

ANNALES SCIENTIFIQUES DE L'É.N.S.

G. MATHET

Sur les polygones réguliers

Annales scientifiques de l'É.N.S. 2^e série, tome 4 (1875), p. 303-310

http://www.numdam.org/item?id=ASENS_1875_2_4__303_0

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1875, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (<http://www.elsevier.com/locate/ansens>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR

LES POLYGONES RÉGULIERS,

PAR M. G. MATHET,

PROFESSEUR AU LYCÉE DE LYON.

Le théorème de Gauss : « Tout polygone régulier dont le nombre des côtés est un nombre premier de la forme $2^n + 1$ peut être construit graphiquement », n'a pas été, je crois, démontré de manière à pouvoir être donné dans des cours élémentaires; l'excellente démonstration que l'on trouve dans le *Cours d'Algèbre supérieure* de M. Serret exige du lecteur des notions d'Analyse assez étendues. La démonstration suivante repose uniquement sur une propriété des racines primitives, relatives à un nombre premier n .

Rappelons d'abord qu'on appelle *racine primitive*, pour le nombre premier n , un nombre a tel que $a^{n-1} - 1$ soit un multiple de n , et tel que, pour aucune valeur de m inférieure à $n - 1$, $a^m - 1$ ne soit un multiple de n .

De cette définition il résulte :

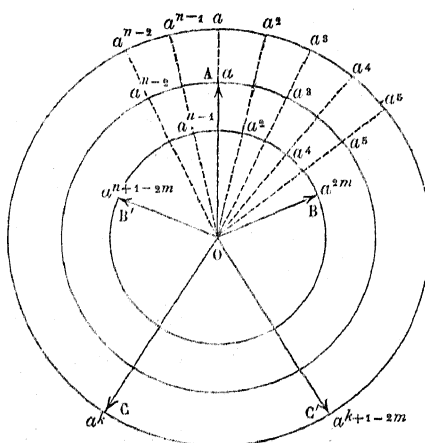
1° Que si a est une racine primitive, si m et m' sont des nombres entiers plus petits que $n - 1$, a^m et $a^{m'}$ divisés par n donnent des restes ou résidus différents; car, si le résidu était le même, $a^m - a^{m'}$ ou $a^{m'}(a^{m-m'} - 1)$ serait un multiple de n : donc $a^{m-m'} - 1$ serait divisible

par n , ce qui est contraire à l'hypothèse, puisque a est une racine primitive. On voit sans peine que, par suite, les résidus fournis par les différents termes de la série $a, a^2, a^3, \dots, a^{n-1}$ sont les nombres entiers de 1 à $n-1$.

2° $a^{\frac{n-1}{2}}$ a pour résidu -1 , car $a^{n-1} - 1$ ou $(a^{\frac{n-1}{2}} - 1)(a^{\frac{n-1}{2}} + 1)$ étant divisible par n , et $a^{\frac{n-1}{2}} - 1$ ne l'étant pas, puisque a est une racine primitive, $a^{\frac{n-1}{2}} + 1$ doit l'être; donc, etc. Donc : quand on multiplie une puissance de a par $a^{\frac{n-1}{2}}$, le résidu change seulement de signe; quand on la multiplie par a^{n-1} , le résidu ne change pas.

3° Soient (*fig. 1*) trois cercles concentriques, sur le plus grand desquels sont disposées, à intervalles égaux, les puissances de a . Sur les

Fig. 1.



deux autres sont les puissances impaires et les puissances paires, chacune, comme l'indique la figure, sur les rayons qui aboutissent aux points correspondants du grand cercle.

Soient un rayon OA du cercle moyen, dont l'extrémité est sur un des points de division de ce cercle, OB et OB' deux rayons du petit cercle, aboutissant à deux divisions de ce cercle, et tels que les angles AOB et

AOB' soient égaux. Si l'on fait tourner le système de ces trois aiguilles, les angles AOB et AOB' restant invariables, de manière à présenter A successivement à chaque division du cercle moyen, et si l'on fait chaque fois la somme des puissances de a qui se trouvent en A et B, en A' et B', ces sommes donnent pour résidu un certain nombre, le même que celui de l'une des puissances de a marquées sur le grand cercle.

