191 : Exemples d'utilisation des techniques d'algèbre en géométrie.

Pandou

31 mai 2022

1 Actions de groupes et géométrie

1.1 Nombres complexes et géométrie plane

Théorème-Définition 1. *Soit $\mathcal{P}$ un plan affine euclidien muni d'un repère orthonormé direct $(O, \vec{e_1}, \vec{e_2})$. On a une bijection isométrique $z = x+iy \in \mathbb{C} \longmapsto M = O+x\vec{e_1}+y\vec{e_2} \in \mathcal{P}$. Le complexe $z = x + iy$ est appelé affixe du point M.*

Remarque 2 : On identifiera désormais les points de $\mathcal{P}$ avec les nombres complexes. Typiquement, si $z, z' \in \mathbb{C}$, alors $\overrightarrow{zz'}$ est un vecteur que l'on identifie à $z' - z$.

Théorème 3. *On a un isomorphisme de groupes entre $\mathbb{U} = \{x + iy \in \mathbb{C}, x^2 + y^2 = 1\}$ et $SO_2(\mathbb{R})$.*

Remarque 4 : L'action de $SO_2(\mathbb{R})$ sur $\mathbb{R}^2$ est la même que l'action de $\mathbb{U}$ sur $\mathbb{C}$ par multiplication à gauche.

Exemple 5 : i correspond à une rotation d'angle $\frac{\pi}{2}$ et -1 une rotation d'angle π.

Théorème 6 (Admis)**.** *L'application $\theta \in]-\pi, \pi] \longmapsto e^{i\theta} \in \mathbb{U}$ est une bijection. Si $u \in \mathbb{U}$, l'élément $\theta \in]-\pi, \pi]$ tel que $u = e^{i\theta}$ est appelée détermination de l'argument de u.*

Définition 7. *Soit $z, z' \in \mathbb{C}^*$, un angle orienté entre z et z' est une détermination de l'argument de la rotation qui envoie $\frac{z}{|z|}$ sur $\frac{z'}{|z'|}$.*
L'angle orienté de deux demi-droites vectorielles D_1, D_2 est l'angle orienté entre z_1 et z_2 où z_i est un vecteur directeur de D_i.

Théorème 8 (Relation de Chasles)**.** *Soit $z_0, ..., z_n \in \mathbb{C}$, on note θ_k l'angle orienté entre z_{k-1} et z_k. Alors, un angle orienté entre z_0 et z_n est $\theta_1 + ... + \theta_n$.*

Proposition 9. *On note $\sigma : z \in \mathbb{C} \longmapsto \overline{z} \in \mathbb{C}$. On a une bijection*

$$u \in \mathbb{U} \longmapsto \rho_u \circ \sigma \in O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$$

où ρ_u est la rotation d'angle u.
L'élément $\rho_u \circ \sigma$ est appelé symétrie orthogonale, dont l'axe est la droite engendrée par $\sqrt{u}$.

Proposition 10. *Soit $a \in \mathbb{C}^*$, l'application $\varphi_a : z \in \mathbb{C} \longmapsto az \in \mathbb{C}$ est une similitude directe (vectorielle) de $\mathbb{C}$, de rapport $|a|$ et d'angle $\arg(a)$.*
L'application $a \in \mathbb{C}^* \longmapsto \varphi_a$ est un isomorphisme de groupes entre $\mathbb{C}^*$ et le groupe des similitudes directes de $\mathbb{C}$.

Proposition 11. *Soit $a \in \mathbb{C}^*$, l'application $\psi_a : z \in \mathbb{C} \longmapsto a\overline{z} \in \mathbb{C}$ est une similitude indirecte (vectorielle) de $\mathbb{C}$, de rapport $|a|$ et de droite principale dirigée par $\frac{1}{2}\arg(a)$.*
L'application $a \in \mathbb{C}^* \longmapsto \psi_a$ est une bijection entre $\mathbb{C}^*$ et l'ensemble des similitudes indirectes de $\mathbb{C}$.

Théorème 12. *Si $(a, b) \in \mathbb{C}^* \times \mathbb{C}$, l'application $f_{a,b} : z \in \mathbb{C} \longmapsto az + b$ est une similitude (affine) directe de partie linéaire φ_a.*

Remarque 13 : $f_{a,b}$ est un déplacement si, et seulement si, $|a| = 1$. Si $a = 1$, $f_{a,b}$ est une translation et sinon, c'est une rotation qui fixe $\frac{1}{1-a}$.

