# GAUSS, NOMBRES CONSTRUCTIBLES ET POLYGONES RÉGULIERS.

Martine BÜHLER.

## I. Rapide survol historique.

### Constructions de polygones réguliers chez les Grecs.

Le livre IV des *Éléments* d'Euclide, consacré au cercle, donne des constructions de polygones réguliers (inscrits dans un cercle donné) à la règle et au compas. Si les constructions du carré et de l'hexagone régulier ne posent aucun problème (propositions 6 et 15), la construction du pentagone régulier est plus délicate. Euclide utilise les propriétés géométriques angulaires du pentagone régulier pour réaliser sa construction : des propositions préliminaires lui permettent d'inscrire dans un cercle un triangle isocèle dont les angles à la base sont doubles de l'angle au sommet, puis d'obtenir le pentagone régulier par bissection de deux arcs (Figure 1).

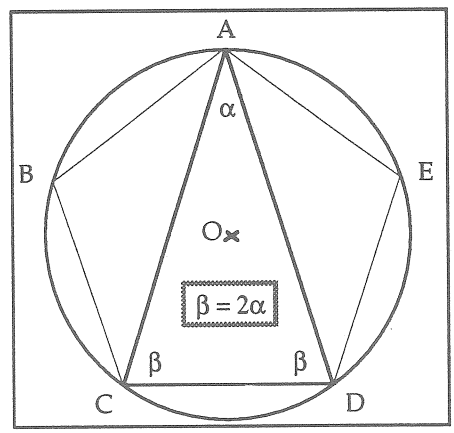


Figure 1.

A partir de ces constructions, Euclide en obtient d'autres : il construit le décagone régulier par bissection des arcs sous-tendus par les côtés du pentagone. Euclide obtient également la construction du polygone régulier à 15 côtés de la manière suivante :

Si $AC$ est le côté du pentagone et $AB$ celui du triangle équilatéral, alors l'arc $(AB)$ est le tiers de la circonférence et l'arc $(AC)$ le cinquième de la circonférence. Donc l'arc $(BC)$, différence des arcs $(AB)$ et $(AC)$, est :

$$\left(\frac{1}{3} - \frac{1}{5}\right) \textit{ circonférence} = \frac{2}{15} \textit{ circonférence.}$$

Soit $E$ le milieu de l'arc $(BC)$, $BE$ est donc le côté du polygone régulier à 15 côtés (Figure 2).

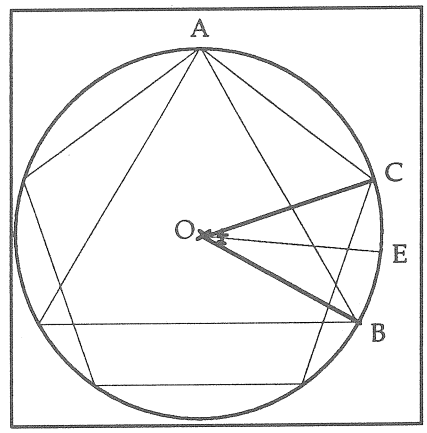


Figure 2.

Nous reviendrons sur cette méthode et sa généralisation. Euclide obtient ensuite le polygone régulier à 30 côtés par bissection de l'arc valant un quinzième de circonférence.

Dans l'*Almageste* de Ptolémée, on trouve également d'astucieuses constructions. Le but de Ptolémée n'est pas cependant l'étude géométrique du cercle. L'*Almageste* est un ouvrage d'astronomie et Ptolémée s'intéresse aux polygones réguliers car il a besoin d'établir une table donnant la longueur des cordes soutendant les arcs d'un cercle, ceux-ci étant donnés de demi-degré en demi-degré (table équivalente à nos tables de sinus puisque, si $d$ est le diamètre du cercle, $\alpha$ la mesure d'un arc et $l$ la longueur de la corde soutendant l'arc :

$$\sin\frac{\alpha}{2} = \frac{\frac{l}{2}}{\frac{d}{2}} = \frac{l}{d}.$$

Des lemmes préliminaires lui permettent d'obtenir les cordes soutendant la différence et la somme d'arcs de sous-tendantes connues, ainsi que la corde correspondant à un arc moitié d'un arc de sous-tendante connue. Mais il lui faut un "point de départ", et, pour cela, une construction du pentagone régulier permettant un calcul simple du côté du pentagone (ce que ne permet pas la construction d'Euclide).

Dans le cercle de centre $O$ et de diamètre $[AC]$, soit $B$ le milieu de l'arc $(AC)$ et $E$ le milieu du segment $[OC]$. On place $Z$ sur $[AO]$ tel que $EZ = EB$. Alors $BZ$ est le côté du pentagone régulier inscrit dans le cercle (Figure 3).

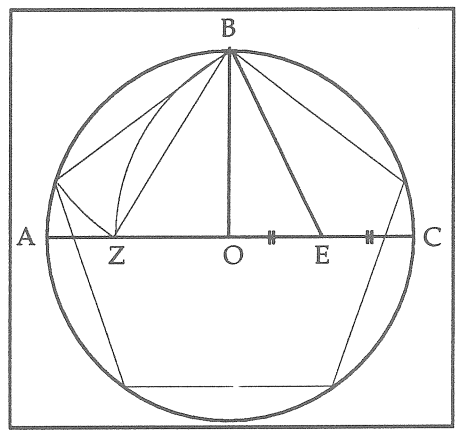


Figure 3.

Ptolémée calcule alors la longueur de la corde $BZ$ soutendant l'arc de 72°, puis par ses lemmes préliminaires, celle de la corde soutendant l'arc de $12° = 72° - 60°$, le côté de l'hexagone étant bien sûr connu. Des bissections successives lui permettent alors d'obtenir les cordes soutendant les arcs de 6°, 3° et 1,5°. La trisection de l'angle de 1,5° n'étant pas possible à la règle et au compas, Ptolémée encadre la corde soutendant l'arc de 1° par un calcul rigoureux d'approximations. Il peut ensuite établir sa table.

On ne trouve pas de constructions exactes à la règle et au compas d'autres polygones réguliers jusqu'à celle du polygone régulier à 17 côtés de Gauss en 1796. Par contre, certains traités de géométrie pratique donnent des constructions approchées des polygones à 7 côtés, 9 côtés, etc., et même des constructions approchées de pentagones, dont, certes, on connaît des constructions exactes, mais dont une construction approchée plus simple que la construction exacte permet une plus grande précision dans l'exécution et est donc plus utile aux "artistes".

