

Polygones Constructibles

Jean-René Licois

Université François-Rabelais
Laboratoire de Mathématiques et Physique Théorique

23 mai 2007 / Journée des Maths

Définition

Construction à la règle et au compas :

Des points étant donnés, on se propose de construire un point qu'ils déterminent en n'usant que de la règle et du compas, la règle ne devant servir qu'à joindre deux points donnés ou précédemment obtenus, le compas ne devant servir qu'à tracer une circonférence dont le centre est un point donné ou déjà obtenu et dont le rayon est la distance de deux points donnés ou déjà obtenus.

Vocabulaire

5 côtés pentagone

6 côtés hexagone

7 côtés heptagone

8 côtés octogone

9 côtés ennéagone

10 côtés décagone

11 côtés hendécagone

12 côtés duodécagone

13 côtés tridécagone

15 côtés pentadécagone (ou pentédécagone)

17 côtés heptadécagone

Enoncés

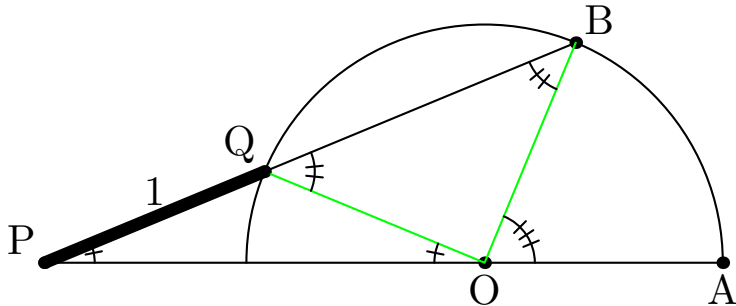
Parmi les nombreux problèmes de construction que se sont posés les anciens, on peut en citer trois

- La duplication du cube : construire un cube de volume double d'un cube donné
- La trisection de l'angle : couper un angle en trois angles égaux, dans le cas général
- La quadrature du cercle : construire un carré de même aire qu'un cercle donné.

- Nous verrons plus loin que ces problèmes ne sont pas résolubles à la règle et au compas, néanmoins les anciens avaient proposé des solutions, généralement en utilisant une courbe auxiliaire.
- C'est d'ailleurs le premier problème qui conduisit les Grecs à l'étude des coniques.
- Les deux premiers problèmes sont de même nature, alors que le troisième est d'une toute autre difficulté.

Archimède

La solution d'ARCHIMÈDE utilise une règle graduée.



Conchoïde de Nicomède

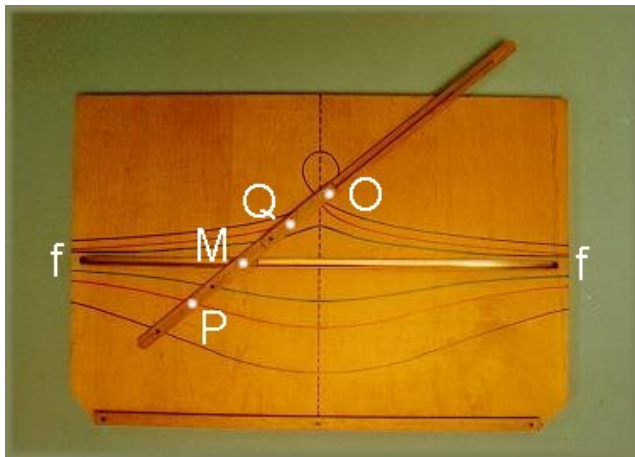
- B étant fixé, lorsque P décrit la droite (OA) le point Q décrit une courbe appelée *Conchoïde de Nicomède*.
- C'est la première courbe à avoir été définie par un procédé mécanique.
- C'est aussi la solution du problème du chien et de son maître ...

Citation

De même que les Grecs anciens (de l'époque de Platon) ignoraient la notion de nombre telle que nous la connaissons, il n'imaginaient pas qu'une courbe puisse être définie autrement que par un procédé mécanique.