Théorème 14. *Soit $(a, b) \in \mathbb{C}^* \times \mathbb{C}$, l'application $g_{a,b} : z \in \mathbb{C} \longmapsto a\overline{z} + b$.*

- *Si $|a| \neq 1$, $g_{a,b}$ admet un unique point fixe z_0, appelé centre de similitude. On note Δ la droite passant par z_0 et dirigée par $\frac{1}{2}\arg(a)$. $g_{a,b}$ est le produit d'une homothétie de centre z_0 et de rapport $|a|$ avec la symétrie orthogonale par rapport à Δ.*
- *Si $|a| = 1$ et $a\overline{b} + b \neq 0$, $g_{a,b}$ ne fixe aucun point, $g_{a,b}$ est le produit d'une symétrie orthogonale et d'une translation parallèle à l'axe de la symétrie.*
- *Si $|a| = 1$ et $a\overline{b} + b = 0$, $g_{a,b}$ est une symétrie orthogonale.*

1.2 Quaternions et isomorphismes exceptionnels

Théorème-Définition 15. *Il existe une $\mathbb{R}$-algèbre de dimension 4, notée $\mathbb{H}$, munie d'une base $(1, i, j, k)$ telle que*

1. *1 est l'élément neutre pour la multiplication.*
2. *$i^2 = j^2 = k^2 = ijk = -1$.*

On identifie $\mathbb{R}$ avec $\mathbb{R}1$ et on note $\mathbb{I} = \mathrm{Vect}(i, j, k)$.

Remarque 16 : $\mathbb{H}$ s'identifie $H := \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}, a, b \in \mathbb{C} \right\} \subset M_2(\mathbb{C})$ auquel cas, on a les identifications :

$$i \simeq \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \simeq \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{et} \qquad k \simeq \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Définition 17. *Si $h = a + bi + cj + dk \in \mathbb{H}$, on définit $\overline{h} = a - bi - cj - dk$ le conjugué et on note $N(h) = h\overline{h}$.*

Proposition 18. *$h \in \mathbb{H} \longmapsto \overline{h} \in \mathbb{H}$ est une involution linéaire qui vérifie $\overline{h_1 h_2} = \overline{h_2 h_1}$.*

Théorème 19.
1. *$\mathbb{H}$ est un corps (non commutatif).*
2. *Le centre de $\mathbb{H}$ est $\mathbb{R}$.*
3. *N est une forme quadratique définie positive. En particulier, $\mathbb{H}$ est un espace euclidien où le produit scalaire est $\langle h, h' \rangle = \frac{1}{2}(h\overline{h'} + h'\overline{h})$.*
4. *N est un morphisme de groupes surjectif entre $\mathbb{H}^*$ et $\mathbb{R}^*$.*
5. *$\mathbb{I} = \left\{ h \in \mathbb{H}, h^2 \in \mathbb{R}_- \right\} = \left\{ h \in \mathbb{H}, \overline{h} = -h \right\}$.*

Proposition 20. *On a des isomorphismes :*

$$\{h \in \mathbb{H}, N(h) = 1\} \simeq SU(2) \simeq \mathbb{S}^3$$

DEVELOPPEMENT 1

Théorème 21. *On a les isomorphismes exceptionnels suivants*

$$PSU(2) \simeq SO(3) \qquad et \qquad PSO(4) \simeq SO(3) \times SO(3)$$

1.3 Isomorphismes exceptionnels

Théorème 22. *Les groupes $SL_n(\mathbb{R})$, $SL_n(\mathbb{C})$, $SO_n(\mathbb{R})$ et $SO_0(p, q)$ sont des sous-variétés différentielles.*

DEVELOPPEMENT 2

Lemme 23.
1. *Soit $A \in GL_n(\mathbb{C})$ telle que $\forall H \in H_n(\mathbb{C}), AHA^* = H$, alors A est une homothétie.*
2. *Soit $M \in M_n(\mathbb{C})$ telle que $\forall H \in H_n(\mathbb{C}), MH + HM^* = 0$, alors $M = 0$.*

Théorème 24.

