JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

G. LAMÉ

Mémoire sur la résolution, en nombres complexes, de l'équation $A^n + B^n + C^n = 0$

Journal de mathématiques pures et appliquées 1re série, tome 12 (1847), p. 172-184.
<http://www.numdam.org/item?id=JMPA_1847_1_12__172_0>

MÉMOIRE

SUR

LA RÉSOLUTION, EN NOMBRES COMPLEXES, DE L'ÉQUATION

$$A^n + B^n + C^n = 0;$$

PAR M. G. LAMÉ.

Dans un travail précédent, j'ai démontré l'impossibilité de cette équation pour l'exposant $n = 5$. Peut-on établir la même impossibilité pour tout exposant n, premier et impair? Avant de répondre à cette question, il est nécessaire de passer en revue les différentes propositions qui composent la démonstration relative à l'exposant 5, et d'examiner si ces propositions sont généralisables, c'est-à-dire si elles ont leurs analogues pour les exposants supérieurs à 5.

1. Pour chaque exposant n premier et impair, tel que $n = 7, 11, 13, 17, 19, 23, \ldots$, les nombres complexes que l'on considère sont de la forme

$$(1) \qquad A = \alpha_0 + \alpha_1 r + \alpha_2 r^2 + \alpha_3 r^3 + \ldots + \alpha_{n-1} r^{n-1} = A(r);$$

les coefficients α_i étant des nombres entiers, et r une des racines imaginaires de l'équation

$$r^n = 1,$$

ou de celle-ci :

$$(2) \qquad \varphi(r) = 1 + r + r^2 + r^3 + \ldots + r^{n-1} = 0.$$

On sait que les autres racines imaginaires de la même équation sont $r^2, r^3, \ldots, r^{n-1}$, et qu'en posant

$$(3) \qquad z_k = r^k + r^{n-k} = r^k + \frac{1}{r^k},$$

les $\left(\frac{n-1}{2}\right)$ nombres $z_1, z_2, z_3, \ldots, z_{\left(\frac{n-1}{2}\right)}$ sont les racines, toutes réelles, d'une équation

$$\psi(z) = z^{\frac{n-1}{2}} + z^{\frac{n-3}{2}} + \ldots \pm 1 = 0, \tag{4}$$

dont les coefficients sont entiers, et d'où l'on conclut les relations

$$1 + z_1 + z_2 + \ldots + z_{\frac{n-1}{2}} = 0, \ldots, \quad z_1 z_2 z_3 \ldots z_{\frac{n-1}{2}} \pm 1, \tag{5}$$

le signe (—) ayant lieu si n est de la forme $4j+1$, et le signe (+) si n est de la forme $4j+3$.

Lorsque tous les coefficients α_i du nombre A sont tels que $\alpha_{n-i} = \alpha_i$, A est réel, et se réduit à la forme

$$\mathfrak{A} = \alpha_0 + \alpha_1 z_1 + \alpha_2 z_2 + \ldots + \alpha_{\frac{n-1}{2}} z_{\frac{n-1}{2}}; \tag{6}$$

sinon, A est imaginaire.

On peut ajouter $\pm m(1 + r + r^2 + \ldots + r^{n-1})$ à l'expression (1) de A, et $\pm m\left(1 + z_1 + z_2 + \ldots + z_{\frac{n-1}{2}}\right)$ à celle (6) de $\mathfrak{A}$, sans changer les valeurs de ces nombres complexes. Le nombre Ar^i, désigné par $A^{(i)}$, est un *associé* de A. Le nombre $A(r^i)$, désigné par A_i, est un *conjugué* de A. Les associés de A sont au nombre de n; leurs $n^{ièmes}$ puissances sont toutes égales à A^n. Les conjugués de A sont au nombre de $(n-1)$; leurs $n^{ièmes}$ puissances sont différentes.

