

# NOMBRES CONSTRUCTIBLES À LA RÈGLE 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<sup>1</sup>.

### 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.

<sup>1</sup> 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.

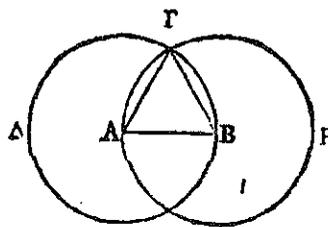
### PROPOSITION PREMIÈRE.

**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  $B\Gamma A$  (dem. 3); et de plus, du centre  $B$  et de l'intervalle  $BA$ , décrivons la circonférence  $A\Gamma E$ ; et du point  $\Gamma$ , où les circonférences se coupent mutuellement, conduisons aux points  $A, B$  les droites  $\Gamma A, \Gamma B$  (dem. 1).



**DÉMONSTRATION.** Car, puisque le point  $A$  est le centre du cercle  $B\Gamma A$ , la droite  $A\Gamma$  est égale à la droite  $AB$  (déf. 15); de plus, puisque le point  $B$  est le centre du cercle  $A\Gamma E$ , la droite  $B\Gamma$  est égale à la droite  $BA$ ; mais on a démontré que la droite  $\Gamma A$  était égale à la droite  $AB$ ; donc chacune des droites  $\Gamma A, \Gamma B$  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  $\Gamma A$  est égale à la droite  $\Gamma B$ ; donc les trois droites  $\Gamma A, AB, \Gamma B$  sont égales entre elles.

**CONCLUSION.** Donc le triangle  $AB\Gamma$  (def. 24) est équilatéral, et il est construit sur la droite donnée et finie  $AB$ . Ce qu'il fallait faire.

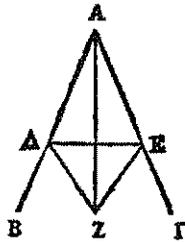
On voit bien là le déroulement usuel d'une proposition chez Euclide, avec un énoncé écrit de manière générale, puis réécrit en nommant les points, puis la construction, enfin la démonstration. La suite du livre I mêle théorèmes et problèmes de construction. Euclide démontre dès la proposition IV un cas 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.

**PROPOSITION IX.**

**Partager un angle rectiligne donné en deux parties égales.**

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

Prenons dans la droite  $AB$  un point quelconque  $\Delta$ , retranchons de la droite  $AC$  une droite  $AE$  égale à la droite  $A\Delta$ , joignons  $BE$ , sur la droite  $BE$ , construisons le triangle équilatéral  $\Delta EZ$  (1), et joignons  $AZ$  ; je dis que l'angle  $BAC$  est partagé en deux parties égales par la droite  $AZ$ .



Puisque  $A\Delta$  est égal à  $AE$ , et que la droite  $AZ$  est commune, les deux droites  $\Delta A$ ,  $AZ$  seront égales aux deux droites  $EA$ ,  $AZ$ , chacune à chacune ; mais la base  $\Delta Z$  est égale à la base  $EZ$  ; donc l'angle  $\Delta AZ$  est égal à l'angle  $EAZ$  (8).

Donc l'angle rectiligne donné  $BAC$  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  $\Delta EZ$ , puis à la proposition 8 pour l'égalité des triangles  $\Delta AZ$  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.

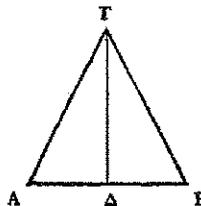
Milieu d'un segment

**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  $AB\Gamma$  (1), et partageons l'angle  $AB\Gamma$  en deux parties égales par la droite  $\Gamma\Delta$  (9) ; je dis que la droite  $AB$  est partagée en deux parties égales au point  $\Delta$ .



Car puisque la droite  $ΑΓ$  est égale à la droite  $ΓΒ$ , et que la droite  $ΓΔ$  est commune, les deux droites  $ΑΓ$ ,  $ΓΔ$  sont égales aux deux droites  $ΒΓ$ ,  $ΓΔ$ , chacune à chacune; mais l'angle  $ΑΓΔ$  est égal à l'angle  $ΒΓΔ$ ; donc la base  $ΑΔ$  est égale à la base  $ΒΔ$  (4).

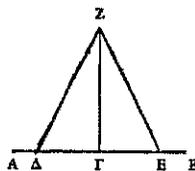
Donc la droite donnée et finie  $ΑΒ$  est partagée en deux parties égales au point  $Δ$ ; ce qu'il fallait faire.

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



Prenons dans la ligne droite  $ΑΓ$  un point quelconque  $Δ$ , faisons  $ΓΕ$  égal à  $ΓΔ$  (3), construisons sur  $ΔΕ$  le triangle équilatéral  $ΖΔΕ$ , et joignons  $ΖΓ$ ; je dis que la droite  $ΖΓ$  est menée à angles droits à la droite  $ΑΒ$  du point  $Γ$  donné dans cette droite.

Car puisque la droite  $ΓΔ$  est égale à la droite  $ΓΕ$ , et que la droite  $ΖΓ$  est commune, les deux droites  $ΔΓ$ ,  $ΖΓ$  sont égales aux deux droites  $ΕΓ$ ,  $ΖΓ$ , chacune à chacune; mais la base  $ΔΖ$  est égale à la base  $ΖΕ$ ; donc l'angle  $ΔΓΖ$  est égal à l'angle  $ΕΓΖ$  (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  $ΔΓΖ$ ,  $ΖΓΕ$  est droit.

Donc la ligne droite  $ΖΓ$  a été menée à angles droits à la droite donnée  $ΑΒ$  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

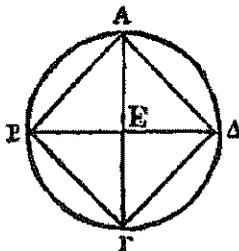
#### PROPOSITION VI.

Inscrire un quarré dans un cercle donné.

Soit  $AB\Gamma\Delta$  le cercle donné ; il faut inscrire un quarré dans le cercle  $AB\Gamma\Delta$ .

Menons les diamètres  $AT$ ,  $BA$  du cercle  $AB\Gamma\Delta$  perpendiculaires l'un à l'autre (II. 1), et joignons  $AB$ ,  $B\Gamma$ ,  $\Gamma\Delta$ ,  $\Delta A$ .

Puisque  $BE$  est égal à  $EA$ , 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  $AA$  (4. 1). Par la même raison, chacune des droites  $B\Gamma$ ,  $\Gamma\Delta$  est égale à chacune des droites  $BA$ ,  $AA$  ; donc le quadrilatère  $AB\Gamma\Delta$  est équilatéral. Je dis aussi qu'il est rectangle. Car puisque la droite  $BA$  est un diamètre du cercle  $AB\Gamma\Delta$ , la figure  $BAA$  est un demi-cercle. Donc l'angle  $BAA$  est droit (31. 1). Par la



même raison, chacun des angles  $AB\Gamma$ ,  $B\Gamma\Delta$ ,  $\Gamma\Delta A$  est droit aussi ; donc le quadrilatère  $AB\Gamma\Delta$  est rectangle. Mais on a démontré qu'il est équilatéral ; donc ce quadrilatère est un quarré. Et ce quarré est inscrit dans le cercle  $AB\Gamma\Delta$ .

Donc on a inscrit le quarré  $AB\Gamma\Delta$  dans le cercle donné  $AB\Gamma\Delta$ . 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 :

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

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

À 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'enneagone (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'enneagone. 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'écris en François, qui est la langue de mon pais, 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 croient 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'assure, 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.

