DES ÉQUATIONS
QUI DÉTERMINENT LES SECTIONS CIRCULAIRES
(suite et fin)

Jean-Pierre FRIEDELMEYER

Nous avons vu dans le précédent numéro de *'L'Ouvert'* (n° 46) comment VANDERMONDE avait préparé le terrain de la résolution de l'équation cyclotomique

$$(c) : \frac{X^n - 1}{X - 1} = 0$$

en traitant complètement le cas $n = 11$. On ne dispose d'aucune information qui indiquerait que GAUSS ait été influencé par le mémoire de VANDERMONDE, mais il est très probable qu'il l'ait lu. Il y a cependant une différence entre les deux auteurs caractérisée par une clarté et une rigueur exemplaire, déjà très moderne chez GAUSS. C'est pourquoi je laisserai souvent la place au texte même des *'Recherches Arithmétiques'* tant celui-ci est une merveille d'exposition mathématique.

L'équation (c) chez GAUSS.

Soit donc l'équation (c) dans laquelle on peut supposer n premier $n = 2m + 1$. L'ensemble (Ω) des $(n-1)$ racines x_k peut être engendré par l'une d'entre elles, soit r^g où r est l'une des racines de (Ω) et g une racine primitive selon le module n. Rappelons que g est racine primitive selon le module n si g engendre le groupe multiplicatif $(\mathbb{Z}\ /n\mathbb{Z})\ ^*$. Supposons donc la racine primitive g fixée. Puisque $n = 2m + 1$, $n - 1$ n'est pas premier. Posons avec GAUSS

$$n - 1 = e.f; h = g^e; [\lambda] = r^\lambda$$
$$(f, \lambda) = [\lambda] + [\lambda h] + [\lambda h^2] + \cdots + [\lambda h^{f-1}]$$

appelée période (*). GAUSS démontre que si λ n'est pas divisible par n, l'ensemble Ω se partage en e classes qui sont les périodes $(f,1);(f,g);\ldots;(f,g^{e-1})$ et cette partition est indépendante de la racine primitive g choisie. Prenons par exemple $n = 19$ $g = 2$ est racine primitive selon le module 19 comme le montre le tableau qui suit :

(*) GAUSS utilise délibérément le même terme *'période'* pour la somme et pour l'ensemble des éléments constitutifs de cette somme.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^k	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Alors :

$$\begin{aligned}(6,1) &= [\,1\,] + [\,8\,] + [\,7\,] + [\,18\,] + [\,11\,] + [\,12\,] \\ (6,2) &= [\,2\,] + [\,16\,] + [\,14\,] + [\,17\,] + [\,3\,] + [\,5\,] \\ (6,4) &= [\,4\,] + [\,13\,] + [\,9\,] + [\,15\,] + [\,6\,] + [\,10\,]\end{aligned}$$

Si f est lui-même composé, la période (f,λ) se décompose à son tour en '*sous-périodes*'.
Par exemple : $(6,1)$ est composée des périodes

$$(2,1) = [1] + [18] \qquad (2,8) = [8] + [11] \quad \textit{et} \quad (2,7) = [7] + [12]$$

Ainsi, par une intuition extraordinaire, GAUSS est tout simplement en train d'utiliser toutes les ressources et propriétés du groupe cyclique des racines de l'unité. L'utilisation de la racine primitive $g = 2$ détermine une permutation circulaire sur Ω.

$$p = (1,2,4,8,16,13,7,14,9,18,17,15,11,3,6,12,5,10)$$

et les périodes (6,1); (6,2); (6,4) sont les parties stables de Ω par p^3 — les périodes (2,1); (2,8) et (2,7) des parties stables de Ω par $(p^3)^3 = p^9$.

Appelant '*semblables*' des périodes formées du même nombre d'éléments GAUSS démontre alors plusieurs résultats permettant le calcul des périodes :

> "**345. (*) Théorème** : *Soient $(f,\lambda),(f,\mu)$ deux périodes semblables, identiques ou différentes, et $[\lambda],[\lambda'],[\lambda"]\ldots$ les racines qui composent (f,λ); le produit de (f,λ) par (f,μ) sera la somme des f périodes semblables, c'est-à-dire,*
>
> $$= (f,\lambda+\mu) + (f,\lambda'+\mu) + (f,\lambda"+\mu), \text{ etc } = w.$$
>
> **346. Théorème** : *Si l'on suppose que λ est un nombre non divisible par n, et que pour abréger on fasse $(f,\lambda) = p$, toute autre période semblable (f,μ) où μ est aussi non-divisible par n, peut être mise sous la forme*
>
> $$\alpha + \beta p + \gamma p^2 + \cdots + \theta p^{e-1}$$
>
> *de manière que les coefficients $\alpha,\beta,\gamma,\ldots,\theta$ soient rationnels et déterminés.*"

(*) Rappelons que ces numéros sont ceux-là même du texte de GAUSS.