Certains ont prétendu [. . .] que Platon blâmait quelques uns de ses disciples (Menechme, Eudoxe. . .) pour avoir, par l'emploi de ces instruments, altéré la pureté de la géométrie. (H. LEBESGUE)

Nicomède II

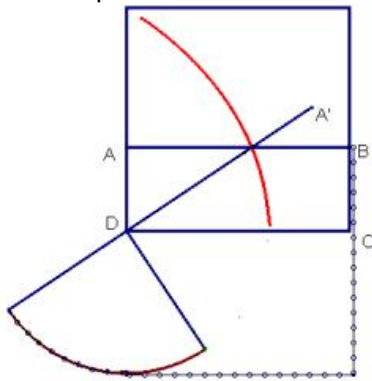
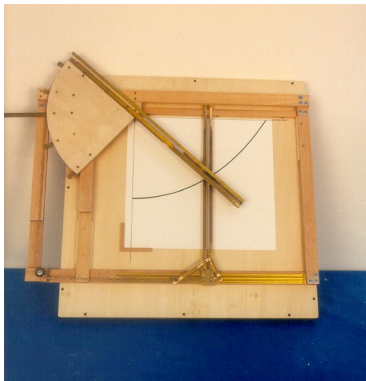


Nicomède III

On peut aussi utiliser une conchoïde de droite.

Dinostrate

Dinostrate utilise une courbe auxiliaire la quadratrice.

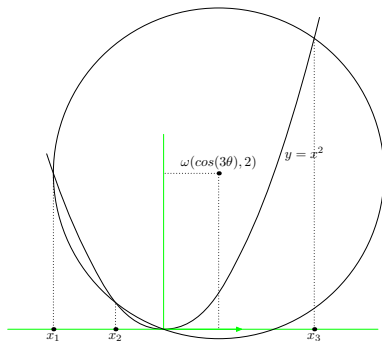
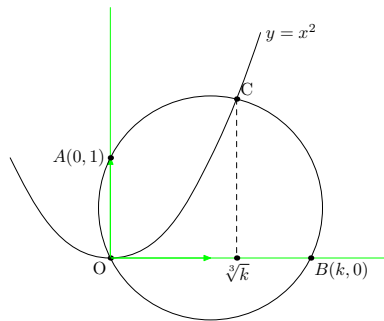


Descartes

Il faudra attendre DESCARTES pour définir une courbe par une (ou plusieurs) équations. Voici les solutions proposées pour les deux premiers problèmes utilisant la parabole $y = x^2$.

Trisection On trace le cercle de centre $\omega(\cos(3\theta), 2)$ passant par 0. Les abscisses x_i des points d'intersection (autre que l'origine) avec la parabole sont $2 \cos(\theta + 2k\pi/3)$.

Racine cubique On trace le cercle de diamètre $[AB]$ avec $B(k, 0)$ et $A(0, 1)$. L'abscisse du deuxième point d'intersection (autre que l'origine) avec la parabole est $\sqrt[3]{k}$.



Trisecteurs divers

- Le limaçon de Pascal
- La francisque
- et même par pliage : voir
http://fr.wikipedia.org/wiki/Trisection_de_l%27angle

L'équation du troisième degré

Considérons l'équation $X^3 + aX^2 + bX + c = 0$ et supposons qu'elle admette trois racines ; par un changement de variable standard $X = x - \frac{a}{3}$ on se ramène à une équation de la forme $x^3 - px = q$ avec $p > 0$. En posant $x = 2u\sqrt{(p/3)}$, on obtient

$$u^3 - \frac{3}{4}u = \frac{3\sqrt{3}}{8} \frac{q}{p^{3/2}}. \quad (1)$$

Soit θ tel que $\cos(\theta) = \frac{3\sqrt{3}}{2} \frac{q}{p^{3/2}}$ (ce qui est possible si et seulement si $4p^3 - 27q^2 > 0$) ; les solutions de (1) sont données par $\cos(\theta/3 + 2k\pi/3)$: la résolution se ramène à une trisection !

Les preuves du XIXème

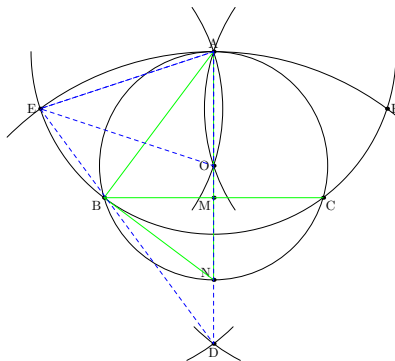
- Les constructions au compas seul.
- Théorème de GAUSS-WANTZEL : Bien que GAUSS n'ait jamais publié de preuve complète il est probable qu'il connaissait le résultat. Par contre il a établi à l'âge de 19 ans, la méthode de construction du polygone à 17 côtés que nous détaillerons plus loin (publiée en 1801). L'article du français Pierre Laurent WANTZEL date de 1837.
- LINDEMANN : il a établi en 1882 la transcendance de π et donc l'impossibilité de la quadrature du cercle.

Le compas seul

L'italien MASCHERONI a prouvé en 1797 que toute construction à la règle et au compas pouvait être effectuée au compas seul (en fait ce résultat avait déjà été établi par le danois MOHR en 1672).