* * * * *

## L'approche de Descartes dans la *Géométrie*.

En 1637, dans la *Géométrie*, Descartes donne, à partir de segments de longueur $a$ et $b$, la construction à la règle et au compas des segments de longueurs $a+b$, $|a-b|$, $a\,b$, $\frac{a}{b}$ et $\sqrt{a}$. Sa préoccupation n'est pas la constructibilité des polygones réguliers, mais nous pouvons voir un lien entre les deux problèmes : construire un polygone régulier à $n$ côtés, c'est construire une corde de longueur appropriée. Si cette longueur s'exprime à l'aide du rayon $R$ par l'intermédiaire des opérations élémentaires (+, ×, -, :) et de la racine carrée, le polygone est constructible à la règle et au compas.

Cependant, Descartes n'aborde pas la réciproque de ce résultat de constructibilité. Nous pourrions exprimer ce résultat de manière plus "actuelle" : des longueurs étant données, on peut construire des segments de longueur $x$ solution d'une équation du second degré dont les coefficients sont des expressions rationnelles des longueurs données, le procédé pouvant s'itérer en ajoutant toute longueur construite aux données.

* * * * *

## Gauss et les polygones réguliers.

Dans les *Disquisitiones Arithmeticæ* (1801, pour la 1ère éd.), Section VII, Gauss donne une étude complète de la constructibilité des polygones réguliers, donnant une condition nécessaire et suffisante sur le nombre de côtés pour cette constructibilité. Cependant, nous verrons qu'il manque à Gauss un résultat (démontré par Wantzel en 1837) pour valider complètement son théorème.

La première remarque de Gauss dans son étude rejoint le procédé d'Euclide pour obtenir la construction du polygone régulier à 15 côtés : si on sait construire les polygones réguliers à $n_1$ côtés et à $n_2$ côtés, $n_1$ et $n_2$ étant premiers entre eux, alors on sait construire le polygone à $(n_1 \,.\, n_2)$ côtés.

En effet, soient $[AB]$ et $[AC]$ les cordes soutendant les arcs de $\left(\frac{360}{n_1}\right)^\circ$ et $\left(\frac{360}{n_2}\right)^\circ$. Comme $n_1$ et $n_2$ sont premiers entre eux, il existe $u$ et $v$ dans $\mathbb{Z}$ tels que : $u \,.\, n_1 + v \,.\, n_2 = 1$ (identité de Bezout) ; alors $u \times \frac{360^\circ}{n_2} + v \times \frac{360^\circ}{n_1} = \frac{360^\circ}{n_1 . n_2}$.

En mettant 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), on obtient une corde soutendant l'arc de $\frac{360°}{n_1 . n_2}$, donc le côté du polygone régulier à $(n_1 . n_2)$ côtés (Figure 4, ci-contre).

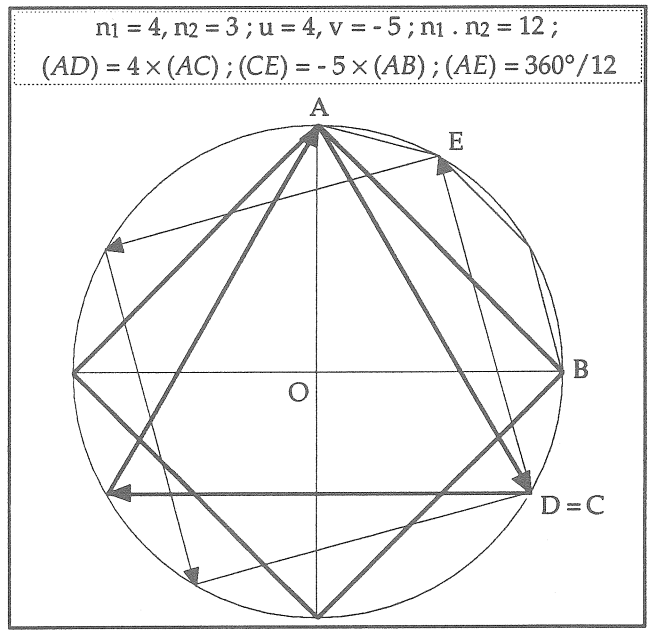


Figure 4.

Gauss conclut qu'il suffit donc de chercher à construire le polygone régulier à $p^\alpha$ côtés où $p$ est un nombre premier impair. En effet, si on sait construire les polygones réguliers à $p^\alpha$ et $q^\beta$ côtés, $p$ et $q$ étant des nombres premiers impairs distincts, alors on sait, d'après ce qui précède, construire le polygone à $(p^\alpha . q^\beta)$ côtés, puis celui à $(2^\gamma . p^\alpha . q^\beta)$ côtés, la bissection d'un arc étant toujours possible à la règle et au compas.

C'est cette étude que nous allons examiner maintenant.

*
* *

# II. Le travail de Gauss.

L'étude de Gauss repose, d'une part sur les résultats d'arithmétique concernant les congruences *modulo n*, d'autre part sur des considérations portant sur les équations polynomiales et les fonctions symétriques.

Je ne démontrerai quasiment aucun résultat, mais j'essaierai, à partir des exemples traités par Gauss ($n = 17$ et $n = 19$), de montrer au lecteur la signification et l'utilisation de ces résultats.

* * * * *

## Congruences *modulo n*.

Soit $n$ un entier premier. Rappelons que, pour tout entier $a$ non divisible par $n$, $a^{n-1} \equiv 1$ (*mod n*), ce qu'on appelle le "petit théorème de Fermat". Gauss démontre qu'il existe toujours des nombres dont aucune puissance strictement inférieure à $n - 1$ n'est congrue à l'unité. Autrement dit, il existe $a$ tel que :

$$a^t \not\equiv 1 \ (mod\ n), \text{ si } 0 < t < n - 1 ;$$

donc les puissances $a^t$ pour $t = 0, 1, ..., n - 2$ sont toutes distinctes : c'est-à-dire que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique, engendré par $a$. Un tel nombre $a$ est appelé "racine primitive selon $n$". La démonstration de l'existence de racine(s) primitive(s) est donnée dans l'annexe 1 (qui reproduit le texte de Gauss).

Par exemple, 2 est racine primitive selon 19 (c'est-à-dire est générateur de $[(\mathbb{Z}/19\mathbb{Z})^*, \times)]$. En effet, on a, *modulo* 19 :

| | | | | | |
|---|---|---|---|---|---|
| $2^0 \equiv 1$ | $2^1 \equiv 2$ | $2^2 \equiv 4$ | $2^3 \equiv 8$ | $2^4 \equiv 16$ | $2^5 \equiv 13$ |
| $2^6 \equiv 7$ | $2^7 \equiv 14$ | $2^8 \equiv 9$ | $2^9 \equiv 18$ | $2^{10} \equiv 17$ | $2^{11} \equiv 15$ |
| $2^{12} \equiv 11$ | $2^{13} \equiv 3$ | $2^{14} \equiv 6$ | $2^{15} \equiv 12$ | $2^{16} \equiv 5$ | $2^{17} \equiv 10$, |

et bien sûr : $2^{18} \equiv 1$ (*mod* 19) car ici $n - 1 = 18$.

