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 $A^5 + B^5 + C^5 = 0$

Journal de mathématiques pures et appliquées 1re série, tome 12 (1847), p. 137-171.
<http://www.numdam.org/item?id=JMPA_1847_1_12__137_0>

MÉMOIRE

SUR

LA RÉSOLUTION, EN NOMBRES COMPLEXES, DE L'ÉQUATION

$$A^5 + B^5 + C^5 = 0;$$

PAR M. G. LAMÉ.

Ce Mémoire se compose de deux parties : la première rappelle les propriétés connues des nombres complexes, relatifs à l'exposant 5, et en signale de nouvelles; la seconde traite directement l'équation proposée, et démontre son impossibilité.

PREMIÈRE PARTIE.

§ I.

Les nombres complexes, dont il s'agit ici, sont de la forme

$$A = \alpha_0 + \alpha_1 r + \alpha_2 r^2 + \alpha_3 r^3 + \alpha_4 r^4 = A(r); \tag{1}$$

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

$$r^5 = 1,$$

ou de celle-ci

$$\varphi(r) = 1 + r + r^2 + r^3 + r^4 = 0. \tag{2}$$

On sait que l'une des racines étant r, les trois autres sont r^2, r^3, r^4, et qu'en posant

$$z_1 = r + r^4 = r + \frac{1}{r}, \quad z_2 = r^2 + r^3 = r^2 + \frac{1}{r^2}, \tag{3}$$

z_1 et z_2 sont les racines réelles de l'équation

$$z^2 + z - 1 = 0, \tag{4}$$

d'où résultent les relations

$$z_1 + z_2 = -1, \quad z_1 z_2 = -1, \quad z_1^2 + z_2^2 = 3. \tag{5}$$

Lorsque $\alpha_4 = \alpha_1$, $\alpha_3 = \alpha_2$, le nombre complexe A se réduit à la forme

$$\mathfrak{A} = a_0 + a_1 z_1 + a_2 z_2 ; \tag{6}$$

il est alors réel.

On peut augmenter ou diminuer d'un même nombre entier m les cinq coefficients de A, (1), sans pour cela en changer la valeur : car cette transformation revient à augmenter ou à diminuer A de $m\varphi(r)$, quantité qui est nulle par l'équation (2). On peut augmenter ou diminuer d'un même nombre entier m les trois coefficients de $\mathfrak{A}$, (6), ce qui revient à mettre à la suite de $\mathfrak{A}$, $\pm m(1 + z_1 + z_2)$, quantité qui est nulle par la première des relations (5).

Si l'on multiplie successivement le nombre A par r, r^2, r^3, r^4, et si l'on réduit les puissances de r, en remplaçant r^5, r^6, r^7, r^8 par leurs égales 1, r, r^2, r^3, on obtient la série de cinq nombres complexes $[A, Ar, Ar^2, Ar^3, Ar^4]$, que l'on désignera par $[A, A', A'', A''', A^{IV}]$. Ces nombres, que M. Dirichlet appelle *associés* de A, ont tous la même puissance cinquième, car

$$(Ar^i)^5 = A^5 r^{5i} = A^5.$$

Lorsqu'on substitue successivement dans $A(r)$, r^2, r^3, r^4 à r, en réduisant les puissances de r, on obtient la série de quatre nombres complexes $[A(r), A(r^2), A(r^3), A(r^4)]$, que l'on désignera par $[A_1, A_2, A_3, A_4]$. Ces nombres, que M. Dirichlet appelle *conjugués* de A, ont des puissances cinquièmes différentes. Chacun d'eux a ses associés, ce qui fait en tout vingt nombres, tous déduits du même nombre A, et qui jouissent de propriétés remarquables. Pour l'intelligence de ce qui va suivre, il convient de placer ici les valeurs de ces vingt nombres complexes :

$$
(7)\quad
\begin{cases}
A_1=\alpha_0+\alpha_1 r+\alpha_2 r^2+\alpha_3 r^3+\alpha_4 r^4, & A_4=\alpha_0+\alpha_4 r+\alpha_3 r^2+\alpha_2 r^3+\alpha_1 r^4,\\
A'_1=\alpha_4+\alpha_0 r+\alpha_1 r^2+\alpha_2 r^3+\alpha_3 r^4, & A'_4=\alpha_1+\alpha_0 r+\alpha_4 r^2+\alpha_3 r^3+\alpha_2 r^4,\\
A''_1=\alpha_3+\alpha_4 r+\alpha_0 r^2+\alpha_1 r^3+\alpha_2 r^4, & A''_4=\alpha_2+\alpha_1 r+\alpha_0 r^2+\alpha_4 r^3+\alpha_3 r^4,\\
A'''_1=\alpha_2+\alpha_3 r+\alpha_4 r^2+\alpha_0 r^3+\alpha_1 r^4, & A'''_4=\alpha_3+\alpha_2 r+\alpha_1 r^2+\alpha_0 r^3+\alpha_4 r^3,\\
A^{iv}_1=\alpha_1+\alpha_2 r+\alpha_3 r^2+\alpha_4 r^3+\alpha_0 r^4, & A^{iv}_4=\alpha_4+\alpha_3 r+\alpha_2 r^2+\alpha_1 r^3+\alpha_0 r^4,
\end{cases}
$$

$$
\begin{cases}
A_2=\alpha_0+\alpha_3 r+\alpha_1 r^2+\alpha_4 r^3+\alpha_2 r^4, & A_3=\alpha_0+\alpha_2 r+\alpha_4 r^2+\alpha_1 r^3+\alpha_3 r^4,\\
A'_2=\alpha_2+\alpha_0 r+\alpha_3 r^2+\alpha_1 r^3+\alpha_4 r^4, & A'_3=\alpha_3+\alpha_0 r+\alpha_2 r^2+\alpha_4 r^3+\alpha_1 r^4,\\
A''_2=\alpha_4+\alpha_2 r+\alpha_0 r^2+\alpha_3 r^3+\alpha_1 r^4, & A''_3=\alpha_1+\alpha_3 r+\alpha_0 r^2+\alpha_2 r^3+\alpha_4 r^4,\\
A'''_2=\alpha_1+\alpha_4 r+\alpha_2 r^2+\alpha_0 r^3+\alpha_3 r^4, & A'''_3=\alpha_4+\alpha_1 r+\alpha_3 r^2+\alpha_0 r^3+\alpha_2 r^4,\\
A^{iv}_2=\alpha_3+\alpha_1 r+\alpha_4 r^2+\alpha_2 r^3+\alpha_0 r^4, & A^{iv}_3=\alpha_2+\alpha_4 r+\alpha_1 r^2+\alpha_3 r^3+\alpha_0 r^4.
\end{cases}
$$

Les conjugués de A étant $[A_1, A_2, A_3, A_4]$, ceux de A′ sont $[A'_1, A''_2, A'''_3, A^{iv}_4]$, ceux de A″, $[A''_1, A^{iv}_2, A'_3, A'''_4]$, ceux de A‴, $[A'''_1, A'_2, A^{iv}_3, A''_4]$, ceux de A^{iv}, $[A^{iv}_1, A'''_2, A''_3, A'_4]$. Si l'on substitue successivement r^2, r^3, r^4 à r, dans A_2, on retrouve respectivement A_1, A_4, A_3; si, dans A_3, on retrouve A_4, A_2, A_1; si, dans A_4, on retrouve A_3, A_2, A_1.