En particulier il est possible de déterminer le centre d'un cercle déjà tracé à l'aide du compas seul (*Problème de Napoléon*).

Construction



Soit Γ le cercle donné $A \in \Gamma$. On trace un cercle Γ_1 de centre A qui recoupe Γ en B et C . On construit le point D symétrique de A par rapport à (BC) comme intersection du cercle de centre B passant par A et du cercle de centre C passant par A . Le cercle de centre D passant par A recoupe Γ_1 en E et F . L'intersection des cercles de centre E et F passant par A donne le point O centre du cercle Γ .

Solution du problème de Napoléon

Soit M le milieu de (BC) et $N \in \Gamma$ le point diamétralement opposé à A . Les points A, M, N et D sont alignés. Les triangles ABM et ANB sont semblables, de même que ADE et AEO . On en déduit

$$\frac{AB}{AM} = \frac{AN}{AB}, \quad \frac{AD}{AE} = \frac{AE}{AO}.$$

Comme $AD = 2AM$ et $AB = AE$ on obtient $AO = \frac{1}{2}AN$, donc O est le centre de Γ .

Théorème de GAUSS-WANTZEL

Théorème

*Un polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est de la forme $2^\alpha p$, p étant égal à 1, ou à un nombre premier de la forme $2^{2^m} + 1$, ou à un produit de tels facteurs premiers **différents**.*

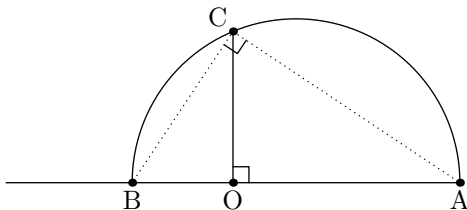
Les nombres premiers de la forme $2^{2^m} + 1$ sont appelés nombre de FERMAT : les seuls connus sont : 3, 5, 17, 257, 65537.

Construction de base

- 1 la somme de deux longueurs
- 2 le produit/quotient de deux longueurs
- 3 la racine carrée d'une longueur
- 4 les racines d'un trinôme

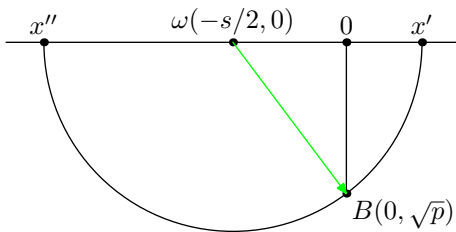
C3

Les constructions 2 et 3 sont basées sur les relations métriques dans le triangle rectangle et/ou la notion de puissance d'un point par rapport à un cercle. Par exemple (construction C3), soient $O(0,0)$, $A(1,0)$, $B(-p,0)$ avec $p > 0$. Le cercle de diamètre AB recoupe l'axe des ordonnées aux points C et C' d'ordonnées respectives $\pm\sqrt{p}$.



C4

Les racines du polynôme $x^2 - sx = p$, ($p > 0$), sont les abscisses x' et x'' des points d'intersection avec l'axe des abscisses du cercle de centre $\omega(-s/2, 0)$ passant par le point $B(0, \sqrt{p})$ (construction C4).



Notations pour les polygones

Pour construire un polygone régulier à n côtés, il suffit de déterminer $e^{2i\pi/n}$, ou sa partie réelle, ou sa partie imaginaire. On notera $\theta = 2i\pi/n$ et

$$(k) = \cos(k\theta).$$

On a alors (transformation des produits en somme)

$$(k)(h) = \frac{1}{2}((k+h) + (k-h))$$

et (somme des racines de $z^n - 1$)

$$(1) + (2) + (3) + \cdots + (n-1) = -1.$$

Pentagone

Bien qu'il existe de nombreuses constructions exactes à la règle et au compas, et même certaines utilisant par exemple une équerre :

Soit (C) le cercle trigonométrique, $A(1, 0)$, $B(0, 1)$, $A'(-1, 0)$ et $B'(0, -1)$. Soit C tel que $OACB'$ soit un carré et $P \in [A'O]$ tel que $PB \perp PC$; alors $BP = s_5$ côté du pentagone.

Pentagone II

Nous allons utiliser une méthode, que l'on espère généraliser.
 Pour $n = 5$, on a évidemment $(1) = (4)$, $(2) = (3)$ d'où les deux relations

$$(1) + (2) = -\frac{1}{2}$$

et

$$(1)(2) = \frac{1}{2}((3) + (1)) = \frac{1}{2}((2) + (1)) = -\frac{1}{4}.$$

Donc (1) et (2) sont racines de $x^2 + \frac{1}{2}x - \frac{1}{4}$.