Supposons, par exemple, que, A étant sur a , B soit sur a^{2m} ; $a + a^{2m}$ aura un résidu, qui sera le même que celui de a^k sur le grand cercle. Soit OC le rayon sur lequel est a^k . B' se trouve en même temps sur a^{n+1-2m} , et le résidu de $a + a^{n+1-2m}$ se trouve sur un point du grand cercle, que nous déterminerons tout à l'heure, et vers lequel nous menons le rayon OC'. Je dis que les deux aiguilles OC et OC' sont invariablement liées aux trois autres OA, OB et OB', tournent avec elles quand A se déplace sur le cercle moyen, et que l'intervalle CC' est d'un nombre impair de divisions.

En effet, si $a + a^{2m}$ a même résidu que a^k , $a^3 + a^{2m+2}$ aura le même que a^{k+2} , $a^5 + a^{2m+4}$ le même que a^{k+4} , et ainsi de suite. Donc, quand A et B avancent chacun d'une division sur leur cercle respectif, C avance de deux divisions sur son cercle, et par conséquent OC tourne du même angle que OA et OB.

Si $a + a^{2m}$ a même résidu que a^k , $a^2 + a^{2m+1}$ a même résidu que a^{k+1} ; mais le résidu de a^2 est le même que celui de $a^2 a^{n-1}$ ou de a^{n+1} . Donc $a^{n+1} + a^{2m+1}$ a même résidu que a^{k+1} . Donc, en divisant chaque terme par a^{2m} , $a^{n+1-2m} + a$ a le même résidu que a^{k+1-2m} . Donc l'intervalle de C à C' est de $2m - 1$ divisions, nombre impair et constant avec m . Donc, quand A se déplace sur son cercle, OC' parcourt le grand cercle, en tournant du même angle que OA, OB, OB', OC.

Si donc A parcourt toutes les divisions de son cercle, C parcourra toutes les divisions du grand cercle, d'une certaine parité, et C' parcourra toutes les autres.

4° Enfin supposons que le nombre premier n soit de la forme $2^p + 1$; p est nécessairement une puissance de 2. La propriété démontrée ci-dessus peut être généralisée de la manière suivante.

Soit α une puissance de 2. Supposons rangées sur un grand cercle toutes les puissances successives de la racine primitive a , à intervalles

égaux; puis décrivons α cercles concentriques, sur chacun desquels nous disposerons l'une des séries

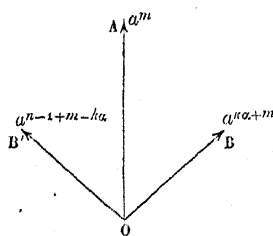
$$(1) \quad \begin{cases} a, & a^{\alpha+1}, & a^{2\alpha+1}, & \dots, & a^{n-\alpha}, \\ a^2, & a^{\alpha+2}, & a^{2\alpha+2}, & \dots, & a^{n-\alpha-1}, \\ a^3, & a^{\alpha+3}, & a^{2\alpha+3}, & \dots, & a^{n-\alpha-2}, \\ \vdots & \vdots & \vdots & & \vdots \\ a^\alpha, & a^{2\alpha}, & a^{3\alpha}, & \dots, & a^{n-1}, \end{cases}$$

chacune de ces puissances se trouvant sur le rayon qui aboutit à cette même puissance sur le cercle extérieur. Dédoublons maintenant l'une de ces suites, par exemple

$$a^m, a^{\alpha+m}, a^{2\alpha+m}, \dots, a^{n-\alpha+m-1},$$

et disposons les termes $a^m, a^{2\alpha+m}, \dots$, ainsi que $a^{\alpha+m}, a^{3\alpha+m}, \dots$ sur deux nouveaux cercles concentriques aux premiers. OA étant dirigée vers a^m et OB vers $a^{k\alpha+m}$, où k est *impair* (fig. 2), pour savoir l'exposant de la

Fig. 2.



puissance de a vers laquelle OB' est dirigée, remarquons que la différence des exposants doit être la même, entre B et A, entre A et B'. Or l'exposant de a^m peut être remplacé par $n-1+m$ sans que le résidu soit changé; donc en B' on aura $a^{n-1+m-k\alpha}$.