Comme nous l'avons signalé dans l'introduction (cf. *'L'Ouvert'* n° 46) l'exemple le plus remarquable — celui qui représente un des premiers et des plus beaux titres de gloire de GAUSS — est sa démonstration de la possibilité de construire à la règle et au compas le polygone régulier de 17 côtés. Citons GAUSS pour l'application des idées développées ci-dessus à ce cas.

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

On a ici $n - 1 = 2.2.2.2$, *ainsi le calcul des racines* Ω *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 :*

$$\begin{array}{l} 0,\ 1,\ 2,\ \ 3,\ \ 4,\ 5,\ \ 6,\ \ 7,\ \ 8,\ \ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15 \\ 1,\ 3,\ 9,\ 10,\ 13,\ 5,\ 15,\ 11,\ 16,\ 14,\ \ 8,\ \ 7,\ \ 4,\ 12,\ \ 2,\ \ 6, \end{array}$$

d'où résulte la distribution suivante en deux périodes de huit termes, quatre périodes de quatre termes et huit de deux termes :

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

L'équation (A) *dont les racines sont les sommes (8,1),(8,3), se trouve être*

$$x^2 + x - 4 = 0, (*)$$

(*) *En effet :*

$$(8,1) = [1] + [9] + [13] + [15] + [16] + [8] + [4] + [2]$$
$$(8,3) = [3] + [10] + [5] + [11] + [14] + [7] + [12] + [6]$$
$$(8,1) + (8,3) = (16,1) = -1$$

et par le § 345

$$\begin{aligned} (8,1) \times (8,3) &= (8,4) + (8,12) + (8,16) + (8,1) + (8,2) + (8,11) + (8,7) + (8,5) \\ &= 4[(8,1) + (8,3)] = -4. \end{aligned}$$

et ses racines sont :

$$-1/2 + 1/2\sqrt{17} = 1,5615528128 \text{ et } -1/2 - 1/2\sqrt{17} = -2,5615528128;$$

nous supposerons que la première soit (8,1), l'autre sera nécessairement (8,3).
L'équation (B), dont les racines sont les sommes (4,1) et (4,9), est

$$x^2 - (8,1)x - 1 = 0,$$

et ses racines sont

$$x = 1/2(8,1) \pm 1/2\sqrt{4 + (8,1)^2} = 1/2(8,1) \pm 1/2\sqrt{12 + 3(8,1) + 4(8,3)}$$

nous supposerons égale à (4,1) celle de ces deux racines dans laquelle le radical est affecté du signe plus; on aura ainsi

$$(4,1) = 2,0494811777, \quad (4,9) = 0,4879283649.$$

Les autres périodes de quatre termes, (4,3) et (4,10) peuvent être calculées de deux manières, savoir :

1° *Par la méthode du n° 346, qui donne les formules suivantes, en faisant, pour abréger, (4,1)=p,*

$$(4,3) = -\frac{3}{2} + 3p - \frac{1}{2}p^3 = 0,3441507314,$$
$$(4,10) = \frac{3}{2} + 2p - p^2 - \frac{1}{2}p^3 = -2,9057035442.$$

La même méthode donne aussi la formule

$$(4,9) = -1 - 6p + p^2 + p^3,$$

d'où l'on tire la même valeur que plus haut.

2° *En résolvant l'équation dont (4,3),(4,10) sont les racines; cette équation est*

$$x^2 - (8,3)x - 1 = 0$$

et donne

$$x = \frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{4 + (8,3)^2},$$
$$\text{ou } \ldots x = \frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)},$$
$$\text{et } \ldots x = \frac{1}{2}(8,3) - 1/2\sqrt{12 + 4(8,1) + 3(8,3)};$$

nous déciderons, par l'artifice suivant annoncé au n° 352, (*) *laquelle de ces deux racines doit être prise pour (4,3). Faisons le produit de* $(4,1)-(4,9)$ *par* $(4,3)-(4,10)$, *il est, calcul fait,* $=2(8,1)-2(8,3)$. *Or la valeur de cette expression est positive, puisqu'elle est* $=2\sqrt{17}$; *d'ailleurs le premier facteur* $(4,1)-(4,9)$ *est aussi positif, comme égal à* $\sqrt{12+4(8,1)+3(8,3)}$ *donc le second facteur doit aussi être positif, et partant (4,3) doit être racine dans laquelle le radical est positif, et (4,10) l'autre racine (*). Au reste, il en résulte les mêmes valeurs que plus haut.*

