(*)$ et $(**)$, on obtient :

$$|H| = |\mathrm{Aut}_{L^H}(L)| = [L : L^H]$$

Finalement, $H \subset \mathrm{Aut}_{L^H}(L)$, et il y a égalité des cardinaux, donc on a bien $H = \mathrm{Aut}_{L^H}(L)$.

- Supposons maintenant que $\Gamma(H_1) = \Gamma(H_2)$, *ie* $L^{H_1} = L^{H_2}$. Alors par le lemme d'Artin, on a :

$$H_1 = \mathrm{Aut}_{L^{H_1}}(L) = \mathrm{Aut}_{L^{H_2}}(L) = H_2$$

d'où l'injectivité.

Ainsi, revenons à notre question : quels sont les cas d'égalité dans la majoration $|\mathrm{Aut}_K(L)| \leqslant [L : K]$? Ce théorème répond à la question :

Théorème fondamental de la théorie de Galois :

Soit L/K une extension finie. Les assertions suivantes sont équivalentes :

- $|\mathrm{Aut}_K(L)| = [L : K]$.
- $L^{\mathrm{Aut}_K(L)} = K$.
- Pour tout $\alpha \in L$, le polynôme minimal $\mu_{\alpha,K}$ est scindé sur L (*ie* factorisable en un produit de polynômes de degré 1 de $L[X]$) et à racines simples.
- Il existe un élément primitif $\alpha \in L$ de L/K tel que $\mu_{\alpha,K}$ soit scindé à racines simples dans $L[X]$.

Une telle extension est alors appelée **extension galoisienne**, et le groupe d'automorphismes $\mathrm{Aut}_K(L)$ est alors appelé **groupe de Galois** de l'extension L/K, et noté $\mathrm{Gal}(L/K)$. Sous ces hypothèses, la correspondance galoisienne Γ est alors bijective, de réciproque :

$$\begin{array}{rcl} \Lambda : \mathrm{ext}(L/K) & \to & \mathrm{gr}(L/K) \\ M & \mapsto & \mathrm{Aut}_M(L) \end{array}$$

Preuve :

- Supposons que $|\mathrm{Aut}_K(L)| = [L : K]$. Puisque $L^{\mathrm{Aut}_K(L)}$ est une extension de K, on a, par la loi de la tour :

$$[L : K] = [L : L^{\mathrm{Aut}_K(L)}][L^{\mathrm{Aut}_K(L)} : K]$$

  Le lemme d'Artin donne : $[L : L^{\mathrm{Aut}_K(L)}] = |\mathrm{Aut}_K(L)|$, et $|\mathrm{Aut}_K(L)| = [L : K]$ par hypothèse. Ainsi, on obtient $[L^{\mathrm{Aut}_K(L)} : K] = 1$, d'où :

$$L^{\mathrm{Aut}_K(L)} = K$$

- Supposons que $L^{\mathrm{Aut}_K(L)} = K$. Soit $\alpha \in L$, et soit $\mu_{\alpha,K}$ son polynôme minimal. Posons :

$$P(X) = \prod_{\sigma \in \mathrm{Aut}_K(L)} (X - \sigma(\alpha))$$

  Par les mêmes arguments que dans la preuve du lemme d'Artin, on obtient $P \in L^{\mathrm{Aut}_K(L)}[X] = K[X]$. Ainsi, P est un polynôme de $K[X]$ qui annule α et qui est scindé sur L. Comme $\mu_{\alpha,K}|P$, alors $\mu_{\alpha,K}$ est lui aussi scindé sur L. Ses racines sont de plus simples.

  En effet, α lui-même est racine simple. Si c'était une racine au moins double, alors $\mu'_{\alpha,K} \in K[X]$ s'annulerait en α, mais il divise strictement $\mu_{\alpha,K}$, ce qui contredit sa minimalité.

  Si β est une autre racine de $\mu_{\alpha,K}$, alors elle est simple aussi. En effet, en considérant $T = \mathrm{PGCD}(\mu_{\alpha,K}, \mu_{\beta,K})$ (le pgcd est considéré dans $K[X]$), par l'identité de Bézout, T s'écrit comme $T = Q\mu_{\alpha,K} + R\mu_{\beta,K}$, et donc s'annule aussi en β. Ainsi, puisque $T|\mu_{\beta,K}$ (il s'agit de son PGCD avec un autre élément) et $\mu_{\beta,K}|T$ (T s'annule en β), on a $T = \mu_{\beta,K}$, et donc $\mu_{\beta,K}|\mu_{\alpha,K}$.

  On a alors : $\mu_{\alpha,K} = \dfrac{\mu_{\alpha,K}}{\mu_{\beta,K}} \times \mu_{\beta,K}$, et $\mu_{\alpha,K}$ et $\mu_{\beta,K}$ irréductibles, donc $\dfrac{\mu_{\alpha,K}}{\mu_{\beta,K}} = 1$, *ie* $\mu_{\alpha,K} = \mu_{\beta,K}$, et β est racine simple de $\mu_{\beta,K}$, donc de $\mu_{\alpha,K}$.

- Si tous les polynômes minimaux sont scindés à racines simples, c'est en particulier vrai pour n'importe quel élément primitif de l'extension.

- Soit $\alpha \in L$ un élément primitif de L/K tel que son polynôme minimal $\mu_{\alpha,K}$ soit scindé à racines simples dans $L[X]$. Notons $n = [L : K] = \deg \mu_{\alpha,K}$, et en posant $\theta_1 = \alpha$, notons $\theta_1, ..., \theta_n$ les racines **simples** de $\mu_{\alpha,K}$ (leur simplicité nous permet bien de dire qu'il y en a n distinctes).

On a : $L = K(\theta_1)$. On veut montrer que $L = K(\theta_k)$ pour tout $k \in [\![1, n]\!]$. Fixons $k \in [\![1, n]\!]$.

Soit $T = \text{PGCD}(\mu_{\alpha,K}, \mu_{\theta_k,K})$, où le PGCD est considéré dans $K[X]$. On a $T = P\mu_{\alpha,K} + Q\mu_{\theta_k,K}$ par l'identité de Bézout, donc $T(\theta_k) = 0$, et donc $\mu_{\theta_k,K}|T$ par minimalité. Or T est un pcdg de $\mu_{\theta_k,K}$, donc $T|\mu_{\theta_k,K}$, et donc $T = \mu_{\theta_k,K}$. Ainsi, on obtient : $\mu_{\alpha,K} = \dfrac{\mu_{\alpha,K}}{\mu_{\theta_k,K}} \times \mu_{\theta_k,K}$, donc $\dfrac{\mu_{\alpha,K}}{\mu_{\theta_k,K}} = 1$ par irréductibilité de $\mu_{\alpha,K}$, et donc $\mu_{\alpha,K} = \mu_{\theta_k,K}$.

En particulier, on a égalité entre les degrés, et donc on en déduit $[K(\theta_k) : K] = [K(\alpha) : K] = [L : K]$, *ie* $K(\theta_k)$ est une extension intermédiaire de degré maximale, donc $K(\theta_k) = L$.

