Traduction d'un extrait de "A History of Algebra" de Bartel L. van der Waerden concernant Gauss (p. 89 à 102) (Denise Vella-Chemla, août 2023).

Chapitre 5

Carl Friedrich Gauss

Les contributions les plus importantes de Gauss à la théorie des équations algébriques sont :

1° la solution complète de l'"équation cyclotomique"

(1) $$x^m - 1 = 0$$

au moyen de radicaux,

2° la preuve que tout polynôme en une variable à coefficients réels est un produit de facteurs linéaires ou quadratiques. Ce théorème implique ce que nous appelons maintenant le "théorème fondamental de l'algèbre" : tout polynôme $f(x)$ à coefficients complexes est un produit de facteurs linéaires. Nous allons maintenant discuter de ces deux contributions extrêmement intéressantes.

L'équation cyclotomique

L'équation (1) est appelée cyclotomique, parce que sa solution est très liée à la construction d'un polygone régulier à n côtés inscrit dans un cercle donné.

Pour voir cela, on a juste à noter que l'équation (1) a n racines complexes

(2) $$\cos(2\pi k/n) + i\sin(2\pi k/n) \quad k = 0, 1, 2, ..., n-1.$$

Cette solution trigonométrique était connue de de Moivre et Euler longtemps avant Gauss. Maintenant, si on représente les nombres complexes $a + ib$ par des points dans le plan complexe de coordonnées (a, b), il est clair que les nombres complexes (2) sont représentés par les sommets d'un n-gone régulier inscrit dans le cercle-unité. Par conséquent, si on réussit à résoudre l'équation (1) au moyen de racines carrées, on peut construire le n-gone régulier à la règle et au compas.

Les pythagoriciens savaient déjà comment construire des polygones réguliers de 3, 4, 5, et 6 côtés. On peut trouver leurs constructions dans le Livre 4 des Éléments d'Euclide. Pour l'attribution de ce livre aux pythagoriciens, se reporter à mon livre "Die Pythagoreer" (Artemis-Verlag, Zürich 1979), p. 348-351.

Lagrange résolut l'équation

(3) $$x^5 - 1 = 0$$

comme suit. Une racine est $x = 1$. Les autres sont les racines de l'équation

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

qui peut s'écrire

$$(x^2 + x^{-2}) + (x + x^{-1}) + 1 = 0. \tag{4}$$

En posant

$$x + x^{-1} = y \tag{5}$$

on obtient

$$y^2 + y - 1 = 0. \tag{6}$$

Cette équation quadratique peut être résolue pour y, et ensuite, (5) peut être résolue pour x. Il en découle, une fois de plus, que le pentagone régulier peut être construit à la règle et au compas.

La construction d'Euclide est aussi basée sur la solution d'une équation quadratique. On lit dans la traduction de Heath du Livre 2 des Éléments d'Euclide la proposition 11 :

> *Couper une droite donnée de telle façon que le rectangle contenu par le tout et l'un des segments soit égal au carré du segment restant.*

Si la droite donnée est appelée a et le second segment y, le problème d'Euclide est de résoudre l'équation

$$a(a - y) = y^2. \tag{7}$$

Dans sa solution du problème II, 11, Euclide résout d'abord l'équation équivalente

$$y^2 + ay = a^2 \tag{8}$$

et ensuite, il soustrait le rectangle ay des deux côtés, obtenant ainsi la solution de (7). Si le segment donné a est pris comme unité de longueur, on voit que (8) est la même équation que l'équation (6) de Lagrange.

Dans le livre 4, Euclide utilise la solution de (7) dans sa construction du pentagone régulier. Juste ainsi, Lagrange utilise la solution de (6) pour la solution de l'équation cyclotomique (3).

Lagrange applique ensuite la même méthode à l'équation

$$x^{11} - 1 = 0 \tag{9}$$

(Œuvres III, p. 246). En divisant par $x - 1$ et ensuite par x^5, Lagrange obtient

(10) $$(x^5 + x^{-5}) + (x^4 + x^{-4}) + (x^3 + x^{-3}) + (x^2 + x^{-2}) + (x + x^{-1}) + 1 = 0.$$

En posant à nouveau

(11) $$x + x^{-1} = y$$

on obtient une équation quintique pour y.