Connaissant toutes les sommes de quatre termes, nous passons maintenant à la recherche des sommes de deux termes. L'équation (C) *dont les racines sont (2,1), (2,13), périodes contenues dans (4,1), est*

$$x^2-(4,1)x+(4,3)=0,$$

qui donne

$$\begin{aligned} x =& 1/2(4,1)\pm 1/2\sqrt{-4(4,3)+(4,1)^2} \\ =& 1/2(4,1)\pm 1/2\sqrt{4+(4,9)-2(4,3)}; \end{aligned}$$

nous prendrons pour valeur de (2,1) celle de ces deux racines dans laquelle le radical est positif, et il en résulte

$$(2,1)=1,8649444588, \quad (2,13)=0,1845367189.$$

(...) Et Gauss termine.

En calculant de la même manière les autres racines, on trouve les valeurs numériques suivantes, dans lesquelles le signe supérieur appartient à la première, et le signe inférieur à la seconde.

[1], [16]... [0,9324722294] ±[0,3612416662] i,
[2], [15]... [0,7390089172] ±[0,6736956436] i,
[3], [14]... [0,4457383558] ±[0,8951633914] i,
[4], [13]... [0,0922683595] ±[0,9957341763] i,
[5], [12]... −[0,2736629901] ±[0,9618256432] i,
[6], [11]... −[0,6026346364] ±[0,7980172273] i,
[7], [10]... −[0,8502171357] ±[0,5264321629] i,
[8], [9]... −[0,9829730997] ±[0,1837495178] i."

Plus loin (...)

(*) *Le fond de cet artifice consiste dans une propriété facile à prévoir, d'après laquelle le développement de ce produit ne contient plus de périodes de quatre termes, mais se trouve exprimé par des périodes de huit termes; les gens instruits en découvriront facilement la raison que l'envie d'abréger nous force d'omettre.*

"**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*

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

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 carrées 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° 354, 361*

$$\cos\frac{P}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

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^ν. *En effet, si m était divisible par un nombre impair plus grand que l'unité, et qu'on eût ainsi* $m = \xi\eta, 2^m + 1$ *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* $2^{2^\delta} + 1$; *ainsi les cinq nombres 3, 5, 17, 257, 65537 s'en déduisent en faisant* $= 0, 1, 2, 3, 4$ *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 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*

(*) P=2π.

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 ETRE 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.** *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 différents 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 :

$$2,3,4,5,6,8,10,12,15,16,17,20,24,30,32,34,40,48,$$
$$51,60,64,68,80,85,96,102,120,128,136,160,170,192,$$
$$204,240,255,256,257,272.\text{"}$$

Pour les valeurs de n qui ne sont pas de cette forme, il se pose pourtant un problème; si $(n-1)$ contient un facteur premier supérieur ou égal à 5, on sera en présence d'une équation d'un degré tel qu'on ne sait pas **en général** la résoudre. Or un des autres résultats remarquables de GAUSS est que, dans le cas particulier étudié ici, ce sera **toujours** possible.

"**359.** *Les recherches précédentes avaient pour but de trouver les équations auxiliaires; nous allons maintenant exposer sur leur résolution une propriété digne de remarque. On sait que tous les travaux des plus grands géomètres ont échoué contre la résolution générale des équations qui passent le premier degré, ou pour mieux définir l'objet de la recherche, contre la réduction des équations complètes à des équations à deux termes, et il est à peine douteux si ce problème ne renferme pas quelque chose d'impossible, plutôt qu'il ne surpasse les forces actuelles de l'analyse. (Voyez ce que nous avons dit sur ce sujet dans le Mémoire intitulé 'Demonstratio nova', etc p. 22). Il est certain néanmoins qu'il y a une infinité d'équations composées dans chaque degré, qui admettent une telle réduction, et nous espérons faire plaisir aux géomètres,* **en prouvent que nos équations auxiliaires sont toujours dans ce cas**. *Mais à cause de l'étendue du sujet, nous ne présenterons que les principes les plus importants qui sont nécessaires pour démontrer cette*

possibilité, différant à un autre temps l'exposition plus complète. Nous mettrons en avant quelques observations générales sur les racines de l'équation $x^e - 1 = 0$ *en comprenant le cas où* e *est un nombre composé.*"