Ainsi, tous les θ_k sont des éléments primitifs de L/K. On peut alors définir de manière unique un morphisme de corps $\sigma_k : L \to L$ par $\sigma_k(\alpha) = \theta_k$, et de même on définit $\tau_k : L \to L$ par $\tau_k(\theta_k) = \alpha$ (on avait vu que l'on définit de manière unique un K-morphisme du corps L par la donnée de l'image d'un élément primitif de l'extension L/K). Il est immédiat de vérifier que σ_k et τ_k sont inverses l'une de l'autre, en observant un élément tantôt dans la famille génératrice $1, \alpha, ..., \alpha^{n-1}$, tantôt dans la famille génératrice $1, \theta_k, ..., \theta_k^{n-1}$. Ainsi, $\sigma_k \in \text{Aut}_K(L)$.

Les θ_k étant tous des éléments distincts, on a construit au moins n automorphismes. Autrement dit, on a obtenu $[L : K] \leqslant |\text{Aut}_K(L)|$. On savait déjà que $|\text{Aut}_K(L)| \leqslant [L : K]$, donc on a égalité.

Remarques : nous ne prouverons pas ici la partie portant sur la correspondance galoisienne, étant donné qu'elle n'interviendra pas dans le cadre de l'extension cyclotomique. Elle est néanmoins fondamentale, et il reste plusieurs points importants à souligner :

- Γ et Λ sont des applications qui renversent l'ordre pour l'inclusion.
- Une extension intermédiaire $M \in \text{ext}(L/K)$ est galoisienne **si et seulement si** elle est image par Γ d'un sous-groupe **distingué** $H \triangleleft \text{Gal}(L/K)$.
- En réalité, on appelle extension galoisienne toute extension **séparable** et **normale**, et les propositions équivalentes du théorème fondamental sont toutes des conséquences de ces propriétés. Cependant, ces notions sont trop hors-sujet pour avoir été abordées ici, et on s'est contenté de la suite d'équivalences.

2.3.3 L'extension cyclotomique

Pour $n \in \mathbb{N}^\star$, on notera μ_n le groupe (multiplicatif) des racines n-èmes de l'unité, et on note μ_n^* celui des racines **primitives** n-èmes de l'unité, *ie* les racines $z \in \mu_n$ telles que $< z >= \mu_n$. Par le lemme chinois, on a :

Lemme :

$\mu_n^* = \left\{e^{2ik\pi/n},\ k \wedge n = 1\right\}$. Ainsi, si on pose $\zeta = e^{2i\pi/n}$, on a : $\mu_n^* = \left\{\zeta^k,\ k \wedge n = 1\right\}$.

On définit alors les **extensions cyclotomiques** :

Définition :

Pour $n \in \mathbb{N}^\star$, on appelle **extension cyclotomique d'ordre** n, notée K_n, l'extension $K_n = \mathbb{Q}(\mu_n)$. C'est une extension finie, et un élément primitif est $\zeta = e^{2i\pi/n}$.

On voit immédiatement qu'en réalité, on a : $K_n = \mathbb{Q}(\mu_n^*) = \mathbb{Q}(\zeta)$. L'extension est de plus galoisienne. En effet, le polynôme $X^n - 1$ est scindé à racines simples sur K_n, puisque ses racines sont exactement les éléments de μ_n, et donc : $\deg(X^n - 1) = n = \operatorname{card} \mu_n$. En particulier, $\mu_{\zeta,\mathbb{Q}}$ divise $X^n - 1$, donc lui aussi est scindé à racines simples sur K_n, et ζ est primitif de $K_n/\mathbb{Q}$. Quel est le degré de l'extension cyclotomique ? La théorie de Galois nous permet de répondre à la question sans utiliser les polynômes cyclotomiques :

Proposition :

Pour tout $n \geqslant 3$, on a $[K_n : \mathbb{Q}] = \varphi(n)$, où φ désigne l'indicatrice d'Euler.

Preuve : on va plutôt démontrer que $\mathrm{Gal}(K_n/\mathbb{Q}) \approx (\mathbb{Z}/n\mathbb{Z})^\times$, et, là encore, le théorème fondamental de la théorie de Galois permettra d'obtenir : $[K_n : \mathbb{Q}] = |\mathrm{Gal}(K_n/\mathbb{Q})| = \operatorname{card}(\mathbb{Z}/n\mathbb{Z}^\times) = \varphi(n)$.

- Tout d'abord, fixons $k \in [\![1, n]\!]$ tel que $k \wedge n = 1$. Définition le morphisme de corps $\sigma_k : K_n \to K_n$ par $\sigma_k(\zeta) = \zeta^k$. En réalité, on obtient un automorphisme qui laisse invariant $\mathbb{Q}$, *ie* $\sigma_k \in \mathrm{Gal}(K_n/\mathbb{Q})$.

  En effet, l'application, vue comme endomorphisme $\mathbb{Q}$-linéaire de K_n, qui est de dimension finie $\leqslant n$, est surjective : si $z \in K_n$, en écrivant $z = \alpha_0 + \alpha_1\zeta + ... + \alpha_{n-1}\zeta^{n-1}$ (la famille des puissances de ζ, à savoir μ_n, est génératrice ; elle n'est pas libre, mais cela n'est pas nécessaire), et en considérant ℓ l'inverse de k dans $\mathbb{Z}/n\mathbb{Z}^\times$, *ie* $k\ell \equiv 1 \pmod{n}$, on a :

  $$\sigma_k\left(\alpha_0 + \alpha_1\zeta^\ell + ... + \alpha_{n-1}\zeta^{(n-1)\ell}\right) = \alpha_0 + \alpha_1\zeta^{k\ell} + ... + \alpha_{n-1}\zeta^{(n-1)k\ell} = \alpha_0 + \alpha_1\zeta + ... + \alpha_{n-1}\zeta^{n-1} = z$$

  Ainsi, σ_k est surjective linéaire entre deux espaces vectoriels de même dimension, donc c'est un isomorphisme, et donc l'application vue comme morphisme de corps, est bijective, et laisse $\mathbb{Q}$ invariant. On a donc bien :

  $$\sigma_k \in \mathrm{Gal}(K_n/\mathbb{Q})$$

- Soit maintenant Φ l'application définie par :

  $$\begin{array}{rccc} \Phi & : & \mathbb{Z}/n\mathbb{Z}^\times & \to & \mathrm{Gal}(K_n/\mathbb{Q}) \\ & & k & \mapsto & \sigma_k \end{array}$$

  On cherche à montrer que cette application est un isomorphisme de groupes. Par le point précédent, elle est bien définie. En effet, par cyclicité de μ_n, l'automorphisme σ_k est indépendant du choix du représentant de la classe de k modulo n.

  * Φ définit bien un morphisme de groupes. En effet, soient $k, \ell \in \mathbb{Z}/n\mathbb{Z}^\times$. On a :

    $$\sigma_k \circ \sigma_k(\zeta) = \sigma_k(\zeta^\ell) = (\sigma_k(\zeta))^\ell = \zeta^{k\ell} = \sigma_{k\ell}(\zeta)$$

    Ainsi, les deux morphismes coïncident sur l'élément primitif, donc ils coïncident partout. On en déduit alors : $\phi(k\ell) = \Phi(k) \circ \Phi(\ell)$.