Soit maintenant a^l la puissance de a , sur l'un des cercles portant les séries (1), vers laquelle est dirigée OC, c'est-à-dire que a^l a même résidu que $a^m + a^{k\alpha+m}$. Donc $a^{2\alpha+m} + a^{(k+2)\alpha+m}$ aura même résidu que

$a^{l+2\alpha}$, et ainsi de suite. L'aiguille OC tourne donc du même angle que OA.

Maintenant, comme a^m peut être remplacé par a^{m+n-1} , $a^{m+n-1} + a^{k\alpha+m}$ a même résidu que a^l : donc, en divisant par $a^{k\alpha}$, $a^{n-1+m-k\alpha} + a^m$ a même résidu que $a^{l-k\alpha}$. Or cette puissance se trouve sur le même cercle que a^l , et séparée de a^l par un nombre impair de divisions.

Donc, quand A parcourt toutes les divisions de son cercle, C' parcourt toutes les divisions du sien que C n'a pas parcourues.

Soit maintenant proposé d'inscrire à un cercle un polygone régulier de n côtés, n étant un nombre premier de la forme $2^p + 1$. Si l'on pose $\varphi = \frac{2\pi}{n}$, la question revient à construire graphiquement le cosinus de φ ou de l'un quelconque de ses multiples. Soit

$$x_1 = 2 \cos a \varphi + 2 \cos a^3 \varphi + 2 \cos a^5 \varphi + \dots + 2 \cos a^{\frac{n-1}{2}-1} \varphi,$$

$$x_2 = 2 \cos a^2 \varphi + 2 \cos a^4 \varphi + 2 \cos a^6 \varphi + \dots + 2 \cos a^{\frac{n-1}{2}} \varphi;$$

ou, ce qui revient au même,

$$x_1 = \cos a \varphi + \cos a^3 \varphi + \dots + \cos a^{\frac{n-1}{2}-1} \varphi + \cos a^{\frac{n-1}{2}+1} \varphi + \dots + \cos a^{n-2} \varphi,$$

$$x_2 = \cos a^2 \varphi + \cos a^4 \varphi + \dots + \cos a^{\frac{n-1}{2}} \varphi + \cos a^{\frac{n-1}{2}+2} \varphi + \dots + \cos a^{n-1} \varphi;$$

car chaque puissance de a peut être réduite à son résidu, et deux puissances dont les exposants diffèrent d'une quantité égale à $\frac{n-1}{2}$ ont des résidus égaux et de signes contraires. On a d'abord, par une formule connue,

$$x_1 + x_2 = -1.$$

Si l'on forme le produit $x_1 x_2$, ce produit est égal à la demi-somme des cosinus des arcs obtenus en ajoutant et en retranchant l'un quel-

conque des arcs de la première suite et l'un quelconque de ceux de la seconde. Or le coefficient de φ , dans chaque terme de la seconde moitié de chaque suite, réduit à son résidu, est égal et de signe contraire à celui qui occupe le même rang dans la première moitié; de sorte qu'au lieu de faire les sommes et les différences il suffit de faire les sommes et de doubler le résultat, le cosinus de deux arcs égaux et de signes contraires étant le même.

Or on obtiendra toutes ces sommes en réglant les aiguilles OB et OB' de toutes les manières possibles par rapport à OA, et en faisant faire chaque fois un tour complet au système. A chaque tour, C et C', dont le réglage change aussi chaque fois, parcourent tout le grand cercle. Donc on obtient en définitive, pour x_1, x_2 , autant de fois la somme des cosinus qu'il y a de modes de réglage possibles, c'est-à-dire $\frac{n-1}{4}$ fois.