§ II.

Lorsqu'on substitue r^2 ou r^3, à r, dans les nombres complexes réels z_1 et z_2, z_1 se change en z_2, et réciproquement; quand on y substitue r^4 à r, ces nombres restent les mêmes. Ainsi les quatre conjugués de z_1 sont $[z_1, z_2, z_2, z_1]$, ceux de z_2, $[z_2, z_1, z_1, z_2]$. D'après cela, les quatre conjugués de tout nombre complexe réel, ou de la forme (6), sont égaux deux à deux; on a

$$
(8)\quad \mathfrak{A}_1=\mathfrak{A}_4=a_0+a_1 z_1+a_2 z_2, \qquad \mathfrak{A}_2=\mathfrak{A}_3=a_0+a_1 z_2+a_2 z_1.
$$

On peut donc n'admettre que deux conjugués pour tout nombre complexe réel; on les désignera par $\mathfrak{A}_1$, $\mathfrak{A}_2$. Le produit de ces deux conjugués est toujours un nombre entier, positif ou négatif; en effet, on a

$$
(9)\quad
\begin{cases}
\mathfrak{A}_1\mathfrak{A}_2=(a_0+a_1 z_1+a_2 z_2)(a_0+a_1 z_2+a_2 z_1)\\
=a_0^2+(a_1+a_2)a_0(z_1+z_2)+(a_1^2+a_2^2)z_1 z_2+a_1 a_2(z_1^2+z_2^2),
\end{cases}
$$

ou, d'après les relations (5),

$$(10)\qquad \begin{cases} \mathfrak{A}_1\mathfrak{A}_2 = a_0^2 - (a_1+a_2)a_0 - a_1^2 - a_2^2 + 3a_1a_2 \\ \qquad = \left(a_0 - \frac{a_1+a_2}{2}\right)^2 - 5\left(\frac{a_1-a_2}{2}\right)^2, \end{cases}$$

ce qui donne une valeur entière, puisque a_0, a_1, a_2 sont des entiers.

Dans le cas général où A est imaginaire, les sommes $A(r)+A(r^4)$ ou A_1+A_4, et $A(r^2)+A(r^3)$ ou A_2+A_3, se reproduisant l'une l'autre, ou restant les mêmes, quand on y substitue r^2, r^3, r^4 à r, sont des nombres complexes de la forme (6); le tableau (7) donne, en effet,

$$(11)\qquad \begin{cases} A_1+A_4 = 2\alpha_0 + (\alpha_1+\alpha_4)z_1 + (\alpha_2+\alpha_3)z_2, \\ A_2+A_3 = 2\alpha_0 + (\alpha_1+\alpha_4)z_2 + (\alpha_2+\alpha_3)z_1; \end{cases}$$

le produit de ces deux sommes est donc un nombre entier, positif ou négatif, qui est

$$(12)\quad (A_1+A_4)(A_2+A_3) = \left(2\alpha_0 - \frac{\alpha_1+\alpha_2+\alpha_3+\alpha_4}{2}\right)^2 - 5\left(\frac{\alpha_1+\alpha_4-\alpha_2-\alpha_3}{2}\right)^2.$$

Si l'on ajoute les équations (11), on trouve, en faisant usage de la première relation (5),

$$(13)\qquad A_1+A_2+A_3+A_4 = 5\alpha_0 - (\alpha_0+\alpha_1+\alpha_2+\alpha_3+\alpha_4);$$

ainsi la somme des quatre conjugués de tout nombre complexe A est un nombre entier: on reconnaîtra facilement, par le tableau (7), que la somme de ses cinq associés est toujours nulle.

Les produits $A(r)A(r^4)$ ou A_1A_4, $A(r^2)A(r^3)$ ou A_2A_3, se reproduisant l'un l'autre, ou restant les mêmes, quand on y substitue r^2, r^3, r^4 à r, sont encore des nombres complexes de la forme (6); le tableau (7) donne, en effet,

$$(14)\qquad A_1A_4 = b_0 + b_1z_1 + b_2z_2, \quad A_2A_3 = b_0 + b_1z_2 + b_2z_1,$$

en posant, pour simplifier,

$$(15)\qquad \begin{cases} \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = b_0, \\ \alpha_0\alpha_1 + \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_0 = b_1, \\ \alpha_0\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_0 + \alpha_4\alpha_1 = b_2. \end{cases}$$

Parmi les quatre nombres $[A_1, A_2, A_3, A_4]$, on peut appeler *conjugués directs* ceux dont le produit donne un nombre complexe réel de la forme (6): A_1, A_4 sont deux conjugués directs, ainsi que A_2, A_3; A_1, A_2 sont deux conjugués indirects.

Le produit $A_1 A_2 A_3 A_4$ est un nombre entier, car on a, en multipliant les deux valeurs (14),

$$A_1 A_2 A_3 A_4 = b_0^2 - (b_1 + b_2) b_0 - b_1^2 - b_2^2 + 3 b_1 b_2 ; \tag{16}$$

on peut appeler ce produit entier, *norme* de A, expression introduite par M. Gauss, et le désigner par le symbole $\mathfrak{N}(A)$; on peut écrire

$$\mathfrak{N}(A) = \left(b_0 - \frac{b_1 + b_2}{2}\right)^5 - 5\left(\frac{b_1 - b_2}{2}\right)^2. \tag{17}$$

Cette norme est essentiellement positive : en effet, l'équation du quatrième degré, qui a pour racines les quatre conjugués $[A_1, A_2, A_3, A_4]$, et qu'il est facile de composer, a pour dernier terme $\mathfrak{N}(A)$, son second membre étant zéro. Si A est imaginaire, les conjugués $[A_1, A_2, A_3, A_4]$ le sont aussi; l'équation aux conjugués a toutes ses racines imaginaires, son dernier terme est donc essentiellement positif. Si A est réel, les conjugués sont réels et égaux deux à deux, savoir, $A_4 = A_1$, $A_3 = A_2$; l'équation aux conjugués a ses racines réelles, égales deux à deux, son premier membre est un carré, et son dernier terme est encore positif.

Ainsi tout nombre complexe réel $\mathfrak{A}_1$ de la forme (6), qui, multiplié par son unique conjugué $\mathfrak{A}_2$, donne un produit entier négatif (10), ne peut pas être le produit (14) de deux nombres complexes imaginaires conjugués $A_1 A_4$ ou $A_2 A_3$. Un tel nombre ne peut être décomposé en deux facteurs de la forme (1), qu'à l'aide de coefficients compliqués d'imaginaires; il doit être considéré, dans ce Mémoire, comme un nombre complexe simple, ayant quatre conjugués, égaux deux à deux, et dont la norme est alors positive.