Lagrange l'a laissée ainsi, mais Vandermonde a réussi à résoudre l'équation quintique par radicaux, comme on l'a vu au chapitre 4.

Alors qu'il avait presque 19 ans, Gauss découvrit que le polygone régulier à 17 côtés peut être construit à la règle et au compas. Dans le chapitre 7 du fameux travail de Gauss intitulé les "Disquisitiones arithmeticae", la preuve complète de la résolubilité de l'équation (1) par radicaux est donnée. L'équation

(12) $$x^{17} - 1 = 0$$

est traitée comme un cas particulier. Puisqu'on ne sait pas comment le jeune Gauss a trouvé la solution de (12) et donc la construction du 17-gone, on n'a d'autre choix que de suivre Gauss et de traiter le cas général en premier.

Gauss montre d'abord que l'équation générale (1) peut se réduire au cas particulier dans lequel n est un nombre premier, en écrivant n comme un produit de puissances de nombres premiers. Un cas particulier, notamment $n = 15$, était déjà connu d'Euclide. Euclide montre : si on peut inscrire dans un cercle un triangle régulier et un pentagone régulier, on peut aussi inscrire un polygone régulier à 15 côtés.

En divisant (1) par $x - 1$, on obtient l'équation

(13) $$X = x^{n-1} + x^{n-2} + \ldots + x + 1 = 0.$$

En supposant que n est un nombre premier, Gauss montre d'abord que le polynôme X est *irréductible rationnellement*. Ensuite, il annonce son résultat principal : si $n - 1$ est un produit de facteurs $\alpha\beta\gamma...$, l'équation (1) peut être résolue en résolvant des équations de degrés $\alpha, \beta, \gamma, \ldots$. Par exemple, si n est égal à 17, on a

$$n - 1 = 2^4,$$

et alors l'équation (12) peut être résolue en résolvant quatre équations quadratiques, et par conséquent le 17-gone peut être construit à la règle et au compas. Plus généralement, si $n-1$ est une puissance de 2, ce qui arrive pour

(14) $$n = 3, 5, 17, 257, 65537,$$

le n-gone régulier peut être construit à la règle et au compas.

Les nombres premiers mentionnés dans (14) étaient connus de Gauss. Les autres nombres premiers de la forme $2^m + 1$ ne sont pas connus à ce jour (3 décembre 1982).

En supposant toujours n comme étant un nombre premier, Gauss dénote par r n'importe quelle racine de (13). Maintenant les racines sont

$$r, r^2, \ldots, r^{n-1}. \tag{15}$$

Deux puissances r^λ et r^μ sont multipliées en ajoutant les exposants et en réduisant la somme $\lambda + \mu$ modulo n.

Gauss note ensuite que toute fonction rationnelle des racines peut être réécrite ainsi

$$A + A'r + A''r^2 + ... + A^{(n-1)}r^{n-1}. \tag{16}$$

Pour simplifier la notation, Gauss écrit $[\lambda]$ à la place de r^λ. Ainsi, les racines (15) sont réécrites comme

$$[1], [2], ..., [n-1]. \tag{17}$$

Dans le chapitre III des Disquisitiones, Gauss a démontré : si n est un nombre premier, le groupe multiplicatif des entiers modulo n est cyclique, i.e. il existe un "élément primitif" g tel que toutes les puissances d'exposants non divisibles par n sont congrues à des puissances de g. Donc les racines (17) peuvent être réordonnées et écrites comme

$$[1], [g], [g^2], \ldots [g^{n-2}]. \tag{18}$$

Ce réordonnancement est un point essentiel dans la théorie de Gauss. les exposants de g sont appelés des *indices*. Ils jouent le rôle des logarithmes : deux puissances de g sont multipliées en ajoutant leurs indices (mod $n-1$).

Maintenant soit e n'importe quel diviseur de $n-1$. En posant

$$n - 1 = ef$$

$$g^e = h,$$

Gauss considère l'ensemble des racines

$$[\lambda], [\lambda h], [\lambda h^2], \ldots, [\lambda h^{f-1}],$$

où λ est un entier arbitraire congru à zéro (mod n), et il forme la somme

$$(f, \lambda) = [\lambda] + [\lambda h] + [\lambda h^2] + \ldots + [\lambda h^{f-1}]. \tag{19}$$

Ces sommes sont indépendantes du choix de g. On les appelle des *périodes*.