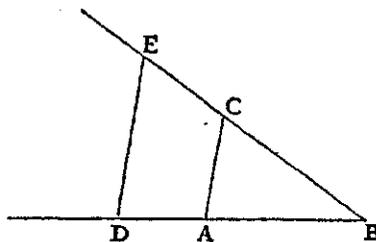
*La Géométrie Livre Premier, Descartes (1637) Ré-édition Dover New-York (1954)*



**T**ous les Problemes de Geometrie se peuvent facilement reduire a tels termes, qu'il n'est besoin par après que de connoître la longueur 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 Division, & l'Extraction des racines, qu'on peut prendre pour vne espece de Division : Ainsi n'at'on autre chose a faire en Geometrie touchant les lignes qu'on cherche, pour les preparer a estre connus, 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 trouver vne quatriesme, qui soit à l'vne de ces deux, comme l'autre est à l'vnité, ce qui est le mesme que la Multiplication; oubien en trouver vne quatriesme, qui soit à l'vne de ces deux, comme l'vnité est à l'autre, ce qui est le mesme que la Division; ou enfin trouver 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, afin de me rendre plus intelligible.

La Multi-  
plication.

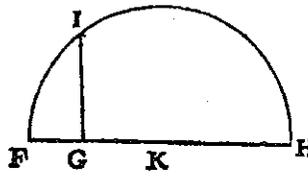


Soit par exemple AB l'vnité, & qu'il faille multiplier BD par BC, ie n'ay qu'a ioindre les points A & C, puisttirer DE parallele a CA, & BE est le produit de cete Multiplication.

La Divi-  
sion.

Oubien s'il faut diuifer BE par BD, ayant ioint les points E & D, ie tire AC parallele a DE, & BC est le produit de cete diuision.

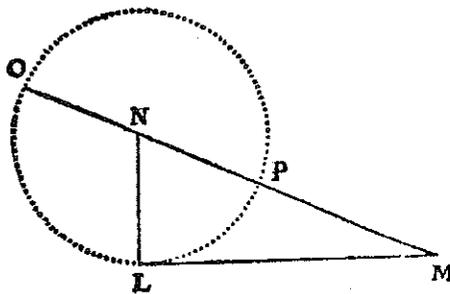
L'Extraction de la racine carrée.



Ou s'il faut tirer la racine carrée 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 F I H, puis esleuant du point G vne ligne droite iusques à I, à angles droits sur FH, c'est GI la racine cherchée. Je ne dis rien icy de la racine cubique, ny des autres, à cause que j'en parleray plus commodement cy après.

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 j'ay par exemple



$z^2 \propto a z + b b$   
ie fais le triangle rectangle N L M, dont le costé LM est esgal à b racine carrée de la quantité connue  $b b$ , & l'autre LN 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 OM est  $z$  la ligne cherchée. Et elle s'exprime en cete forte

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

Ne manipulant que des nombres positifs, Descartes donne une autre construction<sup>2</sup> pour l'équation  $z^2 = a z - b b$ .

## 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  $\{M_1, M_2, M_3, \dots, M_k\}$  tels que  $M_1 = O, M_2 = I, \dots, M_k = M$  et  $M_j$  (pour  $j = 3$  à  $k$ ) est l'intersection de droites et cercles obtenus :

\* Soit en joignant deux points de  $\{M_1, M_2, M_3, \dots, M_{j-1}\} = C_{j-1}$

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

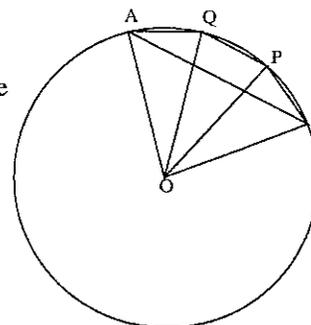
A partir de  $\{O, I\}$ , on peut construire à la règle et au compas le point J tel que, OI étant choisi comme unité,  $(O, I, J)$  est un repère orthonormé. On dit qu'un nombre réel est constructible à la règle et au compas s'il est l'abscisse ou l'ordonnée d'un point constructible. En élargissant les 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  $\mathbb{R}$  (donc contenant  $\mathbb{Q}$ ) 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  $\pi$ .

♣ 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, 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  $OA = 1$ )<sup>3</sup>.



## 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.

<sup>2</sup> Nous donnons dans l'annexe 5 un extrait plus complet du texte de Descartes.

<sup>3</sup> Voir l'annexe 6.

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 soutenant les arcs de  $\frac{360^\circ}{m}$  et de  $\frac{360^\circ}{n}$ . 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  $u$  et  $v$  qui est négatif); comme  $u\frac{360}{n} + v\frac{360}{m} = \frac{360}{mn}$ , on obtient ainsi une corde soutenant l'arc de  $\frac{360^\circ}{mn}$ , 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  $p^\alpha$  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  $e^{i\frac{2k\pi}{n}}$  ( $k=0$  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 :  $x^{n-1} + x^{n-2} + \dots + x + 1 = 0$ , dont les racines sont les racines  $n^{\text{ièmes}}$  de l'unité différentes de 1. On appelle  $\Omega$  l'ensemble des solutions de l'équation.

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

#### 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<sup>4</sup> en un nombre de facteurs de plus en plus grand, et cela de manière à ce que les coefficients 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  $\Omega$ . Nous ferons voir que si l'on décompose le nombre  $p-1$  en facteurs entiers quelconques  $\alpha, \beta, \gamma$ , etc. (pour lesquels on peut prendre les facteurs premiers),  $X$  est décomposable en  $\alpha$  facteurs du degré  $\frac{n-1}{\alpha}$ , dont les coefficients seront déterminés par une équation du degré  $\alpha$ ; que chacun de ces facteurs est décomposable en  $\beta$  facteurs du degré  $\frac{n-1}{\alpha\beta}$ , à l'aide d'une équation de degré  $\beta$ , etc. De sorte que  $v$  étant le nombre des facteurs  $\alpha, \beta, \gamma$ , etc., la recherche des racines  $\Omega$  est ramenée à la résolution de  $v$  équations des degrés  $\alpha, \beta, \gamma$ , etc.

Par exemple, pour  $n=17$ , on a :  $n-1=2 \cdot 2 \cdot 2 \cdot 2$ ; 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  $n=7$ .

<sup>4</sup>  $X$  est le polynôme  $x^n + x^{n-1} + \dots + x + 1$

### Premier exemple : construction du pentagone régulier

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 :

$$\alpha + \beta = r + r^2 + r^3 + r^4 = -1$$

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

Donc  $\alpha$  et  $\beta$  sont solutions de l'équation :  $x^2 + x - 1 = 0$ . On obtient ainsi  $\alpha$  et  $\beta$  comme solutions d'une équation du second degré à coefficients rationnels, donc on peut construire<sup>5</sup>  $\alpha$  et  $\beta$ . On utilise ensuite :

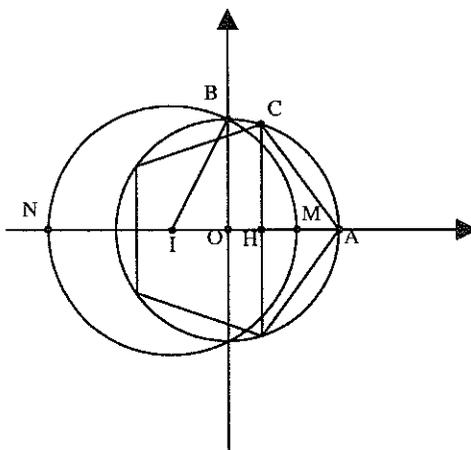
$$r + r^4 = \alpha$$

$$rr^4 = r^5 = 1$$

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  $\alpha$  est la solution positive de l'équation  $x^2 + x - 1 = 0$  et  $\beta$  en est la solution négative.