Pentagone III

On en déduit

- la valeur de $\cos(2\pi/5) = \frac{\sqrt{5} - 1}{4}$, celle de $\cos(4\pi/5) = -\frac{\sqrt{5} + 1}{4}$,
- la longueur du côté du pentagone, d'après la formule d'AL KASHI, $s_5^2 = 1 + 1 - 2\cos(2\pi/5) = \frac{5 - \sqrt{5}}{2}$,
- la construction : on place $B(0, -1/2)$ et $C(-1/4, 0)$; le cercle de centre C passant par B donne les deux cosinus cherchés (cf. Construction C4).

Heptadécagone

Pour $n = 17$, on a $(9) = (8)$, $(10) = (7)$, $(11) = (6)$,... Posons

$$P_1 = (1) + (2) + (4) + (8), \quad P_2 = (3) + (5) + (7) + (6).$$

On a immédiatement $P_1 + P_2 = -\frac{1}{2}$; le calcul du produit $P_1 P_2$ conduit à

$$P_1 P_2 = 2(P_1 + P_2) = -1.$$

Donc P_1 et P_2 sont les racines de $P^2 + \frac{1}{2}P - 1$ et sont donc constructibles à la règle et au compas.

Heptadécagone II

Posons maintenant $Q'_1 = (1) + (4)$ et $Q''_1 = (8) + (2)$; on a alors $Q'_1 + Q''_1 = P_1$ et

$$Q'_1 Q''_1 = \frac{1}{2}((9) + (7) + (3) + (1) + (12) + (4) + (6) + (2)) = -\frac{1}{4}$$

d'ou Q'_1 et Q''_1 sont les racines de $Q_1^2 - P_1 Q_1 - \frac{1}{4}$ et sont constructibles. De même pour $Q'_2 = (3) + (5)$ et $Q''_2 = (7) + (6)$ qui sont racines de $Q_2^2 - P_2 Q_2 - \frac{1}{4}$ et constructibles.

Heptadécagone III

Enfin, pour (1) et (4) on obtient les relations $(1) + (4) = Q'_1$ et $(1)(4) = \frac{1}{2}((5) + (3)) = \frac{1}{2}Q'_2$. On en déduit les valeurs

$$P_1 = \frac{-1 + \sqrt{17}}{4} \quad P_2 = -\frac{1 + \sqrt{17}}{4}$$

$$Q'_1 = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{8} \quad Q'_2 = \frac{-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}}{8}$$

$$Q'_2 = \frac{-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}}{8} \quad Q''_2 = \frac{-1 - \sqrt{17} - \sqrt{34 + 2\sqrt{17}}}{8}$$

$$16 \cos(2\pi/17) = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} \\ + \sqrt{68 + 12\sqrt{17} - \sqrt{34 - 2\sqrt{17}}(6 + 2\sqrt{17})}$$

C'est une démonstration constructive, puisqu'elle montre que par résolutions successives d'équations du second degré on peut obtenir $\cos(2\pi/17)$ (ce qui est une condition nécessaire et suffisante de constructibilité *voir plus loin*).

Dans la dernière partie de l'exposé on montrera pourquoi et comment sont choisis les cosinus qui définissent P_1 et P_2 .

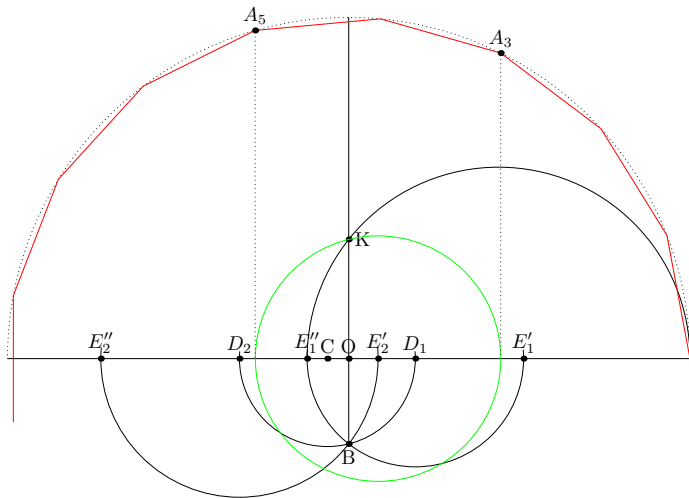
Construction de l'heptadécagone

Voici la construction donnée par GAUSS.