2. Les $(n-1)$ conjugués du nombre $\mathfrak{A}$ (6) sont égaux deux à deux; car z_k (3) restant le même quand on change r en $\frac{1}{r}$, on aura

$$\mathfrak{A}_{n-i} = \mathfrak{A}_i.$$

On peut n'admettre que $\left(\frac{n-1}{2}\right)$ conjugués pour $\mathfrak{A}$; le produit de ces $\left(\frac{n-1}{2}\right)$ conjugués est un nombre entier, positif ou négatif.

Les $(n-1)$ conjugués du nombre complexe imaginaire A (1) se partagent en $\left(\frac{n-1}{2}\right)$ groupes binaires; chacun de ces groupes $[A_i, A_{n-i}]$,

jouissant de cette propriété que les deux nombres qui le composent donnent un produit réel $[A_i, A_{n-i}]$, ou de la forme (6); ces deux nombres sont des conjugués directs.

Le produit des $(n-1)$ conjugués de A est un nombre entier, désigné par $\mathfrak{N}(A)$, et qui est la *norme* de A. Cette norme est essentiellement positive. Les associés et les conjugués de A ont tous la même norme. Cette norme n'est pas affectée par les transformations qu'on peut faire subir à l'expression (1) du nombre complexe A.

Les nombres r, z_k, $(1+r)$, leurs conjugués, leurs associés, leurs puissances et leurs produits divers, ont tous l'unité pour norme commune. Tout nombre complexe peut être appelé un *sous-facteur* de sa norme. La forme la plus générale de tous les sous-facteurs de l'unité est $\left[r^k z_k^l z_{k'}^{l'} z_{k''}^{l''} \ldots\right]$; c'est le produit d'un nombre imaginaire r^k, par un nombre complexe réel $\left[z_k^l z_{k'}^{l'} z_{k''}^{l''} \ldots.\right]$.

3. Lorsqu'on forme le produit C de deux nombres complexes A et B de la forme (1), on obtient d'abord un polynôme en r de degré $(2n-2)$; on le réduit au degré $(n-1)$, en réunissant le coefficient de r^{n+i} à celui de r^i, puisque ces deux puissances sont égales d'après la définition de r; enfin, dans le but de simplifier le produit obtenu et réduit, on en retranche $(1 + r + r^2 + \ldots + r^{n-1}) = \varphi(r)$ multiplié par un entier m, convenablement choisi.

Inversement, veut-on savoir si un nombre complexe C est divisible par A, ou s'il est le résultat transformé du produit de A par un autre nombre complexe B? On ajoute à C l'expression $m\varphi(r)$, m étant un entier indéterminé; on ramène C à la forme d'un polynôme du degré $(2n-2)$, en remplaçant chacun de ses termes $(\gamma_i + m) r^i$ par les deux termes $[(\gamma_i + m - a_i) r^i + a_i r^{n+i}]$, a_i étant un entier indéterminé; puis, regardant comme des inconnues les n coefficients de B, et les n indéterminées m et a_i, on cherche s'il est possible d'identifier, par des valeurs entières de toutes ces inconnues, le nombre C, préparé comme il vient d'être dit, avec le produit effectué et non réduit de A par B. Si cette épreuve réussit, C est *divisible* par A; c'est-à-dire que C est le résultat transformé du produit de A par un autre nombre complexe B, pour les coefficients duquel l'identification a fourni des valeurs entières. Dans le cas contraire, C n'est pas divisible par A.

Tout nombre complexe A, dont la norme est N, ne peut être divisé par un sous-facteur d'un nombre premier N', autre que l'unité, et qui ne divise pas N. Soit $\mathfrak{N}(A) = N$, N un nombre premier; si A est décomposable en deux facteurs complexes B et C, l'un de ces facteurs aura pour norme N, l'autre aura pour norme l'unité.

4. Lorsque A et B sont deux nombres complexes ayant pour norme un même nombre premier N, chacun d'eux est divisible par l'un des conjugués de l'autre.