Vous pouvez vérifier que 3 est racine primitive selon 17 et chercher les racines primitives selon 5 et 7. Remarquons que ce résultat n'est pas évident malgré son énoncé si simple en termes de "groupe cyclique". De plus, la recherche des racines primitives n'est pas du tout facile. Voici ce qu'en dit Gauss lui-même :

> *"73. La plupart des méthodes qui servent à trouver des racines primitives reposent en grande partie sur le tâtonnement* [...] *Euler avoue (opuscula analy. T 1 p. 152) qu'il lui semble extrêmement difficile d'assigner ces nombres, et que leur nature doit être rangée dans les points les plus épineux de la théorie des nombres."*[1]

Enfin une dernière mise en garde avant de poursuivre : nous allons être amenés à parler de nombres complexes, en particulier de $e^{i\frac{2k\pi}{n}}$, et donc, des racines primitives $n^{\text{ièmes}}$ de l'unité, notion totalement différente de celle qui précède (qui, elle, relève de l'arithmétique des nombres entiers), et nous essaierons d'éviter les confusions qui peuvent résulter d'une trop grande similitude de dénominations.

* * * * *

## Polygone régulier à $n$ côtés et racines $n^{\text{ièmes}}$ de l'unité ($n$ premier impair).

Construire le polygone régulier à $n$ côtés, c'est construire, soit la corde sous-tendant l'arc de $\frac{2\pi}{n}$ radians, soit $\cos\left(\frac{2\pi}{n}\right)$ ou $\sin\left(\frac{2\pi}{n}\right)$, chacune de ces constructions permettant les autres.

On sait depuis Descartes construire les solutions d'équations du second degré et Gauss va s'intéresser d'emblée aux équations dont sont solutions les nombres $\cos\left(\frac{2\pi}{n}\right)$ et $\sin\left(\frac{2\pi}{n}\right)$ qu'il cherche à construire. Il commence par donner les équations de degré $n$ dont sont solutions $\cos\left(\frac{2\pi}{n}\right)$ et $\sin\left(\frac{2\pi}{n}\right)$, mais les écarte immédiatement au profit de l'équation $x^n - 1 = 0$, beaucoup plus simple et dont les solutions $e^{2ki\frac{\pi}{n}}$ ($k = 0$ à $n - 1$) permettent d'obtenir facilement $\cos\left(\frac{2\pi}{n}\right)$ et $\sin\left(\frac{2\pi}{n}\right)$[2].

La seule racine réelle de l'équation $[x^n - 1 = 0]$ est 1 et Gauss considère donc plutôt l'équation $[X = 0]$ :

$$x^{n-1} + x^{n-2} + \ldots + x + 1 = 0,$$

1 Gauss, *Disq. Arithm.*, éd. de 1816, p. 53.
2 Cf. le texte en annexe.

dont l'ensemble des racines est $\Omega = \{r, r^2, \ldots, r^{n-1}\}$, $r$ étant une racine primitive $n^{\text{ième}}$ de l'unité, c'est-à-dire $r = e^{2i\frac{k\pi}{n}}$ avec $k = 1$, ou 2, ... , ou $n$ - 1.

> "342. *Le but de nos recherches, qu'il n'est pas inutile d'annoncer ici en plus de mots, est de décomposer* X graduellement *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* $\Omega$. *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 coefficiens 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* $\nu$ *étant le nombre des facteurs* $\alpha$, $\beta$, $\gamma$, *etc., la recherche des racines* $\Omega$ *est ramenée à la résolution de* $\nu$ *équations des degrés* $\alpha$, $\beta$, $\gamma$, *etc.*
>
> *Par exemple, pour* $n = 17$, *on a 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."*[3]

Autrement dit, pour $n = 17$, comme $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$, $X$ est décomposable en 2 facteurs de degré 8, dont les coefficients sont solutions d'une équation à coefficients entiers de degré 2. Puis chacun des facteurs de degré 8 se décompose en 2 facteurs de degré 4 dont les coefficients sont solutions d'une équation de degré 2, etc.

Comme Gauss utilise fréquemment les puissance de $r$, il note $[\lambda] = r^\lambda$. On a donc : $[\lambda] = [\mu]$ ssi $\lambda \equiv \mu \ (mod\ n)$

$[\lambda] \cdot [\mu] = [\lambda + \mu]$

$[\lambda]^\mu = [\lambda \cdot \mu]$

$[0] = 1$

$[0] + [\lambda] + [2\lambda] + \ldots [(n - 1)\lambda] = 0$, si $\lambda$ n'est pas divisible par $n$ car alors $r^\lambda$ est une racine primitive $n^{\text{ième}}$ de l'unité et cette somme est celle des racines $n^{\text{ièmes}}$ de l'unité, ou :

$[0] + [\lambda] + [2\lambda] + \ldots [(n - 1)\lambda] = n$, si $\lambda$ est divisible par $n$, car alors $[h\lambda] = [0] = 1$.

La méthode de Gauss consiste à grouper astucieusement les racines de l'équation $[X = 0]$ afin de les obtenir en résolvant "en cascade" des équations de degré $\alpha$, $\beta$, $\gamma$, etc. ($\alpha$, $\beta$, $\gamma$ étant les facteurs premiers de $n - 1$). Cette méthode est en fait celle des exercices des anciens baccalauréats des séries C et D sur les racines $n^{\text{ième}}$ de l'unité. Nous allons d'ailleurs examiner de près deux exercices

3 *Op. cit.*, pp. 437-438.

de ce type, pour montrer que nos élèves appliquent la méthode de Gauss sans le savoir.

* * * * *

## Le "Bac" C à la manière de ... Gauss.

Un énoncé du "Bac" C, Amiens, 1984, et sa solution.

Soit $r = \cos\frac{2\pi}{5} + i.\sin\frac{2\pi}{5}$.
1°) On pose $\alpha = r + r^4$, et $\beta = r^2 + r^3$.
Montrer que $\alpha$ et $\beta$ sont des solutions de l'équation (1)
(1) $x^2 + x - 1 = 0$.

$\alpha + \beta = r + r^2 + r^3 + r^4 = -1$, car la somme des racines 5èmes de l'unité est nulle.