  * Φ est injective, car si $\Phi(k) = \mathrm{id}$, alors $\sigma_k(\zeta) = \zeta^k = \zeta$, *ie* $\zeta^{k-1} = 1$, donc on a : $e^{2i(k-1)\pi/n} = e^0$, donc $2(k-1)\pi/n \equiv 0 \pmod{2\pi}$, *ie* on obtient bien $k = 1$ dans $\mathbb{Z}/n\mathbb{Z}$, et donc dans $\mathbb{Z}/n\mathbb{Z}^\times$.

  * Soit $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$. On définit $\xi = \sigma(\zeta)$. Alors : $\xi^n = \sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$, donc $\xi \in \mu_n$. De plus, $< \xi >=< \sigma(\zeta) >= \sigma(< \zeta >) =< \zeta >= \mu_n$ car σ automorphisme, donc ξ est une racine primitive de l'unité. Ainsi, $|\mathrm{Gal}(K_n/\mathbb{Q})| \leqslant \operatorname{card} \mu_n^* = \varphi(n) = \operatorname{card} \mathbb{Z}/n\mathbb{Z}^\times$. Φ est donc un isomorphisme, et on obtient bien le résultat souhaité.

2.4 Cosinus des angles rationnels en π

Montrons le résultat suivant :

Théorème :

Si $\theta \in \pi\mathbb{Q}$ est tel que $\cos(\theta) \in \mathbb{Q}$, alors $e^{i\theta} \in \mu_4 \cup \mu_6$.

Preuve : soit donc θ un tel angle. On pose alors : $\dfrac{\theta}{2\pi} = \dfrac{a}{b}$ avec $(a,b) \in \mathbb{Z} \times \mathbb{N}^\star$ et $a \wedge b = 1$. Définissons $\zeta = e^{i\theta} = e^{2ia\pi/b}$. Observons une disjonction des cas selon les valeurs de b :

- Si $b = 1$: alors $\zeta = 1 \in \mu_4 \cup \mu_6$.
- Si $b \in \{2,3,4\}$: alors $\zeta \in \mu_2 \cup \mu_3 \cup \mu_4$, et $\mu_2 \subset \mu_4$, $\mu_3 \subset \mu_6$, donc $\zeta \in \mu_4 \cup \mu_6$.
- Si $b \geqslant 5$: alors $\zeta = e^{2ia\pi/b}$ et $a \wedge b = 1$, donc ζ est une racine **primitive** b-ème de l'unité. En particulier, on a donc : $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(b)$.

  Le polynôme $X^2 - (\zeta + \zeta^{-1})X + 1$ est annulateur de ζ. Or, par hypothèse, $\zeta + \zeta^{-1} = 2\cos(\theta) \in \mathbb{Q}$, donc $X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}[X]$, et donc on a : $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leqslant 2$, *ie* $\varphi(b) \leqslant 2$. Or $\varphi \geqslant 1$, et $\varphi(n) = 1 \iff n = 1$, donc comme $b \geqslant 5$, on a : $\varphi(b) = 2$.

  Écrivons $b = p_1^{\alpha_1} \times ... \times p_r^{\alpha_r}$ la décomposition primaire de b. Si $r \geqslant 3$, alors $b = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times b'$, et donc on a : $\varphi(b) = (p_1 - 1)p_1^{k_1 - 1} \times (p_2 - 1)p_2^{k_2 - 1} \times (p_3 - 1)p_3^{k_3 - 1} \times \varphi(b') \geqslant (p_1 - 1)(p_2 - 1)(p_3 - 1)$.

  Deux des trois p_i sont différents de 2, donc sont $\geqslant 3$ car premiers. Ainsi, $\varphi(b) \geqslant (p-1) \times 2 \times 2 \geqslant 4$, ce qui est impossible.

  Nécessairement, $r < 3$, *ie* $r \in \{1,2\}$, car $r = 0 \implies b = 1$, mais $b \geqslant 5$. Deux cas à étudier :

  * Si $r = 1$: alors $b = p^k$. Si $p \geqslant 5$, alors $\varphi(b) = (p-1) \times p^{k-1} \geqslant p - 1 \geqslant 4$, impossible. Ainsi, $p \in \{2,3\}$.

    Si $p = 2$, alors $\varphi(2^k) = 2^{k-1} = 2 \implies k = 2$, *ie* $b = 4$, donc $\zeta \in \mu_4 \subset \mu_4 \cup \mu_6$.

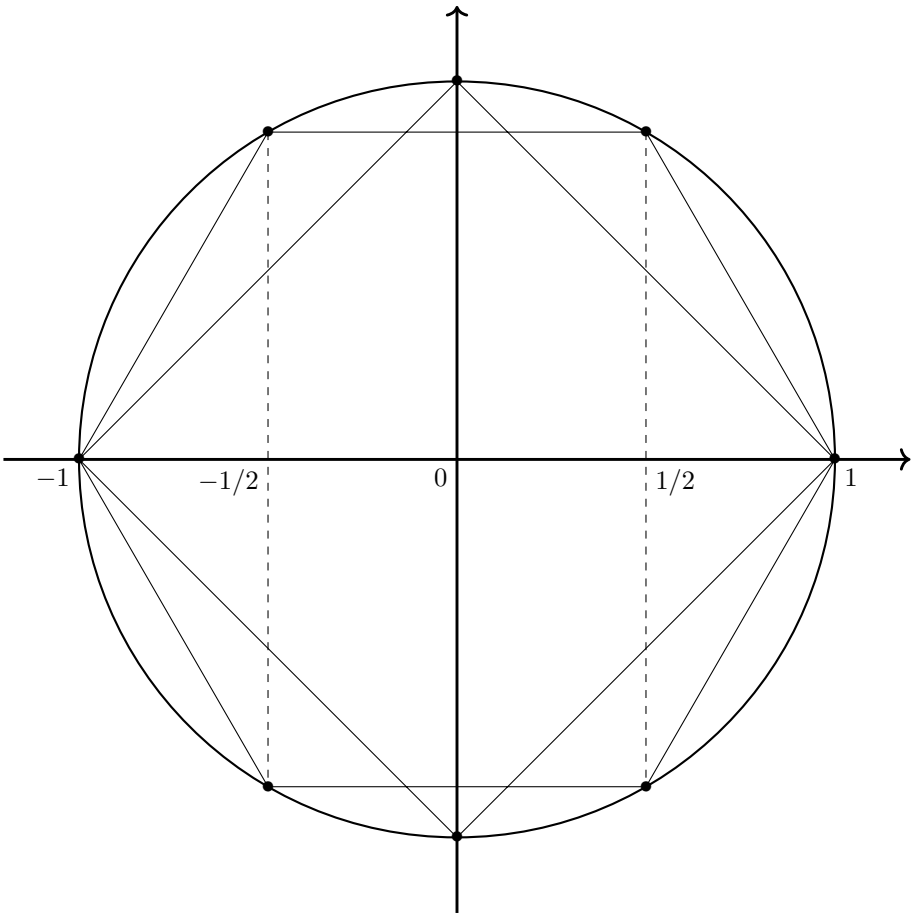
    Si $p = 3$, alors $\varphi(b) = 2 \times 3^{k-1} \implies k = 1$, *ie* $b = 3$, donc $\zeta \in \mu_3 \subset \mu_6 \subset \mu_4 \cup \mu_6$.
  * Si $r = 2$: par le même raisonnement que dans le cas $r = 1$, on a : $p, q \leqslant 3$, *ie* $p = 2$ et $q = 3$ quitte à les réordonner. On a donc $b = 2^k 3^\ell$, d'où : $\varphi(b) = 1 \times 2^{k-1} \times 2 \times 3^{\ell-1} = 2^k \times 3^{\ell-1} = 2$. Par l'unicité de la décomposition primaire de 2, on a : $k = 1$ et $\ell = 1$, *ie* $b = 2 \times 3 = 6$, donc $\zeta \in \mu_6 \subset \mu_4 \cup \mu_6$.