Sur la figure : (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

<sup>5</sup> 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  $\alpha$  et  $\beta$  en remarquant que  $\alpha$  est un nombre réel positif.

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  $r = e^{\frac{2\pi i}{7}}$  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 :

$$S = r + r^2 + r^4$$

$$T = r^3 + r^5 + r^6$$

$$S + T = -1$$

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

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  $\text{Im}(S) > 0$ ). 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  $x^{n-1} + x^{n-2} + \dots + x + 1 = 0$  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  $(\mathbb{Z}/n\mathbb{Z})^*$ , même si Gauss n'utilise pas cette notion.<sup>6</sup> 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.

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

**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  $n$

$$3, 5, 17, 257, 65537, \text{ etc.},$$

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  $n^{\text{os}}$  354, 361

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

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  $2^\mu$ ,  $15$ ,  $3 \cdot 2^\mu$ ,  $5 \cdot 2^\mu$ ,  $15 \cdot 2^\mu$  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  $2^v$ . En effet si  $m$  était divisible par un nombre impair  $\zeta$  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  $2^{2^v} + 1$ ; ainsi les cinq nombres 3, 5, 17, 257, 65537 s'en déduisent en faisant  $v = 0, 1, 2, 3, 4$  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  $v = 5$  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  $N = a^\alpha b^\beta c^\gamma \dots$  parties,  $a, b, c$ , etc. étant des nombres premiers, il suffit de savoir effectuer les divisions en  $a^\alpha, b^\beta, c^\gamma$ , etc parties (n° 336). Ainsi, pour connaître le degré des équations nécessaires, on doit considérer les facteurs premiers des nombres

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

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  $p^\alpha$  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<sup>7</sup>, 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

<sup>7</sup> 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 Mnemosyne n°3.

$x^3 - a^2b = 0$  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<sup>8</sup> 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  $a^\alpha$ , 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  $K \subset L$  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  $K \subset L \subset M$  sont de degrés finis, alors  $[M : K] = [M : L] \times [L : K]$ .
- ♣ Si  $a$  est un élément de  $\mathbf{C}$ , on note  $\mathbf{Q}(a)$  le plus petit sous-corps de  $\mathbf{C}$  contenant  $a$ .
- ♣  $a$  est algébrique (sur  $\mathbf{Q}$ ) signifie : il existe un polynôme  $P$  de  $\mathbf{Q}[X]$  tel que  $P(a) = 0$ . Dans ce cas, il existe un unique polynôme unitaire de  $\mathbf{Q}[X]$  de degré minimum tel que  $P(a) = 0$ . Le degré de ce polynôme est appelé *degré de  $a$* .
- ♣  $a$  est algébrique (sur  $\mathbf{Q}$ ) si et seulement si l'extension  $\mathbf{Q} \subset \mathbf{Q}(a)$  est de degré fini. Dans ce cas, on a :  $[\mathbf{Q}(a) : \mathbf{Q}] = \text{degré de } a$ .

<sup>8</sup> 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  $\mathbf{Q} : L_0 = \mathbf{Q} \subset L_1 \subset L_2 \subset \dots \subset L_m$ , 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  $\{M_1, M_2, M_3, \dots, M_k\}$  tels que  $M_1 = O$ ,  $M_2 = I, \dots$ ,  $M_k = M$  et  $M_j$  (pour  $j = 3$  à  $k$ ) est l'intersection de droites et cercles obtenus :

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

Formons alors une chaîne d'extensions de  $L_0 = \mathbf{Q}$  en prenant pour  $L_{i+1}$  le plus petit sous-corps de  $\mathbf{R}$  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<sup>9</sup>, 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  $\mathbf{Q} \subset \mathbf{Q}(a) \subset L_m$  et comme  $[L_m : \mathbf{Q}] = [L_m : \mathbf{Q}(a)] \times [\mathbf{Q}(a) : \mathbf{Q}]$  avec  $[L_m : \mathbf{Q}]$  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  $\mathbf{Q}(a, b)$ , le corps  $\mathbf{Q}(z)$  est tout simplement le corps  $K(i)$  et l'extension  $K \subset K(i)$  est quadratique<sup>10</sup>. 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  $K = \mathbf{Q}(r)$ . 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  $\mathbf{Q}$ -espace vectoriel  $K$ . Remarquons qu'on sait que  $K$  est de dimension 4 sur  $\mathbf{Q}$  car on peut montrer que le polynôme  $x^4 + x^3 + x^2 + x + 1$  est irréductible sur  $\mathbf{Q}$  (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  $\sigma$  est un automorphisme du corps  $K$ , alors on a :  $\sigma(1) = 1$  et pour  $n$  entier naturel,  $\sigma(n) = \sigma(1 + 1 + \dots + 1) = \sigma(1) + \sigma(1) + \dots + \sigma(1) = 1 + 1 + 1 + \dots + 1 = n$  ; on obtient alors, pour  $\frac{p}{q}$  rationnel,  $\sigma\left(\frac{p}{q}\right) = \frac{p}{q}$ .  $\mathbf{Q}$  est donc invariant par  $\sigma$ . L'image par  $\sigma$  d'une racine d'un polynôme de  $\mathbf{Q}[X]$  ( $x^4 + x^3 + x^2 + x + 1$  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  $\sigma$  car tout élément de  $K$  s'écrit comme combinaisons de puissances

<sup>9</sup> On a alors  $L_{i+1} = L_i$ .

<sup>10</sup> 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  $\{r, r^2, r^3, r^4\}$ <sup>11</sup>. En fait,  $G$  est un groupe cyclique : soit  $g$  l'élément de  $G$  tel que  $g(r) = r^2$ . On a :

$$\begin{aligned}g \circ g(r) &= g(r^2) = (g(r))^2 = (r^2)^2 = r^4 \\g \circ g \circ g(r) &= g(r^4) = (g(r))^4 = (r^2)^4 = r^8 = r^3 \\g \circ g \circ g \circ g(r) &= g(r^3) = (r^2)^3 = r^6 = r\end{aligned}$$

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  $(\mathbb{Z}/5\mathbb{Z})^*$  car  $g^n(r) = r^{2^n}$ . On appelle alors :

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

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  $\alpha$  n'est pas élément de  $\mathbb{Q}$ . En fait  $K_1 = \mathbb{Q}(\alpha)$  et on obtient bien  $\alpha$  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  $1 + r + r^2 + \dots + r^6 = 0$ , 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  $\{(\mathbb{Z}/7\mathbb{Z})^*, \times\}$ . En effet, soit  $g$  l'élément de  $G$  défini par  $g(r) = r^3$  ;  $g$  est un générateur de  $G$  :

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

<sup>11</sup> On obtient bien ainsi 4 automorphismes du corps  $K$ , la définition donnée de  $\sigma$  assurant que  $\sigma$  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 :  $K_0 = \mathbf{Q} \subset K_1 \subset K_2 = K$  avec  $K_0 \neq K_1 \neq K_2$ . On a de plus :  $[K : \mathbf{Q}] = [K : K_1][K_1 : \mathbf{Q}] = 6$  avec  $[K : K_1] = 3$  et  $[K_1 : \mathbf{Q}] = 2$ . 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  $\mathbf{Q}$ . 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  $\mathbf{Q} \subset \mathbf{Q}(r)$  où  $r = e^{\frac{2i\pi}{n}}$  est le groupe multiplicatif  $(Z/nZ)^*$  (d'ordre  $n-1$ ) dont il faut chercher un générateur<sup>12</sup>  $m$  (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  $\mathbf{Q}(r)$  formés des éléments invariants par  $H$ . Dans le cas qui nous occupe<sup>13</sup>, cette correspondance est bijective, le degré  $[\mathbf{Q}(r) : L]$  est l'ordre  $n'$  du groupe  $H$  et  $[L : \mathbf{Q}]$  est  $(n-1)/n'$ . Le groupe de Galois de l'extension  $\mathbf{Q} \subset L$  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  $g^2, g^{2^2}, \dots, g^{2^{p-1}}$  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  $\pi$ . En 1882, Lindemann démontre la transcendance de  $\pi$  et donc l'impossibilité de la quadrature du cercle.