Si le nombre C n'est divisible par aucun des conjugués de B, sous-facteur du nombre premier N, il ne pourra l'être par aucun des conjugués de A, autre sous-facteur du même nombre premier N. Si l'on essaye successivement de diviser C par B_1, par B_2, par B_3,..., par B_{n-1}, et que l'on ne réussisse, dans aucune de ces $(n-1)$ épreuves, à obtenir pour quotient un nombre complexe entier, on pourra affirmer que $\mathfrak{N}(C)$ ne contient pas le facteur premier $N = \mathfrak{N}(B)$.

5. Soient toujours $\mathfrak{N}(B) = \mathfrak{N}(A) = N$, et N un nombre premier autre que l'unité, si N n'est pas l'exposant n, qui a pour sous-facteur $(1-r)$, A est divisible par un seul des conjugués de B. Les $(n-1)$ sous-facteurs imaginaires conjugués d'un nombre premier autre que n sont *premiers entre eux;* c'est-à-dire qu'ils ne peuvent avoir d'autres diviseurs communs que des sous-facteurs de l'unité.

L'exception relative à l'exposant n est caractéristique : n est le seul des nombres premiers, pouvant servir de normes, dont les $(n-1)$ sous-facteurs conjugués ne sont pas premiers entre eux; un quelconque de ses sous-facteurs reproduit tous les autres, lorsqu'on le multiplie par des coefficients dont la norme est 1. L'exposant n n'a réellement qu'un seul sous-facteur; on peut adopter $\lambda_1 = (1-r)$; n est divisible par λ_1^{n-1}, et non par une puissance supérieure de λ_1.

6. Lorsque A a pour norme le produit de deux nombres premiers différents M et N, dont on connaît deux sous-facteurs respectifs a et b, A est divisible par un des conjugués de a, ensuite par un des conjugués de b, et le quotient définitif a pour norme l'unité.

Lorsque $\mathfrak{N}(A)$ contient comme facteur un nombre premier N, élevé à la puissance i, a étant un sous-facteur de N, A est successivement

divisible i fois par un des conjugués de a; le conjugué diviseur pouvant varier d'une division à l'autre.

La décomposition d'un nombre complexe en ses facteurs premiers, et la détermination du plus grand commun diviseur entre deux nombres complexes, résultent de ces diverses propositions.

7. La somme de deux $n^{ièmes}$ puissances $(A^n + B^n)$ est décomposable en n facteurs, et l'on a généralement

$$(7)\quad A^n + B^n = (A + B)(A + Br)(A + Br^2)(A + Br^3)\dots(A + Br^{n-1}),$$

quels que soient les nombres A et B, entiers ou complexes.

Lorsque A et B sont des nombres entiers, le premier membre de l'équation (7), et le premier facteur du second membre, sont aussi des nombres entiers; les quatre derniers facteurs sont complexes et conjugués; leur norme est $\left(\frac{A^n + B^n}{A + B}\right)$. On peut poser généralement

$$(8)\qquad \frac{A^n \pm B^n}{A \pm B} = \mathfrak{N}(A \pm Br), \quad \text{ou} \quad A \pm Br = sf\left(\frac{A^n \pm B^n}{A \pm B}\right).$$

Quand on prend $A = B = 1$, on trouve

$$1 + r = sf(1), \quad 1 - r = sf(n).$$

Si le nombre complexe A (1) est divisible par $\lambda_1 = (1 - r)$, la somme de ses coefficients est un multiple de n : en effet, a désignant cette somme des coefficients, on aura

$$A = B\lambda_1 + a,$$

B étant un quotient complexe à coefficients entiers; si A est divisible par λ_1, il faut que a le soit aussi; mais a, nombre entier, ne peut être divisible par λ_1, que s'il l'est par n, ou par λ_1^{n-1}. Donc a, somme des coefficients de A, est un multiple de n, lorsque A est divisible par λ_1. Alors $\mathfrak{N}(A)$ est divisible par n.

Soient $\mathfrak{N}(A) = N$, et N un nombre premier autre que n, la somme a des coefficients de A ne sera pas divisible par n; les $(n - 1)$ conjugués de A ont la même somme de coefficients; $\mathfrak{N}(A)$, nombre entier, qui est le produit de ces $(n - 1)$ conjugués, sera donc de la forme $(a^{n-1} + nQ)$;

et, employant la notation de M. Gauss, on aura

$$N = \mathfrak{N}(A) \equiv a^{n-1} \equiv 1 \pmod{n},$$

c'est-à-dire que N sera de la forme $(ni+1)$.