$\alpha \times \beta = r^3 + r^4 + r^6 + r^7 = r^3 + r^4 + r + r^2 = -1$, donc $\alpha$ et $\beta$ sont solutions de $[x^2 + x - 1 = 0]$.

2°) Déterminer $\alpha$ en fonction de $\cos\left(\frac{2\pi}{5}\right)$.

Résoudre l'équation (1) et en déduire la valeur de $\cos\left(\frac{2\pi}{5}\right)$.

$r^4 = \bar{r}$, donc $\alpha = 2 . \cos\left(\frac{2\pi}{5}\right)$.

Les solutions de (1) sont $\frac{-1+\sqrt{5}}{2} > 0$ et $\frac{-1-\sqrt{5}}{2} < 0$.

Or $\frac{2\pi}{5} \in \left]0;\frac{\pi}{2}\right[$ donc $\cos\frac{2\pi}{5} > 0$. Finalement : $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$.

La même chose, à la manière de ... Gauss.

$r = e^{2i\frac{\pi}{5}}$. $\Omega = \{ [1], [2], [3], [4] \}$ est l'ensemble des solutions de l'équation :

$$x^4 + x^3 + x^2 + x + 1 = 0.$$

Or 2 est racine primitive selon 5 car $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$.
On réordonne $\Omega$ en utilisant ce résultat : $\Omega = \{ [1], [2], [4], [3] \}$.
Card $\Omega = n - 1 = 2 \times 2$.
On distribue $\Omega$ en deux "périodes" de deux racines.

$$\alpha = (2, 1) = [1] + [4],$$
$$\beta = (2, 2) = [2] + [3].$$

(2, 1) est la somme des racines prises de 2 en 2 à partir de [1], qu'on peut donc aussi bien appeler (2, 4) car $\Omega$ étant "cyclique", on peut partir de [4] pour

grouper de 2 en 2 les racines. De même pour (2, 2), on fait la somme des racines prises de 2 en 2 à partir de [2] et on a (2, 2) = (2, 3).

Alors $\alpha + \beta = (2, 1) + (2, 2)$ est la somme des racines de $\Omega$ donc $\alpha + \beta = -1$ (car ce sont les racines de $[x^4 + x^3 + x^2 + x + 1 = 0]$ et leur somme est donc l'opposé du coefficient de $x^3$).

$$\begin{aligned}
\alpha \times \beta &= (2, 1) \,.\, (2, 2) \\
&= [1] \,.\, [2] + [4] \,.\, [3] + [1] \,.\, [3] + [4] \,.\, [2] \\
&= [3] + [7] + [4] + [6] \\
&= [3] + [2] + [4] + [1] \\
&= (2, 3) + (2, 4) \\
&= (2, 2) + (2, 1) \\
&= \alpha + \beta = -1.
\end{aligned}$$

Remarquons que (2, 1) = [1] + [4], et que :
(2, 1) . (2, 2) = (2, 1 + 2) + (2, 4 + 2) = (2, 3) + (2, 1) (car [6] = [1]).

On comprend ce résultat puisque chacune des périodes consiste en la somme de racines de $\Omega$ prises de 2 en 2. Nous verrons d'autres exemples de calculs qui permettront de bien voir le "fonctionnement" des produits de périodes.

(2, 1) et (2, 2) sont donc solutions de : $X^2 + X - 1 = 0$. Comme [1] + [4] = (2, 1) et [1] . [4] = [0] = 1, [1] et [4] sont solutions de $[X^2 - (2, 1)X + 1 = 0]$.

C'est bien le programme annoncé par Gauss : $n - 1 = 4 = 2 \times 2$. On a trouvé les racines de $\Omega$ en résolvant 2 (nombre de facteurs premiers dans $[n - 1]$) équations, toutes deux de degré 2 (seul nombre premier divisant $[n - 1]$).

Autre exemple : un exercice d'un livre de terminale C [4].

On considère le nombre complexe $r = \cos \frac{2\pi}{7} + i.\sin \frac{2\pi}{7}$.
On pose $S = r + r^2 + r^4$, et $T = r^3 + r^5 + r^6$.

a) Montrer que Im (S) > 0.

$$\begin{aligned}
\text{Im } S &= \sin \frac{2\pi}{7} + \sin \frac{4\pi}{7} + \sin \frac{8\pi}{7} \\
&= \sin \frac{2\pi}{7} + 2 \,.\, \sin \frac{6\pi}{7} \,.\, \cos \frac{2\pi}{7} > 0, \text{ car } \frac{2\pi}{7} \text{ et } \frac{6\pi}{7} \in \left]0, \pi\right[, \text{ et } \frac{2\pi}{7} \in \left]0, \frac{\pi}{2}\right[.
\end{aligned}$$

b) Calculer $S + T$, $S \,.\, T$ puis en déduire $S$ et $T$.

4 *Mathématiques, Terminale C*, Belin ; exercice 32, page 69.

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

Donc $S$ et $T$ sont solutions de $[X^2 + X + 2 = 0]$.

Comme Im $S > 0$, $S = \frac{-1+i\sqrt{7}}{2}$ et $T = \frac{-1-i\sqrt{7}}{2}$.

En termes de périodes :

$r = e^{2i\frac{\pi}{7}}$. $\Omega = \{ [1], [2], [3], [4], [5], [6] \}$.

3 est générateur de $(\mathbb{Z}/7\mathbb{Z})^*$ car $3^0 \equiv 1$, $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$ (et bien sûr $3^6 \equiv 1$).

On réordonne $\Omega$ : $\Omega = \{ [1], [3], [2], [6], [4], [5] \}$. Card $\Omega = n - 1 = 3 \times 2$.

On groupe en deux "périodes" de trois racines.

$S = (3, 1) = [1] + [2] + [4] = (3, 2) = (3, 4)$, (on prend les racines de 2 en 2 à partir de [1]) ;

$T = (3, 3) = [3] + [6] + [5] = (3, 6) = (3, 5)$.

Alors $S + T$ est la somme des racines de $\Omega$ et vaut - 1 (car ce sont les racines de $[x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0]$).

$S \,.\, T = (3, 1) \,.\, (3, 3) = [1] \,.\, [3] + [2] \,.\, [6] + [4] \,.\, [5]$
$+ [2] \,.\, [3] + [4] \,.\, [6] + [1] \,.\, [5]$
$+ [4] \,.\, [3] + [1] \,.\, [6] + [2] \,.\, [5]$
$= [4] + [1] + [2]$ $\{ = (3, 4) \}$
$+ [5] + [3] + [6]$ $\{ = (3, 5) \}$
$+ [0] + [0] + [0]$
$= (3, 4) + (3, 5) + (3, 0)$ {on pose $(3, 0) = [0] + [0] + [0]$}
$= (3, 1) + (3, 3) + (3, 0)$ {car $(3, 4) = (3, 1)$, et $(3, 5) = (3, 3)$}
$= -1 + 3 = 2$.

