NOMBRES CONSTRUCTIBLES A LA REGLE ET AU COMPAS

Martine Bühler

Les constructions géométriques à la règle et au compas sont une source ancienne d'inspiration pour les mathématiciens. Il paraît difficile d'aborder le sujet sans parler des travaux des géomètres grecs. Nous nous intéresserons ici plus particulièrement aux constructions exposées par Euclide dans ses *Eléments*. Nos sources principales sur la géométrie grecque sont les ouvrages de Pappus et Proclus. Proclus (412 ap J.C.– 486 ap J.C.) a écrit un *Commentaire au premier livre des Eléments*, précédé d'un prologue traitant entre autres de la géométrie et de son histoire. Pappus (vers 300 ap J.C.- 350 ap J.C.) est célèbre pour sa *Collection Mathématique* écrite au quatrième siècle après Jésus-Christ. Les commentaires écrits sont donc fort tardifs : on estime généralement qu'Euclide a été actif au début du troisième siècle avant Jésus-Christ et qu'il appartenait à l'école d'Alexandrie. Il a écrit d'autres ouvrages que les *Eléments*, la plupart perdus. Les *Eléments* sont une compilation de travaux antérieurs avec des ajouts personnels. Ce texte a été abondamment édité et commenté ; on possède entre 400 et 500 manuscrits des *Eléments* (tous très tardifs) et il y a eu plus de mille éditions imprimées, ce qui en fait le second best-seller après la Bible. Les *Eléments* ont donc eu une grande influence sur le développement des mathématiques occidentales, mais il ne faudrait cependant pas réduire les mathématiques grecques aux *Eléments*. En particulier, en géométrie, les Grecs ne se sont pas contentés de la règle et du compas ; ils ont étudié les coniques, la spirale, les conchoïdes etc.

Les constructions à la règle et au compas dans les *Eléments*

Les *Eléments* se composent de treize livres. Les quatre premiers livres sont des livres de géométrie « élémentaire ». Le livre I débute par des définitions, des demandes et des notions communes. Les trois premières demandes donnent au géomètre ses instruments : la règle et le compas[1].

DEMANDES.

1. Conduire une droite d'un point quelconque à un point quelconque.
2. Prolonger indéfiniment, selon sa direction, une droite finie.
3. D'un point quelconque, et avec un intervalle quelconque, décrire une circonférence de cercle.

[1] Les extraits donnés sont tirés des *Eléments* traduction Peyrard (1819) Réédition Blanchard. Dans le texte, nous rencontrons les abréviations def, not, dem qui renvoient aux définitions, notions communes et demandes ainsi que des nombres entre parenthèses qui renvoient aux propositions précédentes.

Le livre déroule ensuite 48 propositions, chacune étant démontrée à l'aide des demandes et/ou des propositions précédentes. Les propositions sont, soit des théorèmes affirmant des résultats (par exemple la proposition 47 est ce que nous nommons théorème de « Pythagore »), soit des problèmes de construction (dont nous étudierons quelques exemples). Dans le cas d'un problème de construction, Euclide indique la construction à la règle et au compas, puis en justifie la validité. La première proposition donne la construction du triangle équilatéral.

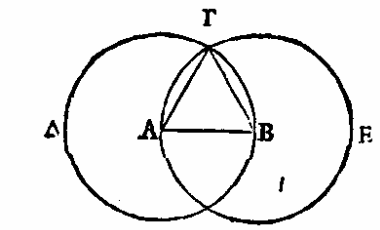
PROPOSITION PREMIÈRE.

Sur une droite donnée et finie, construire un triangle équilatéral.

Exposition. Soit AB une droite donnée et finie.

Détermination. Il faut construire sur la droite finie AB un triangle équilatéral.

Construction. Du centre A et de l'intervalle AB, décrivons la circonférence BΓΔ (dem. 3); et de plus, du centre B et de l'intervalle BA, décrivons la circonférence AΓE; et du point Γ, où les circonférences se coupent mutuellement, conduisons aux points A, B les droites ΓA, ΓB (dem. 1).



Démonstration. Car, puisque le point A est le centre du cercle BΓΔ, la droite AΓ est égale à la droite AB (déf. 15); de plus, puisque le point B est le centre du cercle AΓE, la droite BΓ est égale à la droite BA; mais on a démontré que la droite ΓA était égale à la droite AB; donc chacune des droites ΓA, ΓB est égale à la droite AB; or, les grandeurs qui sont égales à une même grandeur, sont égales entre elles (not. 1); donc la droite ΓA est égale à la droite ΓB; donc les trois droites ΓA, AB, BΓ sont égales entre elles.

Conclusion. Donc le triangle ABΓ (def. 24) est équilatéral, et il est construit sur la droite donnée et finie AB. Ce qu'il fallait faire.

On voit bien là le déroulement usuel d'une proposition chez Euclide, avec un énoncé écrit de manière générale, puis réécrit en nommant les points, puis la construction, enfin la démonstration. La suite du livre I mêle théorèmes et problèmes de construction. Euclide démontre dès la proposition IV un cas d'égalité des triangles (un angle égal entre deux côtés égaux), pierre angulaire d'un grand nombre de démonstrations. La proposition VIII énonce le troisième cas d'égalité (trois côtés égaux). Euclide donne les constructions géométriques élémentaires : bissection d'un angle, milieu d'un segment, perpendiculaire à une droite donnée passant par un point donné, report d'un angle donné, parallèle à une droite donnée. Voici quelques-unes de ces constructions.

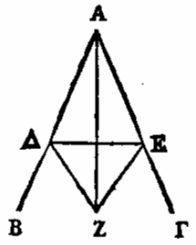
Bissection d'un angle

PROPOSITION IX.

Partager un angle rectiligne donné en deux parties égales.

Soit BAΓ un angle rectiligne donné ; il faut le partager en deux parties égales.

Prenons dans la droite AB un point quelconque Δ, retranchons de la droite AΓ une droite AE égale à la droite AΔ, joignons ΔE, sur la droite ΔE, construisons le triangle équilatéral ΔEZ (1), et joignons AZ ; je dis que l'angle BAΓ est partagé en deux parties égales par la droite AZ.



Puisque AΔ est égal à AE, et que la droite AZ est commune, les deux droites ΔA, AZ seront égales aux deux droites EA, AZ, chacune à chacune ; mais la base ΔZ est égale à la base EZ ; donc l'angle ΔAZ est égal à l'angle EAZ (8).

Donc l'angle rectiligne donné BAΓ est partagé en deux parties égales par la droite AZ ; ce qu'il fallait faire.

On voit bien là fonctionner le raisonnement déductif d'Euclide. Il renvoie à la première proposition pour la construction du triangle équilatéral ΔEZ, puis à la proposition 8 pour l'égalité des triangles ΔAZ et EAZ. Dans la proposition 10, nous allons le voir utiliser la proposition 9 pour bissecter un angle, puis le « deuxième cas d'égalité des triangles » (proposition 4) pour conclure à la validité de sa construction.

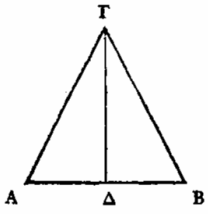
Milieu d'un segment

PROPOSITION X.

Partager une droite donnée et finie en deux parties égales.

Soit donnée une droite finie AB ; il faut partager la droite finie AB en deux parties égales.

Construisons sur cette droite un triangle équilatéral ABΓ (1), et partageons l'angle AΓB en deux parties égales par la droite ΓΔ (9) ; je dis que la droite AB est partagée en deux parties égales au point Δ.