La norme de tout nombre complexe A (1) divise une infinité de nombres entiers de la forme $\left(\frac{X^n \pm Y^n}{X \pm Y}\right)$. Si, dans les formules (8), on donne à A et B des valeurs entières, on obtiendra, comme exemples, les sous-facteurs de plusieurs nombres, premiers ou composés. On pourra en déduire, soit immédiatement, soit par des essais de division, les sous-facteurs des nombres premiers de la forme $(ni+1)$.

8. Quand A et B sont des nombres complexes, il est préférable, pour ce qui suit, de donner à l'équation (7) la forme suivante :

$$(9) \quad A^n + B^n = (A+B)(Ar+Br^{n-1})(Ar^2+Br^{n-2})\dots(Ar^{n-1}+Br).$$

Si l'on désigne par M, M', M'', ..., $M^{(n-1)}$ les n facteurs du second membre, on reconnaît facilement que ces facteurs vérifient les $\left[\frac{n(n-1)}{2}\right]$ équations comprises dans la forme générale

$$(10) \qquad M^{(l)} + M^{(l')} = z_{\left(\frac{l'-l}{2}\right)} \cdot M^{\left(\frac{l'+l}{2}\right)},$$

en ayant soin d'augmenter de n l'un des indices l et l', quand ils sont de parités contraires, ce qui ne change pas le nombre dont l'indice est augmenté.

Il résulte des relations (10), qu'un nombre complexe, dont la norme n'est pas l'unité, ne peut diviser deux des n facteurs $M^{(i)}$ sans diviser tous les autres. L'équation (9) peut se mettre sous la forme

$$(11) \qquad A^n + B^n = K^n . m . m' . m'' \dots m^{(n-1)},$$

K étant le produit des diviseurs communs aux $M^{(i)}$, et $m^{(i)}$ le quotient de $M^{(i)}$ par K. Les nombres $m^{(i)}$, actuellement premiers entre eux, c'est-à-dire n'ayant d'autres diviseurs communs que ceux dont la norme est l'unité, vérifieront les relations (10). Si A et B sont premiers entre eux, K ne peut être que λ_1, à la première puissance seulement.

La somme des $n^{ièmes}$ puissances de deux conjugués directs d'un nombre complexe imaginaire A est le produit de n nombres complexes réels. La différence de ces mêmes puissances est égale à la $n^{ième}$ puissance d'un des sous-facteurs de n, multipliée par n nombres complexes réels; ainsi, cette différence est divisible par λ_1^n.

9. Soit proposé de résoudre, en nombres complexes, l'équation

$$A^n + B^n + C^n = 0. \tag{12}$$

On peut supposer que A, B, C sont premiers entre eux, ou qu'ils ne sont pas divisibles tous les trois, et, par suite, deux d'entre eux, par un même sous-facteur d'un nombre premier autre que l'unité.

On a généralement

$$(A+B+C)^n = A^n + B^n + C^n + n(A+B)(C+A)(B+C)P, \tag{13}$$

P étant une fonction entière et symétrique de A, B, C, dont la forme dépend de l'exposant n. Si A, B, C sont les nombres complexes qui vérifient l'équation proposée, cette équation (13) se réduit à

$$(A+B+C)^n = n(A+B)(C+A)(B+C)P : \tag{14}$$

n est divisible par λ_1^{n-1}; le premier membre, qui est une $n^{ième}$ puissance, est donc divisible par λ_1^n, et $(A+B+C)$ par λ_1. Comme le premier, le second membre doit admettre le diviseur λ_1^n, et, puisque n n'admet que λ_1^{n-1}, il faut que l'un des quatre derniers facteurs soit divisible par λ_1; si c'est l'un des trois facteurs $(A+B)$, $(C+A)$ ou $(B+C)$, puisque $(A+B+C)$ est divisible par λ_1, il s'ensuivra que C, B ou A le sera aussi; si c'est le dernier facteur P qui admet le diviseur λ_1, on déduit encore, pour beaucoup de valeurs de n, que l'un des trois nombres A, B, C est nécessairement divisible par leur sous-facteur.