Par exemple, z_1 et z_2 (3) sont des nombres complexes simples, puisque $z_1 z_2 = -1$; il en est de même de $(3 + 2z_1)$, qui donne

$$(3 + 2z_1)(3 + 2z_2) = -1 ;$$

la norme de ces deux nombres est l'unité : elle est égale à $z_1^2 z_2^2$ dans le

premier exemple, et à $(3+2z_1)^2(3+2z_2)^2$ dans le second. Le nombre $(3+2z_1)$ est d'ailleurs égal à $-z_2^3$; et, en général, tout nombre complexe dont la norme est l'unité, qui représente un des facteurs du premier membre de l'équation

$$x^2 - 5y^2 = \pm 1,$$

et qui est de la forme $(3+2z_1)^i$ ou $(3+2z_2)^i$, est égal à $(-1)^i z_2^{3i}$ ou à $(-1)^i z_1^{3i}$, et s'exprime par une puissance de z_1 ou de z_2. Une puissance quelconque de r a pour norme l'unité, car les quatre conjugués $[r^i, r^{2i}, r^{3i}, r^{4i}]$ donnent pour produit $r^{10i}=1$. Les nombres conjugués $[(1+r), (1+r^2), (1+r^3), (1+r^4)]$ ont aussi pour norme l'unité, car

$$1 + r = r^3(r^2 + r^3) = r^3 z_2,$$

et la norme de chaque facteur r^3 et z_2 est 1; chacun de ces nombres, ou l'une de leurs puissances, se réduit donc aussi à une puissance de r, multipliée par une puissance de z_1 ou de z_2. Il résulte de ce rapprochement, que le produit $r^k z_{1\text{ ou }2}^i$ représente généralement tous les sous-facteurs de l'unité, ou tous les nombres complexes dont la norme est 1.

La forme générale (17) de $\mathfrak{N}(A)$ jouit d'une symétrie remarquable. On vérifie aisément qu'elle reste la même, ou qu'elle conserve la même valeur, lorsqu'on change les coefficients de A_1 en ceux d'un quelconque de ses conjugués, et lorsqu'on augmente ou diminue d'un même nombre, soit ces coefficients eux-mêmes, soit leurs indices, en ayant soin de réduire ceux de ces indices qui surpassent 5, ou ceux qui lui sont inférieurs. C'est-à-dire que les vingt nombres du tableau (7) ont la même norme, et que cette norme n'est pas affectée par toutes les transformations qu'on peut faire subir à l'expression (1) du nombre complexe A. On peut donner à l'un quelconque des vingt nombres du tableau (7), le nom de *sous-facteur* de $\mathfrak{N}(A)$.

§ III.

Lorsqu'on multiplie l'un par l'autre deux nombres complexes

$$(18)\qquad \begin{cases} A = \alpha_0 + \alpha_1 r + \alpha_2 r^2 + \alpha_3 r^3 + \alpha_4 r^4, \\ B = \beta_0 + \beta_1 r + \beta_2 r^2 + \beta_3 r^3 + \beta_4 r^4, \end{cases}$$

on obtient d'abord un polynôme du huitième degré en r, qui est

$$(19)\quad \left\{\begin{array}{l} \alpha_0\beta_0+(\alpha_0\beta_1+\alpha_1\beta_0)r+(\alpha_0\beta_2+\alpha_1\beta_1+\alpha_2\beta_0)r^2+(\alpha_0\beta_3+\alpha_1\beta_2+\alpha_2\beta_1+\alpha_3\beta_0)r^3 \\ \quad +(\alpha_0\beta_4+\alpha_1\beta_3+\alpha_2\beta_2+\alpha_3\beta_1+\alpha_4\beta_0)r^4+(\alpha_1\beta_4+\alpha_2\beta_3+\alpha_3\beta_2+\alpha_4\beta_1)r^5 \\ \quad +(\alpha_2\beta_4+\alpha_3\beta_3+\alpha_4\beta_2)r^6+(\alpha_3\beta_4+\alpha_4\beta_3)r^7+\alpha_4\beta_4r^8; \end{array}\right.$$

puis, observant que $r^5=1$, $r^6=r$, $r^7=r^2$, $r^8=r^3$, on réunit les coefficients des quatre derniers termes aux coefficients des quatre premiers, ce qui donne le polynôme du quatrième degré :

$$(20)\quad \left\{\begin{array}{l} (\alpha_0\beta_0+\alpha_1\beta_4+\alpha_2\beta_3+\alpha_3\beta_2+\alpha_4\beta_1) \\ +(\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_4+\alpha_3\beta_3+\alpha_4\beta_2)r \\ +(\alpha_0\beta_2+\alpha_1\beta_1+\alpha_2\beta_0+\alpha_3\beta_4+\alpha_4\beta_3)r^2 \\ +(\alpha_0\beta_3+\alpha_1\beta_2+\alpha_2\beta_1+\alpha_3\beta_0+\alpha_4\beta_4)r^3 \\ +(\alpha_0\beta_4+\alpha_1\beta_3+\alpha_2\beta_2+\alpha_3\beta_1+\alpha_4\beta_0)r^4; \end{array}\right.$$

enfin, dans le but de simplifier cette nouvelle expression du produit obtenu, on retranche de ce polynôme celui-ci $(1+r+r^2+r^3+r^4)$ (lequel est nul d'après la définition de r), multiplié par un entier convenable m ; et l'on a ainsi un nombre complexe C de la forme

$$(21)\qquad C=\gamma_0+\gamma_1r+\gamma_2r^2+\gamma_3r^3+\gamma_4r^4,$$

qui est l'expression définitive du produit de A par B.

D'après cela, et dans un ordre inverse, veut-on savoir si le nombre C (21) est divisible par A, ou s'il peut être le résultat de la multiplication de A par un autre nombre complexe B de même espèce? on ajoutera un nombre entier indéterminé m à tous les coefficients de C, lequel prendra la forme

$$(22)\quad \left\{\begin{array}{l} (\gamma_0+m)+(\gamma_1+m)r+(\gamma_2+m)r^2 \\ +(\gamma_3+m)r^3+(\gamma_4+m)r^4, \end{array}\right.$$

de valeur identique à celle (21), et qui devra reproduire la forme (20) du produit cherché, pour une certaine valeur de m; puis, retranchant des quatre premiers coefficients du polynôme (22), des nombres entiers différents et indéterminés a_0, a_1, a_2, a_3, pour les ajouter ensuite, respectivement multipliés par r^5, r^6, r^7, r^8, on obtiendra la nouvelle

forme

$$(23)\quad \begin{cases} (\gamma_0 + m - a_0) + (\gamma_1 + m - a_1)r + (\gamma_2 + m - a_2)r^2 \\ + (\gamma_3 + m - a_3)r^3 + (\gamma_4 + m)r^4 + a_0 r^5 + a_1 r^6 + a_2 r^7 + a_3 r^8, \end{cases}$$

encore de même valeur que C (21), et qui devra reproduire la forme (19) du produit cherché, pour certaines valeurs entières de a_0, a_1, a_2, a_3.

Alors, les coefficients $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ et $\gamma_0, \gamma_1, \gamma_2, \gamma_3, \gamma_4$ étant entiers et numériquement connus; $\beta_0, \beta_1, \beta_2, \beta_3, \beta_4$ étant, au contraire, indéterminés; s'il est possible d'identifier les deux polynômes du huitième degré (23) et (19) par des valeurs entières de toutes les indéterminées $\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, m, a_0, a_1, a_2, a_3$, on pourra affirmer que C (21) est divisible par A; c'est-à-dire qu'il sera le résultat transformé du produit de A par un autre polynôme B, pour les coefficients duquel l'identification aura fourni des valeurs entières. Si, au contraire, les deux polynômes ne peuvent être rendus identiques par aucun système de valeurs entières des indéterminées introduites, on pourra dire, d'une manière certaine, que C *n'est pas divisible par* A; c'est-à-dire qu'il ne peut être le résultat transformé du produit de A par un nombre complexe de même espèce, ayant des coefficients entiers.