Donc S + T et S . T sont solutions de $[X^2 + X + 2 = 0]$.

Là encore, lorsqu'on mène le calcul de cette manière, on fait clairement apparaitre :

$(3, 1) \,.\, (3, 3) = (3, 1 + 3) + (3, 2 + 3) + (3, 4 + 3)$, car $(3, 1) = [1] + [2] + [4]$.

Enfin : $[1] + [2] + [4] = (3, 1)$ ;

$[1] \,.\, [2] + [2] \,.\, [4] + [4] \,.\, [1] = [3] + [6] + [5] = (3, 3)$ ;

$[1] \,.\, [2] \,.\, [4] = [7] = [0] = 1$.

Donc [1], [2] et [4] sont solutions de :

$x^3 - (3, 1)x^2 + (3, 3)x - 1 = 0$.

Comme $n - 1 = 6 = 3 \times 2$, on a trouvé [1] en résolvant 2 (nombre de facteurs premiers dans $[n - 1]$) équations ; l'une de degré 2 et l'autre de degré 3 (facteurs premiers de la décomposition de $[n - 1]$).

Remarquons que $6 = 3 \times 2$ mais aussi $2 \times 3$. On aurait donc pu grouper en 3 périodes de 2 racines (qu'on aurait appelées (2, 1), (2, 3) et (2, 2)) et résoudre d'abord une équation de degré 3 pour trouver (2, 1), (2, 3) et (2, 2), puis une équation de degré 2 pour trouver [1] et [6].

Ces deux exemples ont le mérite de la simplicité, mais ils en ont aussi le défaut : $n$ - 1 ne comportant que deux facteurs, on voit mal ce que devient le procédé s'il y a trois facteurs premiers dans [$n$ - 1], ou plus.

Nous allons examiner les deux exemples que Gauss cite constamment pour éclairer son propos : $n = 17$ et $n = 19$.

* * * * *

## Groupement de racines en "périodes".

"*354.* Exemple II. Pour $n = 17$.

*On a ici $n - 1 = 2 . 2 . 2 . 2$, ainsi le calcul des racines $\Omega$ peut se ramener à quatre équations du second degré. Nous choisirons 3 pour racine primitive ; ses puissances fournissent, suivant le module 17, les résidus* minima *suivants :*

*0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15*
*1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6,*

*d'où résulte la distribution suivante en deux périodes de huit termes, quatre périodes de quatre termes et huit de deux termes :* [...]"[5]

On a :
$\Omega$ = { [1], [3], [9], [10], [13], [5], [15], [11], [16], [14], [8], [7], [4], [12], [2], [6] }.

Comme 16 = 8 × 2, on peut grouper en 2 périodes de 8 termes :
(8, 1) = [1] + [9] + [13] + [15] + [16] + [8] + [4] + [2] ;
(8, 3) = [3] + [10] + [5] + [11] + [14] + [7] + [12] + [6].

Mais, comme 16 = 4 × 4, on peut aussi grouper en 4 périodes de 4 termes :
(4, 1) = [1] + [13] + [16] + [4] ;
(4, 3) = [3] + [5] + [14] + [12] ;
(4, 9) = [9] + [15] + [8] + [2] = (4, 2) ;
(4, 10) = [10] + [11] + [7] + [6] = (4, 6).

On remarque que (8, 1) est formé de (4, 1) et (4, 2) et que (8, 3) est formé de (4, 3) et (4, 6), ce qui n'a rien de surprenant puisque les périodes de 8 racines sont obtenues en prenant les racines de 2 en 2 et que les périodes de 4 racines sont obtenues en les prenant de 4 en 4.

Comme 16 = 2 × 8, on peut également grouper $\Omega$ en 8 périodes de 2 racines et on s'apercevra que chaque période de 4 racines est formée de deux périodes de 2 racines. Ce qui donne la distribution suivante :

5 *Op. cit.*, p. 458.

$$\Omega = (16, 1)\begin{cases}(8, 1)\begin{cases}(4, 1)\begin{cases}(2, 1) \ldots\ldots [1], [16]\\ (2, 13) \ldots\ldots [4], [13]\end{cases}\\ (4, 9)\begin{cases}(2, 9) \ldots\ldots [8], [9]\\ (2, 15) \ldots\ldots [2], [15]\end{cases}\end{cases}\\ (8, 3)\begin{cases}(4, 5)\begin{cases}(2, 3) \ldots\ldots [3]^*, [14]\\ (2, 5) \ldots\ldots [5], [12]\end{cases}\\ (4, 10)\begin{cases}(2, 10) \ldots\ldots [7], [10]\\ (2, 11) \ldots\ldots [6], [11]\end{cases}\end{cases}\end{cases}$$

[* Gauss donne [8]].

Remarquons que Gauss note indifféremment (2, 1) la somme [1] + [16] et l'ensemble { [1], [16] }, le contexte permettant de trancher.

Comment maintenant trouver [1] ?
On cherche l'équation dont sont solutions (8, 1) et (8, 3) :
(8, 1) + (8, 3), somme des racines de $\Omega$, vaut - 1 ;
(8, 1) . (8, 3) = (8, 4) + (8, 12) + (8, 16) + (8, 1) + (8, 2) + (8, 11) + (8, 7) + (8, 5) (par le procédé déjà vu plus haut) = 4 . (8, 1) + 4 . (8, 3) = - 4 ;
donc (8, 1) et (8, 3) sont solutions de $[x^2 + x - 4 = 0]$.

On cherche alors l'équation dont sont solutions (4, 1) et (4, 2) :
(4, 1) + (4, 2) = (8, 1) ;
(4, 1) . (4, 2) = (8, 3) + (8, 1) = - 1. Donc (4, 1) et (4, 2) sont solutions de $[X^2 - (8, 1)X - 1 = 0]$.
De même : (4, 3) et (4, 6) sont solutions de $[X^2 - (8, 3)X - 1 = 0]$.

On cherche l'équation dont sont solutions (2, 1) et (2, 4) :
(2, 1) + (2, 4) = (4, 1) ;
(2, 1) . (2, 4) = (2, 5) + (2, 3) = (4, 3). Donc (2, 1) et (2, 4) sont solutions de $[X^2 - (4, 1)X + (4, 3) = 0]$.

Enfin : [1] + [16] = (2, 1) ; [1] . [16] = 1. Donc [1] et [16] sont solutions de $[X^2 - (2, 1)X + 1 = 0]$.