Autrement: soient a, b, c les sommes des coefficients, dans les nombres complexes A, B, C; n étant divisible par λ_1^{n-1}, et non par une puissance supérieure, l'équation (12) se met sous la forme

$$P\lambda_1^n + (a^n + b^n + c^n) = 0,$$

et le second membre étant zéro, le premier doit être divisible par λ_1^n;

ce qui exige que la somme $(a^n + b^n + c^n)$ soit un multiple de n^2. Or on démontre, pour une classe très-nombreuse d'exposants n (tels que $n = 5, 11, 17, 23, \ldots$), que cette somme des $n^{ièmes}$ puissances de trois nombres entiers ne peut être un multiple de n^2, sans que l'un des trois nombres a, b, c soit divisible par n (LEGENDRE, *Mémoires de l'Académie*, 1823); pour tous ces exposants, l'un des trois nombres complexes A, B, C sera divisible par λ_1. Nous supposerons que notre exposant n appartient à cette classe, et que C soit divisible par λ_1.

10. Soit proposé de résoudre, en nombres complexes, l'équation

$$A^n + B^n = \rho C^n, \tag{15}$$

ρ étant un coefficient complexe réel, dont la norme est l'unité, et qui a pour forme générale $[z_h^l z_{h'}^{l'} z_{h''}^{l''} \ldots]$. Le nombre des z_k (3), qui entrent dans le produit ρ, est au plus $\frac{1}{2}(n-3)$, car l'une des $\frac{1}{2}(n-1)$ valeurs de z_k est exclue par la relation

$$z_1 z_2 z_3 \ldots z_{\frac{n-1}{2}} = \mp 1.$$

Les exposants l, l', l'',... sont tous inférieurs à n, car $z_h^{l+nj}.C^n$ est égal à $z_h^l (z_h^i C)^n$, et l'on peut prendre $(z_h^i C)$ pour C.

Soit i la somme des exposants $[l + l' + l'' + \ldots]$; 2^i sera la somme des coefficients du nombre complexe ρ; le nombre $(\rho - 2^i)$ est divisible par λ_1, puisque la somme de ses coefficients est nulle; on a donc

$$\rho = 2^i + \lambda_1 \rho'_1,$$

ρ'_1 étant un nombre complexe; on aura aussi, en changeant r en $\frac{1}{r}$. ou en r^{n-1},

$$\rho = 2^i + \lambda_{n-1} \rho'_{n-1},$$

car ρ reste le même; égalant ces deux valeurs de ρ, il vient

$$\lambda_1 \rho'_1 = \lambda_{n-1} \rho'_{n-1};$$

mais on a

$$\lambda_1 = 1 - r, \quad \lambda_{n-1} = 1 - r^{n-1} = -r^{n-1} \lambda_1;$$

substituant et divisant par λ_1, il vient

$$\rho'_1 + r^{n-1} \rho'_{n-1} = 0.$$

Le second membre étant zéro, le premier est divisible par λ_1; d'où il suit que la somme des coefficients ρ'_1 est un multiple de n, ou que ρ'_1 est divisible par λ_1; conséquemment $(\rho - 2^i)$ est divisible par λ_1^2. Posons

$$\rho = 2^i + \lambda_1^2 \rho''_1,$$

d'où

$$\rho = 2^i + \lambda_{n-1}^2 \rho''_{n-1}, \quad \text{et} \quad \rho''_1 = r^{n-2} \rho''_{n-1};$$

on ne pourra rien conclure relativement à la divisibilité de ρ''_1 par λ_1; mais il est facile de voir que, si $(\rho - 2^i)$ est divisible par une puissance impaire de λ_1, il le sera nécessairement par la puissance paire qui la suit.