Car puisque la droite AΓ est égale à la droite ΓB, et que la droite ΓΔ est commune, les deux droites AΓ, ΓΔ sont égales aux deux droites BΓ, ΓΔ, chacune à chacune; mais l'angle AΓΔ est égal à l'angle BΓΔ; donc la base AΔ et égale à la base BΔ (4).

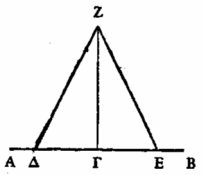
Donc la droite donnée et finie AB est partagée en deux parties égales au point Δ; ce qu'il fallait faire.

Perpendiculaire à une droite donnée

PROPOSITION XI.

A une droite donnée, et à un point donné dans cette droite, mener une ligne droite à angles droits.

Soit AB une droite donnée, et Γ le point donné dans cette droite; il faut du point Γ mener à la droite AB une ligne droite à angles droits.



Prenons dans la ligne droite AΓ un point quelconque Δ, faisons ΓE égal à ΓΔ (3), construisons sur ΔE le triangle équilatéral ZΔE, et joignons ZΓ; je dis que la droite ΓZ est menée à angles droits à la droite AB du point Γ donné dans cette droite.

Car puisque la droite ΓΔ est égale à la droite ΓE, et que la droite ΓZ est commune, les deux droites ΔΓ, ΓZ sont égales aux deux droites EΓ, ΓZ, chacune à chacune; mais la base ΔZ est égale à la base ZE; donc l'angle ΔΓZ est égal à l'angle EΓZ (8); mais ces deux angles sont de suite, et lorsqu'une droite placée sur une droite fait les angles de suite égaux entre eux, chacun des angles égaux est droit (déf. 10); donc chacun des angles ΔΓZ, ZΓE est droit.

Donc la ligne droite ZΓ a été menée à angles droits à la droite donnée AB du point Γ donné dans cette droite.

Le livre II, assez court, est constitué de propositions démontrant ce qu'on pourrait appeler des « identités remarquables » géométriques. Comme on a pu le remarquer en lisant quelques propositions du livre I, il n'y a aucune numérisation de la géométrie chez Euclide : il traite d'égalités de figures, de grandeurs, mais pas de nombres. Le livre II donne des égalités de figures en aire et ces égalités sont utilisées dans des problèmes ultérieurs à la manière de nos identités remarquables en algèbre, mais à aucun moment Euclide n'attribue un nombre à une grandeur. Nous donnons dans l'annexe 1 un exemple d'une de ces identités (proposition VI) et son utilisation pour résoudre un problème de construction. Le livre II résout deux problèmes de construction : un partage de segment (proposition 11 dans l'annexe 1) et la quadrature d'une figure rectiligne, c'est-à-dire la construction à la règle et au compas d'un carré ayant même aire qu'une figure rectiligne donnée.

Le livre III est consacré au cercle. Le livre IV débute par des définitions de figures inscrites et circonscrites ; il donne des constructions de polygones réguliers inscrits dans un cercle donné. Euclide construit ainsi un carré, un pentagone régulier, un hexagone régulier et un quindécagone régulier. Rappelons qu'un polygone régulier est un polygone à côtés et à angles égaux. Nous ne suivrons pas l'ordre d'exposition d'Euclide, et commencerons par les figures les plus simples à obtenir, le carré et l'hexagone régulier.

Construction du carré

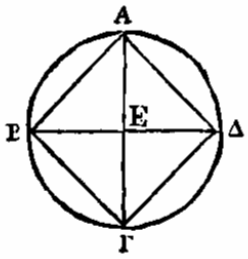
PROPOSITION VI.

Inscrire un quarré dans un cercle donné.

Soit ABΓΔ le cercle donné ; il faut inscrire un quarré dans le cercle ABΓΔ.

Menons les diamètres AΓ, BΔ du cercle ABΓΔ perpendiculaires l'un à l'autre (11. 1), et joignons AB, BΓ, ΓΔ, ΔA.

Puisque BE est égal à EΔ, car le point E est le centre, et que la droite EA est commune et à angles droits, la base AB est égale à la base AΔ (4. 1). Par la même raison, chacune des droites BΓ, ΓΔ est égale à chacune des droites BA, AΔ ; donc le quadrilatère ABΓΔ est équilatéral. Je dis aussi qu'il est rectangle. Car puisque la droite BΔ est un diamètre du cercle ABΓΔ, la figure BAΔ est un demi-cercle. Donc l'angle BAΔ est droit (31. 1). Par la



même raison, chacun des angles ABΓ, BΓΔ, ΓΔA est droit aussi ; donc le quadrilatère ABΓΔ est rectangle. Mais on a démontré qu'il est équilatéral ; donc ce quadrilatère est un quarré. Et ce quarré est inscrit dans le cercle ABΓΔ.

Donc on a inscrit le quarré ABΓΔ dans le cercle donné ABΓΔ. Ce qu'il fallait faire.

Si la construction est bien celle dont nous avons l'habitude, la démonstration diffère de celle que nous donnerions sans doute à nos élèves. On voit de nouveau utilisée la proposition 4 du livre I. La construction de l'hexagone régulier est également habituelle, mais la démonstration en est un peu lourde ; nous la renvoyons à l'annexe 2.

La construction du pentagone régulier est plus délicate à obtenir. Euclide utilise des propriétés angulaires du pentagone pour obtenir une construction « élémentaire » n'utilisant pas d'autres théorèmes que ceux des livres I et II, et en particulier n'utilisant pas les proportions. Il commence par construire un triangle isocèle ayant les angles à la base doubles de l'angle au sommet, puis l'inscrit dans un cercle donné et en déduit la construction du pentagone. Nous donnons dans l'annexe 3 le texte complet d'Euclide.

Il est intéressant de voir comment les constructions précédentes lui permettent alors de construire le quindécagone, car la méthode sera reprise par les mathématiciens ultérieurs et généralisée par Gauss, qui la reliera clairement à des propriétés arithmétiques. Le texte d'Euclide (proposition 16 du livre IV) est donné dans l'annexe 4. Examinons la méthode utilisée. On inscrit dans le cercle donné les cordes AB et AC (B étant sur l'arc AC) telles que AC est le côté d'un triangle équilatéral inscrit dans le cercle (facile à obtenir à partir de l'hexagone par exemple) et AB est le côté d'un pentagone régulier. Alors l'arc AC vaut un tiers de circonférence et l'arc AB vaut un cinquième de circonférence ; donc l'arc BC vaut :

$$\frac{1}{3}\textit{circonférence}-\frac{1}{5}\textit{circonférence}=\frac{2}{15}\textit{circonférence}\,.$$

Il suffit donc de bissecter l'arc BC en E pour obtenir le côté du quindécagone régulier inscrit dans le cercle donné.

A la fin du livre IV des *Eléments*, nous avons donc les moyens de construire les polygones réguliers à 3, 4, 5, 6, 15 côtés et tous les polygones obtenus par simple bissection (décagone à partir du pentagone par exemple). On trouve chez les mathématiciens ultérieurs d'autres constructions, éventuellement plus simples, de ces mêmes polygones. Mais il faut attendre Gauss au dix-neuvième siècle pour trouver des constructions d'autres polygones, qui ne peuvent pas être obtenus à partir de ceux construits par Euclide.

La construction des polygones réguliers n'est pas le seul problème de construction abordé par les Grecs. La construction de l'ennéagone (polygone à 9 côtés) régulier mène directement à un problème célèbre, celui de la trisection de l'angle, qui permettrait de passer du triangle équilatéral à l'ennéagone. Le fait également qu'on puisse bissecter facilement un angle a pu amener les mathématiciens à se poser le problème de la trisection. Les deux autres plus célèbres problèmes de construction sont ceux de la quadrature du cercle (construire un carré d'aire égale à celle d'un cercle donné) et de la duplication du cube (construire un cube de volume double de celui d'un cube donné). Nous aurons l'occasion de reparler de ces trois problèmes.