- 1 Il commence par considérer $p_1 = \frac{1}{4}P_1$, $p_2 = \frac{1}{4}P_2$ qui sont racines de $x^2 - \frac{1}{8}x - \frac{1}{16}$. On construit les points $B(0, -1/4)$ et $C = (-1/16, 0)$: le cercle de centre C passant par B donne les points D_1 et D_2 d'abscisses p_1 et p_2 (cf. C4).
- 2 De même pour $q'_1 = \frac{1}{2}Q'_1$, $q''_1 = \frac{1}{2}Q''_1$ qui sont racines de $x^2 - 2p_1x - \frac{1}{16}$ et $q'_2 = \frac{1}{2}Q'_2$, $q''_2 = \frac{1}{2}Q''_2$ qui sont racines de $x^2 - 2p_2x - \frac{1}{16}$. Les cercles de centre D_1 et D_2 passant par B donnent les points E'_1, E''_1, E'_2, E''_2 d'abscisses respectives q'_1, q''_1, q'_2 et q''_2 (cf. C4).

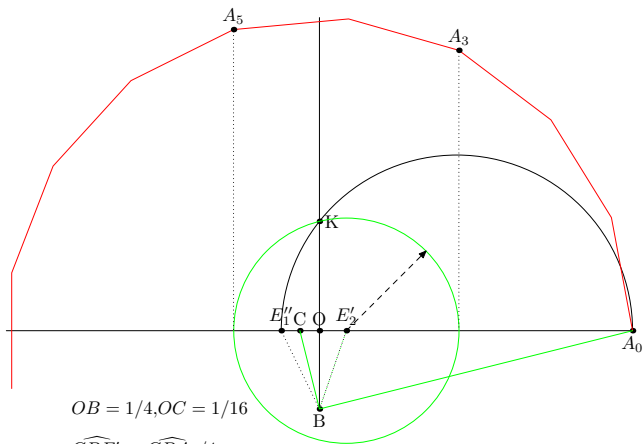
Construction de l'heptadécagone II

- Le cercle de diamètre A_0E_1'' coupe OB en K tel que $OK^2 = -q_1''$ (cf. C3) et le cercle de centre E_1'' passant par K coupe OA_0 aux points d'abscisses (3) et (5) solutions de $x^2 - q_2'x + q_1''$ (cf. C4).



Construction de l'heptadécagone III

La construction a été simplifiée par ROBINSON en 1893, en remarquant que les cercles passant par B n'ont servi qu'à construire des pieds de bissectrices : D_1 et D_2 sont les pieds des bissectrices de l'angle CBA_0 , les points E'_2 et E''_1 correspondent aux bissectrices de CBD_1 et CBD_2 . On construit donc E'_2 en divisant l'angle CBA_0 en quatre, puis E''_1 tel que $E''_1BE'_2$ mesure $\pi/4$.



$$OB = 1/4, OC = 1/16$$

$$\widehat{CBE_2'} = \widehat{CA_0}/4$$

$$\widehat{E_1'BE_2'} = \pi/4$$

Heptagone

Pour $n = 7$, on a $(6) = (1)$, $(4) = (3)$, $(5) = (2)$. On ne peut partager les cosinus en deux groupes, cherchons donc directement une équation dont les racines sont (1) , (2) et (3) . Comme toujours $(1) + (2) + (3) = -\frac{1}{2}$. Puis

$$(1)(2)(3) = \frac{1}{2}(1)((2) + (1)) = \frac{1}{4}((3) + (1) + (2) + (0)) = \frac{1}{8}$$

et enfin

$$(1)(2) + (2)(3) + (3)(1) = \frac{1}{2}((3) + (1) + (2) + (1) + (3) + (2)) = -\frac{1}{2}.$$

Heptagone II

Les trois cosinus sont donc racines de $X^3 + \frac{1}{2}X^2 - \frac{1}{2}X - \frac{1}{8}$ qui devient par changement de variable $X = -\frac{1}{6} + \frac{\sqrt{7}}{3}u$

$$u^3 - \frac{3}{4}u = \frac{1}{8\sqrt{7}}.$$

Ce qui fournit une construction à l'aide du trisecteur.