$$PSL_2(\mathbb{C}) \simeq SO_0(3, 1)$$

Remarque 25 : En étudiant d'autres actions de groupe, on trouve les autres isomorphismes suivants :

$$PSL_2(\mathbb{C}) \simeq SO_3(\mathbb{C}) \qquad \text{et} \qquad PSL_2(\mathbb{R}) \simeq SO_0(2, 1) \simeq PSU(1, 1)$$

2 Géométrie euclidienne

2.1 Coniques et formes quadratiques

Définition 26. *Soit q une forme quadratique réelle, on dit que q est positive (resp. définie positive) si $\forall E \setminus \{0\}, q(x) \geqslant 0$ (resp. $q(x) > 0$).*

Définition 27. *On note r la dimension maximale d'un sous-espace F tel que $q_{|F}$ est définie positive et s la dimension maximale d'un sous-espace G tel que $q_{|G}$ est définie négative. Le couple (r, s) est appelé signature de q.*

Théorème 28 (Inertie de Sylvester)**.** *Soit q une forme quadratique de signature (r, s), alors il existe une base dans laquelle la matrice de q est $\mathrm{diag}(I_r, -I_s, 0)$.*

Théorème 29 (Spectral)**.** *On suppose que E est un espace euclidien, il existe une base orthonormée qui est orthogonale pour q.*

Définition 30. *Soit q une forme quadratique non nulle, ℓ une forme linéaire sur $\mathbb{R}^n$, une quadrique est un ensemble*

$$\mathcal{Q} = \{v \in \mathbb{R}^n, q(v) + \ell(v) = k\} \qquad avec \qquad k \in \mathbb{R}$$

On parle de conique si $n = 2$.

Proposition 31. *Il existe une base orthogonale $(v_1, ..., v_n)$ de q pour le produit scalaire canonique de $\mathbb{R}^n$. Les directions $v_1, ..., v_n$ sont appelées les directions principales de $\mathcal{Q}$.*

Théorème 32. *Soit $\mathcal{C}$ une conique non vide et non réduit à un point. On suppose que q est non dégénérée. Alors, il existe une transformation orthogonale et une translation qui envoie $\mathcal{C}$ sur une conique d'équation*

$$ax^2 + by^2 = h$$

- *Si q est de signature $(2, 0)$ (ou $(0, 2)$), $\mathcal{C}$ est une ellipse dont une équation générique est $\frac{x^2}{A^2} + \frac{y^2}{B^2} = 1$.*
  A est appelée longueur du demi-grand axe et B la longueur du demi-petit arc.
- *Si q est de signature $(1, 1)$ et $h \neq 0$, alors $\mathcal{C}$ est une hyperbole dont une équation générique est $\frac{x^2}{A^2} - \frac{y^2}{B^2} = 1$.*
- *Si q est de signature $(1, 1)$ et $h = 0$, alors $\mathcal{C}$ est une réunion de deux droites sécantes.*

Théorème 33. *Soit $\mathcal{C}$ une conique non vide et non réduit à un point. On suppose que q est dégénérée, disons de signature $(1, 0)$. Alors, il existe une transformation orthogonale et une translation qui envoie $\mathcal{C}$ sur une conique d'équation*

$$ax^2 - 2sy = h$$

- *Si $s \neq 0$, $\mathcal{C}$ est une parabole dont une équation générique est $y = 2ax^2$.*
- *Si $s = 0$, $\mathcal{C}$ est une réunion de deux droites parallèles.*

2.2 Distance et volume

Théorème-Définition 34. *L'espace des applications n-linéaires alternées sur un espace de dimension n est de dimension 1. Plus précisément, si $(e_1, ..., e_n)$ est une base de E et f n-linéaires alternées, alors*

$$f(v_1, ..., v_n) = \det_{(e_i)}(v_1, ..., v_n) f(e_1, ..., e_n)$$

La quantité $\det(v_1|...|v_n)$ est appelée le déterminant de la famille $(v_1, ..., v_n)$ dans la base $(e_1, ..., e_n)$.