L'apport de Descartes : l'irruption de l'algèbre dans les problèmes de géométrie (1637)

Nous avons souligné la séparation totale du numérique et du géométrique chez les Grecs. En 1637, paraît à Leyde le *Discours de la Méthode* de Descartes, qui est l'un des textes décisifs de la pensée scientifique au dix-septième siècle. Le titre complet est : *Discours de la Méthode. Pour bien conduire sa raison et chercher la vérité dans les sciences.* Le *Discours* a pour but essentiellement de proposer les règles permettant de construire une science dont la certitude égale celle des mathématiques, puis d'en déduire une métaphysique rationnelle, conciliant l'Homme et Dieu.

Ce texte introductif est suivi de trois essais scientifiques : *La Dioptrique, Les Météores* et *La Géométrie*. Cet ouvrage est écrit en français, et non en latin comme le voudrait la tradition. Descartes s'en explique :

> *Et si j'escris en François, qui est la langue de mon païs, plutost qu'en Latin, qui est celle de mes Precepteurs, c'est à cause que j'espere que ceux qui ne se servent que de leur raison naturelle toute pure, jugeront mieux de mes opinions que ceux qui ne croiyent qu'aux livres anciens et, pour ceux qui joignent le bon sens avec l'estude, lesquels seuls je souhaite pour mes juges, ils ne seront point, je m'asseure, si partiaux pour le Latin qu'ils refusent d'entendre mes raisons pour ce que je les explique en langue vulgaire.*

La Géométrie fut perçue comme un ouvrage difficile par les contemporains et disparut souvent des éditions ultérieures du *Discours de la Méthode*. Par contre, elle fut très étudiée par les mathématiciens et souvent éditée « à part » avec d'abondants commentaires. L'apport principal de Descartes est la numérisation de la géométrie par le choix d'une longueur unité. Il ramène les problèmes géométriques à des problèmes algébriques de résolution d'équations en désignant par des lettres les quantités géométriques (a, b, c … pour les quantités connues, x, y, z…pour les quantités inconnues). A l'inverse, des constructions géométriques permettent de résoudre graphiquement des équations. Le premier livre nous intéresse particulièrement, car il traite des problèmes plans, c'est-à-dire de ceux qui ne font intervenir que des droites et des cercles.

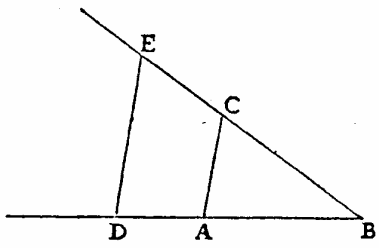
***La Géométrie Livre Premier,* Descartes (1637) Ré-édition Dover New-York (1954)**

TOus les Probleſmes de Geometrie ſe peuuent facilement reduire a tels termes, qu'il n'eſt beſoin par aprés que de connoiſtre la longeur de quelques lignes droites, pour les conſtruire.

Et comme toute l'Arithmetique n'eſt compoſée, que de quatre ou cinq operations, qui ſont l'Addition, la Souſtraction, la Multiplication, la Diuiſion, & l'Extraction des racines, qu'on peut prendre pour vne eſpece de Diuiſion : Ainſi n'at'on autre choſe a faire en Geometrie touchant les lignes qu'on cherche, pour les preparer a eſtre connuës, que leur en adiouſter d'autres, ou en oſter, Oubien en ayant vne, que ie nommeray l'vnité pour la rapporter d'autant mieux aux nombres, & qui peut ordinairement eſtre priſe a diſcretion, puis en ayant encore deux autres, en trouuer vne quatrieſme, qui ſoit à l'vne de ces deux, comme l'autre eſt a l'vnité, ce qui eſt le meſme que la Multiplication; oubien en trouuer vne quatrieſme, qui ſoit a l'vne de ces deux, comme l'vnité eſt a l'autre, ce qui eſt le meſme que la Diuiſion; ou enfin trouuer vne, ou deux, ou pluſieurs moyennes proportionnelles entre l'vnité, & quelque autre ligne; ce qui eſt le meſme que tirer la racine quarrée, ou cubique, &c. Et ie ne craindray pas d'introduire ces termes d'Arithmetique en la Geometrie, affin de me rendre plus intelligibile.

Comme le calcul d'Arithmetique ſe rapporte aux operations de Geometrie.

La Multiplication.

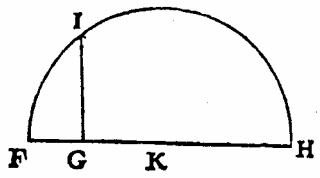


Soit par exemple A B l'vnité, & qu'il faille multiplier B D par B C, ie n'ay qu'a ioindre les poins A & C, puis tirer D E parallele a C A, & B E eſt le produit de cete Multiplication.

La Diuiſion.

Oubien s'il faut diuiſer B E par B D, ayant ioint les poins E & D, ie tire A C parallele a D E, & B C eſt le produit de cete diuiſion.

l'Extraction de la racine quarrée.

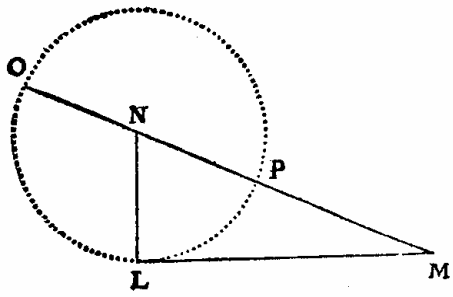


Ou s'il faut tirer la racine quarrée de GH, ie luy adiouſte en ligne droite FG, qui eſt l'vnité, & diuiſant FH en deux parties eſgales au point K, du centre K ie tire le cercle FIH, puis eſleuant du point G vne ligne droite iuſques à I, à angles droits ſur FH, c'eſt GI la racine cherchée. Ie ne dis rien icy de la racine cubique, ny des autres, à cauſe que i'en parleray plus commodement cy aprés.

Ainsi, connaissant deux longueurs, Descartes en construit la somme, la différence, le produit, le quotient ; il sait également construire la racine carrée d'une longueur et les solutions positives d'une équation du second degré à coefficients donnés.

Car ſi i'ay par exemple

$z^2 \propto a z + bb$



ie fais le triangle rectangle N L M, dont le coſté L M eſt eſgal à b racine quarrée de la quantité connue bb, & l'autre L N eſt $\frac{1}{2} a$, la moitié de l'autre quantité connue, qui eſtoit multipliée par z que ie ſuppoſe eſtre la ligne inconnue. puis prolongeant M N la baze de ce triangle, iuſques a O, en ſorte qu'N O ſoit eſgale a N L, la toute O M eſt z la ligne cherchée. Et elle s'exprime en cete ſorte

$z \propto \frac{1}{2} a + \sqrt{\frac{1}{4} aa + bb}.$

Ne manipulant que des nombres positifs, Descartes donne une autre construction[2] pour l'équation $z^2=az-bb$.

Une interprétation moderne des résultats de Descartes : nombres constructibles à la règle et au compas

On se donne deux points distincts O et I. On dit qu'un point M est constructible à la règle et au compas à partir de {O, I} s'il existe une chaîne finie de points $\{M_1, M_2, M_3,\ldots,M_k\}$ tels que $M_1 = O$, $M_2 = I$,…, $M_k = M$ et Mj (pour j = 3 à k) est l'intersection de droites et cercles obtenus :

- Soit en joignant deux points de $\{M_1, M_2, M_3,\ldots,M_{j-1}\}=\mathcal{C}_{j-1}$

[2] Nous donnons dans l'annexe 5 un extrait plus complet du texte de Descartes.