C'est ainsi qu'il faut entendre la divisibilité des nombres complexes. On voit que cette propriété repose sur la possibilité de l'identification de deux polynômes du huitième degré, quelle que soit d'ailleurs la lettre ou la quantité r, dont les diverses puissances constituent ces polynômes.

Tout nombre complexe A, dont la norme est N, ne peut être divisé par un sous-facteur a_1 d'un nombre premier n autre que l'unité, qui ne diviserait pas N; car, si l'on avait

$$A_1 = a_1 B_1,$$

il en résulterait

$$A_2 = a_2 B_2, \quad A_3 = a_3 B_3, \quad A_4 = a_4 B_4,$$

et, en multipliant,

$$A_1 A_2 A_3 A_4 = a_1 a_2 a_3 a_4 . B_1 B_2 B_3 B_4,$$

c'est-à-dire,

$$\mathfrak{N}(A_1) = \mathfrak{N}(a_1) \cdot \mathfrak{N}(B_1), \quad \text{ou} \quad N = n \cdot \mathfrak{N}(B_1),$$

équation absurde, puisque n ne divise pas N, et que B étant, par hypothèse, un quotient complexe à coefficients entiers, sa norme serait un nombre entier.

Soit $\mathfrak{N}(A) = N$, et 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. En effet, si l'on a

$$A_1 = B_1 C_1,$$

on en conclura

$$\mathfrak{N}(A) = \mathfrak{N}(B) \cdot \mathfrak{N}(C) = N;$$

or $\mathfrak{N}(B)$ et $\mathfrak{N}(C)$ sont des nombres entiers, leur produit devant être un nombre premier N, l'un de ces facteurs est N, et l'autre 1.

§ IV.

Lorsque A et B sont deux nombres complexes, ayant pour norme un même nombre premier N, A est divisible par un des conjugués de B. En effet, on peut admettre que le polynôme algébrique, au moyen duquel s'exprime B, ne soit pas décomposable en deux facteurs rationnels, puisque, s'il l'était, l'un de ces facteurs ayant pour norme l'unité, on prendrait l'autre facteur pour B. Les équations

$$\mathfrak{N}(A) = N, \quad \mathfrak{N}(B) = N$$

expriment uniquement l'égalité des deux produits $A_1 A_2 A_3 A_4$, $B_1 B_2 B_3 B_4$, quand on a égard à la définition de r, et quand tous les calculs sont effectués. On peut donc poser

$$A_1 A_2 A_3 A_4 = B_1 B_2 B_3 B_4, \tag{24}$$

avant d'entreprendre ces calculs. Supposons que, ne faisant subir aucune transformation aux polynômes du quatrième degré B_1, B_2, B_3, B_4, et regardant r comme une lettre indéterminée, on effectue leur multiplication; le produit du second membre de l'équation (24) sera un polynôme P du seizième degré en r. Mettons chacun des polynômes, facteurs du premier membre, sous la forme (23); les nombres m, a_0,

a_1, a_2, a_3 étant différents pour chaque facteur. Dans le produit effectué du premier membre ainsi transformé, on peut regarder r comme une quantité indéterminée; ce produit sera un polynôme M du trente-deuxième degré, qui se réduira à P, quand on introduira la condition que r soit une racine de l'équation (2). On peut toujours composer un polynôme Q, du seizième degré en r, contenant un grand nombre d'indéterminées, qui satisfasse à la condition de devenir égal à l'unité lorsque r vérifie l'équation (2); en effet, $\varphi(r)$ étant le premier membre de cette équation, et $\psi(r)$ un polynôme complet du douzième degré, dont les treize coefficients soient indéterminés, on prendra

$$Q = 1 + \varphi(r)\,\psi(r).$$

Cela posé, le polynôme M et le produit PQ, qui sont déjà identiques pour les quatre valeurs de r, racines imaginaires de l'équation (2), pourront être identifiés à l'aide des indéterminées introduites, lesquelles sont au nombre de trente-trois. Mise sous cette forme, l'équation

$$(25) \qquad A_1 A_2 A_3 A_4 = B_1 B_2 B_3 B_4 [1 + \varphi(r)\,\psi(r)]$$

peut être regardée comme une identité en r; alors le polynôme B, indécomposable en facteurs rationnels, devra diviser l'un des facteurs du premier membre. Soit

$$A_3 = B_1 R_1,$$

on en conclura

$$A_1 = B_2 R_2, \quad A_4 = B_3 R_3, \quad A_3 = B_4 R_4,$$

et, par l'équation (24),

$$\mathfrak{N}(R_1) = 1.$$

Ainsi A_1, A_2, A_3, A_4 sont respectivement divisibles par les quatre conjugués de B, et les quotients sont des nombres complexes dont la norme est l'unité.

Ainsi, lorsque les nombres complexes A et B ont tous deux pour norme un nombre premier N, autre que l'unité, un des conjugués de B doit diviser A. Et l'on peut dire que, réciproquement, B est divisible par l'un des conjugués de A : en effet, si l'on trouve, comme

ci-dessus,

$$A_4 = B_3 R_3,$$

et, comme conséquence,

$$A_3 = B_1 R_4,$$

puisque $R_1 R_2 R_3 R_4 = 1$ nécessairement, on en conclura

$$R_2 R_3 R_4 A_3 = B_1;$$

c'est-à-dire que B_1 sera égal à A_3 multiplié par $R_2 R_3 R_4$, multiplicateur complexe dont la norme est 1.

De ce qui précède, il résulte que si un nombre complexe C est divisible par un des conjugués de A, diviseur complexe qui a pour norme le nombre premier N, il sera aussi divisible par l'un des conjugués de tout autre diviseur complexe B, qui aurait la même norme N que A : en effet, si l'on trouve

$$C_1 = D_1 A_k,$$

comme A_k est nécessairement divisible par l'un des conjugués de B, on doit avoir

$$A_k = R_1 B_i, \quad \text{d'où} \quad C_1 = D_1 R_1 B_i,$$

R_1 ayant d'ailleurs pour norme l'unité. Donc C_1 est divisible par B_i, ou par l'un des conjugués de B, s'il l'est par A_k, ou par l'un des conjugués de A.

Inversement, si C n'est pas divisible par l'un 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 de diviser C par B_1, par B_2, par B_3, par B_4, et que l'on ne réussisse, dans aucune de ces quatre épreuves, à obtenir pour quotient un nombre complexe entier, on pourra affirmer que $\mathfrak{N}(C)$ ne contient pas le facteur premier N.

§ V.