Ainsi $(\rho - 2^i)$ est divisible par une puissance paire de λ_1. Mais, afin de n'être pas arrêté dans la résolution des équations proposées, il faut admettre que cette puissance paire est toujours inférieure à λ_1^{n-1}, pour toutes les valeurs de ρ, qui ne sont pas des $n^{ièmes}$ puissances. Par une méthode de vérification qu'il serait trop long de développer ici, on reconnaît que ce théorème existe dans le cas des exposants $n = 5, 7, 11, 13, 19, 23, \ldots$; mais qu'il n'a pas lieu pour $n = 17, 31, \ldots$.

11. Il est une autre manière d'énoncer le théorème dont il s'agit. Si la différence $(\rho - 2^i)$ est divisible par λ_1^{2k}, il est facile de voir que $(\rho^n - 2^{in})$ est divisible par λ_1^{2k+n-1}. Cela posé, on a identiquement

$$\rho - 2^i = (\rho^n - 2^{in}) + 2^i(2^{i(n-1)} - 1) + \rho(1 - \rho^{n-1});$$

si le premier membre, ou $(\rho - 2^i)$, est divisible par λ_1^{n-1}, ou par n, il en sera de même du second; mais $(\rho^n - 2^{in})$ est alors divisible par $\lambda_1^{2(n-1)}$ ou par n^2, $(2^{i(n-1)} - 1)$ l'est par n; il faut donc que $\rho(1 - \rho^{n-1})$, et, par suite, $(1 - \rho^{n-1})$ soit divisible par λ_1^{n-1} ou par n.

Si donc on établit, pour un exposant donné, que $(1 - \rho^{n-1})$ ne peut être divisible par n, il sera démontré que $(\rho - 2^i)$ ne peut l'être par λ_1^{n-1}. Ce qui revient à prouver que la congruence

$$1 - x^{n-1} \equiv 0 \pmod{n},$$

laquelle est satisfaite en prenant pour x un nombre entier quelconque premier avec n, ne peut être vérifiée lorsqu'on prend pour x un sous-facteur réel de l'unité qui ne soit pas une $n^{ième}$ puissance.

12. Admettons que la différence $(\rho - 2^i)$ ne puisse être divisible que par une puissance paire de λ_1 inférieure à λ_1^{n-1}, quel que soit d'ailleurs le nombre complexe ρ ayant pour norme l'unité, et qui n'est pas une $n^{ième}$ puissance. Alors, l'équation (15) ne peut exister, si C n'est pas divisible par λ_1 : en effet, on a généralement

$$(A + B - 2^i C)^n = A^n + B^n - 2^{ni} C^n + n(A + B)(A - 2^i C)(B - 2^i C) P.$$

et, dans le cas de l'équation (15),

$$(16) \quad \begin{cases} (A + B - 2^i C)^n = (\rho - 2^i) C^n + 2^i (1 - 2^{i(n-1)}) C^n \\ + n(A + B)(A - 2^i C)(B - 2^i C) P. \end{cases}$$

Par les facteurs $(\rho - 2^i)$, $(1 - 2^{i(n-1)})$, n, les trois parties du second membre sont divisibles par λ_1 ; le premier membre, qui est une $n^{ième}$ puissance, est donc divisible par λ_1^n, et $(A + B - 2^i C)$ par λ_1 ; alors le second membre doit admettre le diviseur λ_1^n, et puisque n ou λ_1^{n-1} divise les deux dernières parties, il faudra que la première, ou $(\rho - 2^i) C^n$, soit au moins divisible par λ_1^{n-1} ; mais, d'après le théorème admis, $(\rho - 2^i)$ ne peut être divisé par une puissance aussi élevée de λ_1 : donc C, et, par suite, $A + B$, doit être divisible par λ_1.