- Soit en prenant comme centre un point de $\mathcal{C}_{j-1}$ et comme rayon la distance entre deux points de $\mathcal{C}_{j-1}$.

A partir de {O, I}, on peut construire à la règle et au compas le point J tel que, OI étant choisi comme unité, (O, I, J) est un repère orthonormé. On dit qu'un nombre réel est constructible à la règle et au compas s'il est l'abscisse ou l'ordonnée d'un point constructible. En élargissant les résultats de Descartes aux nombres réels négatifs (ce qui n'offre aucune difficulté, car, si a est constructible, -a l'est aussi), on voit que, si a et b sont constructibles, a+b, a-b, ab, a/b (si b≠0) le sont aussi. De même, si un nombre réel a positif est constructible, sa racine carrée est constructible. L'ensemble des nombres réels constructibles est donc un sous-corps de $\mathcal{R}$ (donc contenant $\mathcal{Q}$) stable par racine carrée. On peut étendre la définition aux nombres complexes : un nombre complexe est constructible à la règle et au compas s'il est l'affixe d'un point constructible, ou, ce qui revient au même, si ses parties réelle et imaginaire sont constructibles. Comment s'inscrivent dans cette théorie les problèmes « classiques » de construction à la règle et au compas ?

- La construction d'un polygone régulier à n côtés dans un cercle donné (dont on peut toujours prendre le rayon comme unité) revient à construire la longueur de son côté (point de vue de Descartes) ou à construire le nombre $e^{i\frac{2\pi}{n}}$ (nous verrons comment Gauss utilise magistralement ce point de vue).
- La quadrature du cercle : il s'agit de construire à la règle et au compas, à partir d'un cercle donné (dont le rayon peut être pris comme unité), un carré de même aire que le cercle, c'est-à-dire de côté $\sqrt{\pi}$. Il s'agit donc de construire le nombre $\sqrt{\pi}$, ou, ce qui revient au même avec les constructions effectuées par Descartes, le nombre π.
- La duplication du cube : il s'agit de construire le nombre $\sqrt[3]{2}$.
- La trisection de l'angle : là encore, on peut travailler dans un cercle de rayon unité. I et A étant donnés sur un cercle de centre O, il faut construire P et Q tels que les angles IOP, POQ, QOA sont égaux. Le point de vue de Descartes l'amène à chercher à construire la longueur z =IP dont il montre qu'elle est solution d'une équation du troisième degré : $z^3 = 3z - q$ où q =AI (avec OA = 1)[3].

Le travail de Gauss : polygones réguliers et équations cyclotomiques (1801)

Descartes a montré que les solutions d'une équation du second degré sont constructibles à partir de segments dont les longueurs sont les coefficients de l'équation (rappelons que Descartes ne considère que les nombres réels positifs). Il y a donc un lien entre la théorie des équations algébriques et la constructibilité à la règle et au compas. Dans le cas des polygones réguliers, Gauss explicite totalement ce lien et donne une caractérisation des polygones réguliers constructibles à la règle et au compas.

Gauss commence par généraliser la remarque d'Euclide permettant de construire le quindécagone à partir du triangle équilatéral et du pentagone. Si on sait construire les côtés des polygones réguliers à m et n côtés avec m et n premiers entre eux, alors on sait construire le côté du polygone à mn côtés.

En effet, d'après le théorème de Bézout, on peut trouver u et v tels que $um+nv = 1$, c'est-à-dire $\frac{u}{n}+\frac{v}{m}=\frac{1}{mn}$. On appelle [AB] et [CD] les cordes soutendant les arcs de $\frac{360°}{m}$ et de $\frac{360°}{n}$. On met à la suite u cordes de longueur AC et v cordes de longueur AB (en changeant de sens pour celui des deux nombres u

[3] Voir l'annexe 6.

et v qui est négatif) ; comme $u\frac{360}{n}+v\frac{360}{m}=\frac{360}{mn}$, on obtient ainsi une corde soutendant l'arc de $\frac{360°}{mn}$, c'est-à-dire le côté du polygone régulier à mn côtés.

Gauss en conclut qu'il suffit de chercher à construire les polygones réguliers à p^{α} côtés, où p est un nombre premier impair, la bissection d'un angle étant toujours possible à la règle et au compas. Il s'attaque alors au problème de la construction du polygone à n côtés, avec n premier impair. Un repère orthonormé étant donné, il faut construire les points d'affixe $e^{i\frac{2k\pi}{n}}$ $(k=0 \text{ à } n)$ c'est-à-dire les solutions de l'équation $x^n-1=0$. Cette équation n'est pas irréductible sur $\mathbb{Q}$ car elle possède la racine 1. Après division par $x-1$, on obtient l'équation cyclotomique : $x^{n-1}+x^{n-2}+...+x+1=0$, dont les racines sont les racines $n^{ièmes}$ de l'unité différentes de 1. On appelle Ω l'ensemble des solutions de l'équation.

$$\Omega=\left\{r,r^2,...,r^{n-1}\right\} \text{avec } r=e^{i\frac{2\pi}{n}}.$$

Extrait des *Recherches Arithmétiques*, Gauss

"342. Le but de nos recherches, qu'il n'est pas inutile d'annoncer ici en plus de mots, est de décomposer X graduellement[4] *en un nombre de facteurs de plus en plus grand, et cela de manière à ce que les coefficiens de ces facteurs puissent être déterminés par des équations du degré le plus bas possible, jusqu'à ce que, de cette manière, on parvienne à des facteurs simples, ou aux racines Ω. Nous ferons voir que si l'on décompose le nombre p - 1 en facteurs entiers quelconques α, β, γ, etc. (pour lesquels on peut prendre les facteurs premiers), X est décomposable en α facteurs du degré* $\frac{n-1}{\alpha}$*, dont les coefficiens seront déterminés par une équation du degré α ; que chacun de ces facteurs est décomposable en β facteurs du degré* $\frac{n-1}{\alpha\beta}$*, à l'aide d'une équation de degré β, etc. De sorte que ν étant le nombre des facteurs α, β, γ, etc., la recherche des racines Ω est ramenée à la résolution de ν équations des degrés α, β, γ, etc.*

Par exemple, pour n = 17, on a : n - 1 = 2 . 2 . 2 . 2 ; il faut résoudre quatre équations du second degré ; pour n = 73, il faut en résoudre trois du second et deux du troisième."

La méthode de Gauss consiste à grouper astucieusement les racines de l'équation cyclotomique et à les obtenir par la résolution « en cascade » d'équations de degré moindre. Nous allons examiner la méthode en détail pour deux exemples : n=5 et n=7.

Premier exemple : construction du pentagone régulier

[4] X est le polynôme $x^n+x^{n-1}+...+x+1$

Il faut construire $r=e^{\frac{2i\pi}{5}}$, solution de $x^4+x^3+x^2+x+1=0$. L'ensemble des solutions de cette équation est $\Omega=\{r,r^2,r^3,r^4\}$. On groupe les racines deux par deux :

$$\alpha = r + r^4$$
$$\beta = r^2 + r^3$$

La somme des racines cinquièmes de l'unité est nulle, donc on obtient :

$$\alpha+\beta = r+r^2+r^3+r^4 = -1$$
$$\alpha\beta = \left(r+r^4\right)\left(r^2+r^3\right) = r^3+r^6+r^4+r^7 = r^3+r+r^4+r^2 = -1$$

Donc α et β sont solutions de l'équation : $x^2+x-1=0$. On obtient ainsi α et β comme solutions d'une équation du second degré à coefficients rationnels, donc on peut construire[5] α et β. On utilise ensuite :

$$r+r^4 = \alpha$$
$$rr^4 = r^5 = 1$$

Donc r et r^4 sont solutions de l'équation : $x^2-\alpha x-1=0$.