Je ne citerai pas ces '*principes les plus importants*' car ce sont ceux-là même que ABEL va développer et étendre dans le mémoire "*Sur une classe particulière d'équations résoluble par radicaux*". Signalons simplement que GAUSS indique (§ 360) que pour certaines puissances

$$T = t^\beta = (a + Rb + \cdots R^{\beta-1}m)^\beta$$

est rationnel où $a, b, \ldots, m$ sont les périodes de longueur déterminée et R une racine $\beta^{ième}$ de l'unité. Par là, il généralise vraiment le résultat et la méthode utilisée par VANDERMONDE pour le cas $N = 11$ (voir '*L'Ouvert*' n° 46).

Mais il m'a paru intéressant de présenter de très larges extraits de cette section VII des '*Recherches arithmétiques*', d'abord à cause de leur beauté et de leur rigueur, ensuite parce que GAUSS y développe des idées et des méthodes qui anticipent de façon extraordinaire sur ce qu'on appelle la théorie de GALOIS — au moins en ce qui concerne l'équation cyclotomique. Reprenons en effet l'exemple II pour $n = 17$ et les diverses décompositions en périodes (voir p. 23) :

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

On y associe sans peine les deux suites

$$C_{16} \supset C_8 \supset C_4 \supset C_2 \supset \{Id\}$$

et

$$\mathbb{Q} \subset \mathbb{Q}[(8,1)] \subset \mathbb{Q}[(4,1)] \subset \mathbb{Q}[(2,1)] \subset \mathbb{Q}\Big[[1]\Big]$$

en notant C_n le groupe cyclique d'ordre n et $\mathbb{Q}[a]$ l'extention de $\mathbb{Q}$ obtenue par l'adjonction du nombre a.

•C_{16} est le groupe cyclique engendré par la permutation (cyclique d'ordre 16) :

$$p = (1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6)$$

définie par l'automorphisme de $(Z/17\ Z)^*$: $h \to 3^h = \varphi(h)$. Tous les éléments de ce groupe C_{16} conservent la période $(16, 1) = \Omega$ somme de toutes les racines de $(X^{17} - 1)/(X - 1) = 0$. Cette somme est connue, égale à (-1) et appartient au corps Q.