13. Ainsi, dans les équations proposées,

$$(17) \quad \begin{cases} A^n + B^n = (-C)^n, \\ A^n + B^n = \rho C^n, \end{cases}$$

C est divisible par λ_1, A et B ne l'étant pas. Alors C, divisible par λ_1, l'est nécessairement par λ_1^2 ; ce que l'on démontre de la même manière que pour l'exposant 5. D'après cela, si l'on décompose le premier membre en ses n facteurs complexes, comme l'indique l'équation (9), on établit, tout comme pour $n = 5$, que le premier facteur $(A + B)$ doit être divisible par λ_1^{n+1}, et chacun des $(n - 1)$ autres facteurs par λ_1 seulement. D'où suit, qu'en divisant ces facteurs, et C, par λ_1, désignant les quotients par M, M', M'',..., $M^{(n-1)}$, et R, on aura à résoudre ou à vérifier une équation de la forme

$$(18) \quad M.M'.M''.M'''.... M^{(n-1)} = \rho R^n ;$$

R^n et M sont divisibles par λ_1^n ; les facteurs $M^{(i)}$, premiers entre eux,

vérifient les relations (10); ρ est ou 1, ou le coefficient complexe défini au n° **10**. Chaque facteur $M^{(i)}$ doit être de la forme $\nu^{(i)}\mu^{(i)n}$, ou égal à la n^{ieme} puissance d'un nombre complexe, multipliée par un coefficient dont la norme est l'unité. Tout coefficient $\nu^{(i)}$ est de la forme générale $[r^k z_h^l z_{h'}^{l'}\dots]$, produit du nombre imaginaire r^k par le nombre complexe réel $[z_h^l z_{h'}^{l'}\dots]$.

On peut réduire à l'unité l'un des coefficients $\nu^{(i)}$, en multipliant, dans l'équation (18), tous les facteurs $M^{(i)}$, et R, par $[r^{n-k} z_h^{n-l} z_{h'}^{n-l'}\dots]$, ce qui ne troublera pas cette équation (18), et ce qui n'empêchera pas les nouvelles valeurs des $M^{(i)}$ de vérifier les équations (10). Nous supposerons qu'on ait ainsi réduit à l'unité le coefficient de $\mu^{(n-1)n}$, dans $M^{(n-1)}$ qui n'est pas divisible par λ_1.

14. Parmi les équations (10), qui ne comportent réellement que $(n-2)$ relations distinctes, on prendra les $(n-1)$ équations qui contiennent M dans leur premier membre; et retranchant, de chacune d'elles, sa conjuguée de l'ordre $(n-1)$; observant que la différence des $n^{ièmes}$ puissances de deux conjugués directs $\left[\mu_1^{(n-1)n} - \mu_n^{(n-1)n}\right]$ est divisible par λ_1^n, et que μ_1^n, μ_{n-1}^n admettent le même diviseur, on établira, comme dans le cas de l'exposant 5, que la différence

$$\nu_1^{(i)}\mu_1^{(i)n} - \nu_{n-1}^{(i)}\mu_{n-1}^{(i)n} = (\nu_1^{(i)} - \nu_{n-1}^{(i)})\mu_1^{(i)n} + \nu_{n-1}^{(i)}\left(\mu_1^{(i)n} - \mu_{n-1}^{(i)n}\right)$$

doit être divisible par λ_1^n, pour toutes les valeurs de l'indice $i = 1, 2, 3, \dots, (n-2)$; et qu'il en est de même, conséquemment, de la différence $(\nu_1^{(i)} - \nu_{n-1}^{(i)})$. Or, $\nu_1^{(i)}$ étant de la forme $[r^k z_h^l z_{h'}^{l'}\dots]$, on a

$$\nu_1^{(i)} - \nu_{n-1}^{(i)} = r^k(1 - r^{3k}).z_h^l z_{h'}^{l'}\dots,$$

et cette différence ne peut être divisible par λ_1^n, que si $k = 0$. Donc tous les coefficients ν', ν'',..., $\nu^{(n-2)}$, et, par suite, ν, sont réels; c'est-à-dire qu'ils ne peuvent admettre de multiplicateur r^k.

