Gauss

SECTION SEPTIÈME.

Des Equations qui déterminent les Sections circulaires.

335. PARMI les accroissemens importans dont les travaux des modernes ont enrichi les Mathématiques, les fonctions circulaires tiennent sans aucun doute le premier rang. Cette étonnante espèce de quantités, à laquelle nous sommes conduits à chaque instant dans des recherches qui y semblent tout-à-fait étrangères, et du secours desquelles ne peut se passer aucune partie des Mathématiques, a occupé avec tant d'assiduité la pénétration des plus grands géomètres, et ils en ont fait une théorie si vaste, qu'on ne pouvait guère s'attendre qu'une partie de cette théorie, partie élémentaire et pour ainsi dire placée à l'entrée, pût recevoir des accroissemens considérables. Je parle de la théorie des fonctions trigonométriques, qui répondent aux arcs commensurables avec la circonférence, ou de la théorie des polygones réguliers, dont on ne connaît jusqu'à présent que la plus petite partie, ainsi qu'on le verra par cette Section. Le lecteur pourrait s'étonner de rencontrer une semblable recherche dans un ouvrage consacré à une doctrine qui paraît au premier abord absolument hétérogène; mais l'exposition fera voir bien clairement quelle est la liaison de ce sujet et de l'Arithmétique transcendante.

[...]

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

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

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 différens cas, la division du cercle en n parties, ou la description du polygone régulier de n côtés, peut s'exécuter par des constructions géométriques. Par exemple, pour $n=17$, on tire facilement des n^{os} 354, 361

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

les cosinus des multiples de cet angle ont une forme semblable, les sinus ont un radical de plus. Il y a certainement bien lieu de s'étonner que la divisibilité du cercle en 3 et 5 parties ayant été connue dès le temps d'*Euclide*, on n'ait rien ajouté à ces découvertes dans un intervalle de deux mille ans, et que tous les géomètres aient annoncé comme certain, qu'excepté ces divisions et celles qui s'en déduisent (les divisions en 2^μ, 15, 3.2^μ, 5.2^μ, 15.2^μ parties), on ne pouvait en effectuer aucune par des constructions géométriques.

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

$$2^{32}+1=4294967297,$$

nombre divisible par 641.

Toutes les fois que $n-1$ renferme des facteurs différens 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.

366. Si l'on veut diviser le cercle en a^α 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 $\alpha = 1$).

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

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

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.