On trouve donc r en résolvant deux (nombre de facteurs premiers dans n-1=4) équations de degré 2 (seul nombre premier intervenant dans la décomposition de n-1=4).

Cette méthode est celle utilisée dans les exercices de Terminale S sur les nombres complexes pour faire construire le pentagone régulier. Simplement, pour simplifier les choses, on fait remarquer aux élèves que $\alpha = r+r^4 = r+\bar{r} = 2\cos\frac{2\pi}{5}$ donc α est la solution positive de l'équation $x^2+x-1=0$ et β en est la solution négative.

Pour la construction : (O, A, B) est un repère orthonormal. On place le point I d'affixe $-\frac{1}{2}$; le cercle de centre I passant par B coupe l'axe des abscisses en M et N. On a alors : $\overline{OM}+\overline{ON}=2\overline{OI}=-1$ et $\overline{OM}\times\overline{ON}=-OB^2=-1$ donc on a $\overline{OM}=\alpha$ et $\overline{ON}=\beta$. Le milieu H de [OM] a alors pour affixe $\cos\frac{2\pi}{5}$. La construction du pentagone régulier inscrit dans le cercle trigonométrique est ensuite immédiate.

Deuxième exemple : impossibilité de la construction de l'heptagone

Cette fois, il s'agit de construire $r=e^{\frac{2i\pi}{7}}$ solution de l'équation : $x^6+x^5+x^4+x^3+x^2+x+1=0$ et on a , n – 1 = 6 = 2.3 (deux facteurs). La théorie de Gauss prévoit donc qu'il faudra résoudre deux équations pour déterminer r, l'une de degré 2 et l'autre de degré 3. On groupe les racines 3 par 3 :

[5] Descartes a montré ce résultat pour les solutions réelles positives de telles équations, mais ceci s'étend sans problème aux solutions complexes car construire les racines carrées d'un nombre complexe revient à bissecter un angle (son argument) et construire la racine carrée de son module. On peut même dans le cas qui nous intéresse différencier α et β en remarquant que α est un nombre réel positif.

$$S = r + r^2 + r^4$$
$$T = r^3 + r^5 + r^6$$
$$S + T = -1$$
$$ST = r^4 + r^6 + r^7 + r^5 + r^7 + r^8 + r^7 + r^9 + r^{10} = 3 + r^4 + r^6 + r^5 + r + r^2 + r^3 = 3 - 1 = 2$$

Donc S et T sont solutions de l'équation du second degré : $x^2 + x + 2 = 0$ (on peut même distinguer S et T en remarquant que Im(S)> 0). On a alors :

$$r + r^2 + r^4 = S$$
$$rr^2 + rr^4 + r^2r^4 = r^3 + r^5 + r^6 = T$$
$$rr^2r^4 = r^7 = 1$$

Donc r, r^2, r^4 sont solutions de l'équation du troisième degré $x^3 - Sx^2 + Tx - 1 = 0$.

Or, comme nous le verrons plus loin, il est impossible de construire à la règle et au compas les solutions d'une équation irréductible de degré 3.

Gauss fait un travail général sur l'équation cyclotomique $x^{n-1} + x^{n-2} + ... + x + 1 = 0$ et prouve qu'on peut toujours faire le travail que nous avons fait pour n = 5 et n = 7, en groupant astucieusement les racines. La façon dont il groupe les racines repose sur des propriétés du groupe multiplicatif $(Z/nZ)^*$, même si Gauss n'utilise pas cette notion.[6] Il fait un travail convaincant, mais peu éclairant, sur les racines de l'équation ci-dessus. Nous verrons plus loin comment la théorie de Galois permet de mieux comprendre les ressorts de la démonstration.

[6] Il utilise des propriétés des résidus modulo n, démontrées dans les chapitres précédents : en termes modernes, le groupe multiplicatif $(Z/nZ)^*$ est cyclique et ce que Gauss appelle une racine primitive modulo n (dont il démontre l'existence) est en fait un générateur du groupe $(Z/nZ)^*$.

Recherches arithmétiques (Gauss)

"365. Nous avons ainsi réduit par les recherches précédentes la division du cercle en n parties, si n est un nombre premier, à la solution d'autant d'équations qu'il y a de facteurs dans le nombre n - 1, et dont le degré est déterminé par la grandeur des facteurs. Ainsi, toutes les fois que n - 1 est une puissance de 2, ce qui arrive pour les valeurs de n

3, 5, 17, 257, 65537, etc.,

la division du cercle est réduite à des équations du second degré seulement, et les fonctions trigonométriques des angles $\frac{P}{n}$, $\frac{2P}{n}$, *etc. peuvent être exprimées par des racines quarrées plus ou moins compliquées, suivant la grandeur de n ; donc, dans ces différents cas, la division du cercle en n parties, ou la description du polygone régulier de n côtés, peut s'exécuter par des constructions géométriques. Par exemple, pour n = 17, on tire facilement des n^os 354, 361*

$$\cos\frac{P}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{\left(34 - 2\sqrt{17}\right)} - \frac{1}{8}\sqrt{\left\{\left(17 + 3\sqrt{17}\right) - \sqrt{\left(34 - 2\sqrt{17}\right)} - 2\sqrt{\left(34 + 2\sqrt{17}\right)}\right\}} \quad ;$$

les cosinus des multiples de cet angle ont une forme semblable, les sinus ont un radical de plus. Il y a certainement bien lieu de s'étonner que la divisibilité du cercle en 3 et 5 parties ayant été connue dès le temps d'Euclide, on n'ait rien ajouté à ces découvertes dans un intervalle de deux mille ans, et que tous les géomètres aient annoncé comme certain, qu'excepté ces divisions et celles qui s'en déduisent (les divisions en 2^μ, *15, 3 . 2^μ, 5 . 2^μ, 15 . 2^μ parties), on ne pouvait en effectuer aucune par des constructions géométriques.*

Au reste on prouve facilement que si un nombre premier n est = $2^m + 1$, *le nombre m lui-même ne peut avoir d'autres diviseurs que 2, et qu'il est par conséquent de la forme* 2^ν. *En effet si m était divisible par un nombre impair* ζ *plus grand que l'unité, et qu'on eût ainsi m =* $\zeta\eta$, $2^m + 1$ *serait divisible par* $2^\eta + 1$, *et partant composé. Toutes les valeurs de n qui ne conduisent qu'à des équations du second degré, sont donc contenues sous la forme* $2^{2^\nu} + 1$ *; ainsi les cinq nombres 3, 5, 17, 257, 65537 s'en déduisent en faisant* $\nu = 0$, *1, 2, 3, 4 ou m = 1, 2, 4, 8, 16. Mais la réciproque n'est pas vraie, et la division du cercle n'a lieu géométriquement que pour les nombres premiers compris dans cette formule. A la vérité Fermat, trompé par l'induction, avait affirmé que tous les nombres compris sous cette forme étaient nécessairement premiers ; mais Euler a remarqué le premier que cette règle était en défaut dès la supposition* $\nu = 5$ *ou m = 32, qui donne* $2^{32} + 1 = 4\,294\,967\,297$, *nombre divisible par 641.*

Toutes les fois que n - 1 renferme des facteurs différents de 2, on est toujours conduit à des équations plus élevées, par exemple, à une ou plusieurs équations du troisième degré, si 3 est une ou plusieurs fois facteur ; à des équations du cinquième degré, quand n - 1 est divisible par 5, etc. , et NOUS POUVONS DÉMONTRER EN TOUTE RIGUEUR QUE CES ÉQUATIONS NE SAURAIENT EN AUCUNE MANIÈRE ÊTRE ÉVITÉES NI ABAISSÉES, et quoique les limites de cet Ouvrage ne nous permettent pas de développer ici la démonstration de cette vérité, nous avons cru devoir en avertir, pour éviter que quelqu'un ne voulût essayer de réduire à des constructions géométriques d'autres divisions que celles données par notre

théorie, et n'employât inutilement son temps à cette recherche.