Gauss élucide la formation des périodes en étudiant l'exemple $n = 19$. Je préfère donner l'exemple $n = 17$, élaboré par Gauss dans la section 354 (Werke, Vol. I, p. 437). Comme élément primitif (mod 17) Gauss choisit $g = 3$. Ainsi les indices (mod 16)

$$i = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15$$

donnent les puissances de 3 (mod 17)

$$\mu = g^i = 1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6$$

et les racines

$$[\mu] = r^\mu = r, r^3, r^9, r^{10}, ..., r^6.$$

Les diviseurs de $n - 1 = 16$ sont

$$e = 1, 2, 4, 8, 16$$

correspondant à

$$f = 16, 8, 4, 2, 1.$$

Il y a seulement une période (16, 1), notamment la somme de toutes les racines. Il y a deux périodes avec $f = 8$, notamment

$$(8, 1) = [1] + [9] + [13] + [15] + [16] + [8] + [4] + [2]$$

et

$$(8, 3) = [3] + [10] + [5] + [11] + [14] + [7] + [12] + [6].$$

Il y a quatre périodes avec $f = 4$, notamment

$$(4, 1), (4, 3), (4, 9), (4, 10).$$

Il y a huit périodes avec $f = 2$, notamment

$$(2, 1) = [1] + [16] = r + r^{-1},$$

et il y a 16 périodes avec $f = 16$, notamment les racines uniques.

Gauss considère aussi la période $(f, 0)$, qui est une somme de f unités et est par conséquent égale à f.

Dans la section 345 Gauss prouve le théorème général qui énonce qu'un produit

$$(f, \lambda) \cdot (f, \mu)$$

peut être exprimé comme une somme de périodes ainsi :

$$(f, \lambda) \cdot (f, \mu) = (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \ldots. \tag{20}$$

Maintenant, appliquons la formule (20) au cas $n = 17$. La somme

$$(8, 1) + (8, 3)$$

est la somme de toutes les racines et par conséquent elle est égale à -1. Le produit

$$(8,1)\cdot(8,3)$$

peut être calculé par (20) : il est égal à -4. Donc (8, 1) et (8,3) sont les racines de l'équation quadratique

$$y^2+y-4=0. \tag{21}$$

En résolvant cette équation, on obtient (8, 1) et (8,3). Ensuite (4, 1) et (4,9) peuvent être calculés par la même méthode. Leur somme est (8,1) et leur produit est -1, donc ce sont les racines de l'équation quadratique

$$x^2-(8,1)x-1=0. \tag{22}$$

Juste ainsi, (4,3) et (4,10) sont les racines de l'équation

$$x^2-(8,3)x-1=0. \tag{23}$$

Par la même méthode, les périodes $(2,\lambda)$ et finalement les racines $[\mu]$ peuvent être obtenues comme racines des équations quadratiques.

Dans le cas général, on doit factoriser $n-1$

$$n-1=\alpha\beta\gamma...$$

et résoudre des équations de degrés α,β,γ,.... Dans la section 359, Gauss montre que ces équations peuvent être résolues par radicaux.

Je suppose que ces exemples sont suffisants pour expliquer les idées principales de Gauss au sujet de l'équation cyclotomique.

Le "théorème fondamental"

Dans la notation de Gauss, toute équation algébrique de degré m peut s'écrire

$$x^m+Ax^{m-1}+Bx^{m-2}+\ldots+M=0 \tag{24}$$

ou $X=0$. Le "théorème fondamental de l'algèbre" comme on l'appelle, dit que tout polynôme X avec des coefficients réels ou complexes peut être factorisé en facteurs linéaires dans le corps des nombres complexes.

Il est suffisant de démontrer le théorème pour les polynômes à coefficients réels, car si X a des coefficients complexes, le produit $X\overline{X}$ est réel, et sa factorisation implique la factorisation des facteurs X et $\overline{X}$. Ainsi on a la justification du fait que Gauss se restreigne aux polynômes réels X.