Ces résultats donnent d'ailleurs la constructibilité à la règle et au compas du polygone régulier à 17 côtés puisque $\cos \frac{2\pi}{17} = \frac{1}{2} . ( [1] + [16] ) = \frac{1}{2} . (2, 1)$ et qu'on a obtenu (2, 1) en résolvant uniquement des équations du second degré à coefficients, soit entiers, soit obtenus comme solutions d'équations du second degré. Donc (2, 1) s'exprime à l'aide uniquement des opérations algébriques élémentaires et de radicaux carrés, appliqués à des entiers.

* * * * *

## Généralité de la méthode.

De plus, Gauss démontre que ce procédé fonctionne toujours. Pour $n$ entier premier impair, il existe toujours $g$, racine primitive, ce qui signifie que :

$\{ 1, g, g^2, \ldots, g^{n-2} \} = \{ 1, 2, \ldots, (n-1) \}$ (compte non tenu de l'ordre évidemment). Alors on ordonne $\Omega$ : $\Omega = \{ [1], [g], \ldots, [g^{n-2}] \}$.

Pour $e$ diviseur de $n - 1$, on a $n - 1 = e \,.\, f$ et on peut grouper $\Omega$ en $e$ périodes de $f$ termes :

$$(f, 1) = \{ [1], [g^e], \ldots, [g^{(f-1)e}] \} ;$$
$$(f, g) = \{ [g], [g^{e+1}], \ldots, [g^{(f-1)e+1}] \} ;$$
$$\ldots$$
$$(f, g^{e-1}) = \{ [g^{e-1}], \ldots, [g^{ef-1}] \}.$$

Pour $(f, 1)$, on a pris les racines de $\Omega$, de $e$ en $e$ à partir de $[1]$ ; pour $(f, g)$, on a fait la même chose à partir de $[g]$, etc.

Les groupements "efficaces" sont ceux correspondants à la décomposition de $n - 1$ en facteurs premiers.

Si $n - 1 = \alpha \,.\, \beta \,.\, \gamma \ldots \zeta$, on distribue les racines de $\Omega$ en $\alpha$ périodes de $a = \frac{n-1}{\alpha} = \beta \,.\, \gamma \ldots \zeta$ termes, puis celles-ci en $\beta$ périodes de $b = \frac{n-1}{\alpha\beta} = \gamma \ldots \zeta$ termes, puis celles-ci en $\gamma$ périodes de c termes, etc.

Puis on cherche l'équation $A$ (de degré $\alpha$) dont sont racines les $\alpha$ premières périodes : Gauss a démontré que les coefficients sont entiers ; puis on cherche l'équation $B$ (de degré $\beta$) dont sont racines les $\beta$ périodes suivantes : Gauss a démontré que les coefficients s'expriment de manière rationnelle à l'aide des $\alpha$ premières périodes.

Et on continue jusqu'à arriver aux racines de $\Omega$.

> "352. *Les théorèmes précédens, avec leurs corollaires, contiennent les bases principales de toute la théorie, et le moyen de trouver les racines $\Omega$ peut s'exposer maintenant en peu de mots.*
>
> *On doit, avant tout, prendre un nombre g qui soit racine primitive pour le module n, et trouver les résidus* minima *des puissances de g jusqu'à $g^{n-2}$. On décomposera n - 1 en facteurs, et même en facteurs premiers, si l'on veut réduire le problème à des équations du degré le plus simple possible. Soient $\alpha, \beta, \gamma, \ldots\ldots \zeta$ les facteurs de n - 1, et soit fait*
>
> $$\frac{n-1}{\alpha} = \beta\gamma \ldots\ldots \zeta = a, \quad \frac{n-1}{\alpha\beta} = \gamma \ldots\ldots \zeta = b, \text{ etc.}$$
>
> *On distribuera les racines $\Omega$ en $\alpha$ périodes de a termes ; chacune de celles-ci en $\beta$ périodes de b termes ; chacune de ces dernières en $\gamma$ périodes, etc. On cherchera, par le n° 350, l'équation (A) de degré $\alpha$ qui aura pour racines ces $\alpha$ sommes de a termes, sommes dont on connaîtra les valeurs par la résolution de cette équation."*[6]

6 *Op. cit.*, p. 452.

Les démonstrations de Gauss reposent sur des considérations sur les polynômes symétriques et sur le caractère cyclique de $\Omega$.

Je ne ferai pas ici d'exposé de ces démonstrations mais seulement, à la suite du texte de Gauss donnant ses conclusions sur la constructibilité des polygones réguliers, quelques remarques.

*"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 nos 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 . $2^\mu$, 5 . $2^\mu$, 15 . $2^\mu$ *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* $2^\nu$. *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* $2^{2^\nu} + 1$ ; *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."*[7]

Gauss a effectivement montré que si $n = 2^{2^m} + 1$ est un nombre premier, on sait construire le polygone régulier à $n$ côtés puisqu'alors, on obtient $\cos \frac{2\pi}{n}$ en résolvant des équations du second degré dont chacune a des coefficients s'exprimant rationnellement à l'aide des racines de la précédente.

La valeur qu'il donne pour $\cos \frac{2\pi}{17}$ permet d'ailleurs théoriquement la construction du polygone régulier à 17 côtés. Notons cependant qu'il ne s'est pas lancé dans celle-ci. Richmond, en 1893, en donnera une construction plus élégante avec une autre résolution de $[x^{17} - 1 = 0]$[8].

Cependant Gauss se contente d'affirmer qu'il peut *"démontrer en toute rigueur que ces équations ne sauraient en aucune manière être évitées ni abaissées"*, mais ne donne pas cette démonstration. En admettant même que l'irréductibilité des équations soit prouvée, la réciproque du résultat de Descartes n'est pas démontrée lorsque Gauss écrit les *Disquisitiones*. Il faut attendre 1837 pour que Wantzel démontre effectivement qu'on ne peut pas construire à la règle et au compas les solutions d'équations irréductibles de degré $n$, où $n$ n'est pas une puissance de 2.

Laissons Gauss conclure sur la *"division géométrique du cercle"*.

*"366. Si l'on veut diviser le cercle en $a^\alpha$ parties, a étant un nombre premier et $\alpha > 1$, il est aisé de voir que la construction géométrique n'est possible qu'autant que $a = 2$. En effet, si $a > 2$, outre les équations nécessaires pour la division du cercle en a parties, il faut encore résoudre $\alpha - 1$ équations du degré a, que l'on ne peut non plus ni éviter, ni abaisser. Ainsi le degré des équations nécessaires se connaîtra généralement par les facteurs premiers du nombre $(a - 1) . a^{\alpha - 1}$ (y compris le cas où $\alpha = 1$)."*

En effet : $$e^{\frac{2i\pi}{a^{\alpha-1}}} = \left(\cos \frac{2\pi}{a^{\alpha-1}} + i.\sin \frac{2\pi}{a^{\alpha-1}}\right) = \left(e^{\frac{2i\pi}{a^\alpha}}\right)^a$$

7 *Op. cit.*, pp. 487-488.
8 Voir [CARREGA].