Construction

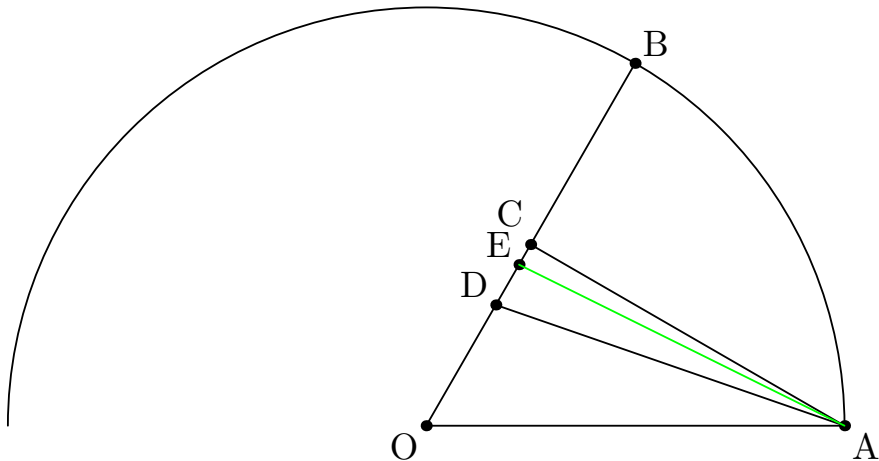
- On construit $\overline{O\omega} = -\frac{1}{6}$ puis $\overline{\omega I} = \frac{1}{2\sqrt{7}}$.
- On construit l'angle $\widehat{X\omega T}$ tel que son cosinus vaut ωI .
- On divise trisecte l'angle, ce qui donne le point U
- Enfin, on place $\omega J = \frac{\sqrt{7}}{3}\overline{\omega U}$. OJ donne le cosinus cherché.

Heptagone III

Une autre construction, utilisant le trisecteur est donnée par la méthode suivante due à J. PLEMELJ publiée en 1912.

Sur le cercle trigonométrique, avec $A(1, 0)$, soit B tel que OAB soit équilatéral. Soit C le milieu de $[OB]$ et D tel que $\overrightarrow{OD} = \frac{1}{3}\overrightarrow{OB}$. Soit $E \in [DC]$ défini par $\widehat{CAE} = \frac{1}{3}\widehat{CAD}$; alors $AE = s_7$ est le côté de l'heptagone régulier.

Figure 2



Heptagone IV

Il est particulièrement aisé d'en déduire une construction approchée, les angles considérés étant petits. Remarquons que l'approximation $s_7 \approx AC$ qui est assez précise était connue de HÉRON d'Alexandrie et des Arabes.

Heptagone V

On a $s_7 = 2 \cos(\pi/14)$ et la relation

$$2 \cos(7\theta) = 128x^7 - 224x^5 + 112x^3 - 14x \quad \text{avec } x = \cos(\theta).$$

Donc s_7 est racine de l'équation $y^6 = 7(y^4 - 2y^2 + 1)$ soit

encore $y^3 = \sqrt{7}(1/y^2)$ qui peut encore s'écrire

$(1/y)^3 - (1/y) - 1/\sqrt{7} = 0$. On se ramène à une trisection par la méthode habituelle pour obtenir

$$\frac{1}{y} = \frac{2 \cos(\alpha)}{\sqrt{3}} \quad \text{avec } \cos(3\alpha) = \frac{3}{2} \sqrt{\frac{3}{7}}$$

et $0 < \alpha < \pi/2$. On a immédiatement $\tan(\alpha) = \frac{1}{3\sqrt{3}}$.

Miraculeusement la tangente de l'angle \widehat{CAD} vaut exactement $\frac{1}{3\sqrt{3}}$ d'où la construction annoncée.

Extensions de corps

- **Définition** : Soit K un sous-corps de L , on dit alors que L est une extension de K ; on peut considérer L comme un espace vectoriel sur K : la dimension de cet espace, notée $[L : K]$, est appelée degré de l'extension. Si ce degré est 2, on parle d'extension quadratique.
- **Proposition** : Soient $K \subset L \subset M$; si $[L : K]$ et $[M : L]$ sont finis, alors $[M : K] = [M : L] \times [L : K]$.
- **Définition** : $a \in L$ est dit algébrique sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(a) = 0$.

Polynôme minimal

Théorème

Si a est algébrique sur K il existe un unique polynôme $P \in K[X]$ unitaire tel que $P(a) = 0$ et P est irréductible dans $K[X]$; P est appelé polynôme minimal de a . Son degré est appelé degré de a .

Théorème

Soit L est une extension de K et $a \in L$. Si a est algébrique sur K et de degré n alors $[K(a) : K] = n$ et une base de $K(a)$ est donnée par $\{1, a, a^2, \dots, a^{n-1}\}$.

Remarque : En particulier si $[L : K] = 2$ alors, il existe α tel que $L = K(\sqrt{\alpha}) = \{a + b\sqrt{\alpha} \mid a, b \in K\}$.