Un corollaire (en fait strictement équivalent au théorème) dont nous nous servirons plutôt est le suivant :

Corollaire :

Si $\theta \in \pi\mathbb{Q}$ est tel que $\cos(\theta) \in \mathbb{Q}$, alors $\cos(\theta) \in \left\{0, \pm\dfrac{1}{2}, \pm 1\right\}$.

Preuve : immédiate en observant directement l'ensemble $\big\{\Re(\zeta),\ \zeta \in \mu_4 \cup \mu_6\big\}$.



3 Le contre-exemple de Dehn

3.1 L'invariant de Dehn

L'invariant de Dehn associe à un polyèdre la somme des tenseurs de $\mathbb{R} \otimes_{\mathbb{Z}} \Delta$ formée de la longueur des arêtes et de leur angle dièdre :

$$D(\mathbf{P}) = \sum_{a \text{ arête de } \mathbf{P}} \ell(a) \otimes_{\mathbb{Z}} \theta(a)$$

Cependant, cette "définition" (*cf* **[Ca]**, **[Sy]** ou **[Sc]**) n'est pas une bonne définition, dans le sens où nous n'avons défini l'angle dièdre que dans le cas des tétraèdres, et dans le sens où il resterait à définir la notion d'arête d'un polyèdre quelconque. Cependant, il est possible d'utiliser la construction faisant intervenir les complexes polyédraux qui engendrent le polyèdre, puisque les arêtes des tétraèdres sont bien définies, et puisque celles du polyèdre seront une partie de toutes celles-ci.

Montrons le résultat suivant :

Proposition :

Soit $\mathbf{P} \in \wp_3$ un polyèdre non dégénéré de $\mathbb{R}^3$. On note $\mathfrak{K}_{\mathbf{P}}$ l'ensemble des complexes polyédraux $\mathcal{K}$ tels que $\mathbf{P} = \bigcup_{\mathbf{T} \in \mathcal{K}} \mathbf{T}$. On rappelle qu'on note $\mathcal{K}_k$ l'ensemble des simplexes de $\mathcal{K}$ de rang k, et qu'on note $\mathcal{F}_k(\mathbf{X})$ l'ensemble des faces de $\mathbf{X}$ de rang k, pour $\mathbf{X}$ simplexe de rang $\mathrm{rg}(\mathbf{X}) \geqslant k$.
Considérons l'application suivante :

$$\begin{array}{rccc} D_{\mathbf{P}} : \mathfrak{K}_{\mathbf{P}} & \to & \mathbb{R} \otimes_{\mathbb{Z}} \Delta \\ \mathcal{K} & \mapsto & \displaystyle\sum_{\mathbf{T} \in \mathcal{K}_3} \left(\sum_{a \in \mathcal{F}_1(\mathbf{T})} \ell(a) \otimes_{\mathbb{Z}} \theta_{\mathbf{T}}(a) \right) \end{array}$$

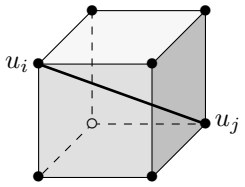
Alors cette application est constante.

Preuve : pour commencer, on peut ré-écrire $D_{\mathbf{P}}(\mathcal{K})$ en intervertissant les deux sommes, et donc en sommant sur les arêtes de tous les tétraèdres plutôt que sur les tétraèdres eux-même :

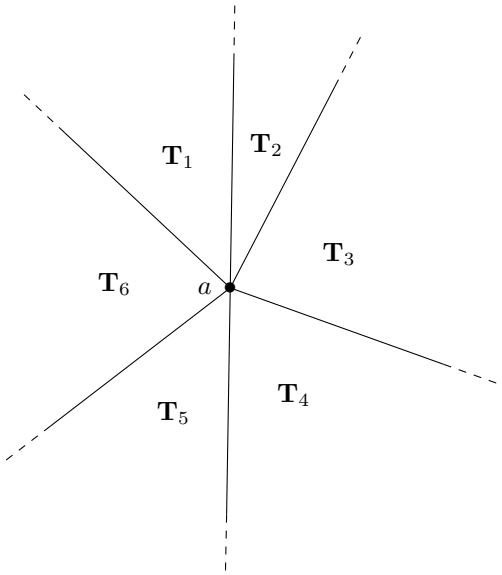
$$D_{\mathbf{P}}(\mathcal{K}) = \sum_{a \in \mathcal{K}_1} \left(\sum_{\mathbf{T} \in \mathcal{K}_3 \,/\, a \in \mathcal{F}_1(\mathbf{T})} \ell(a) \otimes_{\mathbb{Z}} \theta_{\mathbf{T}}(a) \right) = \sum_{a \in \mathcal{K}_1} \left(\ell(a) \otimes_{\mathbb{Z}} \sum_{\mathbf{T} \in \mathcal{K}_3 \,/\, a \in \mathcal{F}_1(\mathbf{T})} \theta_{\mathbf{T}}(a) \right)$$

Observons alors, à $a \in \mathcal{K}_1$ fixé, la quantité $\displaystyle\sum_{\mathbf{T} \in \mathcal{K}_3 \,/\, a \in \mathcal{F}_1(\mathbf{T})} \theta_{\mathbf{T}}(a) \in \Delta$. En notant $a = co(u_i, u_j)$, où u_i et u_j sont deux sommets d'un certain tétraèdre, on définit $]a[= a \setminus \{u_i, u_j\}$ l'arête privée de ses extrémités. Plusieurs cas se distinguent :

- Si $a \not\subset \partial\mathbf{P}$: de manière équivalente, si $]a[\subset \overset{\circ}{\mathbf{P}}$, alors soient $\mathbf{T}_1, ..., \mathbf{T}_r$ les tétraèdres $\mathbf{T} \in \mathcal{K}_3$ tels que $a \in \mathcal{F}_1(\mathbf{T})$.