Théorème 35. *Soit $v_1, ..., v_n \in \mathbb{R}^n$, on note $\mathrm{Vol}(v_1, ..., v_n)$ le volume du parallélipipède engendré par $v_1, ..., v_n$, alors on a*

$$\mathrm{Vol}(v_1, ..., v_n) = \left|\det(v_1|...|v_n)\right|$$

Corollaire 36. *Soit X une partie mesurable de $\mathbb{R}^n$ et $u \in \mathcal{L}(\mathbb{R}^n)$, alors $u(X)$ est mesurable et*

$$\lambda\big(u(X)\big) = \left|\det(u)\right|\lambda(X)$$

Application 37 : Soit $v_1, ..., v_n \in \mathbb{R}^n$, on a $\left|\det(v_1|...|v_n)\right| \leqslant \|v_1\|...\|v_n\|$.

Définition 38. *Soit $v_1, ..., v_n \in E$ où E est préhilbertien. La matrice de Gram est $\mathrm{Gram}(v_1, ..., v_n) = \big(\langle v_i, v_j\rangle\big)_{1\leqslant i,j\leqslant n}$ et on note $G(v_1, ..., v_n) = \det\big(\mathrm{Gram}(v_1, ..., v_n)\big)$.*

Proposition 39. *Soit $(v_1, ..., v_n)$ une base de E où E est préhilbertien, alors $G(v_1, ..., v_n) = \mathrm{Vol}(v_1, ..., v_n)^2$.*

Corollaire 40. *Soit E un espace préhilbertien et F un sous-espace de dimension finie dont une base est $(v_1, ..., v_n)$. Alors,*

$$d(x, F)^2 = \frac{G(v_1, ..., v_n, x)}{G(v_1, ..., v_n)}$$

Application 41 : (Théorème de Müntz) Soit (α_n) une suite de réels strictement positifs et strictement croissant. Alors, $\mathrm{Vect}(x^{\alpha_n})_{n\in\mathbb{N}}$ est dense dans L^2 si, et seulement si, $\sum \frac{1}{\alpha_n}$ diverge.

Proposition 42. *Soit $A \in S_n^{++}(\mathbb{R})$ et $B \in S_n(\mathbb{R})$, il existe $P \in GL_n(\mathbb{R})$ et D une matrice diagonale réelle telles que*

$$A = PP^T \qquad et \qquad B = PDP^T$$

DEVELOPPEMENT 3

Lemme 43. *Soit $A, B \in S_n^{++}(\mathbb{R})$ et $\alpha + \beta = 1$ positifs tels que*

$$\det(\alpha A + \beta B) \geqslant \det(A)^\alpha \det(B)^\beta$$

Proposition 44. *Soit un ellipsoïde définie par une forme quadratique définie positive $A \in S_n^{++}(\mathbb{R})$: $\mathcal{E}_A = \{x \in \mathbb{R}^n, \langle Ax, x\rangle \leqslant 1\}$. Alors,*

$$\lambda(\mathcal{E}_A) = \frac{V_0}{\sqrt{\det(A)}}$$

où V_0 est le volume de la boule unité de $\mathbb{R}^n$.

Théorème 45 (Ellipsoïde de John-Loewner)**.** *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe un unique ellipsoïde centré en 0 de volume minimal contenant K.*

Application 46 : Soit G un sous-groupe compact de $GL(E)$. En considérant $K = \{g \cdot x, g \in G, \|x\| = 1\}$, il existe une forme quadratique q définie positive telle que $G \subset O(q)$.

2.3 Système de racines

On fixe un espace euclidien E de dimension n.

Définition 47. *Soit $\alpha \in E$, on note σ_α la réflexion par rapport à l'hyperplan $\alpha^\perp$:*

$$\forall \beta \in E, \sigma_\alpha(\beta) = \beta - \frac{2(\beta, \alpha)}{(\alpha, \alpha)}\alpha$$

On note $\langle \beta, \alpha\rangle = \frac{2(\beta, \alpha)}{(\alpha, \alpha)}$.

Définition 48. *Un système de racines est une partie finie Φ de E telle que*

1. *$0 \notin \Phi$ et $\mathrm{Vect}(\Phi) = E$.*
2. *Si $\alpha \in \Phi$, les seuls multiples de α dans Φ sont $\pm\alpha$.*
3. *Si $\alpha \in \Phi$, alors σ_α laisse Φ invariant.*
4. *Si $\alpha, \beta \in \Phi, \langle \beta, \alpha\rangle \in \mathbb{Z}$.*

Exemple 49 : Voir annexe.