<sup>12</sup> Gauss démontre que ce groupe est cyclique (sans le vocabulaire des groupes bien sûr). Voir en annexe le texte de Gauss.

<sup>13</sup> L'extension cyclotomique est normale, c'est-à-dire que  $\mathbf{Q}(r)$  contient toutes les racines du polynôme cyclotomique.

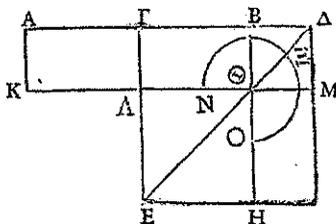
## PROPOSITION VI.

Si une ligne droite est coupée en deux parties égales, et si on lui ajoute directement une droite, le rectangle compris sous la droite entière avec la droite ajoutée, et sous la droite ajoutée, avec le carré de la moitié de la droite entière, est égal au carré décrit avec la droite composée de la moitié de la droite entière et de la droite ajoutée, comme avec une seule droite.

Qu'une ligne droite AB soit coupée en deux parties égales au point Γ; qu'on lui ajoute directement une autre droite ΒΔ; je dis que le rectangle compris sous ΑΔ, ΔΒ, avec le carré de ΓΒ, est égal au carré de ΓΔ.

Avec la droite ΓΔ décrivons le carré ΓΕΖΑ (46. 1); joignons ΔΕ; par le point Β conduisons ΒΗ parallèle à l'une ou à l'autre des droites ΓΕ, ΔΖ (31. 1); par le point Θ, conduisons ΚΜ parallèle à l'une ou à l'autre des droites ΑΔ, ΕΖ, et enfin par le point Α conduisons ΑΚ parallèle à l'une ou à l'autre des droites ΓΑ, ΔΜ.

Puisque ΑΓ est égal à ΓΒ, le rectangle ΑΑ est égal au rectangle ΓΘ (36. 1). Mais le rectangle ΓΘ est égal au rectangle ΘΖ (45. 1); donc le rectangle ΑΑ est égal au rectangle ΘΖ; ajoutons le rectangle commun ΓΜ, le rectangle entier ΑΜ sera égal au gnomon ΝΕΘ. Mais ΑΜ est le rectangle sous ΑΔ, ΔΒ, car ΔΜ est égal à ΔΒ (4. 2); donc le gnomon ΝΕΘ est égal au rectangle compris sous ΑΔ, ΔΒ. Ajoutons le carré ΑΗ qui est égal au carré de ΓΒ, le rectangle compris



sous ΑΔ, ΔΒ avec le carré de ΓΒ sera égal au gnomon ΝΕΘ et au carré ΑΗ. Mais le gnomon ΝΕΘ, et le carré ΑΗ sont le carré entier ΓΕΖΑ, qui est le carré de ΓΔ; donc le rectangle compris sous ΑΔ, ΔΒ avec le carré de ΓΒ est égal au carré de ΓΔ. Donc, etc.

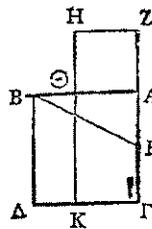
<sup>14</sup> Pour une utilisation possible de ces textes en classe, voir *Mnémosyne* n°1 ou Brochure M. :A.T.H. tome 3(n°90 de l'IREM Paris VII).

PROPOSITION XI.

Couper une droite donnée, de manière que le rectangle compris sous la droite entière et l'un des segments, soit égal au carré du segment restant.

Soit  $AB$  la droite donnée; il faut couper  $AB$  de manière que le rectangle compris sous la droite entière et l'un des segments, soit égal au carré du segment restant.

Avec la droite  $AB$  décrivons le carré  $ABAT$  (46. 1); coupons  $AT$  en deux parties égales au point  $E$  (10. 1); joignons  $BE$ , prolongeons  $TA$  vers  $Z$ ; faisons  $EZ$  égal à  $BE$  (3. 1); décrivons avec  $AZ$  le carré  $Z\Theta$ ; et prolongeons  $H\Theta$  vers  $K$ ; je dis que la droite  $AB$  est coupée en  $\Theta$ , de manière que le rectangle compris sous  $AB$ ,  $B\Theta$  est égal au carré de  $A\Theta$ .



Puisque la droite  $AT$  est coupée en deux parties égales en  $E$ , que  $AZ$  lui est ajoutée; le rectangle compris sous les droites  $TZ$ ,  $ZA$  avec le carré de  $AE$  est égal au carré de  $EZ$  (6. 2). Mais  $EZ$  est égal à  $EB$ ; donc le rectangle compris sous  $TZ$ ,  $ZA$  avec le carré de  $AE$ , est égal au carré de  $EB$ . Mais les carrés des droites  $BA$ ,  $AE$  sont égaux au carré de  $EB$  (47. 1), car l'angle en  $A$  est droit; donc le rectangle sous  $TZ$ ,  $ZA$  avec le carré de  $AE$  est égal aux carrés des droites  $BA$ ,  $AE$ . Retranchons le carré commun de  $AE$ ; le rectangle restant compris sous  $TZ$ ,  $ZA$  sera égal au carré de  $AB$ . Mais le rectangle sous les droites  $TZ$ ,  $ZA$  est le rectangle  $ZK$ , parce que  $AZ$  est égal à  $ZH$ , et le carré de  $AB$  est le carré  $AA$ ; donc le rectangle  $ZK$  est égal au carré  $AA$ . Retranchons le rectangle commun  $AK$ ; le carré restant  $Z\Theta$  sera égal au rectangle  $\Theta A$ . Mais  $Z\Theta$  est le carré de  $A\Theta$ , et  $\Theta A$  est le rectangle sous  $AB$ ,  $B\Theta$ ; donc le rectangle compris sous  $AB$ ,  $B\Theta$  est égal au carré de  $A\Theta$ .

Donc la droite  $AB$  est coupée en  $\Theta$ , de manière que le rectangle compris sous  $AB$ ,  $B\Theta$  est égal au carré de  $A\Theta$ ; ce qu'il fallait faire.

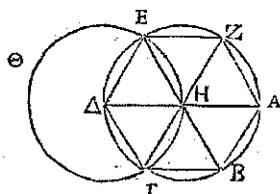
## PROPOSITION XV.

Inscrire dans un cercle donné un hexagone équilatéral et équiangle.

Soit  $AB\Gamma\Delta EZ$  le cercle donné; il faut dans ce cercle inscrire un hexagone équilatéral et équiangle.