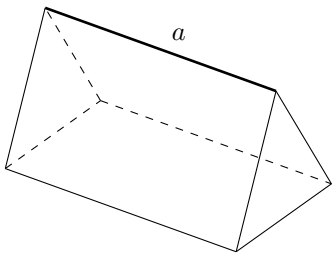


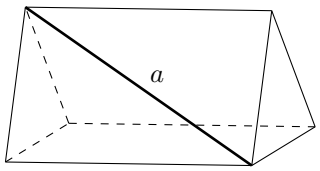
Alors $\mathbf{T}_i \cap \mathbf{T}_j = a$ et $]a[\subset \text{int}(\mathbf{T}_1 \cup ... \cup \mathbf{T}_r)$. Ces deux relations signifient respectivement que les tétraèdres sont agencés autour de a, et que l'intérieur de la réunion des $\mathbf{T}_i$ forme un voisinage tubulaire de $]a[$ au sein de $\overset{\circ}{\mathbf{P}}$. Une vue en coupe transversale à a donne :

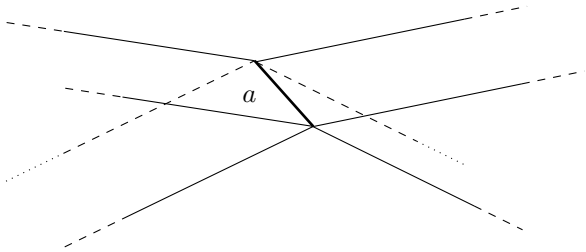


En particulier, la somme des angles dièdres $\theta_{\mathbf{T}_i}(a)$ vaut alors 2π, *ie* vaut 0 dans Δ.

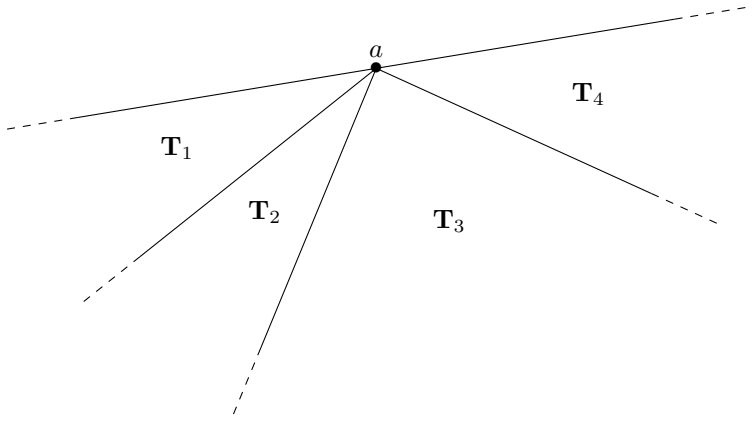
- Si $a \subset \partial\mathbf{P}$: alors il y a trois cas possibles, correspondant aux trois représentations ci-après (dans le cas de la troisième, il ne s'agit que d'une représentation locale du polyèdre, et dans le cas de deux "branches", mais il peut y en avoir $n \in \mathbb{N}^\star$ quelconque) :





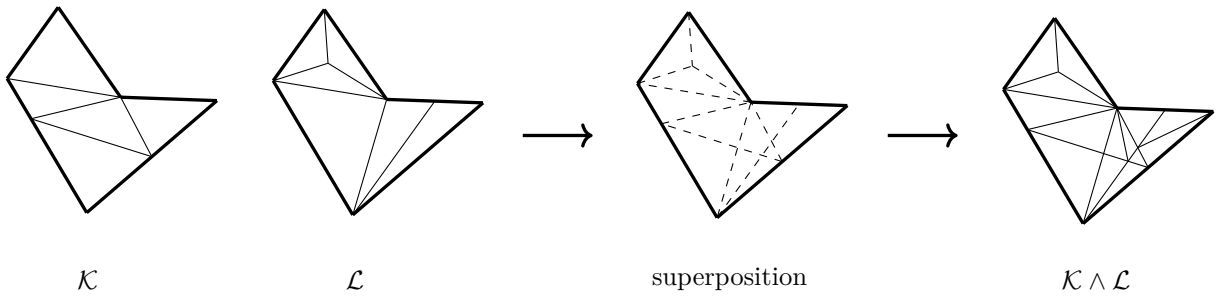


Dans les premier et troisième cas, on ne peut rien dire. En revanche, dans le deuxième, en notant à nouveau $\mathbf{T}_1, ..., \mathbf{T}_r$ les tétraèdres qui possèdent a pour arête, on a toujours $\mathbf{T}_i \cap \mathbf{T}_j = a$. Par contre, on ne peut plus écrire $]a[\subset \text{int}(\mathbf{T}_1 \cup ... \cup \mathbf{T}_r)$ comme précédemment, parce que, justement, on a $a \subset \partial(\mathbf{T}_1 \cup ... \cup \mathbf{T}_r)$! On observe, par une nouvelle vue en coupe transversale à a :



Cette fois-ci, la somme des angles s'évalue à π, donc à 0 encore une fois dans Δ.

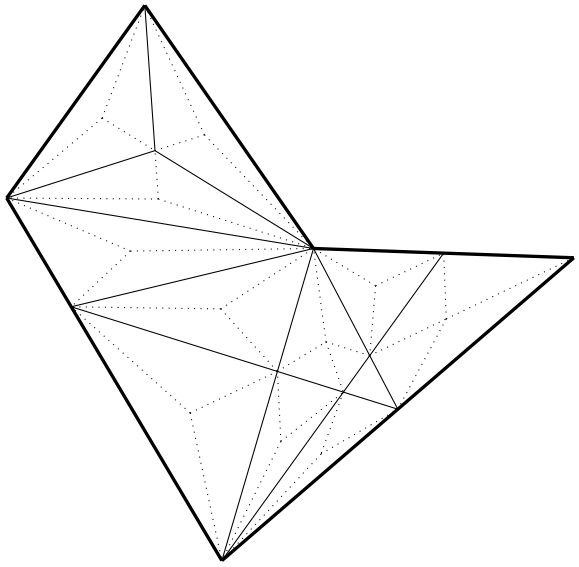
- Ainsi, seules les arêtes $a \in \mathcal{K}_1$ contenues dans $\partial\mathbf{P}$ et correspondant aux premiers et troisièmes cas apportent une contribution dans l'expression de $D_{\mathbf{P}}(\mathcal{K})$. Maintenant, si l'on considère deux complexes $\mathcal{K}, \mathcal{L} \in \mathfrak{K}_{\mathbf{P}}$, alors ils engendrent le même ensemble d'arêtes de ce type. En effet, on pourra construire un nouveau complexe $\mathcal{K} \wedge \mathcal{L} \in \mathfrak{K}_{\mathbf{P}}$ qui engendre les mêmes arêtes contributrices que $\mathcal{K}$ et $\mathcal{L}$ (le dessin est représenté dans $\mathbb{R}^2$ pour simplifier ; les arêtes deviennent alors les sommets) :



Il n'y a pas unicité de la construction, et il faut effectuer des choix après la superposition. En effet, il se peut que l'intersection de deux tétraèdres n'en soit pas un !

En revanche, on peut simplement considérer, pour chaque intersection de tétraèdres, l'isobarycentre de tous les sommets, et le lier à ces sommets, pour obtenir plusieurs nouveaux tétraèdres.