"Enfin si l'on doit diviser le cercle en $N = a^{\alpha}b^{\beta}c^{\gamma}\ldots$ *parties, a, b, c, etc. étant des nombres premiers, il suffit de savoir effectuer les divisions en* a^{α}, b^{β}, c^{γ}, *etc parties (n° 336). Ainsi, pour connaître le degré des équations nécessaires, on doit considérer les facteurs premiers des nombres*

$$(a-1)\,.\,a^{\alpha-1},\ (b-1)\,.\,b^{\beta-1},\ (c-1)\,.\,c^{\gamma-1},\ \text{etc.},$$

ou, ce qui revient au même, les facteurs de leur produit. On remarquera que ce produit indique combien il y a de nombres moindres que N et premiers avec lui (n° 38). Ainsi la division ne pourra s'exécuter géométriquement que lorsque ce nombre est une puissance de 2 ; mais quand il renferme d'autres facteurs premiers p, p' etc., on ne peut éviter en aucune manière les équations de degré p, p', etc.

Gauss montre ensuite que, pour construire le polygone régulier à p^{α} côtés ($\alpha > 1$), avec p premier, il faut résoudre des équations dont les degrés sont les facteurs premiers de $(p-1)p^{\alpha-1}$.

Il suit de là généralement que pour que la division géométrique du cercle en N parties soit possible, N doit être 2 ou une puissance de 2, ou bien *un nombre premier de la forme* $2^m + 1$, ou encore *le produit d'une puissance de 2 par un ou plusieurs nombres premiers différens de cette forme ; ou d'une manière plus abrégée, il est nécessaire que N ne renferme aucun diviseur impair qui ne soit de la forme* $2^m + 1$, *ni plusieurs fois un même diviseur premier de cette forme.*

On trouve de cette manière, au dessous de 300, les trente-huit valeurs suivantes pour le nombre N :

2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272."

Dans son texte, Gauss affirme qu'il peut « démontrer en toute rigueur que ces équations ne sauraient en aucun cas être abaissées » mais ne le démontre pas. En admettant même qu'il le démontre, il faudrait encore prouver qu'on ne peut pas construire les solutions d'équations irréductibles de degré p, avec p premier impair. Il faut attendre 1837 pour que Wantzel (1814-1848), alors encore élève ingénieur à l'Ecole des Ponts et Chaussées[7], démontre qu'on ne peut pas construire à la règle et au compas les solutions d'équations irréductibles de degré n, si n n'est pas une puissance de 2.

Il résulte immédiatement du théorème précédent que tout problème qui conduit à une équation irréductible dont le degré n'est pas une puissance de 2, ne peut être résolu avec la ligne droite et le cercle. Ainsi la ***duplication du cube****, qui dépend de l'équation* $x^3 - 2a^3 = 0$ *toujours irréductible, ne peut être obtenue par la Géométrie élémentaire. Le problème* ***des deux moyennes proportionnelles****, qui conduit à l'équation*

[7] Wantzel : *Recherche sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas* Journal de Mathématiques Pures et Appliquées (1837). Pour une courte introduction à ce texte et pour le lire en entier, voir *Mnémosyne* n°3.

$x^3 - a^2 b = 0$ *est dans le même cas toutes les fois que le rapport de b à a n'est pas un cube. La* ***trisection de l'angle*** *dépend de l'équation* $x^3 - \frac{3}{4}x + \frac{1}{4}a = 0$ *; cette équation*[8] *est irréductible si elle n'a pas de racine qui soit une fonction rationnelle de a et c'est ce qui arrive tant que a reste algébrique ; ainsi le problème ne peut être résolu en général avec la règle et le compas. Il nous semble qu'il n'avait pas encore été démontré rigoureusement que ces problèmes, si célèbres chez les anciens, ne fussent pas susceptibles d'une solution par les constructions géométriques auxquelles ils s'attachaient particulièrement.*

La division de la circonférence en parties égales peut toujours se ramener à la résolution de l'équation $x^m - 1 = 0$ *dans laquelle m est un nombre premier ou une puissance d'un nombre premier. Lorsque m est premier, l'équation* $\frac{x^m - 1}{x - 1} = 0$ *du degré m-1 est irréductible, comme M.Gauss l'a fait voir dans ses* ***Disquisitiones arithmeticae****, section VII ; ainsi la division du cercle ne peut être effectuée par les constructions géométriques que si m-1 =* 2^n*. Quand m est de la forme* a^α*, on peut prouver, en modifiant légèrement la démonstration de M. Gauss que l'équation de degré* $(a-1)a^{\alpha-1}$*, obtenue en égalant à zéro le quotient de* $x^{a^\alpha} - 1$ *par* $x^{a^{\alpha-1}} - 1$*, est irréductible ; il faudrait donc que* $(a-1)a^{\alpha-1}$ *fut de la forme* 2^n *en même temps que a-1, ce qui est impossible à moins que a = 2. Ainsi,* ***la division de la circonférence en N parties ne peut être effectuée avec la règle et le compas que si les facteurs premiers de N différents de 2 sont de la forme*** 2^n ***+1 et s'ils entrent seulement à la première puissance dans ce nombre.*** *Ce principe est annoncé par M. Gauss à la fin de son ouvrage, mais il n'en a pas donné la démonstration.*

Théorie de Galois et constructions à la règle et au compas

Ce qui est sous-jacent dans le travail de Gauss, c'est en fait la théorie des extensions de corps et de leurs groupes d'automorphismes. Rappelons quelques définitions et résultats de cette théorie.

- Soit K ⊂ L une extension de corps. L est un K-espace vectoriel et, si la dimension de L sur K est finie, on la note [L : K] et on l'appelle *degré de L sur K* ou *degré de l'extension*.
- Si les extensions successives K ⊂ L ⊂ M sont de degrés finis, alors [M : K] = [M : L] x [L : K].
- Si a est un élément de ℂ, on note ℚ(a) le plus petit sous-corps de ℂ contenant a.
- a est algébrique (sur ℚ) signifie : il existe un polynôme P de ℚ[X] tel que P(a) = 0. Dans ce cas, il existe un unique polynôme unitaire de ℚ[X] de degré minimum tel que P(a) = 0. Le degré de ce polynôme est appelé *degré de a.*
- a est algébrique (sur ℚ) si et seulement si l'extension ℚ ⊂ ℚ(a) est de degré fini. Dans ce cas, on a : [ℚ(a) : ℚ] = degré de a.

[8] Il s'agit bien de la même équation que celle de Descartes en posant a=q/2 et x=z/2(et en prenant pour données et inconnues les demi-cordes plutôt que les cordes, c'est-à-dire en pensant en termes de sinus plutôt que de cordes).