Proposition 50. *Soit Φ un système de racines et $\alpha, \beta \in \Phi$ non colinéaires et $\|\beta\| \geqslant \|\alpha\|$, les angles et les rapports de longueur peuvent être :*

- *$\frac{\pi}{2}$ et $\frac{\|\beta\|^2}{\|\alpha\|^2}$ quelconque.*
- *$\frac{\pi}{3}$ ou $\frac{2\pi}{3}$ et $\frac{\|\beta\|^2}{\|\alpha\|^2} = 1$.*

- $\frac{\pi}{4}$ *ou* $\frac{3\pi}{4}$ *et* $\frac{\|\beta\|^2}{\|\alpha\|^2} = 2$.
- $\frac{\pi}{6}$ *ou* $\frac{5\pi}{6}$ *et* $\frac{\|\beta\|^2}{\|\alpha\|^2} = 3$.

Définition 51. *Une base Δ de Φ est une partie de Φ telle que*

1. *Δ est une base de E.*
2. *Tout élément de Φ est combinaison linéaire à coefficients entiers tous de même signe d'éléments de Δ.*

Les éléments de Δ sont appelés racines simples de Φ.

Proposition 52. *Si α, β sont deux racines simples, alors $(\alpha, \beta) \leqslant 0$.*

Théorème 53. *Φ admet toujours une base.*

Définition 54. *On dit que Φ est irréductible si on ne peut pas écrire $\Phi = \Phi_1 \sqcup \Phi_2$ avec $\Phi_1 \perp \Phi_2$.*

Définition 55. *Soit $(\alpha_1, ..., \alpha_n)$ une base de Φ. On définit le graphe de Coxeter de Φ comme le graphe à n sommets où i et j sont reliés par $\langle \alpha_i, \alpha_j \rangle \langle \alpha_j, \alpha_i \rangle$ arêtes.*

Théorème 56. *Les graphes de Coxeter d'un système de racines irréductible sont parmi les suivants : (insérer dessin).*

Remarque 57 : En fait, ces graphes de Coxeter réalisent tous un système de racines irréductible, mais ceci s'éloigne du sujet.

3 Constructibilité à la règle et au compas

3.1 Extensions de corps

Définition 58. *On dit que L/K est une extension de corps si L est un surcorps de K. Alors, L est naturellement un K-espace vectoriel, on dit que l'extension est finie si L est de dimension finie sur K et on note $[L : K] = \dim_K(L)$ le degré de l'extension.*

Théorème 59 (Base téléscopique)**.** *Soit $M/L/K$ une tour d'extensions de corps, $(e_i)_{i \in I}$ une base de L sur K, $(f_j)_{j \in J}$ une base de M sur L. Alors, $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K.*

Corollaire 60. *Soit $M/L/K$ une tour d'extensions de corps. Alors, $[M : K]$ est fini si, et seulement si, $[L : K]$ et $[M : L]$ sont finis et dans ce cas,*

$$[M : K] = [M : L] \times [L : K]$$

Définition 61. *Soit L/K une extension et $\alpha \in L$. On dit que α est algébrique sur K s'il existe $P \in K[X]$ non nul tel que $P(\alpha) = 0$. Le polynôme unitaire générateur de l'idéal annulateur de α est appelé le polynôme minimal de α sur K.*
Sinon, on dit que α est transcendant sur K.

Exemple 62 :

- $\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$.
- Il existe des nombres transcendants sur $\mathbb{Q}$.

Théorème 63. *Soit L/K une extension et $\alpha \in L$. On a équivalence entre :*

1. *α est algébrique sur K.*
2. *$K[\alpha] = K(\alpha)$.*
3. *$K(\alpha)$ est de dimension finie sur K.*

3.2 Construction à la règle et au compas

On munit $\mathbb{R}^2$ de sa structure d'espace affine orienté canonique.

Définition 64. *Soit $X \subset \mathbb{R}^2$ de cardinal au moins 2. On distingue deux constructions à la règle et au compas :*

1. *Les droites affines (AB) pour $A \neq B$ des points de X.*
2. *Les cercles centrés en un point $A \in X$ et passant par un point $B \neq A \in X$.*

On dit que M est constructible en un pas à partir de X si, et seulement si, M est un point d'intersection de $1. \cap 1.$, $2. \cap 2.$ ou $1. \cap 2.$.