Menons le diamètre  $AA$  du cercle  $AB\Gamma\Delta EZ$ , prenons le centre  $H$  de ce cercle, du centre  $\Delta$ , et de l'intervalle  $\Delta H$  décrivons le cercle  $E\text{H}\Gamma\Theta$  (dém. 3), joignons les droites  $EH$ ,  $\Gamma H$ , prolongeons-les vers les points  $B$ ,  $Z$ , et joignons  $AB$ ,  $B\Gamma$ ,  $\Gamma\Delta$ ,  $\Delta E$ ,  $EZ$ ,  $ZA$ ; je dis que l'hexagone  $AB\Gamma\Delta EZ$  est équilatéral et équiangle.

Puisque le point  $H$  est le centre du cercle  $AB\Gamma\Delta EZ$ , la droite  $HE$  est égale à  $H\Delta$ . De plus, puisque le point  $\Delta$  est le centre du cercle  $E\text{H}\Gamma\Theta$ , la droite  $\Delta E$  est égale à  $\Delta H$ . Mais on a démontré que  $HE$  est égal à  $H\Delta$ ; donc  $HE$  est égal à  $\Delta E$ ; donc le triangle  $EHA$  est équilatéral; donc les trois angles  $EHA$ ,  $H\Delta E$ ,  $\Delta EH$  sont égaux entr'eux, puisque dans les triangles isocèles, les angles à la base sont égaux entr'eux (5. 1). Mais les trois angles d'un triangle sont égaux à deux droits (32. 1); donc l'angle  $EHA$  est le tiers de deux droits. Nous démontrerons semblablement que  $\Delta H\Gamma$  est le tiers de deux droits. Mais la droite  $\Gamma H$  tombant sur la droite  $EB$  fait les angles de suite  $E\text{H}\Gamma$ ,  $\Gamma HB$  égaux à deux droits (13. 1); donc l'angle restant  $\Gamma HB$  est le tiers de deux droits;



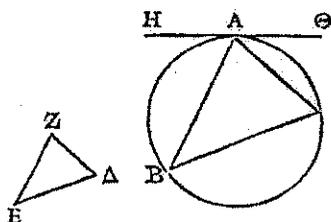
donc les angles  $EHA$ ,  $\Delta H\Gamma$ ,  $\Gamma HB$  sont égaux entr'eux; mais les angles  $BHA$ ,  $\Delta HZ$ ,  $ZHE$  sont égaux aux angles  $EHA$ ,  $\Delta H\Gamma$ ,  $\Gamma HB$ , parce que ces angles sont opposés par le sommet (15. 1), donc les six angles  $EHA$ ,  $\Delta H\Gamma$ ,  $\Gamma HB$ ,  $BHA$ ,  $\Delta HZ$ ,  $ZHE$  sont égaux entr'eux. Mais des angles égaux s'appuient sur des arcs égaux (26. 3); donc les six arcs  $AB$ ,  $B\Gamma$ ,  $\Gamma\Delta$ ,  $\Delta E$ ,  $EZ$ ,  $ZA$  sont égaux entr'eux. Mais des arcs égaux sont soutendus par des droites égales (29. 3); donc ces six droites sont égales entr'elles; donc l'hexagone  $AB\Gamma\Delta EZ$  est équilatéral. Je dis qu'il est équiangle. Car puisque l'arc  $ZA$  est égal à l'arc  $EA$ , ajoutons l'arc commun  $AB\Gamma\Delta$ , l'arc entier  $ZAB\Gamma\Delta$  sera égal à l'arc entier  $EAB\Gamma\Delta$ . Mais l'angle  $ZEA$  s'appuie sur l'arc  $ZAB\Gamma\Delta$ , et l'angle  $AZE$  s'appuie sur l'arc  $EAB\Gamma\Delta$ ; donc l'angle  $AZE$  est égal à l'angle  $ZEA$  (27. 3). On démontrera semblablement que les angles restants de l'hexagone  $AB\Gamma\Delta EZ$  sont égaux un à un à l'un et à l'autre des angles  $AZE$ ,  $ZEA$ ; donc l'hexagone  $AB\Gamma\Delta EZ$  est équiangle. Mais on a démontré qu'il est équilatéral, et il est inscrit dans le cercle  $AB\Gamma\Delta EZ$ .

Donc on a inscrit un hexagone équilatéral et équiangle dans le cercle donné. Ce qu'il fallait faire.

## PROPOSITION II.

Dans un cercle donné, inscrire un triangle qui soit équiangle avec un triangle donné.

Soit  $AB\Gamma$  le cercle donné, et  $\Delta EZ$  le triangle donné ; il faut dans le cercle  $AB\Gamma$  inscrire un triangle qui soit équiangle avec le triangle donné  $\Delta EZ$ .



Menons la droite  $H\Theta$ , de manière qu'elle touche le cercle  $AB\Gamma$  en un point  $A$ , et sur la droite  $A\Theta$ , et au point  $A$  de cette droite faisons l'angle  $\Theta A\Gamma$  égal à l'angle  $\Delta EZ$  (23. 1). De plus sur la droite  $HA$ , et au point  $A$  de cette droite faisons l'angle  $HAB$  égal à l'angle  $Z\Delta E$ , et joignons  $B\Gamma$ .

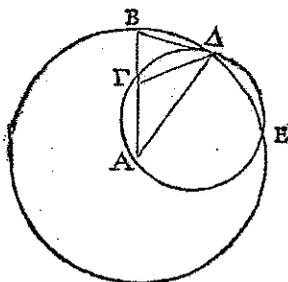
Puisque la droite  $A\Theta$  touche le cercle  $AB\Gamma$ , et que la droite  $A\Gamma$  a été menée dans le cercle du point de contact  $A$ , l'angle  $\Theta A\Gamma$  est égal à l'angle  $AB\Gamma$  placé dans le segment alterne du cercle (32. 5). Mais l'angle  $\Theta A\Gamma$  est égal à l'angle  $\Delta EZ$  ; donc l'angle  $AB\Gamma$  est égal à l'angle  $\Delta EZ$ . Par la même raison l'angle  $A\Gamma B$  est égal à l'angle  $Z\Delta E$  ; donc l'angle restant  $B A \Gamma$  est égal à l'angle restant  $E Z \Delta$  (32. 1) ; donc le triangle  $AB\Gamma$  est équiangle avec le triangle  $\Delta EZ$ , et il est inscrit dans le cercle  $AB\Gamma$  (déf. 3. 4).

Donc dans le cercle donné, on a inscrit un triangle équiangle avec un triangle donné. Ce qu'il fallait faire.

## PROPOSITION X.

Construire un triangle isocèle, qui ait chacun des angles de la base double de l'angle restant.

Soit une droite  $AB$ ; que cette droite soit coupée en un point  $\Gamma$ , de manière que le rectangle compris sous  $AB$ ,  $B\Gamma$  soit égal au carré de  $\Gamma A$  (II. 2); du centre  $A$  et de l'intervalle  $AB$  décrivons le cercle  $B\Delta E$  (dém. 3); dans le cercle  $B\Delta E$  adaptons une droite  $B\Delta$  égale à la droite  $A\Gamma$ , qui n'est pas plus grande que le diamètre du cercle  $B\Delta E$  (I. 4); joignons  $A\Delta$ ,  $\Gamma\Delta$ , et circonscrivons le cercle  $A\Gamma\Delta$  au triangle  $A\Gamma\Delta$  (5. 4).