Dans sa première démonstration, Gauss n'introduit pas les nombres complexes. Il démontre le théorème fondamental sous la forme suivante :

Tout polynôme X à coefficients réels peut être factorisé en facteurs linéaires et quadratiques.

Gauss a considéré que ce théorème était si important qu'il en a donné quatre démonstrations. Les principes, sur lesquels la première preuve est basée, ont été découverts par Gauss en octobre 1797. La première démonstration a été publiée en 1799, la seconde et la troisième en 1816, et la quatrième en 1849. La quatrième preuve est basée sur les mêmes principes que la première. Je me restreindrai ici aux trois premières démonstrations.

Les quatre preuves ont été traduites du latin à l'allemand par E. Netto et publiées sous le titre "Die vier Gauss'schen Beweise für die Zerlegung ganzer algebraischer Funktionen in reelle Faktoren ersten oder zweiten Grades", Ostwald's Klassiker der exakten Wissenschaften[1], Vol. 14 (Leipzig 1913).

La première démonstration

La première preuve de Gauss a été publiée dans sa thèse (Werke III, p. 1-30). Avant d'exposer sa propre preuve, Gauss critique des démonstrations antérieures données par d'Alembert, Euler, Fontenex, et Lagrange. Sa principale objection est que dans toutes ces preuves, l'existence de racines est présupposée. Il est montré que des racines complexes peuvent être obtenues, en supposant qu'elles existent d'une manière ou d'une autre. Il y a d'autres objections à chacune des preuves individuelles qui ne seront pas discutées ici.

Gauss commence avec un polynôme réel.

$$X = x^m + Ax^{m-1} + B^{m-2} + ... + Lx + M, \tag{25}$$

dans lequel x est une indéterminée ("unbestimmte Größe"). Ce qu'il veut démontrer c'est qu'un facteur linéaire ou quadratique de X existe. Un facteur réel linéaire implique l'existence d'une racine réelle $\pm r$, où r est positif ou nul. Un facteur irréductible quadratique implique l'existence de deux racines complexes

$$r(\cos\varphi + i\sin\varphi), \tag{26}$$

par conséquent, les facteurs quadratiques peuvent s'écrire

$$x^2 - 2xr\cos\varphi + r^2 \qquad (r > 0). \tag{27}$$

En substituant l'une des racines (26) dans l'équation $X = 0$ et en séparant les parties réelle et imaginaire, on obtient une paire d'équations réelles pour r et φ :

[1] "Les quatre preuves de Gauss de la décomposition de toute fonction algébrique en facteurs réels du premier et second degrés", Les classiques des sciences exactes de Ostwald.

(28) $$r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + ... + Lr \cos \varphi + M = 0$$
(29) $$r^m \sin m\varphi + Ar^{m-1} \sin(m-1)\varphi + ... + Lr \sin \varphi = 0.$$

Gauss note qu'Euler a obtenu cette paire d'équations en utilisant les nombres complexes. Gauss évite les nombres complexes : il dérive (28) et (29) directement de la supposition que le polynôme X a un facteur linéaire $x \pm r$ ou un facteur quadratique (27).

Gauss interprète (28) et (29) comme des équations de courbes algébriques en coordonnées polaires, et il réussit à prouver que ces courbes s'intersectent en un point au moins. Si ceci est démontré, il en découle que X a un facteur linéaire ou quadratique, et en continuant le processus, on obtient une factorisation de X en facteurs linéaires et quadratiques.

L'équation (28) est notée $U = 0$, et (29) est notée $T = 0$. Pour illustrer la preuve, j'ai dessiné les courbes $U = 0$ et $T = 0$ dans le cas d'une équation quadratique