Donc

$$x_1 x_2 = -\frac{n-1}{4}.$$

x_1 et x_2 sont donc les racines de l'équation

$$x^2 + x - \frac{n-1}{4} = 0.$$

Soit maintenant *

$$y_1 = 2 \cos a \varphi + 2 \cos a^3 \varphi + \dots + 2 \cos a^{\frac{n-1}{2}-3} \varphi,$$

$$y_2 = 2 \cos a^3 \varphi + 2 \cos a^7 \varphi + \dots + 2 \cos a^{\frac{n-1}{2}-1} \varphi,$$

ou bien

$$y_1 = \cos a \varphi + \cos a^3 \varphi + \dots + \cos a^{\frac{n-1}{2}-3} \varphi + \cos a^{\frac{n-1}{2}+1} \varphi + \dots + \cos a^{n-4} \varphi,$$

$$y_2 = \cos a^3 \varphi + \cos a^7 \varphi + \dots + \cos a^{\frac{n-1}{2}-1} \varphi + \cos a^{\frac{n-1}{2}+3} \varphi + \dots + \cos a^{n-2} \varphi;$$

et de même

$$z_1 = 2 \cos a^2 \varphi + 2 \cos a^6 \varphi + \dots + 2 \cos a^{\frac{n-1}{2}-2} \varphi,$$

$$z_2 = 2 \cos a^4 \varphi + 2 \cos a^8 \varphi + \dots + 2 \cos a^{\frac{n-1}{2}} \varphi,$$

ou bien

$$z_1 = \cos a^2 \varphi + \cos a^4 \varphi + \dots + \cos a^{\frac{n-1}{2}-2} \varphi + \cos a^{\frac{n-1}{2}+2} \varphi + \dots + \cos a^{n-3} \varphi,$$

$$z_2 = \cos a^4 \varphi + \cos a^8 \varphi + \dots + \cos a^{\frac{n-1}{2}} \varphi + \cos a^{\frac{n-1}{2}+4} \varphi + \dots + \cos a^{n-1} \varphi.$$

On voit d'abord que

$$y_1 + y_2 = x_1, \quad z_1 + z_2 = x_2.$$

Pour les produits $y_1 y_2$ et $z_1 z_2$, on voit, comme ci-dessus, que chacun de ces produits est égal à la somme des cosinus de tous les arcs obtenus en ajoutant chacun des arcs qui entrent dans y_1 ou dans z_1 , avec chacun de ceux qui entrent dans y_2 ou dans z_2 .

Or, si l'on range sur deux cercles concentriques les deux séries a, a^3, \dots et a^2, a^4, \dots , puis si l'on dédouble l'une d'elles, la première par exemple, sur deux nouveaux cercles, pour chaque mode de réglage des aiguilles OA, OB, OB', dirigées vers les divisions de ces derniers cercles, les points C et C' parcourront toutes les divisions de l'un des deux cercles primitifs. Lorsque C et C' parcourront le premier de ces cercles, la somme des cosinus obtenus sera égale à x_1 ; quand ils parcourront l'autre, cette somme sera égale à x_2 . Donc $y_1 y_2$ sera une fonction linéaire de x_1 et de x_2 , de la forme $\alpha x_1 + \beta x_2$, α et β étant des nombres qui se trouveront aisément dans toute application numérique, mais dont la présente théorie ne donne pas l'expression. Il en sera de même de $z_1 z_2$; donc y_1 et y_2 , z_1 et z_2 sont les racines de deux équations du second degré, à coefficients connus.

Que l'on pose maintenant

$$t_1 = 2 \cos a \varphi + 2 \cos a^3 \varphi + \dots + 2 \cos a^{\frac{n-1}{2}-7} \varphi,$$

$$t_2 = 2 \cos a^5 \varphi + 2 \cos a^{13} \varphi + \dots + 2 \cos a^{\frac{n-1}{2}-3} \varphi,$$

et ainsi de suite; on voit sans peine, par un raisonnement identique, que t_1 et t_2 sont les racines d'une équation du second degré, dans la-

quelle le coefficient du second terme est $-\gamma_1$ et dont le terme indépendant est une fonction linéaire de $\gamma_1, \gamma_2, z_1, z_2$. Chacune des suites y, z, t, \dots renferme toujours un nombre de termes qui est une puissance de 2 : donc chacune d'elles peut être dédoublée comme on vient de le voir, et l'on arrivera à la fin à une équation du second degré à coefficients connus, dont les racines seront les cosinus de deux multiples de φ .