Puisque le rectangle sous  $AB$ ,  $B\Gamma$  est égal au carré  $A\Gamma$ , et que  $A\Gamma$  est égal à  $B\Delta$ , le rectangle sous  $AB$ ,  $B\Gamma$  est égal au carré de  $B\Delta$ . Et puisque le point  $B$  a été pris hors du cercle  $A\Gamma\Delta$ , que les droites  $BA$ ,  $B\Delta$  vont du point  $B$  au cercle  $A\Gamma\Delta$ , que l'une d'elles le coupe, et que l'autre ne le coupe point, et que le rectangle sous  $AB$ ,  $B\Gamma$  est égal au carré de  $B\Delta$ , la droite  $B\Delta$  est tangente au cercle  $A\Gamma\Delta$  (37. 3). Donc, puisque la droite  $B\Delta$  est tangente, et que la droite  $A\Gamma$  a été menée du point de contact  $\Delta$ , l'angle  $B\Delta\Gamma$  est égal à l'angle  $\Delta A\Gamma$  placé dans le segment alterne du cercle (32. 3). Puisque l'angle  $B\Delta\Gamma$  est égal à l'angle  $\Delta A\Gamma$ , ajoutons l'angle commun  $\Gamma\Delta A$ , l'angle entier  $B\Delta A$  sera égal aux deux angles  $\Gamma\Delta A$ ,  $\Delta A\Gamma$ . Mais l'angle extérieur  $B\Gamma\Delta$  est égal aux angles  $\Gamma\Delta A$ ,  $\Delta A\Gamma$  (32. 1); donc l'angle  $B\Delta A$  est égal à l'angle  $B\Gamma\Delta$ . Mais l'angle  $B\Delta A$  est égal à l'angle  $\Gamma B\Delta$  (5. 1), puisque le côté  $\Delta A$  est égal au côté  $A\Gamma$ ; donc l'angle  $\Delta B A$  est égal à l'angle  $B\Gamma\Delta$ . Donc les trois angles  $B\Delta A$ ,  $\Delta B A$ ,  $B\Gamma\Delta$  sont égaux entr'eux. Et puisque l'angle  $\Delta B\Gamma$  est égal à l'angle  $B\Gamma\Delta$ , le côté  $B\Gamma$  est égal au côté  $A\Gamma$  (6. 1). Mais le côté  $B\Delta$  est supposé égal au côté  $A\Gamma$ ; donc le côté  $A\Gamma$  est égal au côté  $A\Delta$ ; donc l'angle  $\Gamma\Delta A$  est égal à l'angle  $\Delta A\Gamma$  (5. 1); donc les angles  $\Gamma\Delta A$ ,  $\Delta A\Gamma$  sont doubles de l'angle  $\Delta A\Gamma$ . Mais l'angle  $B\Gamma\Delta$  est égal aux angles  $\Gamma\Delta A$ ,  $\Delta A\Gamma$  (32. 1); donc l'angle  $B\Gamma\Delta$  est double de l'angle  $\Delta A\Gamma$ . Mais l'angle  $B\Gamma\Delta$  est égal à chacun des angles  $B\Delta A$ ,  $\Delta B A$ ; donc chacun des angles  $B\Delta A$ ,  $\Delta B A$  est double de l'angle  $B\Delta A$ .

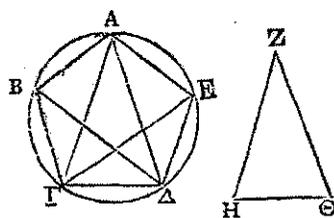
Donc on a construit un triangle isocèle  $A\Delta B$ , ayant chacun des angles de la base  $B\Delta$  double de l'angle restant. Ce qu'il fallait faire.

## PROPOSITION XI.

Dans un cercle donné, inscrire un pentagone équilatéral et équiangle.

Soit  $AB\Gamma\Delta E$  le cercle donné ; il faut inscrire dans le cercle  $AB\Gamma\Delta E$  un pentagone équilatéral et équiangle.

Soit posé le triangle isocèle  $ZH\Theta$ , ayant chacun des angles en  $H, \Theta$  double de l'angle  $Z$  (10. 4) ; inscrivons dans le cercle  $AB\Gamma\Delta E$  le triangle  $A\Gamma\Delta$  équiangle avec le triangle  $ZH\Theta$  (2. 4), de manière que l'angle  $\Gamma A\Delta$  soit égal à l'angle  $Z$ , et que chacun des angles  $H, \Theta$  soit égal à chacun des angles  $A\Gamma\Delta, \Gamma\Delta A$  ; chacun des angles  $A\Gamma\Delta, \Gamma\Delta A$  sera double de l'angle  $\Gamma A\Delta$ . Coupons chacun des angles  $A\Gamma\Delta, \Gamma\Delta A$  en deux parties égales par les droites  $\Gamma E, \Delta B$  (9. 1), et joignons  $AB, \Gamma E, \Delta E, EA$ .



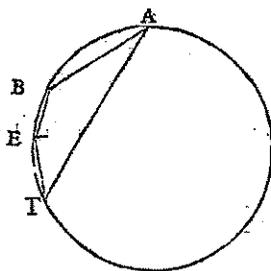
Puisque chacun des angles  $A\Gamma\Delta, \Gamma\Delta A$  est double de l'angle  $\Gamma A\Delta$ , et que ces angles sont coupés en deux parties égales par les droites  $\Gamma E, \Delta B$ , les cinq angles  $\Delta A\Gamma, A\Gamma E, E\Gamma\Delta, \Gamma\Delta B, B\Delta A$  sont égaux entr'eux. Mais les angles égaux sont appuyés sur des arcs égaux (26. 3) ; donc les cinq arcs  $AB, \Gamma E, \Delta E, EA$  sont égaux entr'eux. Mais les arcs égaux sont soutenus par des droites égales (29. 3) ; donc les cinq droites  $AB, \Gamma E, \Delta E, EA$  sont égales entr'elles ; donc le pentagone  $AB\Gamma\Delta E$  est équilatéral. Je dis aussi qu'il est équiangle. Car puisque l'arc  $AB$  est égal à l'arc  $\Delta E$ , ajoutons l'arc commun  $B\Gamma\Delta$  ; l'arc entier  $AB\Gamma\Delta$  sera égal à l'arc entier  $E\Delta\Gamma B$ . Mais l'angle  $A E \Delta$  est appuyé sur l'arc  $AB\Gamma\Delta$ , et l'angle  $B A E$  sur l'arc  $E\Delta\Gamma B$  ; donc l'angle  $B A E$  est égal à l'angle  $A E \Delta$  (27. 3). Par la même raison, chacun des angles  $A B \Gamma, \Gamma E \Delta, \Delta E \Gamma$  est égal à chacun des angles  $B A E, A E \Delta$  ; donc le pentagone  $AB\Gamma\Delta E$  est équiangle. Mais il a été démontré qu'il est équilatéral ;

Donc dans un cercle donné, on a inscrit un pentagone équilatéral et équiangle. Ce qu'il fallait faire.

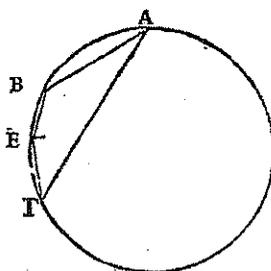
## PROPOSITION XVI.

Inscrire dans un cercle donné un quindécagone équilatéral et équiangle.

Soit  $AB\Gamma A$  le cercle donné ; il faut dans ce cercle inscrire un quindécagone équilatéral et équiangle.