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

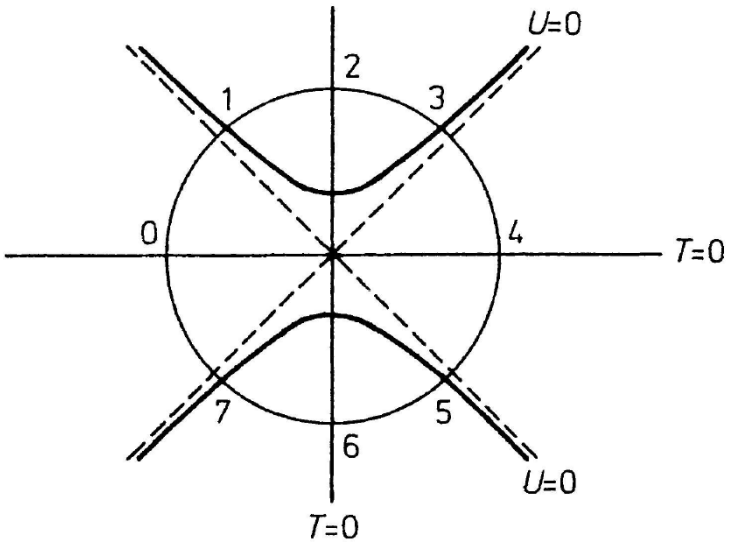

FIG. 23

En coordonnées orthogonales x et y, on a deux courbees d'ordre m. L'axe $y = 0$ est toujours une partie de la seconde courbe $T = 0$.

Gauss étudie maintenant les intersections des deux courbes avec un cercle de rayon R, et il démontre :

Pour un rayon suffisamment large R, il y a exactement $2m$ intersections du cercle avec $T = 0$ et $2m$ intersections avec $U = 0$, et tout point d'intersection du second type est entre deux points du premier type.

Gauss présente une preuve complète de ce lemme. Il note ensuite que les $4m$ points changent seulement très peu si R est rendu un peu plus grand ou un peu plus petit. En terminologie moderne, on dirait que les $4m$ points sont des fonctions continues de R. Gauss ne démontre pas

cette continuité : il dit seulement qu'elle est "facile à voir". Ensuite, Gauss étudie le comportement des branches des courbes $U = 0$ et $T = 0$ à l'intérieur du cercle, et il affirme : il existe un point d'intersection d'une branche de la première courbe avec une branche de la seconde courbe. Pour cette conclusion, il donne une preuve intuitive, géométrique. Il dénote le point d'intersection du cercle avec l'axe des x par 0, le prochain point voisin sur le cercle par 1, et etc., comme dans la figure Fig. 23. Les nombres impairs dénotent des points sur $U = 0$, les nombres pairs des points sur $T = 0$. Maintenant il dit : si une branche d'une courbe algébrique entre dans un certain domaine, elle doit aussi quitter le même domaine quelque part. Dans une note de bas de page, il ajoute :

> *Il semble bien démontré qu'une courbe algébrique ne se termine jamais abruptement (comme cela arrive dans le cas de la courbe transcendante $y = 1/\log x$), ni ne se perd jamais après un nombre infini d'enroulements en un point (comme une spirale logarithmique). Aussi loin que je m'en souvienne, personne n'a jamais douté de cela, mais si quelqu'un le nécessite, je prends sur moi de présenter de cela, à une autre occasion, une preuve indubitable.*

Si ce point de départ est accepté, il en découle que tout "point pair" est relié à (au moins) un autre point pair par une branche de la courbe $T = 0$, et que tout "point impair" est relié à un autre point impair par une branche de la courbe $U = 0$. Maintenant, aussi compliquées que ces relations puissent être, on peut montrer qu'un point d'intersection existe toujours. Cela se démontre comme suit.

Supposons qu'aucun point d'intersection n'existe. Le point 0 est relié au point $2m$ par l'axe des x. Le point 1 ne peut pas être relié à un point quel qu'il soit de l'autre côté de cet axe sans intersecter l'axe. Donc, si le point 1 est relié au point impair n, on doit avoir $n < 2m$. Juste ainsi, si 2 est relié à n', on doit avoir $n' < n$. Notons que la différence $n' - 2$ est paire, parce que 2 et n' sont tous les deux pairs. En continuant de cette manière, on trouve finalement un point h relié à $h + 2$. Mais maintenant la branche qui entre dans le cercle au point $h + 1$ doit nécessairement intersecter la branche reliant h et $h+2$, contrairement à notre hypothèse. Par conséquent, il existe un point d'intersection.