Un nombre réel a est constructible si et seulement s'il existe une chaîne d'extensions de $\mathbb{Q}$: $L_0 = \mathbb{Q} \subset L_1 \subset L_2 \subset \ldots \subset L_m$, où $[L_i : L_{i+1}] = 2$ et $a \in L_m$.

En effet, si a est constructible, il est l'abscisse d'un point constructible et on peut trouver une chaîne de points $\{M_1, M_2, M_3, \ldots, M_k\}$ tels que $M_1 = O$, $M_2 = I$,…, $M_k = M$ et M_j (pour j = 3 à k) est l'intersection de droites et cercles obtenus :

- Soit en joignant deux points de $\{M_1, M_2, M_3, \ldots, M_{j-1}\} = \mathcal{C}_{j-1}$
- Soit en prenant comme centre un point de $\mathcal{C}_{j-1}$ et comme rayon la distance entre deux points de $\mathcal{C}_{j-1}$.

Formons alors une chaîne d'extensions de $L_0 = \mathbb{Q}$ en prenant pour L_{i+1} le plus petit sous-corps de $\mathbb{R}$ contenant L_i et les coordonnées de M_{i+1} ; celles-ci sont dans L_i si M_{i+1} est obtenu par intersection de droites[9], et solutions d'équations de degré 2 à coefficients dans L_i sinon. L'extension $L_i \subset L_{i+1}$ est donc quadratique si $L_i \neq L_{i+1}$ et on obtient ainsi la chaîne désirée, en supprimant éventuellement les corps inutiles. Réciproquement, une telle chaîne d'extensions permet la construction de a puisqu'on sait construire les solutions d'équations de degré 2. Ceci redonne le résultat de Wantzel, car on a alors $\mathbb{Q} \subset \mathbb{Q}(a) \subset L_m$ et comme $[L_m : \mathbb{Q}] = [L_m : \mathbb{Q}(a)] \times [\mathbb{Q}(a) : \mathbb{Q}]$ avec $[L_m : \mathbb{Q}]$ égal à une puissance de 2, a est obligatoirement de degré une puissance de 2.

Quant aux nombres complexes constructibles, ils s'obtiennent à partir des nombres réels constructibles et, si z = a + bi et si K est le corps $\mathbb{Q}(a,b)$, le corps $\mathbb{Q}(z)$ est tout simplement le corps K(i) et l'extension $K \subset K(i)$ est quadratique[10]. On dispose donc d'un théorème analogue pour les nombres complexes constructibles.

Reprenons nos deux exemples de constructions de polygones réguliers à n côtés pour n = 5 et n = 7 et voyons comment intervient la théorie des corps.

Construction du pentagone régulier

Il faut construire le nombre $r = e^{\frac{2i\pi}{5}}$. On s'occupe donc du corps $K = \mathbb{Q}(r)$.On a : $1 + r + r^2 + r^3 + r^4 = 0$ donc $r^4 = -1 - r - r^2 - r^3$; toute puissance de r^n où n > 3 s'exprime à l'aide de puissances inférieures. Donc, $\{1, r, r^2, r^3\}$ est une famille génératrice du $\mathbb{Q}$-espace vectoriel K. Remarquons qu'on sait que K est de dimension 4 sur $\mathbb{Q}$ car on peut montrer que le polynôme $x^4 + x^3 + x^2 + x + 1$ est irréductible sur $\mathbb{Q}$ (comme d'ailleurs tous les polynômes cyclotomiques) ; donc notre famille génératrice est une base. On appelle G le groupe des automorphismes du corps K. Si σ est un automorphisme du corps K, alors on a : $\sigma(1) = 1$ et pour n entier naturel, $\sigma(n) = \sigma(1 + 1 + \ldots + 1) = \sigma(1) + \sigma(1) + \ldots + \sigma(1) = 1 + 1 + 1 + \ldots + 1 = n$; on obtient alors, pour $\frac{p}{q}$ rationnel, $\sigma\left(\frac{p}{q}\right) = \frac{p}{q}$. $\mathbb{Q}$ est donc invariant par σ. L'image par σ d'une racine d'un polynôme de $\mathbb{Q}[X]$ ($x^4 + x^3 + x^2 + x + 1$ par exemple) est donc une racine du même polynôme ; donc $\sigma(r) = r$ ou r^2 ou r^3 ou r^4. La connaissance de $\sigma(r)$ suffit pour déterminer σ car tout élément de K s'écrit comme combinaisons de puissances

[9] On a alors $L_{i+1} = L_i$.

[10] Une extension quadratique est une extension de degré 2.

de r à coefficients rationnels et $\sigma(r^i) = \sigma(r)^i$. Le groupe G est donc d'ordre 4 et en bijection avec $\{r, r^2, r^3, r^4\}$[11]. En fait, G est un groupe cyclique : soit g l'élément de G tel que $g(r) = r^2$. On a :

$$g \circ g(r) = g(r^2) = (g(r))^2 = (r^2)^2 = r^4$$
$$g \circ g \circ g(r) = g(r^4) = (g(r))^4 = (r^2)^4 = r^8 = r^3$$
$$g \circ g \circ g \circ g(r) = g(r^3) = (r^2)^3 = r^6 = r$$

Ainsi, g est un générateur du groupe G et $G = \{Id, g, g^2, g^3\}$. Ceci vient de ce que 2 est un générateur du groupe multiplicatif $(Z/5Z)^*$ car $g^n(r) = r^{2^n}$. On appelle alors :

$G_0 = G$ le groupe engendré par g
$G_1 = \{Id, g^2\}$ le sous - groupe engendré par g^2
$G_2 = \{Id\}$

On a une chaîne de groupes : $G_2 \subset G_1 \subset G_0$ à laquelle correspond une chaîne d'extensions de corps ; en effet, au sous-groupe G_i de G, on associe le sous-corps K_i de K des éléments de K invariants par les automorphismes de G_i. On a alors :

$K_0 = \mathbb{Q} \subset K_1 \subset K_2 = K$ avec $K_0 \neq K_1 \neq K_2$ et on a : $[K : \mathbb{Q}] = [K : K_1][K_1 : \mathbb{Q}] = 4$ donc $[K : K_1] = [K_1 : \mathbb{Q}] = 2$. On a trouvé la chaîne d'extensions quadratiques montrant la constructibilité de r. Où sont les groupements de racines de Gauss ? On peut les retrouver grâce au générateur g de G. On pose : $\alpha = r + g^2(r) = r + r^4$. Alors : $g^2(\alpha) = g^2(r) + g^4(r) = r^4 + r = \alpha$ donc $\alpha \in K_1$ mais $g(\alpha) = r^2 + r^3 \neq \alpha$ donc α n'est pas élément de $\mathbb{Q}$. En fait $K_1 = \mathbb{Q}(\alpha)$ et on obtient bien α en résolvant une équation de degré 2 à coefficients rationnels.