Inscrivons dans le cercle  $AB\Gamma A$  le côté  $AI$  d'un triangle équilatéral inscrit, et le côté  $AB$  d'un pentagone équilatéral. Puisque la circonférence entière  $AB\Gamma A$  doit être partagée en quinze parties égales, l'arc  $ABI$  qui est la troisième partie de la circonférence, en contiendra cinq, et l'arc  $AB$  qui est le cinquième de la circonférence, en contiendra trois ; donc l'arc restant  $BI$  en contiendra deux. Partageons l'arc restant  $BI$  en deux parties égales au point  $E$  (30. 3), chacun des arcs  $BE$ ,  $EI$  sera la quinzième partie de la circonférence du cercle  $AB\Gamma A$ . Donc, si ayant joint les droites  $BE$ ,  $EI$ , nous adaptons dans le cercle  $AB\Gamma A$ , à la suite les unes des autres, des droites égales à ces droites (1. 4), on aura inscrit dans ce cercle un quindécagone équilatéral et équiangle. Ce qu'il fallait faire.



Conformément à ce qui a été dit pour le pentagone, si par les points de divisions d'un cercle, on mène des tangentes à ce cercle, on circonscrira à ce cercle un quindécagone équilatéral et équiangle. De plus, conformément à ce qui a été dit pour les démonstrations du pentagone, nous inscrirons et nous circonscrirons une circonférence de cercle à un quindécagone équilatéral et équiangle donné.

Comme  
il faut ve-  
nir aux  
Equations  
qui ser-  
uent a re-  
soudre les  
problèmes.

Ainsi voulant résoudre quelque problème, on doit d'abord le considérer comme déjà fait, & donner des noms a toutes les lignes, qui semblent nécessaires pour le construire, aussi bien a celles qui sont inconnues, qu'aux autres. Puis sans considérer aucune différence entre ces lignes connues, & inconnues, on doit parcourir la difficulté, selon l'ordre qui montre le plus naturellement de tous en quelle sorte elles dependent mutuellement les unes des autres, jusques a ce qu'on ait trouvé moyen d'exprimer une mesme quantité en deux façons: ce qui se nomme une Equation; car les termes de l'une de ces deux façons sont esgaux a ceux de l'autre. Et on doit trouver autant de telles Equations, qu'on a supposé de lignes, qui estoient inconnues. Oubien s'il ne s'en trouve pas tant, & que nonobstant on n'omette rien de ce qui est désiré en la question, cela tesmoigne qu'elle n'est pas entierement déterminée. Et lors on peut prendre a discretion des lignes connues, pour toutes les inconnues aussi qu'elles ne correspondent aucune Equation. Après cela s'il en reste encore plusieurs, il se faut servir par ordre de chacune des Equations qui restent aussi, soit en la considérant toute seule, soit en la comparant avec les autres, pour expliquer chacune de ces lignes inconnues, & faire ainsi en les demeslant, qu'il n'en demeure qu'une seule, esgale a quelque autre, qui soit connue, ou bien dont le carré, ou le cube, ou le carré de carré, ou le sursolide, ou le carré de cube, &c. soit esgal a ce, qui se produit par l'addition, ou soustraction de deux ou plusieurs autres quantités, dont l'une soit connue, & les autres soient composées de quelques moyennes proportionnelles entre l'unité, & ce carré, ou cube, ou carré de carré, &c. multipliées par d'autres connues. Ce que j'écris en cete sorte.

$$x \propto b. \text{ ou}$$

$$x^2 \propto -ax + bb. \text{ ou}$$

$$x^3 \propto +ax^2 + bbx - c. \text{ ou}$$

$$x^4 \propto ax^3 - cx^2 + d. \text{ \&c.}$$

C'est a dire,  $x$ , que ie prens pour la quantité inconnüe, est esgalé a  $b$ , ou le quarré de  $x$  est esgal au quarré de  $b$  moins  $a$  multiplié par  $x$ . ou le cube de  $x$  est esgal a  $a$  multiplié par le quarré de  $x$  plus le quarré de  $b$  multiplié par  $x$  moins le cube de  $c$ . & ainsi des autres.

Et on peut tousiours reduire ainsi toutes les quantités inconnuës à vne seule, lorsque le Probleme se peut construire par des cercles & des lignes droites, ou aussy par des sections coniques, ou mesme par quelque autre ligne qui ne soit que d'un ou deux degres plus composée. Mais ie ne m'arreste point a expliquer cecy plus en detail, a cause que ie vous osterois le plaisir de l'apprendre de vous mesme, & l'utilité de cultiuer vostre esprit en vous y exerçant, qui est a mon auis la principale, qu'on puisse tirer de cete science. Aussy que ie n'y remarque rien de si difficile, que ceux qui seront vn peu versés en la Geometrie commune, & en l'Algebre, & qui prendront garde a tout ce qui est en ce traité, ne puissent trouver.

C'est pourquoy ie me contenteray icy de vous auertir, que pourvü qu'en demeslant ces Equations on ne manque point a se seruir de toutes les diuisions, qui seront possibles, on aura infalliblement les plus simples termes, aufquels la question puisse estre reduite.

Quels  
sont les  
proble-  
mes plans

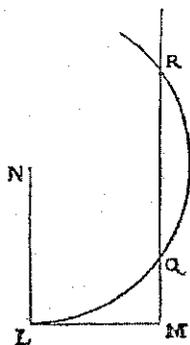
Et que si elle peut estre resolue par la Geometrie ordinaire, c'est a dire, en ne se seruant que de lignes droites & circulaires tracées sur vne superficie plate, lorsque la derniere Equation aura esté entierement demeslée, il n'y restera tout au plus qu'un quarré inconnu, esgal a ce qui se produit de l'Addition, ou soustraction de sa racine multipliée par quelque quantité connue, & de quelque autre quantité aussy connue

[...]

Enfin si i'ay

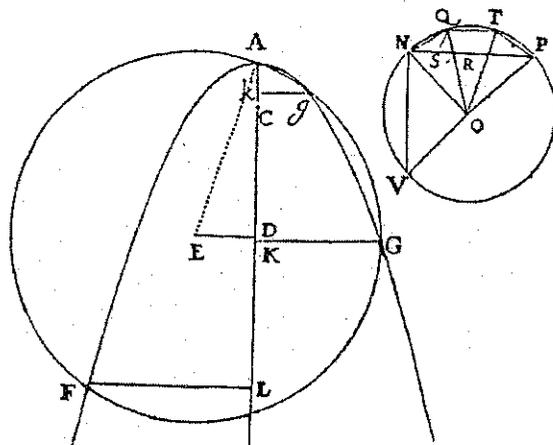
$$x^2 \propto ax - bb:$$

ie fais  $NL$  esgale à  $\frac{1}{2}a$ , &  $LM$  esgale à  $b$  cõme deuãt, puis, au lieu de ioindre les poins  $M N$ , ie tire  $MQR$  parallele a  $LN$ . & du centre  $N$  par  $L$  ayant descrit vn cercle qui la coupe aux poins  $Q$  &  $R$ , la ligne cherchée  $x$  est  $MQ$ , oubiẽ  $MR$ , car en ce cas elle s'ex-



prime en deux façons, a sçauoir  $x \propto \frac{1}{2}a + \sqrt{\frac{1}{4}aa - bb}$ ,  
&  $x \propto \frac{1}{2}a - \sqrt{\frac{1}{4}aa - bb}$ .