Sur le dessin précédent, voici ce que l'on devrait faire pendant l'étape de superposition :



Pour ce nouveau complexe, on aura alors, par toutes les observations précédentes :

$$D_{\mathbf{P}}(\mathcal{K}) = D_{\mathbf{P}}(\mathcal{K} \wedge \mathcal{L}) = D_{\mathbf{P}}(\mathcal{L})$$

Ceci permet de conclure que $D_{\mathbf{P}}$ est contante.

On peut alors définir :

Définition :

Soit $\mathbf{P} \in \wp_3$ un polyèdre non dégénéré de $\mathbb{R}^3$. On appelle **invariant de Dehn** de $\mathbf{P}$ l'unique élément de $D_{\mathbf{P}}(\mathfrak{K}_{\mathbf{P}})$, et on le note $D(\mathbf{P})$. Dans le cas où $\mathbf{P} \in \wp_3$ serait dégénéré, on définit $D(\mathbf{P}) = 0$.

Cette définition vérifie alors :

Théorème :

L'application ainsi construite $D : \wp_3 \to \mathbb{R} \otimes_{\mathbb{Z}} \Delta$ définit un invariant, appelé **invariant de Dehn**.

Preuve :

- Remarquons d'abord que si $\mathbf{P} = \bigcup_{\mathbf{T} \in \mathcal{K}_3} \mathbf{T}$, alors $D(\mathbf{P}) = \sum_{\mathbf{T} \in \mathcal{K}_3} D(\mathbf{T})$. En effet, $\mathbf{T}$ est lui-même un polyèdre : un complexe qui l'engendre est $\mathcal{T} = \{\mathbf{T}\} \cup \mathcal{F}(\mathbf{T})$, pour lequel $\mathcal{T}_3 = \{\mathbf{T}\}$.
- Soient $\mathbf{P}, \mathbf{Q} \in \wp_3$ deux polyèdres d'intersection dégénérée (éventuellement vide). On écrit alors :

$$\mathbf{P} = \bigcup_{\mathbf{T} \in \mathcal{K}_3} \mathbf{T} \qquad \text{et} \qquad \mathbf{Q} = \bigcup_{\mathbf{S} \in \mathcal{L}_3} \mathbf{S}$$

de telle sorte que $\mathbf{P} \uplus \mathbf{Q} = \bigcup_{\mathbf{T} \in (\mathcal{K} \cup \mathcal{L})_3} \mathbf{T}$. On obtient alors :

$$D(\mathbf{P} \uplus \mathbf{Q}) = \sum_{\mathbf{T} \in (\mathcal{K} \cup \mathcal{L})_3} D(\mathbf{T}) = \sum_{\mathbf{T} \in \mathcal{K}_3} D(\mathbf{T}) + \sum_{\mathbf{S} \in \mathcal{L}_3} D(\mathbf{S}) = D(\mathbf{P}) + D(\mathbf{Q})$$

- Soient donc maintenant $\mathbf{P}, \mathbf{Q} \in \wp_3$ deux polyèdres d'intersection quelconque. On développe, en utilisant le point précédent :

$$\begin{aligned} D(\mathbf{P}) + D(\mathbf{Q}) &= \Big[D(\mathbf{P} \setminus \mathbf{Q}) + D(\mathbf{P} \cap \mathbf{Q})\Big] + \Big[D(\mathbf{Q} \setminus \mathbf{P}) + D(\mathbf{P} \cap \mathbf{Q})\Big] \\ &= \Big[D(\mathbf{P} \setminus \mathbf{Q}) + D(\mathbf{Q} \setminus \mathbf{P}) + D(\mathbf{P} \cap \mathbf{Q})\Big] + D(\mathbf{P} \cap \mathbf{Q}) \\ &= D(\mathbf{P} \cup \mathbf{Q}) + D(\mathbf{P} \cap \mathbf{Q}) \end{aligned}$$

  L'application D ainsi définie décrit donc bien un invariant.

3.2 Condition d'annulation de l'invariant

On cherche dans cette partie à mieux appréhender l'invariant de Dehn, à travers son lieu d'annulation. Commençons d'abord avec le lemme suivant, similaire à ce qui a été fait en partie **2.1.3** :

Lemme :

Si $\Gamma \cup \{\pi\}$ désigne une **base de Hamel** (à savoir une $\mathbb{Q}$-base de $\mathbb{R}$), alors pour tout $\ell \otimes \overline{\theta} \in \mathbb{R} \otimes \Delta$, il existe une unique famille à support fini $(\ell_\gamma)_{\gamma \in \Gamma} \in \mathbb{R}^{(\Gamma)}$ telle que :

$$\ell \otimes \overline{\theta} = \sum_{\gamma \in \Gamma} \ell_\gamma \otimes \overline{\gamma}$$

où $\overline{\gamma}$ désigne la classe de γ dans $\Delta = \mathbb{R}/\pi\mathbb{Z}$.

Preuve : par un raisonnement analogue à la partie **2.1.3**, montrons que $\mathbb{R} \otimes_{\mathbb{Z}} \Delta \approx \mathbb{R}^{(\Gamma)}$.

- Observons d'abord le résultat suivant : si $f : X \times Y \to M$ est une application $\mathbb{Z}$-bilinéaire entre les $\mathbb{Q}$-modules X et Y et le $\mathbb{Z}$-module M, alors pour tout $q \in \mathbb{Q}$, $f(qx, y) = f(x, qy)$. En effet, en notant $q = \dfrac{a}{b}$, on a :

$$\begin{aligned} f(qx, y) = f\left(\frac{a}{b}x, y\right) &= af\left(\frac{1}{b}x, y\right) && \text{par linéarité à gauche} \\ &= f\left(\frac{1}{b}x, ay\right) && \text{par linéarité à droite} \\ &= f\left(\frac{1}{b}x, \frac{b}{b}ay\right) = bf\left(\frac{1}{b}x, \frac{1}{b}ay\right) = f(x, qy) \end{aligned}$$

- Définissons $\varphi : \mathbb{R} \times \Delta \to \mathbb{R}^{(\Gamma)}$ de la manière suivante : pour $\overline{\theta} \in \Delta$, il existe, par définition de Γ, une unique famille à support fini $(\lambda_\gamma)_{\gamma \in \Gamma} \in \mathbb{Q}^{(\Gamma)}$ et un unique rationnel $q \in \mathbb{Q}$ de sorte que $\theta = \sum_{\gamma \in \Gamma} \lambda_\gamma + q\pi$. On note alors $\gamma^*(\overline{\theta})$ le coefficient d'indice γ dans la somme, *ie* $\gamma^* : \Delta \to \mathbb{Q}$ est la forme $\mathbb{Z}$-linéaire (et même $\mathbb{Q}$-linéaire) sur Δ qui associe le coefficient devant γ dans la décomposition dans Γ de θ. Cette application ne dépend pas du

choix du représentant, justement car $\pi\mathbb{Q} \cap \Gamma = \varnothing$, puisqu'on a demandé que $\Gamma \cup \{\pi\}$ soit une base de Hamel (on peut toujours compléter la famille libre $\{\pi\}$ en une base du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$, *via* l'axiome du choix).