De cet exposé, on voit que la première démonstration de Gauss est basée sur des suppositions à propos des branches de courbes algébriques, qui semblent plausibles à notre intuition géométrique, mais qui ne sont strictement pas démontrées par Gauss. Alexander Ostrowski a montré dans un article très intéressant "Über den ersten und vierten Gauss'schen Beweis des Fundamentalsatzes der Algebra", que toutes les suppositions faites par Gauss peuvent être justifiées par des démonstrations indubitables. L'article d'Ostrowski a été d'abord publié dans les Nachrichten der Gesellschaft der Wissenschaften Göttingen 1920, et réimprimé dans les Travaux de Gauss X, 2.

La seconde preuve

La seconde preuve est purement algébrique. Les seules suppositions faites à propos du corps des nombres réels sont :

1° que toute équation réelle de degré impair a une racine réelle,

2° que toute équation quadratique à coefficients complexes a deux racines complexes.

L'idée sous-tendant la seconde preuve est simple, mais la mise en œvre est assez difficile. Gauss commence avec un polynôme réel de degré m

(30) $$Y = x^m - L'x^{m-1} + \check{L}''x^{m-2} - ... + ...$$

Si on suppose un instant que Y peut être factorisé en facteurs linéaires

(31) $$Y = (x-a)(x-b)(x-c)...$$

dans une certaine extension de corps, alors une combinaison linéaire

(32) $$(a+b)t - ab$$

peut être formée avec une nouvelle indéterminée t. Si les racines $a, b, c, ...$ sont permutées, la fonction linéaire (32) prend

$$m' = \tfrac{1}{2}m(m+1)$$

valeurs, par conséquent, elle est racine d'une équation de degré m'. Les racines de cette équation auxiliaire sont des fonctions linéaires de t de la forme (32). Dès qu'une racine de l'équation auxiliaire est connue, $a+b$ et ab sont connus, donc a et b peuvent être exprimés au moyen de racines carrées. Cela reste vrai si l'indéterminée t est spécialisée de telle façon que des fonctions linéaires différentes (32) restent différentes après la spécialisation.

Maintenant si m est un nombre de la forme

(33) $$m = 2^\mu k$$

où k est impair, le degré de l'équation auxiliaire est de la forme

(34) $$m' = 2^{\mu-1}k'$$

où k' est à nouveau impair.

Dès qu'une racine complexe de cette équation auxiliaire est connue, deux racines a et b de l'équation originale peuvent être calculées qui sont des nombres complexes en extrayant une racine carrée.

En continuant de cette manière, on arrive finalement à une équation de degré impair. Les coefficients de cette équation sont des fonctions symétriques des racines $a, b, ...$ avec coefficients réels, donc ce sont des nombres réels connus. Puisque le degré est impair, cette équation a au moins une racine réelle. En revenant à travers la séquence des équations auxiliaires, on peut calculer au moins une racine complexe de l'équation originale.

Dans cette forme simplifiée, la preuve fonctionne si on sait que l'équation $Y = 0$ a m racines $a, b, ...$ dans une certaine extension du corps des nombres réels. L'existence d'une telle extension peut être démontrée par la méthode de Kronecker de l'"adjonction symbolique" : on peut en trouver la démonstration dans n'importe quel livre d'algèbre moderne. Pourtant, Gauss ne suit pas cette voie. Il construit ses équations auxiliaires sans supposer l'existence des racines. Par exemple, il construit l'équation auxiliaire de degré m' comme suit :

D'abord, le polynôme spécial (30) est remplacé par un polynôme y, dont les racines sont les indéterminées $a, b, c, ...$

$$y = (x - a)(x - b)(x - c)....\tag{35}$$

Gauss forme ensuite un polynôme auxiliaire en une nouvelle variable u, définissant ζ comme le produit des m' expressions

$$u - (a + b)t + ab\tag{36}$$

obtenues en permutant les racines. Ce polynôme ζ est symétrique en les indéterminées $a, b, c, ...$, donc il peut être exprimé de manière unique comme un polynôme en u et t et les coefficients de y, qui sont les fonctions élémentaires symétriques de $a, b, c, ...$ Après ça, les coefficients de y sont remplacés par les coefficients $L', L'', ...$ du polynôme donné (30), et ainsi le polynôme auxiliaire Z est obtenu.