Soit toujours $\mathfrak{N}(B) = \mathfrak{N}(A) = N$, et N un nombre premier; A_1 est divisible par l'un des conjugués de B, soit par B_3 : peut-il l'être par un

autre conjugué de B, par B_2 par exemple? Soit $A_1 = R_1 B_3 = P_1 B_2$; R_1 et P_1 sont nécessairement des nombres complexes dont la norme est l'unité. De l'équation

$$R_1 B_3 = P_1 B_2$$

on conclura, en multipliant par $R_2 R_3 R_4$, et faisant $R_2 R_3 R_4 P_1 = Q_1$,

$$B_3 = Q_1 B_2.$$

Si l'on change, dans cette dernière équation, r en r^4, elle devient

$$B_2 = Q_1 R_3;$$

d'où résulte, par la multiplication,

$$B_3 B_2 = Q_1 Q_4 B_2 B_3,$$

et, en divisant par $B_3 B_2$,

$$Q_1 Q_4 = 1:$$

or on a

$$R_2 R_3 R_4 P_1 = Q_1,$$

d'où, en changeant r en r^4,

$$R_3 R_2 R_1 P_4 = Q_4;$$

multipliant et réduisant, il vient

$$R_2 R_3 P_1 P_4 = 1.$$

On reconnaît facilement que cette équation ne peut être satisfaite que si $P_1 = \pm R_1$, ce qui donnera

$$B_3 = B_2, \quad \text{ou} \quad B_3 + B_2 = 0.$$

Soient prises pour B_1, B_2, B_3 les expressions A_1, A_2, A_3 du tableau (7).

1°. Si $B_2 = B_3$, il faudra que l'on ait, en supprimant α_0 dans les deux membres, et divisant par r,

$$\alpha_3 + \alpha_1 r + \alpha_4 r^2 + \alpha_2 r^3 = \alpha_2 + \alpha_4 r + \alpha_1 r^2 + \alpha_3 r^3;$$

or cette équation ne peut subsister, à moins que les coefficients des mêmes puissances de r ne soient respectivement égaux dans les deux membres, car r ne peut être racine d'une équation du troisième degré;

donc il faut que $\alpha_3 = \alpha_2$, $\alpha_4 = \alpha_1$: alors

$$B_1 = \alpha_0 + \alpha_1 z_1 + \alpha_2 z_2 = B_4, \quad B_2 = \alpha_0 + \alpha_1 z_2 + \alpha_2 z_1 = B_3,$$

et

$$B_1 B_2 = B_3 B_4 = n,$$

n étant un entier. On aurait donc

$$B_1 B_2 B_3 B_4 = \mathfrak{N}(B) = N = n^2;$$

ce qui ne peut être, puisque N est un nombre premier, et non pas un carré.

2°. Si $B_3 + B_2 = 0$, on aura

$$2\alpha_0 + (\alpha_3 + \alpha_2) z_1 + (\alpha_1 + \alpha_1) z_2 = 0,$$

ce qui exige que

$$\alpha_3 + \alpha_2 = \alpha_1 + \alpha_4 = 2\alpha_0;$$

de là on tire

$$\alpha_3 = 2\alpha_0 - \alpha_2, \quad \alpha_4 = 2\alpha_0 - \alpha_1,$$

et B_1 devient successivement

$$\begin{aligned} B_1 &= \alpha_0 (1 + 2r^3 + 2r^4) + \alpha_1 (r - r^4) + \alpha_2 (r^2 - r^3) \\ &= \alpha_0 (-r - r^2 + r^3 + r^4) + \alpha_1 (r - r^4) + \alpha_2 (r^2 - r^3) \\ &= (1 - r)[(\alpha_1 - \alpha_0)(r + r^2 + r^3) + (\alpha_2 - \alpha_0) r^2], \end{aligned}$$

c'est-à-dire que B_1 est décomposable en deux facteurs, dont l'un, $(1 - r)$, a pour norme 5; car

$$\begin{aligned} (1 - r)(1 - r^4) &= 2 - z_1, \quad (1 - r^2)(1 - r^3) = 2 - z_2, \\ (2 - z_1)(2 - z_2) &= 4 - 2(z_1 + z_2) + z_1 z_2 = 5. \end{aligned}$$

Or on a vu que si B_1 était décomposable en deux facteurs, l'un de ces facteurs devait avoir pour norme N, et l'autre l'unité; donc il faudra que $N = 5$, et que le second facteur ait pour norme 1.

Ainsi, excepté lorsque la norme est 5, si A_1 est divisible par B_3, il ne peut l'être par son conjugué direct B_2, et réciproquement. Il faut voir, en outre, si l'on peut avoir

$$A_1 = R_1 B_1 = P_1 B_2,$$

ou si A peut être divisible par deux conjugués indirects de B. On aurait

$$R_1 B_1 = P_1 B_2,$$

d'où, changeant r en r^3,

$$R_3 B_3 = P_3 B_1;$$

de ces deux équations on déduit

$$B_1 = R_2 R_3 R_4 P_1 B_2 = P_1 P_2 P_4 R_3 B_3,$$

c'est-à-dire que B_3 et B_2, respectivement multipliés par deux coefficients complexes ayant pour norme l'unité, pourraient donner des produits égaux; ce qui vient d'être démontré impossible, lorsque N n'est pas 5.

Donc si $\mathfrak{N}(A) = \mathfrak{N}(B) = N$, N étant un nombre premier autre que 5, A sera divisible par un des conjugués de B et ne sera divisible par aucun des trois autres; et A pouvant être précisément un des conjugués de B, cette proposition démontre que les quatre sous-facteurs conjugués d'un nombre premier autre que 5 *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 5 est caractéristique : 5 est le seul des nombres, pouvant servir de normes, dont les quatre sous-facteurs conjugués ne sont pas premiers entre eux. On peut prendre pour ces sous-facteurs

$$(26) \qquad 1 - r = \lambda_1, \quad 1 - r^2 = \lambda_2, \quad 1 - r^3 = \lambda_3, \quad 1 - r^4 = \lambda_4,$$

et l'on reconnaît aisément que l'un quelconque de ces quatre conjugués reproduit les trois autres, lorsqu'on le multiplie par des sous-facteurs de l'unité : en effet, on a identiquement

$$(27) \qquad \left\{ \begin{array}{rrrr} \lambda_1 = -r^2 z_1 \lambda_2 = & r^4 z_1 \lambda_3 = & -r\lambda_4, \\ r^3 z_2 \lambda_1 = & \lambda_2 = & -r^2 \lambda_3 = & -r^4 z_2 \lambda_4, \\ -r z_2 \lambda_1 = & -r^2 \lambda_2 = & \lambda_3 = & r^2 z_2 \lambda_4, \\ -r^4 \lambda_1 = & r z_1 \lambda_2 = & -r^3 z_1 \lambda_3 = & \lambda_4; \end{array} \right.$$

et puisque $5 = \lambda_1 \lambda_2 \lambda_3 \lambda_4$, on trouve, en multipliant les quatre membres

de ces équations qui occupent le même rang vertical,

$$5 = r^3 z_2^2 \lambda_1^4 = r z_1^2 \lambda_2^4 = r^4 z_1^2 \lambda_3^4 = r^2 z_2^2 \lambda_4^4, \tag{28}$$

c'est-à-dire que 5 est égal à la quatrième puissance d'un de ses sous-facteurs, multiplié par un coefficient complexe dont la norme est 1 ; tandis que toute norme première, autre que 5, est égale au produit de quatre sous-facteurs conjugués et premiers entre eux. D'après cela, 5 n'a réellement qu'un seul sous-facteur ; on peut adopter $\lambda_1 = 1 - r$: 5 sera divisible par sa quatrième puissance, et non par une puissance supérieure ; car on a

$$5 = r^3 z_2^2 \lambda_1^4,$$

et ni r, ni z_2 ne sont divisibles par λ_1.