15. Parmi les relations (10) se trouve celle-ci :

$$M^{(n-1)} + M' = z_1 M, \tag{19}$$

qui va nous suffire pour achever la démonstration. D'après ce qui

précède, on a

$$M = \nu\mu^n, \quad M' = \nu'\mu'^n, \quad M^{(n-1)} = \mu^{(n-1)^n}; \tag{20}$$

μ est divisible par λ_1, et non μ', ni $\mu^{(n-1)}$; le coefficient de $\mu^{(n-1)^n}$ a été réduit à l'unité; les coefficients ν, ν' sont réels et de la forme attribuée à ρ, n° **10**. Les valeurs (20), substituées dans l'équation (19), donnent

$$\mu^{(n-1)^n} + \nu'\mu'^n = z_1\nu\mu^n. \tag{21}$$

Or, le théorème des n^os^ **10** et **11** étant admis, l'équation (21) ne peut subsister, si ν' n'est pas l'unité: en effet, soit $2^{i'}$ la somme des coefficients du nombre complexe ν', on a généralement

$$(\mu^{(n-1)} + 2^{i'}\mu' + k\mu)^n = \mu^{(n-1)^n} + 2^{ni'}\mu'^n + k^n\mu^n + n\mathrm{Q}, \tag{22}$$

k et Q étant des nombres complexes; substituant à $\mu^{(n-1)^n}$ sa valeur tirée de l'équation (21), on a

$$\left\{\begin{aligned}(\mu^{(n-1)} + 2^{i'}\mu' + k\mu)^n = {} & [2^{i'}(2^{(n-1)i'} - 1) - (\nu' - 2^{i'})]\mu'^n \\ & + [k^n + z_1\nu]\mu^n + n\mathrm{Q}.\end{aligned}\right. \tag{23}$$

Par les facteurs $(2^{(n-1)i'} - 1)$, $(\nu' - 2^{i'})$, μ^n, n, toutes les parties du second membre sont divisibles par λ_1; le premier membre est donc divisible par λ_1^n, et le second doit admettre le même diviseur; mais μ^n est divisible par λ_1^n, $(2^{(n-1)i'} - 1)$ et n le sont par λ_1^{n-1}, il faut donc que le terme $(\nu' - 2^{i'})\mu'^n$ soit aussi divisible par λ_1^{n-1}; et puisque, d'après le théorème admis, $(\nu' - 2^{i'})$ ne peut avoir pour diviseur une puissance aussi élevée de λ_1, il faudrait que μ' fût divisible par λ_1, ce qui n'est pas. Donc ν' est nécessairement égal à 1; alors l'équation (22), ou

$$\mu^{(n-1)^n} + \mu'^n = z_1\nu.\mu^n = \rho'.\mu^n \tag{24}$$

a la même forme générale que la seconde équation (17) d'où nous sommes partis, mais est exprimée en nombres complexes dont les normes sont beaucoup plus petites.

Si ρ' est le même que ρ, cette nouvelle solution en nombres plus petits démontre l'impossibilité de l'équation proposée. Si ρ' diffère de ρ, on peut traiter l'équation (24) comme celle d'où l'on est parti, pour en déduire une troisième de la même forme générale. Après un

nombre limité de déductions semblables, on retombera nécessairement sur une équation (24), pour laquelle ρ' sera égal au coefficient ρ d'une des équations antécédentes, et il s'ensuivra encore que toutes sont impossibles, en nombres complexes ayant des normes finies.

On peut démontrer d'ailleurs, en s'appuyant sur le théorème admis, qu'il n'est pas possible que deux des facteurs $M^{(i)}$ n'aient pour normes que l'unité; ce qui met hors de doute le décroissement rapide des nombres, dans la série des équations déduites.

Conclusion.

Les équations proposées (17) sont impossibles en nombres complexes ayant des normes finies, si l'exposant n appartient à la classe définie au n° **9**, et si le théorème énoncé au n° **11** a lieu pour cet exposant. Exemples : $n = 5, 11, 23$.

Si la dernière condition est seule satisfaite, la seconde des équations (17) est impossible, ρ n'étant pas l'unité. Exemples : $n = 7, 13, 19$.