Donc $\cos \frac{2\pi}{a^\alpha}$ et $\sin \frac{2\pi}{a^\alpha}$ sont solutions d'équations de degré $a$ dont les coefficients s'expriment rationnellement à l'aide de $\cos \frac{2\pi}{a^{\alpha-1}}$ et $\sin \frac{2\pi}{a^{\alpha-1}}$.

*"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 $a^\alpha$, $b^\beta$, $c^\gamma$, 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.*

*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."*[9]

La lecture du texte de Gauss est convaincante quant à la validité de la méthode mais elle n'est pas éclairante sur les raisons profondes qui font fonctionner le procédé. Dans [CARREGA], on trouvera des explications claires sur le lien entre les méthodes de Gauss et la théorie de Galois, que nous allons essayer de résumer ici.

*
* *

# III. Problèmes de constructibilité.

Il nous faut d'abord "théoriser" la notion de base de ces problèmes, celle de "nombre constructible à la règle et au compas".

* * * * *

9 *Op. cit.*, pp. 488-489.

## Nombres constructibles.

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

* soit en joignant 2 points de $\{M_1 ; M_2 ; \ldots ; M_{j-1}\} = C_{j-1}$
* soit en prenant comme centre un point de $C_{j-1}$ et comme rayon la distance entre deux points de $C_{j-1}$.

Notre problème de constructibilité d'un polygone régulier entre bien dans ce cadre puisqu'il s'agit d'inscrire un polygone dans un cercle donné : or, se donner un cercle, c'est se donner 2 points ($O$ : centre du cercle et $I$, un point du cercle) et construire le polygone régulier, c'est construire $A$ tel que $[AI]$ soit un des côtés du polygone cherché.

À partir de $\{O ; I\}$, on peut construire $J$ tel que $(O, I, J)$ soit un repère orthonormé et on dira qu'un nombre réel est constructible s'il est l'abscisse ou l'ordonnée d'un point constructible. L'ensemble des nombres constructibles est un corps contenant $\mathbb{Q}$ et stable par racines carrées (expression moderne du résultat de Descartes).

* * * * *

## Extensions de corps et nombres constructibles.

Rappelons quelques résultats sur les extensions de corps avant de voir le lien entre celles-ci et la constructibilité du polygone à 17 côtés.

* 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 le degré de l'extension.
* Si $K \subset L \subset M$ sont de degré fini, alors $[M : K] = [M : L] \times [L : K]$.
* Si $a \in \mathbb{C}$, $Q(a)$ est le plus petit sous-corps de $\mathbb{C}$ contenant $a$.
* $a$ algébrique sur $\mathbb{Q}$ signifie : il existe un polynôme $P$ de $\mathbb{Q}[X]$ t. q. : $P(a) = 0$.

Dans ce cas, il existe un unique polynôme unitaire de degré minimum tel que $P(a) = 0$. Le degré de ce polynôme est appelé "degré de $a$".

* $a$ algébrique sur $\mathbb{Q}$ si et seulement si $Q \subset Q(a)$ est de degré fini ;
  et alors, $[Q(a) : Q]$ est le degré de $a$.
* Soit $a \in \mathbb{R}$. $a$ est constructible si et seulement s'il existe une suite de sous-corps de $\mathbb{R}$ : $L_1 = \mathbb{Q} \subset L_2 \subset L_3 \subset \ldots \subset L_p$ telle que $a \in L_p$ et $[L_j : L_{j-1}] = 2$.

Ceci implique que le degré de $a$ est une puissance de 2 (Résultat de Wantzel), mais la réciproque est fausse : il existe des nombres algébriques de degré $2^m$ non constructibles[10].

* * * * *

## Méthode de Gauss et extensions de corps. Exemple $n = 17$.

Soit $r = e^{2i\frac{\pi}{17}}$. $\Omega = \{ r, r^2, r^3, \ldots, r^{16} \}$.

Soit $K = \mathbb{Q}(r)$. Alors K est un $\mathbb{Q}$-espace vectoriel de base $\{ 1, r, r^2, r^3, \ldots, r^{15} \}$ car $r^{16} = - r^{15} - r^{14} - \ldots - r - 1$ et toute puissance de $r$ supérieure à 15 s'exprime comme un polynôme à coefficients entiers en $1, r, \ldots, r^{15}$. Donc $[K : \mathbb{Q}] = 16$.

Soit G le groupe des automorphismes de K.

Soit $\sigma \in G$ :

* $\sigma(1) = 1$ donc $\sigma(x) = x$ pour $x \in \mathbb{Q}$. Tout automorphisme de K laisse $\mathbb{Q}$ invariant point par point.

* $\sigma$ est entièrement déterminé par $\sigma(r)$. En effet, $\sigma(r^k) = \sigma(r)^k$ et tout élément $x$ de K s'écrit : $x = a_0 + a_1 . r + \ldots + a_{15} . r^{15}$ ($a_i \in \mathbb{Q}$) donc :

$$\sigma(x) = a_0 + a_1 . \sigma(r) + \ldots + a_{15} . \sigma(r)^{15} \quad (\text{car } \sigma(a_i) = a_i).$$

* Or $\sigma(r) \in \Omega$. En effet, on a : $1 + r + r^2 + \ldots + r^{16} = 0$, donc :

$1 + \sigma(r) + \sigma(r)^2 + \ldots + \sigma(r)^{16} = 0$, donc $\sigma(r)$ est solution de :

$1 + X + X^2 + \ldots + X^{16} = 0$.

Il y a donc bijection entre G et $\Omega$.

Or $\Omega = \{ 1, 2, \ldots, 16 \} = (\mathbb{Z}/17\mathbb{Z})^*$. On peut munir $\Omega$ d'une structure de groupe par la loi "$\times$" et alors il y a isomorphisme de groupe entre G et $[(\mathbb{Z}/17\mathbb{Z})^*, \times]$. Car : $\sigma' \circ \sigma\,(r) = r^{\lambda\lambda'}$ si $\sigma(r) = r^{\lambda}$ et $\sigma'(r) = r^{\lambda'}$.

Soit $g$ (= 3) générateur de $[(\mathbb{Z}/17\mathbb{Z})^*, \times]$, i. e. racine primitive selon 17.