Algèbricité

- **Définition** : L est dite algébrique sur K si tout élément de L est algébrique sur K .
- **Proposition** : Si $[L : K]$ est fini, alors L est algébrique sur K .
- La réciproque est fautive : l'ensemble \mathcal{A} des nombres algébriques sur \mathbb{Q} est une extension de \mathbb{Q} qui n'est pas de degré fini. Néanmoins \mathcal{A} est dénombrable.

Théorie de Galois

- **Définition** : Soit L est une extension de K ; l'ensemble \mathcal{G} des automorphismes de L qui laissent K invariant est un groupe appelé groupe de Galois de l'extension $K \subset L$.
- **Proposition** : Soit L est une extension de K et $a, b \in L$ algébriques sur K . Si a et b ont le même polynôme minimal sur K , alors il existe un isomorphisme de corps σ de $K(a)$ sur $K(b)$ tel que $\sigma(a) = b$ et qui laisse K invariant.
- Il y a généralement une correspondance entre les sous-groupes de \mathcal{G} et les corps intermédiaires M ($K \subset M \subset L$) de l'extension.

Nombre constructible

- **Définition** : Un nombre α est *constructible* s'il existe une chaîne d'extensions quadratiques telles que $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_n$ avec $\alpha \in K_n$ et K_{i+1} est une extension quadratique de K_i .
- Il est clair qu'un nombre *constructible* est constructible à la règle et au compas : si les éléments de K_i sont constructibles alors ceux de K_{i+1} le sont aussi.

Réciproque

La réciproque est immédiate : il y a trois cas à considérer

- le point est à l'intersection de deux droites : on ne sort pas de K_i ,
- le point est à l'intersection d'une droite et d'un cercle,
- le point est à l'intersection de deux cercles : se ramène au cas précédent.

Théorème de Wantzel

Théorème

Si α est constructible à la règle et au compas, il est algébrique et son degré sur \mathbb{Q} est une puissance de 2.

Exemples et contre-exemples

- $\sqrt{2} + \sqrt{3}$ est constructible
- $\sqrt[3]{2}$ n'est pas constructible
- La trisection de l'angle est impossible à la règle et au compas.
- Contre-exemple. Soit $P(X) = X^4 - X - 1$. Le polynôme P est irréductible dans $\mathbb{Q}[X]$ et possède une racine réelle δ de degré 4 qui n'est pas constructible.

Justifications

Il est évident que $\alpha = \sqrt{2} + \sqrt{3}$ est constructible ! Néanmoins en calculant $\alpha^2 = 5 + 2\sqrt{6}$ on voit que α ne peut être racine d'un polynôme de degré 2 à coefficients *rationnels*. Par contre α est racine de $P = X^4 - 10X^2 + 1$. Donc α est algébrique de degré 4 et son polynôme minimal est P . La factorisation $P(X) = (X^2 + 2X\sqrt{3} + 1)(X^2 - 2X\sqrt{3} + 1)$ fournit la chaîne d'extensions quadratiques souhaitées $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}] \subset \mathbb{Q}[\alpha]$ et α est de degré 2 sur $\mathbb{Q}[\sqrt{3}]$ avec comme polynôme minimal $(X^2 - 2X\sqrt{3} + 1)$.

Justifications II

Le polynôme minimal (car irréductible sur \mathbb{Q}) de $\beta = \sqrt[3]{2}$ est $X^3 - 2$: donc β est de degré 3 sur \mathbb{Q} et donc inconstructible. Même raisonnement pour la trisection de $\pi/3$: $\gamma = \cos(\pi/9)$ est racine de $P_1 = 4X^3 - 3X - \frac{1}{2}$: le polynôme P_1 ne possède pas de racine dans \mathbb{Q} et est donc irréductible. Par contre si $4X^3 - 3X - a$ possède une racine dans \mathbb{Q} , l'angle tel que $\cos(\theta) = a$ est « trisectable » à la règle et au compas.

Restriction du problème

- 1 Soit p un nombre premier ; le polygone à p^2 côtés n'est pas constructible. La factorisation de
$$x^{p^2} - 1 = (x-1)(1+x+\dots+x^{p-1})(1+x^p+x^{2p}+\dots+x^{p(p-1)})$$
 montre que le degré correspondant est $p(p-1)$ qui n'est jamais une puissance de 2.
- 2 Soit p un nombre premier ; le polygone à p^k ($k > 2$) côtés n'est pas constructible : s'il l'était, on pourrait construire le polygone à p^2 côtés, ce qui est impossible.