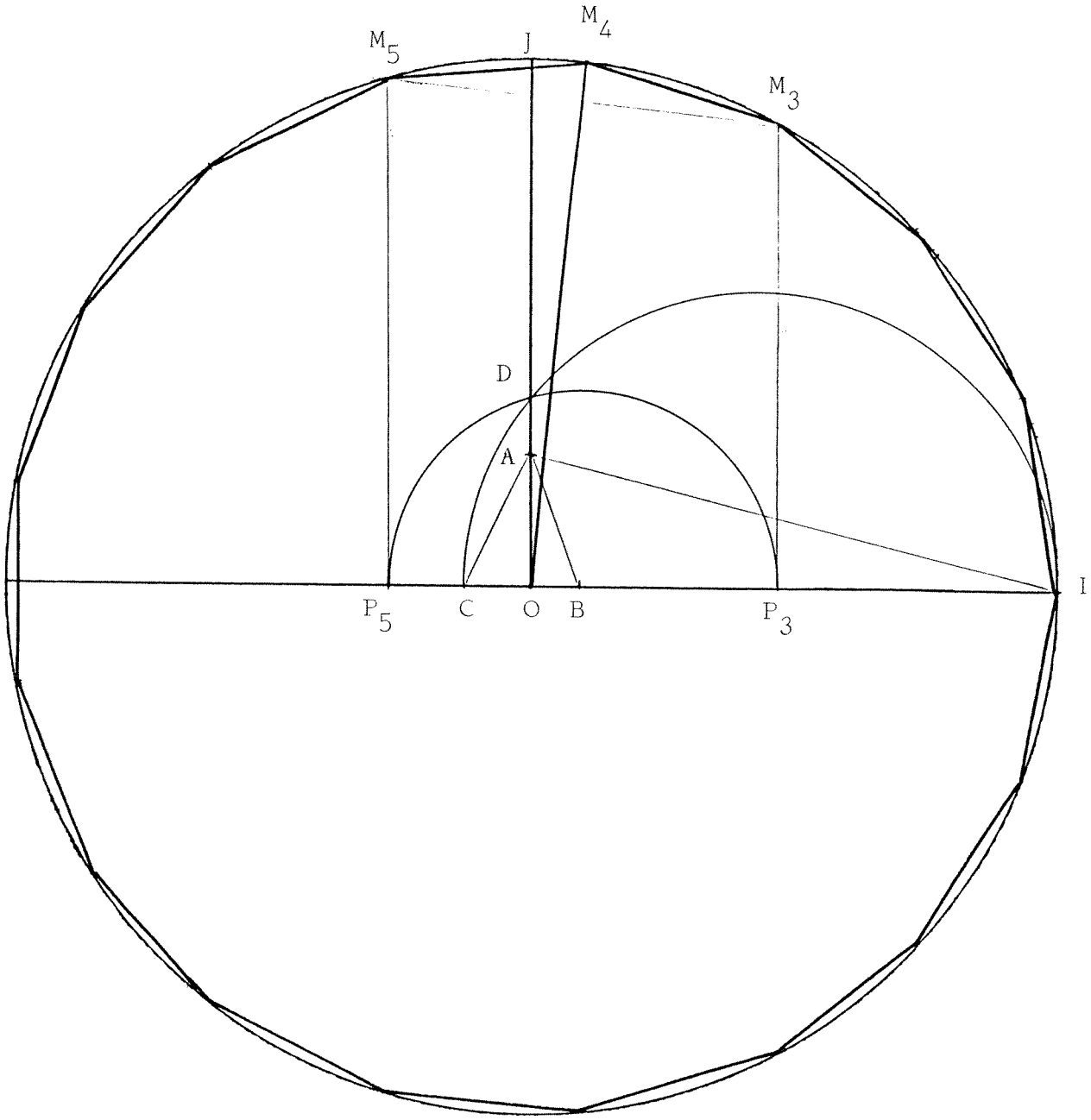
•C_8 est le groupe cyclique, sous-groupe d'indice 2 de C_{16}, engendré par $p^2 = (1, 9, 13, 15, 16, 8, 4, 2)$ et les éléments de C_8 laissent invariantes les périodes (8,1) et (8,3), donc aussi tout élément de l'extension Q [(8,1)]. Cette extension est en fait le corps de rupture de l'équation $x^2 + x - 4 = 0$ dont les racines sont ainsi **adjointes** au corps Q.

•C_4 est le groupe cyclique engendré par (1,13,16,4) etc (pour une présentation complète de la question en liaison avec la théorie de Galois, voir par exemple J.-Cl. Carrega '*Théorie des corps - La règle et le compas*', Chap. X § 4).

On comprend que ce texte ait marqué les contemporains de Gauss, donnant pour la première fois une méthode de résolution pour une classe d'équations d'un degré quelconque, ou du moins montrant comment abaisser leur degré par l'adjonction de racines auxiliaires à l'ensemble des rationnels. Si Lagrange a posé les principes généraux et les lieux de recherche pour l'équation générale, Gauss a exibé une situation où ces principes deviennent opérants. Il a dégagé un modèle qui servira de référence et de levier dans la recherche, jusque là quasi aveugle, de ce qui fait qu'une équation est résoluble algébriquement ou ne l'est pas. Une première brèche est ainsi ouverte dans laquelle Abel va s'engager et qu'il va élargir en montrant que la méthode de Gauss s'applique dans bien d'autres cas. Et Galois à son tour s'appuiera sur le texte de Gauss qui lui servira d'exemple pour illustrer ses propres découvertes.

La méthode de Gauss, si elle justifie la possibilité de construire le polygone régulier à 17 côtés, n'est guère pratique pour la construction effective. H.-W. Richmond en a proposé une en 1893 dont on trouvera la justification complète dans le livre déjà cité de Carrega, et une réalisation ci-après.

Les rayons OI, OJ sont perpendiculaires. $\overrightarrow{OA} = \frac{1}{4}\overrightarrow{OJ}$, $\widehat{OAB} = \frac{1}{4}\widehat{OAI}$ et $\widehat{BAC} = \frac{\pi}{4}$.
Le cercle de diamètre IC coupe OJ en D. Le cercle de centre B passant par D coupe la droite (OI) en P_3 et P_5 qui sont les projections orthogonales des points M_3 et M_5 qui représentent les 3^e et 5^e sommets d'un polygone régulier à 17 côtés dont I est le 17^e sommet.


M5
J
M4
M3
D
A
I
P5
C
O
B
P3