Appelons : $G_0$ le sous-groupe de G engendré par $g$ (= 3), i. e. $G_0 = G$.

$G_1$ le sous-groupe de G engendré par $g^2$ (= 9).

$G_2$ le sous-groupe de G engendré par $g^{2^2}$ ($\equiv 13$).

$G_3$ le sous-groupe de G engendré par $g^{2^3}$ ($\equiv 16$).

$G_4$ le sous groupe de G engendré par $g^{2^4}$ ($\equiv 1$), i. e. $G_4 = \{1\}$.

Soit $K_i = \left\{ x \in K \,;\, g^{2^i}(x) = x \right\}$, pour $i \in \{0, 1, 2, 3, 4\}$ : $K_i$ est l'ensemble des éléments de K invariants par $G_i$.

Alors on a : $K_0 = \mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset K_4 = K$. Et $[K_4 : K_0] = [K : \mathbb{Q}] = 16$.

10 Voir [CARREGA] pour un contre exemple.

On peut montrer $K_i \neq K_{i+1}$, donc :
comme $[K_4 : K_0] = [K_4 : K_3] . [K_3 : K_2] . [K_2 : K_1] . [K_1 : K_0]$, on a $[K_i : K_{i-1}] = 2$, donc on peut construire le polygone régulier à 17 côtés.

* * * * *

## Et les périodes dans tout çà ?

On a $(8, 1) = r^1 + r^9 + r^{13} + r^{15} + r^{16} + r^8 + r^4 + r^2$.

Ici $g = 3$ et $g^2 = 9$. L'automorphisme $\sigma$ défini par $g^2$ est donc celui tel que $\sigma(r) = r^9$.

On a alors : $\sigma(r^9) = r^{13}$, $\sigma(r^{13}) = r^{15}$, $\sigma(r^{15}) = r^{16}$, $\sigma(r^{16}) = r^8$, $\sigma(r^8) = r^4$, $\sigma(r^4) = r^2$, $\sigma(r^2) = r$. Ce qui est lié à la manière dont on a ordonné les racines $r^k$ de $\Omega$ à l'aide des puissances de $g$ modulo 16, ainsi qu'à la formation de (8, 1) en prenant les racines de deux en deux.

Donc : $\sigma[(8, 1)] = (8, 1)$ donc $(8, 1) \in K_1$ (puisque (8, 1) est invariant par $\sigma$, automorphisme défini par $g^2$).

De même pour (8, 3).

Donc (8, 1) et (8, 3) sont dans $K_1$. Comme $[K_1 : \mathbb{Q}] = 2$, il est "normal" de trouver que (8, 1) et (8, 3) sont les solutions d'une équation de degré 2 à coefficients dans $\mathbb{Q}$.

De même : $(4, 1) = r^1 + r^{13} + r^{16} + r^4$, et , par l'automorphisme $\sigma' = \sigma^2$ défini par $g^4$, on a : $\sigma'(r^1) = r^{13}$, $\sigma'(r^{13}) = r^{16}$, $\sigma'(r^{16}) = r^4$, $\sigma'(r^4) = r$.

Donc $\sigma'[(4, 1)] = (4, 1)$, donc $\sigma' \in K_2$.

De même (4, 2), (4, 3), (4, 6) sont dans $K_2$.

Donc, comme $[K_2 : K_1] = 2$, ces quatres périodes s'obtiennent en résolvant des équations de degré 2, dont les coefficients sont dans $K_1$, et s'expriment rationnellement à partir de (8, 1) et (8, 3).

Quant à (2, 1), on a : $(2, 1) = r^1 + r^{16}$.

Or par $\sigma^8 = \sigma''$, défini par $g^{2^3}$ , on a : $\sigma''(r^1) = r^{16}$ et $\sigma''(r^{16}) = r^1$.

Donc $(2, 1) \in K_3$. Or $(2, 1) = \cos \frac{2\pi}{17}$. Donc $\cos \frac{2\pi}{17}$ s'obtient comme solution d'une équation de degré 2 à coefficients dans $K_2$.

On voit bien là que le résultat sur les racines primitives est fondamental car le caractère cyclique de $\Omega$ est essentiel pour conclure à l'existence de cette chaîne de sous-corps de degré 2 sur le précédent, donc à la constructibilité du polygone régulier à 17 côtés.

*
* *

# Annexe.

## Ch.-Fr. GAUSS (de Brunswick) : Extrait[11] des *RECHERCHES ARITHMÉTIQUES*, traduites par A.-C.-M. Poullet-Delisle (1807), pp. 37-39.

// p. 37 // [...]

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. // p. 38 //

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 $h^{a^{\alpha-2}}$,

11 Le lecteur pourra retrouver cet extrait, ainsi que ceux inclus dans le texte, dans la réédition de la Librairie Blanchard, Paris, 1979, § 55, pp. 37-39. Le texte ici réédité en typographie moderne n'a pas été modifié quant à l'orthographe et aux notations.

$h^{a^{\alpha-3}}$ 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 [$h$][12] appartient. On démontrera de la même manière, qu'on peut trouver des nombres appartenants 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 // p. 39 // 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 $A^{\frac{p-1}{a}}.B^{\frac{p-1}{a}}.C^{\frac{p-1}{a}}$. 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.

*
* *

12 Le texte donne "$b$".

# Bibliographie.

## Sources.

EUCLIDE.

- *Les Éléments*. Trad. du grec par F. Peyrard. Paris, 1819. Réédition Lib. Blanchard, Paris, 1966 (nouveau tirage).

GAUSS, K.-F.

- *Recherches Arithmétiques*. Trad. A.-C.-M. Poullet Delisle, Paris, 1807. Réédition Lib. Blanchard, Paris, 1979.

KLEIN, F.

- *Leçons sur certaines questions de géométrie élémentaire*, Nouy, Paris, 1896. Réédition Lib. Vuibert, Paris, 1931 (3ème éd.). Reproduction par l'IREM de Paris-VII, coll. *Reproduction de textes anciens* n° 2, fév. 1981..

WANTZEL, L.

- "*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. 366-372. Reproduction in *Mnémosyne* n° 3, IREM de Paris-VII, avril 1993, pp. 8-14.

## Bibliographie secondaire.

CARREGA, J.-C.

- *Théorie des Corps. La règle et le compas*. Éd. Hermann, coll. *Formation des enseignants et formation continue*. Paris, 1981. Nouvelle édition enrichie d'exercices, Paris, 1989.

FRIEDELMEYER, J.-P.

- "*Des équations qui déterminent les sections circulaires*", in *L'Ouvert* nos 46 & 47, IREM de Strasbourg, mars & juin 87.

* *
*