Cas de l'heptagone régulier

On s'occupe du corps $K = \mathbb{Q}(r)$ avec $r = e^{\frac{2i\pi}{7}}$. Comme $1 + r + r^2 + ... + r^6 = 0$, toute puissance r^n avec $n \geq 6$ s'exprime comme combinaison linéaire à coefficients rationnels de $\{1, r, r^2, r^3, r^4, r^5\}$, qui est donc une famille génératrice de K comme $\mathbb{Q}$-espace vectoriel (et même une base car l'irréductibilité du polynôme cyclotomique garantit que $[\mathbb{Q}(r) : \mathbb{Q}] = 6$). Soit G le groupe des automorphismes de $K = \mathbb{Q}(r)$. Si $g \in G$, g est entièrement déterminé par $g(r)$ et on a $g(r) = r$ ou r^2 ou r^3 ou r^4 ou r^5 ou r^6. G est un groupe d'ordre 6 isomorphe à $\{(Z/7Z)^*, \times\}$. En effet, soit g l'élément de G défini par $g(r) = r^3$; g est un générateur de G :

$$g^2(r) = g \circ g(r) = g(r^3) = [g(r)]^3 = (r^3)^3 = r^{3^2} = r^9 = r^2$$
$$g^3(r) = g(g^2(r)) = g(r^2) = [g(r)]^2 = (r^3)^2 = r^6$$
$$g^4(r) = g(r^6) = (r^3)^6 = r^4$$
$$g^5(r) = g(r^4) = (r^3)^4 = r^5$$
$$g^6(r) = g(r^5) = (r^3)^5 = r \text{ donc } g \text{ est l' identité.}$$

[11] On obtient bien ainsi 4 automorphismes du **corps** K, la définition donnée de σ assurant que σ est non seulement un automorphisme d'espace vectoriel, mais aussi un automorphisme de corps.

Ceci vient de ce que 3 est un générateur du groupe multiplicatif $\{(Z/7Z)^*,\times\}$. En effet : $g^n(r)=r^{3^n}$. Le groupe G admet un sous-groupe G' d'ordre 3 engendré par g^2 : $\{g^2;g^4;Id\}$. On appelle K_1 le sous-corps de K des éléments invariants par G'. On obtient une chaîne de corps emboîtés : $K_0 = \mathbb{Q} \subset K_1 \subset K_2 = K$ avec $K_0 \neq K_1 \neq K_2$. On a de plus : $[K : \mathbb{Q}] = [K : K_1][K_1 : \mathbb{Q}] = 6$ avec $[K : K_1] = 3$ et $[K_1 : \mathbb{Q}] = 2$. On retrouve encore là les groupements de racines de Gauss ; soit $S = r + g^2(r)+g^4(r) = r + r^2 + r^4$.
On a : $g^2(S) = S$ et S est élément de K_1 mais pas de $\mathbb{Q}$. On détermine donc S en résolvant une équation de degré 2 à coefficients rationnels. La racine cherchée *r* est élément de K mais pas de K_1 ; on la détermine donc en résolvant une équation de degré 3 dont les coefficients s'expriment rationnellement à l'aide de S. On obtient ainsi $e^{\frac{2i\pi}{7}}$ en résolvant en cascade deux équations irréductibles de degré 2 et 3 ; donc l'heptagone régulier n'est pas constructible à la règle et au compas.

Ces deux exemples montrent le lien entre groupes de Galois et groupements de racines. Le groupe de Galois de l'extension $\mathbb{Q} \subset \mathbb{Q}(r)$ où $r=e^{\frac{2i\pi}{n}}$ est le groupe multiplicatif $(Z/nZ)^*$ (d'ordre n-1) dont il faut chercher un générateur[12] *m* (ce qui n'est d'ailleurs pas une tâche facile ; Gauss admet lui-même ne pas connaître d'autre voie que le tâtonnement). Ce générateur *m* (ou racine primitive selon n pour reprendre la terminologie de Gauss) fournit alors un générateur g du groupe de Galois, g étant défini par $g(r)=r^m$. Les sous-groupes du groupe de Galois sont également cycliques, engendrés par un élément du type g^i ; une chaîne de sous-groupes emboîtés correspond à une chaîne de sous-corps, de la manière suivante : à chaque sous-groupe H de G correspond le sous-corps L de $\mathbb{Q}(r)$ formés des éléments invariants par H. Dans le cas qui nous occupe[13], cette correspondance est bijective, le degré $[\mathbb{Q}(r) : L]$ est l'ordre n' du groupe H et $[L : \mathbb{Q}]$ est (n-1)/n'. Le groupe de Galois de l'extension $\mathbb{Q} \subset L$ est le groupe-quotient G/H. Ces emboîtements fournissent les équations à résoudre en cascade pour déterminer $e^{\frac{2i\pi}{n}}$ ainsi que leurs degrés. Quant aux groupements de racines, ils sont obtenus grâce aux générateurs des sous-groupes du groupe de Galois, comme on l'a bien vu dans l'exemple de l'heptagone. Si on veut que chaque extension intermédiaire soit de degré 2, il faut donc que n-1 soit une puissance de 2. Réciproquement, si G est un groupe d'ordre 2^p de générateur g, alors la chaîne des sous-groupes engendrés par $g^2, g^{2^2}, ..., g^{2^{p-1}}$ correspond à une chaîne d'extensions quadratiques. On retrouve ainsi les résultats de Gauss concernant les polygones constructibles à la règle et au compas.

Les grands problèmes grecs

Ainsi, les problèmes de construction à la règle et au compas sont régis par la structure des groupes de Galois des équations correspondantes. Wantzel avait montré dans son article l'impossibilité de la trisection de l'angle et de la duplication du cube. Il avait également situé le problème de la quadrature du cercle : ce qui importe, c'est la nature du nombre π. En 1882, Lindemann démontre la transcendance de π et donc l'impossibilité de la quadrature du cercle.

[12] Gauss démontre que ce groupe est cyclique (sans le vocabulaire des groupes bien sûr). Voir en annexe le texte de Gauss.
[13] L'extension cyclotomique est normale, c'est-à-dire que $\mathbb{Q}(r)$ contient toutes les racines du polynôme cyclotomique.

Bibliographie

Sources

ARCHIMEDE *La mesure du cercle* in *Les œuvres complètes d'Archimède,* T.1 Traduction du grec par Paul Ver Eecke, Ré-édition Blanchard, Paris, 1960

EUCLIDE *Les Eléments* Traduction du grec par F. Peyrard, Paris, 1819. Ré-édition Blanchard, Paris, 1966

DESCARTES *La géométrie. Appendice au Discours de la Méthode,* 1637 Ré-édition Dover, 1954

GAUSS *Recherches Arithmétiques* Traduction Poullet-Delisle Paris, 1807 Ré-édition Blanchard Paris, 1979

KLEIN *Leçons sur certaines questions de géométrie élémentaire* Nouy, Paris, 1896 Ré-édition Vuibert, Paris, 1931. Reproduction par l'IREM Paris VII, collection *Reproduction de textes anciens* n°2 Février 1981

WANTZEL *Recherches sur les moyens de reconnaître si un problème peut se résoudre avec la règle et le compas* in *Journal de mathématiques pures et appliquées* (de Liouville) 1837 pp. 366-371 Reproduction in *Mnémosyne* n°3 IREM Paris VII avril 1993

Bibliographie secondaire

CARREGA J.C. *Théorie des corps. La règle et le compas* Ed. Hermann, collection *Formation des enseignants et formation continue,* Paris, 1981, Nouvelle collection enrichie d'exercices, 1989

FRIEDELMEYER J.P. *Recherche inconnue désespérément* pp299-325 in *Histoires de problèmes, histoire des mathématiques,* Ellipses, 1997

FRIEDELMEYER J.P. *Des équations qui déterminent les sections circulaires* in *L'Ouvert* n° 46 et 47, IREM de Strasbourg, mars et juin 1987

FRIEDELMEYER J.P. *Emergence du concept de groupe* Brochure APMEP n°83 1991 Collection *Fragments d'histoire des mathématiques III*

AYMES J. *Ces problèmes qui font les mathématiques : la trisection de l'angle* Brochure APMEP n°70

BÜHLER M. *Gauss : nombres constructibles et polygones réguliers* in *Si le nombre m'était compté* Commission inter-IREM d'histoire et épistémologie des mathématiques. Ellipses 2000