- ① Si p et q sont premiers entre eux et si on sait construire les polygones réguliers à p et q côtés, on sait construire le polygone à pq côtés. Soient a et b tels que $ap + bq = 1$: on a alors

$$\frac{2\pi}{pq} = a\frac{2\pi}{q} + b\frac{2\pi}{p}.$$

En reportant a fois l'un des angles et b fois l'autre on obtient donc l'angle cherché.

Polygone à p côtés

On peut donc se limiter aux nombres de côtés p premiers.

Théorème

Si le polygone à p côtés (p premier impair) est constructible, alors p est de la forme $2^m + 1$.

DÉMONSTRATION : Il suffit de vérifier que le degré de l'extension est $p - 1$, c'est-à-dire que le polynôme cyclotomique

$$Q_p(x) = 1 + x + x^2 + \dots + x^{p-1}$$

est irréductible sur \mathbb{Q} . Cela résulte de critère d'EISENSTEIN.

Critère d'EISENSTEIN

Théorème

Soit $f(X) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que p divise a_0, a_1, \dots, a_{n-1} , p ne divise pas a_n et p^2 ne divise pas a_0 ; alors f est irréductible dans $\mathbb{Q}[X]$.

On applique le résultat au polynôme $Q_p(X + 1) = \frac{(X + 1)^p - 1}{(X + 1) - 1}$
en remarquant que les C_p^k sont divisibles par p .

Nombres de Fermat

Enfin il suffit de remarquer que si m possède un facteur impair, le nombre $2^m + 1$ est composé : en effet d'après l'identité

$$a^k - b^k = (a - b)(a^{k-1} + \dots + b^{k-1})$$

on obtient pour k impair $a^k + b^k = (a + b)(a^{k-1} + \dots + b^{k-1})$ et pour $m = kq$ avec k impair

$$2^m + 1 = (2^q)^k + 1 = (2^q + 1)(2^{q(k-1)} + \dots + 1).$$

Conclusion si $n = 2^m + 1$ est premier, m est une puissance de 2 et n est un nombre premier de FERMAT.

Lemme

Théorème

*Si p est premier, alors $(\mathbb{Z}/p\mathbb{Z} - \{0\}, *)$ est cyclique.*

DÉMONSTRATION : On pose $\omega = e^{2i\pi/p}$ et $K = \mathbb{Q}(\omega)$. On note G l'ensemble des automorphismes de K ; $g \in G$ est entièrement déterminé par $g(\omega)$. Les valeurs possibles pour $g(\omega)$ sont les ω^k , donc $G = \{1_K = g_1, g_2, \dots, g_{p-1}\}$ où g_k est défini par $g_k(\omega) = \omega^k$. Par un isomorphisme évident entre G et $(\mathbb{Z}/p\mathbb{Z})^*$ on en déduit que G est cyclique d'ordre $p - 1$. Il existe donc dans G un élément d'ordre $p - 1$ et on a $G = \{g^h \mid 1 \leq h \leq p - 1\}$. Déterminer un générateur est compliqué, mais par exemple pour $p = 17$, g_3 est un générateur. Dans notre cas, G est d'ordre 2^n engendré par g .

Démonstration à la GALOIS

Si on pose pour $0 \leq i \leq 4$, G_i égal au sous-groupe de G engendré par g^{2^i} et K_i égal au sous-corps de K formé des z invariants par g^{2^i} , on a

$$G = G_0 \supset G_1 \supset G_2 \supset G_3 \supset G_4 = \{1_K\}$$
$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset K_3 \subset K_4 = K. \quad (2)$$

En écrivant les itérées successives $\omega, g(\omega), \dots, g^{15}(\omega)$ on obtient alors la séquence des puissances

$$1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6.$$

Alors $u_1 = (1) + (9) + (13) + (15) + (16) + (8) + (4) + (2)$ et $u_2 = (3) + (10) + (5) + (11) + (14) + (7) + (12) + (6)$ sont invariants par g^2 et sont dans K_1 (on a pris un terme sur 2 !).

De même $v_1 = (1) + (13) + (16) + (4)$ et les autres qui s'en déduisent sont invariants par g^4 et sont donc dans K_2 ; enfin $(1) + (16) = 2 \cos(2\pi/17)$ et les termes analogues sont invariants par g^8 et sont dans K_3 .

Un résultat de Gauss

Le résultat suivant, énoncé par GAUSS, aurait aussi permis de conclure

Théorème

Pour construire le polygone de n côtés, n premier impair, il suffit de savoir construire le polygone régulier de $n - 1$ côtés et d'utiliser une seule racine $(n - 1)^{\text{ième}}$

A ma connaissance personne n'a jamais mis en pratique cette construction.