§ VI.

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. De l'équation

$$A_1 A_2 A_3 A_4 = a_1 a_2 a_3 a_4 . b_1 b_2 b_3 b_4$$

on peut conclure, par une méthode semblable à celle du § IV, que a_1 doit diviser l'un des facteurs du premier membre. Soit $A_2 = a_1 B_1$, il en résultera

$$A_4 = a_2 B_2, \quad A_1 = a_3 B_3, \quad A_3 = a_4 B_4,$$

et, en substituant,

$$B_1 B_2 B_3 B_4 = b_1 b_2 b_3 b_4 ;$$

donc b_1 doit diviser un des conjugués de B. Soit $B_4 = b_1 R_1$, on en conclura

$$B_3 = b_2 R_2, \quad B_2 = b_3 R_3, \quad B_1 = b_4 R_4,$$

et, en substituant,

$$\mathfrak{N}(R_1) = 1 ;$$

on aura donc

$$A_1 = a_3 b_2 R_2.$$

c'est-à-dire que A sera divisible par l'un des conjugués de a, ensuite par l'un des conjugués de b, et que le quotient définitif aura pour norme l'unité.

Lorsque la norme N de A contient comme facteur un nombre premier n élevé à la puissance i, A est successivement divisible i fois par un des sous-facteurs conjugués de n. Soit N′ le quotient de N par n^i, a un sous-facteur de n, B un sous-facteur de N′, on aura

$$A_1 A_2 A_3 A_4 = a_1^i a_2^i a_3^i a_4^i \cdot B_1 B_2 B_3 B_4 ;$$

a_1 diviseur complexe du second membre doit diviser le premier, et conséquemment l'un des quatre facteurs qui le composent ; soit $A_3 = a_1 R_1$, on en conclura

$$A_1 = A_2 R_2, \quad A_4 = A_3 R_3, \quad A_2 = a_4 R_4,$$

et, en substituant,

$$R_1 R_2 R_3 R_4 = a_1^{i-1} a_2^{i-1} a_3^{i-1} a_4^{i-1} \cdot B_1 B_2 B_3 B_4 ;$$

il faudra encore que l'un des facteurs du premier membre soit divisible par a_1, etc.

Si la norme N de A, décomposée en ses facteurs premiers, est le produit $n^{\alpha} . n'^{\beta} . n''^{\gamma} \ldots$, de l'unité, par α fois n, dont un sous-facteur est a, par β fois n', dont un des sous-facteurs est b, par γ fois n'', dont un des sous-facteurs est $c \ldots$, A sera le produit d'un sous-facteur de l'unité, par α sous-facteurs égaux à un ou à plusieurs des conjugués de a, par β sous-facteurs égaux à un ou à plusieurs des conjugués de b, par γ sous-facteurs égaux à un ou à plusieurs des conjugués de $c \ldots$. Ainsi, pour décomposer ce nombre A en ses facteurs premiers, on essayera successivement α fois la division par les conjugués de a, et l'on réussira à toutes les fois (si $n = 5$, $a = \lambda_1$, on pourra diviser de suite A par λ_1^{α}); ensuite on procédera aux β divisions par les conjugués de b, aux γ divisions par les conjugués de $c, \ldots$: le quotient définitif aura pour norme l'unité. De là, et de ce qu'un nombre complexe ne peut être divisible par un sous-facteur d'un nombre premier qui ne divise pas sa norme, on conclura aisément qu'un nombre complexe ne peut être réductible que d'une seule manière en ses facteurs premiers.

Quand il s'agit de trouver le plus grand commun diviseur D, entre

deux nombres complexes A et B, il faut calculer d'abord $\mathfrak{N}(A)$ et $\mathfrak{N}(B)$. Si ces deux normes sont premières entre elles, les nombres complexes A et B sont premiers entre eux, et D ne pouvant avoir pour norme que l'unité, tout calcul ultérieur est inutile. Si $\mathfrak{N}(A)$ et $\mathfrak{N}(B)$ ont un plus grand commun diviseur N, il faut dégager, dans A et dans B, tous les sous-facteurs conjugués des nombres premiers qui divisent N, et ceux-là seulement; il est facile ensuite de composer D. Si N est divisible par 5^t, λ_t est un facteur de D, et il est inutile de s'occuper des facteurs λ_t dans les opérations à effectuer sur A et B.

§ VII.

La somme de deux cinquièmes puissances $(A^5 + B^5)$ est divisible par $(A + B)$; mais cette somme pouvant s'écrire ainsi : $[A^5 + (Br^i)^5]$, sera aussi divisible par $(A + Br^i)$; la somme $(A^5 + B^5)$ est donc divisible par $A + B$, $A + Br$, $A + Br^2$, $A + Br^3$, $A + Br^4$: d'ailleurs elle est égale au produit de ces cinq facteurs. En effet, si l'on représente par $r^{(0)}$, r', r'', r''', r^{IV} les cinq racines de l'équation

$$r^5 - 1 = 0,$$

et si l'on désigne par S_k la somme des produits k à k de ces racines, le produit dont il s'agit peut se mettre sous la forme

$$(A + Br^{(0)})(A + Br')(A + Br'')(A + Br''')(A + Br^{IV})$$
$$= A^5 + S_1 BA^4 + S_2 B^2A^3 + S_3 B^3A^2 + S_4 B^4 A + S_5 B^5 = A^5 + B^5;$$

car, d'après l'équation

$$r^5 - 1 = 0,$$

on a

$$S_1 = S_2 = S_3 = S_4 = 0, \quad S_5 = 1.$$

On a donc, généralement,

$$(29) \quad A^5 + B^5 = (A + B)(A + Br)(A + Br^2)(A + Br^3)(A + Br^4),$$

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 (29) et le premier facteur du second membre le sont aussi;

les quatre derniers facteurs sont complexes et conjugués; leur norme est $\left[\frac{A^5+B^5}{A+B}\right]$. L'équation (29) ayant encore lieu lorsque B est négatif, on peut poser, généralement,

$$\frac{A^5 \pm B^5}{A \pm B} = \mathfrak{N}(A \pm Br); \tag{30}$$

ou, inversement, si l'on désigne par le symbole $sf(N)$ un sous-facteur complexe dont la norme est N, on pourra écrire

$$A \pm Br = sf\left(\frac{A^5 \pm B^5}{A+B}\right). \tag{30 bis}$$

En donnant dans ces formules à A et B des valeurs entières, on a immédiatement les sous-facteurs complexes de nombres premiers ou composés, sur lesquels on peut vérifier les propriétés relatives à la divisibilité des nombres complexes. Lorsqu'on prend $A = B = 1$, l'équation (30 *bis*) donne

$$1 + r = sf(1), \quad 1 - r = sf(5).$$

Voici quelques autres exemples :

(1) $2 + r = sf(11)$,
(2) $2 - r = sf(31)$,
(3) $3 + r = sf(61)$,
(4) $4 + r = sf(5.41)$,
(5) $3 - r = sf(11^2)$,
(6) $5 + 2r = sf(11.41)$,
(7) $4 - r = sf(11.31)$,
(8) $9 - r = sf(11^2.61)$,
(9) $5 - 4r = sf(11.191)$,
(10) $7 + r = sf(11.191)$.