On définit maintenant $\varphi(\ell, \overline{\theta}) = (\gamma^*(\overline{\theta})\ell)_{\gamma\in\Gamma}$, qui est bien une famille à support fini puisque seul un nombre fini de $\gamma^*(\overline{\theta})$ est non nul. φ est $\mathbb{Z}$-bilinéaire :

$$\begin{aligned}
\varphi(\ell, \overline{\theta} + \mu\overline{\theta}') &= \varphi(\ell, \overline{\theta + \mu\theta'}) && \text{car } \mu \in \mathbb{Z} \\
&= \left(\gamma^*(\overline{\theta + \mu\theta'})\ell\right)_{\gamma\in\Gamma} \\
&= \left(\gamma^*(\overline{\theta} + \mu\overline{\theta}')\ell\right)_{\gamma\in\Gamma} \\
&= \left(\left[\gamma^*(\overline{\theta}) + \mu\gamma^*(\overline{\theta}')\right]\ell\right)_{\gamma\in\Gamma} && \text{car } \gamma* \text{ est } \mathbb{Z}\text{-linéaire} \\
&= \left(\gamma^*(\overline{\theta})\ell\right)_{\gamma\in\Gamma} + \mu\left(\gamma^*(\overline{\theta}')\ell\right)_{\gamma\in\Gamma} \\
&= \varphi(\ell, \overline{\theta}) + \mu\varphi(\ell, \overline{\theta}')
\end{aligned}$$

Il en va de même pour la linéarité à gauche.

- Soit $f : \mathbb{R} \times \Delta \to M$ une application bilinéaire vers un $\mathbb{Z}$-module M quelconque. Posons :

$$f_* : (\ell_\gamma)_{\gamma\in\Gamma} \in \mathbb{R}^{(\Gamma)} \mapsto \sum_{\gamma\in\Gamma} f(\ell_\gamma, \overline{\gamma})$$

Cette application est $\mathbb{Z}$-linéaire :

$$\begin{aligned}
f_*\left((\ell_\gamma)_{\gamma\in\Gamma} + \mu(\ell_\gamma)_{\gamma\in\Gamma}\right) &= f_*\left((\ell_\gamma + \mu\ell'_\gamma)_{\gamma\in\Gamma}\right) \\
&= \sum_{\gamma\in\Gamma} f(\ell_\gamma + \mu\ell'_\gamma, \gamma) \\
&= \sum_{\gamma\in\Gamma} f(\ell_\gamma, \gamma) + \mu f(\ell'_\gamma, \gamma) && \text{par linéarité à gauche de } f \\
&= \sum_{\gamma\in\Gamma} f(\ell_\gamma, \gamma) + \mu \sum_{\gamma\in\Gamma} f(\ell'_\gamma, \gamma) \\
&= f_*\left((\ell_\gamma)_{\gamma\in\Gamma}\right) + \mu f_*\left((\ell'_\gamma)_{\gamma\in\Gamma}\right)
\end{aligned}$$

De plus, elle factorise f :

$$\begin{aligned}
f_* \circ \varphi(\ell, \overline{\theta}) &= f_*\left((\gamma^*(\overline{\theta})\ell)_{\gamma\in\Gamma}\right) \\
&= \sum_{\gamma\in\Gamma} f(\gamma^*(\overline{\theta})\ell, \overline{\gamma}) \\
&= \sum_{\gamma\in\Gamma} f(\ell, \gamma^*(\overline{\theta})\overline{\gamma}) && \text{car } \gamma^*(\overline{\theta}) \in \mathbb{Q} \text{ et } f \text{ bilinéaire, par le premier point de la preuve} \\
&= f\left(\ell, \sum_{\gamma\in\Gamma} \gamma^*(\overline{\theta})\overline{\gamma}\right) && \text{car la somme est à support fini} \\
&= f(\ell, \overline{\theta}) && \text{car } \overline{\theta} = \sum_{\gamma\in\Gamma} \gamma^*(\overline{\theta})\overline{\gamma}
\end{aligned}$$

Ainsi, encore une fois, on a bien vérifié les hypothèses du produit tensoriel, *ie* on a obtenu : $\mathbb{R} \otimes_{\mathbb{Z}} \Delta \approx \mathbb{R}^{(\Gamma)}$. Par le même argument que celui détaillé en partie **2.1.3**, on obtient alors la décomposition souhaitée des tenseurs, de la forme :

$$\ell \otimes_{\mathbb{Z}} \overline{\theta} = \sum_{\gamma \in \Gamma} \ell_\gamma \otimes_{\mathbb{Z}} \overline{\gamma} \qquad \text{avec } \ell_\gamma = \gamma^*(\overline{\theta})\ell$$

Ce lemme nous permet alors d'obtenir la caractérisation suivante des tenseurs nuls :

Proposition :

Pour tout $\ell \neq 0$, $\ell \otimes_{\mathbb{Z}} \overline{\theta} = 0 \iff \theta \in \pi\mathbb{Q}$

Preuve : montrons les deux implications. Fixons $\ell \in \mathbb{R}^\star$.

- Si $\theta \in \pi\mathbb{Q}$, *ie* $\theta = q\pi$ avec $q \in \mathbb{Q}$, alors par le premier point de la preuve précédente, puisque l'application $\otimes_{\mathbb{Z}} : \mathbb{R} \times \Delta \to \mathbb{R} \otimes_{\mathbb{Z}} \Delta$ est bilinéaire, on a :

$$\ell \otimes_{\mathbb{Z}} \overline{\theta} = \ell \otimes_{\mathbb{Z}} (q\overline{\pi}) = (q\ell) \otimes_{\mathbb{Z}} \overline{\pi} = 0 \qquad \text{car } \overline{\pi} = 0 \text{ dans } \Delta$$

- Inversement, supposons que $\ell \otimes_{\mathbb{Z}} \overline{\theta} = 0$. On écrit :

$$\ell \otimes_{\mathbb{Z}} \overline{\theta} = \sum_{\gamma \in \Gamma} \gamma^*(\overline{\theta})\ell \otimes_{\mathbb{Z}} \overline{\gamma}$$

  Or, on a : $0 = \sum_{\gamma \in \Gamma} 0 \otimes_{\mathbb{Z}} \overline{\gamma}$, et la décomposition de cette forme est unique. On a ainsi :

$$\forall \gamma \in \Gamma,\ \gamma^*(\overline{\theta})\ell = 0,\ \ ie\ \ \gamma^*(\overline{\theta}) = 0 \qquad (\ell \neq 0)$$

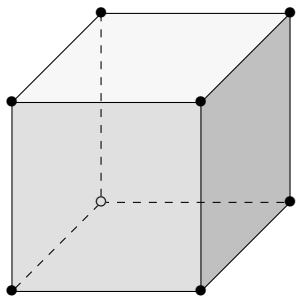
  On obtient alors $\overline{\theta} = 0$ dans $\mathbb{R}/\pi\mathbb{Q}$, *ie* $\theta \in \pi\mathbb{Q}$.