Définition 65. *On note $\mathcal{C}_0 = \{(0,0), (0,1)\}$, puis $\mathcal{C}_i$ l'ensemble des points constructibles en un point à partir de $\mathcal{C}_{i-1}$.*
On dit qu'un point $M \in \mathbb{R}^2$ est constructible lorsque $\exists n \in \mathbb{N}, M \in \mathcal{C}_n$.

Proposition 66. *Soit M, A et B des points constructibles. Alors,*

1. *Le symétrique de M par rapport à O est constructible.*
2. *Le milieu de $[A, B]$ est constructible. Plus généralement, la médiatrice de $[A, B]$ est constructible.*
3. *La perpendiculaire à (AB) passant par M est constructible.*
4. *La parallèle à (AB) passant par M est constructible.*

Définition 67. *On dit que $x \in \mathbb{R}$ est constructible lorsque $(0, x)$ est constructible. On note E l'ensemble des nombres constructibles.*

Proposition 68. *E est une extension de $\mathbb{Q}$ stable par la racine carrée.*

Lemme 69. *Soit F un sous-corps de $\mathbb{R}$, on note $\mathcal{D}$ l'ensemble des droites passant par deux points de F^2 et $\mathcal{C}$ l'ensemble des cercles centrés en un point de F^2 et de rayon égal à la distance entre deux points de F^2. Alors,*

1. *Si $d \in \mathcal{D}$, alors d a une équation cartésienne à coefficients dans F.*
2. *Si $c \in \mathcal{C}$, alors c a une équation cartésienne à coefficients dans F.*

Proposition 70. *On reprend les notations du lemme précédent. Soit $d_1, d_2 \in \mathcal{D}$ deux droites et $\gamma_1, \gamma_2 \in \mathcal{C}$. Alors,*

1. *Si d_1 et d_2 sont sécantes, alors leur point d'intersection est dans F^2.*

2. *Si $M \in d_1 \cap \gamma$, alors $M \in F^2$, ou il existe une extension quadratique K/G telle que $M \in K^2$.*
3. *Si $M \in \gamma_1 \cap \gamma_2$, alors $M \in F^2$, ou il existe une extension quadratique K/G telle que $M \in K^2$.*

Théorème 71. *Soit $t \in \mathbb{R}$, alors t est constructible si, et seulement s'il existe une tour finie d'extensions quadratiques $\mathbb{Q} < F_1 < ... < F_p$ (ie F_{i+1}/F_i est quadratique) tel que $t \in F_p$.*

Applications 72 :
- On ne peut pas dupliquer le cube.
- On ne peut pas trissecter l'angle.

Remarque 73 : La quadrature du cercle est aussi impossible, car π est transcendant (admis).

3.3 Construction de polygones réguliers

Proposition 74. *Soit $\theta \in \mathbb{R}$. On a équivalence entre :*

1. $(\cos\theta, \sin\theta)$ *est constructible.*
2. $(\cos\theta, 0)$ *est constructible.*
3. $(\sin\theta, 0)$ *est constructible.*

On dit alors que θ est un angle constructible.

Définition 75. *On dit que le polygone régulier à n côtés, noté P_n, est constructible si, et seulement si, l'angle $\dfrac{2\pi}{n}$ est constructible.*

Lemme 76. *P_{nm} est constructible si, et seulement si, P_n et P_m sont constructibles.*

Théorème-Définition 77. *Soit $q \in \mathbb{N}^*$, si $2^q + 1$ est premier, alors q est une puissance de 2. On note $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat.*

Exemples 78 : $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ sont premiers, mais F_5 n'est pas premier.

Théorème 79 (Gauss)**.** *Soit $n \geqslant 2$, alors P_n est constructible si, et seulement si, n est de la forme 2^α ou $2^\alpha p_1 ... p_k$ où les p_i sont des nombres de Fermat premiers distincts.*

Exemples 80 : Les polygones à $2, 4, 5, 10, 17$ côtés sont constructibles, mais par exemple l'heptagone régulier ne l'est pas.

Références :

- Arnaudiès, Fraysse, Cours de mathématiques Tome 1.
- Arnaudiès, Fraysse, Cours de mathématiques Tome 4.
- Caldero, Germoni, H2G2.
- Gourdon, Algèbre.
- Gozard, Théorie de Galois.
- Perrin, Cours d'algèbre.