Les trois premiers donnent les sous-facteurs des nombres premiers 11, 31, 61. Du quatrième on déduit, en essayant la division de $(4+r)$ par un sous-facteur de 5,

$$(4 + r) = (1 - r^2)(2 + r^2 - r^3);$$

on a donc

$$2 + r^2 - r^3 = sf(41.).$$

D'après le cinquième exemple, $(3 - r)$ doit être divisible deux fois par un sous-facteur de 11; si l'on essaye successivement la division de $(3 - r)$ par les conjugués de $(2 + r)$, elle réussit pour $(2 + r^2)$, et l'on

trouve

$$(3 - r) = (2 + r^2)(1 - r - r^2) :$$

donc $(1 - r - r^2)$ est aussi un sous-facteur de 11, ce qui se vérifie; on a d'ailleurs

$$(2+r^2) = (1+r^2)(1-r-r^2), \quad \text{d'où} \quad (3-r) = (1+r^2)(1-r-r^2)^2.$$

D'après le sixième exemple, $(5 + 2r)$ doit être divisible par un des sous-facteurs de 11, ensuite par un des sous-facteurs de 41, et le quotient définitif doit avoir pour norme l'unité. Les épreuves de division donnent, en effet,

$$5 + 2r = (2 + r)(2 + r^2 - r^3)(1 + r).$$

Le septième exemple est facile à vérifier, car

$$(2 + r) = sf(11), \quad (2 - r) = sf(31);$$

donc

$$(2 + r)(2 - r) = 4 - r^2 = sf(11.31),$$

et aussi

$$4 - r = sf(11.31).$$

De même pour le huitième exemple, car

$$3 - r = sf(11^2), \quad 3 + r = sf(61);$$

donc

$$(9 - r^2) = sf(11^2.61),$$

et aussi

$$(9 - r) = sf(11^2.61).$$

Le neuvième et le dixième exemple donnent, pour sous-facteurs de (11.191), les deux nombres complexes $(5 - 4r)$ et $(7 + r)$. Les essais de division rendent compte de cette coïncidence; on trouve

$$(5 - 4r) = (2 + r)(4 + 2r^3 + r^4), \quad \text{d'où} \quad 4 + 2r^3 + r^4 = sf(191);$$

et ensuite

$$(7 + r) = (1 + r^3)(2 + r^3)(4 + 2r^3 + r^4).$$

Ainsi, $(5 - 4r)$ et $(7 + r)$ sont divisibles par le même sous-facteur de 191, mais par deux sous-facteurs différents de 11.

Toute norme non divisible par 5, et décomposable en quatre sous-facteurs conjugués de la forme (1), est nécessairement un nombre de la forme $(5i+1)$. En effet, d'après l'équation (17), le nombre complexe A (1) a pour norme $\left\{\left[b_0-\frac{1}{2}(b_1+b_2)\right]^2-5\left[\frac{1}{2}(b_1-b_2)\right]^2\right\}$, b_0, b_1, b_2 ayant les valeurs (15); désignant par a la somme $(\alpha_0+\alpha_1+\alpha_2+\alpha_3+\alpha_4)$ des coefficients de A, on aura

$$b_0 = a^2 - 2(b_1+b_2),$$

et, conséquemment,

$$(31) \qquad \mathfrak{N}(A) = \left[a^2 - 5\left(\frac{b_1+b_2}{2}\right)\right]^2 - 5\left(\frac{b_1-b_2}{2}\right)^2.$$

Si a est un multiple de 5, $\mathfrak{N}(A)$ sera divisible par 5, et A par λ_1, ou par l'un des sous-facteurs de 5. Si $\mathfrak{N}(A)$ n'est pas divisible par 5, a sera premier avec 5; et, employant la notation de M. Gauss, on aura

$$\mathfrak{N}(A) \equiv a^4 \equiv 1 \pmod 5,$$

c'est-à-dire

$$\mathfrak{N}(A) = 5i+1.$$

Cette propriété a été signalée par M. Jacobi (tome VIII de ce Journal, page 171).

La norme de tout nombre complexe A (1) divise une infinité de nombres entiers de la forme $\left(\frac{X^5 \pm Y^5}{X \pm Y}\right)$. En effet, il est toujours possible, et cela d'une infinité de manières, de trouver un nombre complexe B (18), qui, multipliant A, donne un produit (20) dont trois coefficients soient nuls; car ce problème conduit à trois équations du premier degré entre les cinq coefficients de B, et l'on trouve, par une analyse facile, mais longue, des valeurs entières, et cependant encore très-indéterminées, de ces cinq coefficients, qui vérifient les trois équations posées. On aura alors

$$A.B = \gamma_0 + \gamma_i r^i = sf\left(\frac{\gamma_0^5+\gamma_i^5}{\gamma_0+\gamma_i}\right),$$

γ_0 et γ_i dépendant des coefficients de A, et de deux autres entiers arbitraires.

Ces remarques expliquent pourquoi, dans tous les exemples déduits de la formule (30) ou (30 *bis*), on ne trouve que des normes décomposables en facteurs premiers de la forme 5 et $(5i+1)$. Elles indiquent aussi qu'en augmentant le nombre de ces exemples, on parviendrait à composer une table des sous-facteurs des nombres premiers $(5i+1)$, soit directement, soit par déduction, comme on l'a fait plus haut à l'égard de 41 et de 191. Il suffit déjà de calculer les cinquièmes puissances des nombres au-dessous de 12, pour obtenir, à peu d'exceptions près, les sous-facteurs des nombres premiers $(5i+1)$ inférieurs à 1021, avec ceux de beaucoup d'autres nombres, supérieurs à cette limite.

§ VIII.

Quand A et B sont des nombres complexes, il est préférable, pour ce qui suit, de donner à l'équation (29) la forme suivante :

$$(32)\quad A^5+B^5=(A+B)(Ar+Br^4)(Ar^2+Br^3)(Ar^3+Br^2)(Ar^4+Br),$$

laquelle en est une conséquence; car les quatre derniers facteurs de (32), respectivement divisés par la puissance de r qui accompagne A, donnent, dans un autre ordre, les quatre derniers facteurs de (29), et le produit des diviseurs est $r^{10}=1$.

Si l'on désigne par M, M′, M″, M‴, M$^{\text{IV}}$ les cinq facteurs du second membre de l'équation (32), les accents n'ayant plus ici la signification de ceux du tableau (7), on reconnaît facilement que ces facteurs vérifient les dix équations

$$(33)\quad \begin{cases} (1)\quad M''+M'''=z_2M, & (6)\quad M^{\text{IV}}+M'=z_1M,\\ (2)\quad M'''+M^{\text{IV}}=z_2M', & (7)\quad M+M''=z_1M',\\ (3)\quad M^{\text{IV}}+M=z_2M'', & (8)\quad M'+M'''=z_1M'',\\ (4)\quad M+M'=z_2M''', & (9)\quad M''+M^{\text{IV}}=z_1M''',\\ (5)\quad M'+M''=z_2M^{\text{IV}}, & (10)\quad M'''+M=z_1M^{\text{IV}}, \end{cases}$$

qui n'en comportent réellement que trois distinctes, puisque A et B étant connus, ou les deux premiers facteurs $(A+B)$, $(Ar+Br^4)$, les trois autres doivent s'ensuivre.