Et si le cercle, qui ayant son centre au point  $N$ , passe par le point  $L$ , ne coupe ny ne touche la ligne droite  $MQR$ , il n'y a aucune racine en l'Equation, de façon qu'on peut assurer que la construction du probleme proposé est impossible.



La façon  
de diuiser  
vn angle  
en trois.

Tout de mesme si on veut diuiser l'angle  $NO P$ , ou bien l'arc, ou portion de cercle  $N Q T P$ , en trois parties esgales; faisant  $NO \propto 1$ , pour le rayon du cercle, &  $NP \propto q$ , pour la subtendue de l'arc donné, &  $NQ \propto x$ , pour la subtendue du tiers de cet arc; l'Equation vient,

$x^3 \propto 3x - q$ . Car ayant tiré les lignes  $NQ, OQ, OT$ ; & faisant  $QS$  parallele a  $TO$ , on voit que comme  $NO$  est a  $NQ$ , ainsi  $NQ$  a  $QR$ , &  $QR$  a  $RS$ ; en sorte que  $NO$  estant  $1$ , &  $NQ$  estant  $x$ ,  $QR$  est  $xx$ , &  $RS$  est  $x^3$ : Et a cause qu'il s'en faut seulement  $RS$ , ou  $x^3$ , que la ligne  $NP$ , qui est  $q$ , ne soit triple de  $NQ$ , qui est  $x$ , ou à  $q \propto 3x - x^3$  ou bien,

$$x^3 \propto 3x - q.$$

Puis la Parabole  $FAG$  estant descrite, &  $CA$  la moitié de son costé droit principal estant  $\frac{1}{2}$ , si on prend  $CD \propto \frac{1}{2}$ , & la perpendiculaire  $DE \propto \frac{1}{2}q$ , & que du centre  $E$ , par  $A$ , on descrine le cercle  $FAG$ , il coupe cete Parabole aux trois points  $F, g, \& G$ , sans conter le point  $A$  qui en est le sommet. Ce qui monstre qu'il y a trois racines en cete Equation, à sçauoir les deux  $GK, \& gk$ , qui sont vrayes; & la troisieme qui est fausse, à sçauoir  $FL$ . Et de ces deux vrayes c'est  $gk$  la plus petite qu'il faut prendre pour la ligne  $NQ$  qui estoit cherchée. Car l'autre  $GK$ , est esgale à  $NV$ , la subtendue de la troisieme partie de l'arc  $NVP$ , qui avec l'autre arc  $NQP$  acheue le cercle. Et la fausse  $FL$  est esgale a ces deux ensemble  $QN \& NV$ , ainsi qu'il est aysé a voir par le calcul.

<sup>15</sup> Pour une utilisation de ce texte en classe, voir Brochure M. :A.T.H. tome 2 (Brochure n°79 de l'IREM Paris VII).

55. Il y a un cas particulier de la proposition précédente qui mérite de fixer notre attention ; le voici : *il existe toujours des nombres dont aucune puissance plus petite que  $p - 1$  n'est congrue à l'unité* ; il y en a même autant entre 1 et  $p - 1$ , qu'il y a au-dessous de  $p - 1$  de nombres qui lui soient premiers. Comme il s'en faut bien que la démonstration de ce théorème soit aussi évidente qu'elle le paraît d'abord, nous en donnerons une un peu différente de celle qui précède, d'autant plus que la diversité des méthodes aide beaucoup à jeter du jour sur les points les plus obscurs.

On décomposera  $p - 1$  en facteurs premiers, de manière qu'on ait  $p - 1 = a^\alpha b^\beta c^\gamma$  etc.  $a$ ,  $b$ ,  $c$ , etc. étant des nombres premiers inégaux. Alors nous composerons la démonstration des deux propositions suivantes :

1°. On peut toujours trouver un nombre  $A$ , ou plusieurs appartenant à l'exposant  $a^\alpha$ , et de même des nombres  $B$ ,  $C$ , etc. appartenant aux exposants  $b^\beta$ ,  $c^\gamma$ , etc.

2°. Le produit des nombres  $A$ ,  $B$ ,  $C$ , etc. ou le résidu *minimum* de ce produit appartiendra à l'exposant  $p - 1$  ; ce qui se démontre ainsi qu'il suit.

1°. Soit  $g$  un des nombres 1, 2, 3 ...  $p - 1$  qui ne satisfasse pas à la congruence  $x^{\frac{p-1}{a}} \equiv 1 \pmod{p}$  ; car tous les nombres ne peuvent pas satisfaire à cette congruence, dont le degré est  $< p - 1$ . Alors je dis que si l'on fait  $g^{\frac{p-1}{a^\alpha}} \equiv h$  ou son résidu *minimum* appartiendra à l'exposant  $a^\alpha$ .

En effet il est évident que  $h^{a^\alpha} \equiv g^{p-1} \equiv 1$  ; mais  $h^{a^{\alpha-1}} \equiv g^{\frac{p-1}{a}}$ , et par conséquent sera incongru à l'unité, et à plus forte raison les puissances  $h^{a^{\alpha-2}}$ ,  $h^{a^{\alpha-3}}$  le seront aussi. Or l'exposant de la plus petite puissance de  $h$  congrue à l'unité, c'est-à-dire l'exposant auquel  $h$  appartient, doit être un diviseur de  $a^\alpha$  (n° 48) ; et comme  $a^\alpha$  n'est divisible que par lui-même, ou par les puissances inférieures de  $a$ , il s'ensuit nécessairement que  $a^\alpha$  sera l'exposant

auquel  $[h]^{16}$  appartient. On démontrera de la même manière, qu'on peut trouver des nombres appartenant aux exposants  $b^\beta, c^\gamma$ , etc.

2°. Si nous supposons que le produit de tous les nombres  $A, B, C$ , etc. n'appartienne pas à l'exposant  $p - 1$ , etc., mais à un exposant  $t$  plus petit,  $t$  devra être un des diviseurs de  $p - 1$  (n° 48), ou  $\frac{p-1}{t}$  sera un entier  $> 1$ . Il suit de là que ce quotient sera un des nombres premiers,  $a, b, c$ , etc., ou du moins qu'il sera divisible par quelqu'un d'eux (n° 17), par  $a$ , par exemple, car le raisonnement est le même pour les autres.  $t$  divisera ainsi  $\frac{p-1}{a}$  ; donc le produit  $ABC$  etc. serait encore congru à l'unité, en l'élevant à la puissance  $\frac{p-1}{a}$  (n° 46). Mais il est évident que tous les nombres,  $B, C, D$ , etc. (excepté  $A$ ) deviennent congrus à l'unité, si on les élève à la puissance  $\frac{p-1}{a}$ , puisque les exposants auxquels ils appartiennent  $b^\beta, c^\gamma$ , etc. divisent  $\frac{p-1}{a}$ . Donc  $A^{\frac{p-1}{a}} \cdot B^{\frac{p-1}{a}} \cdot C^{\frac{p-1}{a}}$  etc.  $\equiv A^{\frac{p-1}{a}} \equiv 1$  ; donc  $a^\alpha$  doit diviser  $\frac{p-1}{a}$  (n° 48), c'est-à-dire que  $\frac{p-1}{a^{\alpha+1}}$  doit être entier, ce qui est absurde (n° 15). Donc enfin notre supposition ne peut subsister, c'est-à-dire que le produit  $ABC$  etc. appartient réellement à l'exposant  $p - 1$ .

\*

\* \*

---

16 Le texte donne "b".

## 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 Pouillet-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