3.3 Le contre-exemple

Dehn eut donc l'idée de montrer qu'un cube et qu'un tétraèdre régulier n'ont pas le même invariant de Dehn, quel que soit leur volume. Observons donc ces deux invariants.

3.3.1 Le cube

Le cube **C** possède 12 arêtes, chacune de longueur $\ell > 0$, et d'angle dièdre $\dfrac{\pi}{2}$.



On a donc :

$$D(\mathbf{C}) = 12\ell \otimes \left(\frac{\pi}{2}\right) = 0$$

3.3.2 Le tétraèdre

Le tétraèdre régulier **T** est composé de 6 arêtes, chacune de longueur ℓ. Soit θ l'angle dièdre commun à chacune de ces arêtes.

On obtient alors :

$$D(\mathbf{T}) = 6\ell \otimes \theta$$

Que vaut l'angle dièdre θ du tétraèdre régulier ? Rappelons la **loi des cosinus**, connue aussi sous le nom de **règle d'Al-Kashi** :

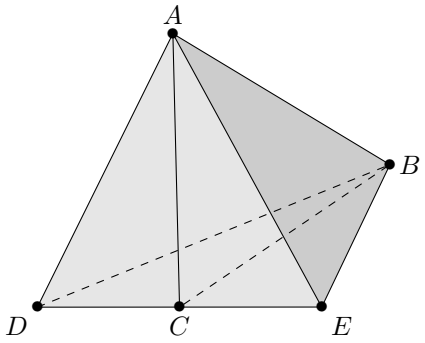
Règle d'Al-Kashi :

Étant donné un triangle ABC **quelconque**, on a :

$$AB^2 = AC^2 + BC^2 - 2AC \times BC \cos\widehat{ACB}$$

En réalité, il s'agit juste d'une manière savante et purement géométrique de développer $\|u-v\|^2$ à l'aide du produit scalaire, en écrivant $\langle u|v\rangle = \|u\| \times \|v\| \times \cos(\theta)$.

Soit donc un tétraèdre $ABDE$ de côté de longueur ℓ, soit C le milieu de DE, de sorte que $DE \perp AC$. Ainsi, l'angle dièdre est égal à $\theta = \widehat{ACB}$, par des raisons de symétries, et on a $AB = \ell$ et $AC = BC = \sqrt{\frac{3}{4}}\ell$ en appliquant le théorème de Pythagore au triangle ACD.



En appliquant la règle d'Al-Kashi au triangle ABC, on obtient :

$$\cos\theta = \frac{AC^2 + BC^2 - AB^2}{2AC \times BC} = \frac{3\ell^2/4 + 3\ell^2/4 - \ell^2}{2 \times 3\ell^2/4} = \frac{1}{3}$$

Ainsi, on a $D(\mathbf{T}) \neq 0$. En effet, si on avait $D(\mathbf{T}) = 0$, alors on aurait $\theta \in \pi\mathbb{Q}$, et $\cos(\theta) = \frac{1}{3} \in \mathbb{Q}$. Or, le théorème de la section 2.4 n'autorisait que les valeurs 0, $\pm\frac{1}{2}$ et ± 1 pour de tels angles.

3.3.3 Conclusion

Un tétraèdre régulier de côté de longueur a a pour volume $V = \frac{a^3}{6\sqrt{2}}$. La fonction $a > 0 \mapsto \frac{a^3}{6\sqrt{2}}$ est bijective de $\mathbb{R}_+^\star$ sur $\mathbb{R}_+^\star$, puisque $a \mapsto a^3$ l'est. Ainsi, il existe un tétraèdre $\mathbf{T}$ de volume 1. Soit $\mathbf{C}$ un cube de côté 1, donc de volume $1^3 = 1$ aussi.

On a : $D(\mathbf{C}) = 0$ et $D(\mathbf{T}) \neq 0$, mais $\mathrm{vol}(\mathbf{C}) = \mathrm{vol}(\mathbf{T})$. Le cube régulier et le tétraèdre régulier de même volume ne sont donc **pas** congrus, puisque leur invariant de Dehn diffère.

C'est un contre-exemple qui répond finalement à la question de Hilbert.

Des suites à ce troisième problème

En définitive, le troisième problème de Hilbert fut le plus rapide à être résolu, et était alors considéré comme le plus simple des vingt-trois proposés. Cependant, les ouvertures qui s'ensuivent sont, elles, d'un tout autre niveau.

Pour commencer, Jean-Pierre Sydler proposa une réciproque en 1965, aujourd'hui connue sous le nom de *théorème de Dehn-Sydler*. Ce théorème affirme que deux polyèdres sont congrus *si et seulement si* ils ont même volume **et** même invariant de Dehn. La preuve fut par la suite simplifiée en 1990, par Dupont et Sah, en faisant intervenir l'homologie de certains groupes (les modules des différentielles de Kähler).

Quant aux dimensions supérieures, la question se pose de savoir à quelle condition on aura la réciproque, *ie* on cherche à généraliser le théorème de Dehn-Sydler. Hugo Hadwiger résuma le théorème de Dehn-Sydler en 1968 à l'aide d'un unique invariant, l'invariant de Dehn-Hadwiger, qu'il généralisa à tout $\mathbb{R}^n$. Il exprima ainsi la condition nécessaire et suffisante pour la congruence de deux polyèdres en termes de cet invariant. Par la suite, Børge Jessen généralisa en 1972 cette condition nécessaire et suffisante dans la dimension 4.

Jessen se posa alors la question de savoir si le résultat se maintenait en travaillant en géométrie sphérique ou hyperbolique. Dans ces cadres-ci, la méthode proposée par Dehn fonctionne encore, avec plus de travail, et produit le même contre-exemple que celui mis en avant ici. Cependant, le problème reste ouvert à ce jour de savoir si le théorème de Dehn-Sydler reste vrai en géométrie sphérique ou hyperbolique.

Bibliographie

[Je] B. Jessen & A. Thorup, *"The algebra of polytopes in affine spaces"*, 1978, *Mathematica Scandinavia*, Volume 43, pages 211 à 240.

[La] S. Lang, *"Algebra"*, 1965, *Addison-Wesley*, Chapitre XVI, pages 409 à 419.

[Se] J.P. Serre & H. Cartan, *"Produits tensoriels"*, 1949, *Séminaire H. Cartan*, Tome 1, exposé n°11, pages 11-01 à 11-12.

[Ca] P. Cartier, *"Décomposition des polyèdres : le point sur le troisième problème de Hilbert"*, 1985, *Séminaire Bourbaki*, Volume 27, exposé n°646, pages 261 à 288.

[Sy] J.P. Sydler, *"Conditions nécessaires et suffisantes pour l'équivalence de polyèdres de l'espace euclidien à trois dimensions"*, 1965, *Commentarii mathematici Helvetici*, Volume 40, pages 43 à 80.

[Sc] R. Schwartz, *The Dehn-Sydler theorem explained*, 2010.

[Ne] S. C. Newman, *"A Classical introduction to Galois Theory"*, 1952, *Wiley*, Chapitre 9, pages 151 et suivantes.