Il résulte des relations (33), qu'un nombre complexe dont la

norme n'est pas l'unité, ne peut diviser deux des cinq facteurs $M^{(i)}$, sans diviser tous les autres. Par exemple, si un nombre complexe δ divise M et M', d'après la sixième (33), δ divisera M^{IV}, d'après la septième M'', d'après la première M'''. Ainsi le second membre de l'équation (32) sera divisible par δ^5, et les cinq quotients des $M^{(i)}$ par δ vérifieront encore les équations (33). On peut supposer que l'on ait ainsi divisé les $M^{(i)}$ par tous les sous-facteurs communs à deux d'entre eux, et par conséquent aux trois autres. Alors l'équation (32) pourra se mettre sous la forme

$$A^5 + B^5 = K^5 . m . m' . m'' . m''' . m^{IV}, \tag{34}$$

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 équations (33).

On peut toujours supposer que A et B sont premiers entre eux, car si δ est le plus grand diviseur complexe, commun à A et B, δ^5 divisera A^5, B^5, et nécessairement K^5 dans l'équation (34), et l'on pourra supprimer ce diviseur commun. Alors, si A et B sont premiers entre eux, K ne pourra être que le sous-facteur de 5 : en effet, les deux équations

$$A + B = M = Km, \quad Ar + Br^4 = M' = Km'$$

donnent

$$A(r - r^4) = K(m' - r^4 m), \quad B(r - r^4) = K(rm - m'),$$

et K ne pouvant diviser à la fois A et B, qui sont premiers entre eux, divisera nécessairement $(r - r^4)$ ou $(1 - r^3)$; K ne pourra donc être que le sous-facteur de 5, à la première puissance seulement.

La somme des cinquièmes puissances de deux conjugués directs d'un nombre complexe imaginaire A est le produit de cinq nombres complexes réels. Les deux sommes $(A_1^5 + A_4^5)$ et $(A_2^5 + A_3^5)$ sont conjuguées, et leur produit donne cinq facteurs entiers. En effet, la formule (32) donne

$$\begin{cases} A_1^5 + A_4^5 = (A_1 + A_4)(A'_1 + A^{IV}_4)(A''_1 + A'''_4)(A'''_1 + A''_4)(A^{IV}_1 + A'_4), \\ A_2^5 + A_3^5 = (A_2 + A_3)(A'_2 + A^{IV}_3)(A''_2 + A'''_3)(A'''_2 + A''_3)(A^{IV}_2 + A'_3), \end{cases} \tag{35}$$

en reprenant ici, pour les accents supérieurs, la même signification qu'au tableau (7), lequel fournit les valeurs suivantes :

$$(36)\quad \begin{cases} A_1+A_4=2\alpha_0+(\alpha_1+\alpha_4)z_1+(\alpha_2+\alpha_3)z_2, & A_2+A_3=2\alpha_0+(\alpha_1+\alpha_4)z_2+(\alpha_2+\alpha_3)z_1,\\ A_1^{IV}+A_4'=2\alpha_1+(\alpha_2+\alpha_0)z_1+(\alpha_3+\alpha_4)z_2, & A_2'''+A_3''=2\alpha_1+(\alpha_2+\alpha_0)z_2+(\alpha_3+\alpha_4)z_1,\\ A_1'''+A_4''=2\alpha_2+(\alpha_3+\alpha_1)z_1+(\alpha_4+\alpha_0)z_2, & A_2'+A_3^{IV}=2\alpha_2+(\alpha_3+\alpha_1)z_2+(\alpha_4+\alpha_0)z_1,\\ A_1''+A_4'''=2\alpha_3+(\alpha_4+\alpha_2)z_1+(\alpha_0+\alpha_1)z_2, & A_2^{IV}+A_3'=2\alpha_3+(\alpha_4+\alpha_2)z_2+(\alpha_0+\alpha_1)z_1,\\ A_1'+A_4^{IV}=2\alpha_4+(\alpha_0+\alpha_3)z_1+(\alpha_1+\alpha_2)z_2, & A_2''+A_3'''=2\alpha_4+(\alpha_0+\alpha_3)z_2+(\alpha_1+\alpha_2)z_1, \end{cases}$$

pour les facteurs des seconds membres des équations (35). Les facteurs de $(A_2^5+A_3^5)$ sont évidemment les conjugués de ceux qui appartiennent à $(A_1^5+A_4^5)$. Les cinq nombres que donnent les produits de deux facteurs conjugués sont

$$(37)\quad \begin{cases} (A_1+A_4)(A_2+A_3)=\left(2\alpha_0-\frac{\alpha_1+\alpha_1+\alpha_2+\alpha_3}{2}\right)^2-5\left(\frac{\alpha_1+\alpha_4-\alpha_2-\alpha_3}{2}\right)^2,\\ (A_1^{IV}+A_4')(A_2'''+A_3'')=\left(2\alpha_1-\frac{\alpha_2+\alpha_0+\alpha_3+\alpha_4}{2}\right)^2-5\left(\frac{\alpha_2+\alpha_0-\alpha_3-\alpha_4}{2}\right)^2,\\ (A_1'''+A_4'')(A_2'+A_3^{IV})=\left(2\alpha_2-\frac{\alpha_3+\alpha_1+\alpha_4+\alpha_0}{2}\right)^2-5\left(\frac{\alpha_3+\alpha_1-\alpha_4-\alpha_0}{2}\right)^2,\\ (A_1''+A_4''')(A_2^{IV}+A_3')=\left(2\alpha_3-\frac{\alpha_4+\alpha_2+\alpha_0+\alpha_1}{2}\right)^2-5\left(\frac{\alpha_4+\alpha_2-\alpha_0-\alpha_1}{2}\right)^2,\\ (A_1'+A_4^{IV})(A_2''+A_3''')=\left(2\alpha_4-\frac{\alpha_0+\alpha_3+\alpha_1+\alpha_2}{2}\right)^2-5\left(\frac{\alpha_0+\alpha_3-\alpha_1-\alpha_2}{2}\right)^2. \end{cases}$$

On reconnaît facilement qu'ils sont entiers, et que leur somme est nulle.

La différence $(A_1^5-A_4^5)$ est le produit de λ_1^5 par cinq facteurs complexes et réels. La différence $(A_2^5-A_3^5)$ est le produit de λ_2^5 par cinq autres facteurs complexes et réels, conjugués des cinq premiers. En effet, la formule (32) donne aussi

$$(38)\quad \begin{cases} A_1^5-A_4^5=(A_1-A_4)(A_1'-A_4^{IV})(A_1''-A_4''')(A_1'''-A_4'')(A_1^{IV}-A_4'),\\ A_2^5-A_3^5=(A_2-A_3)(A_2'-A_3^{IV})(A_2''-A_3''')(A_2'''-A_4'')(A_2^{IV}-A_4'), \end{cases}$$

et le tableau (7) conduit, par des transformations faciles, aux valeurs

$$(39)\quad \begin{cases} A_1 - A_4 = r^2\lambda_1[(\alpha_2-\alpha_3)-(\alpha_1-\alpha_4)z_2], & A_2 - A_3 = r^4\lambda_2[(\alpha_2-\alpha_3)-(\alpha_1-\alpha_4)z_1], \\ A_1' - A_4^{iv} = r^2\lambda_1[(\alpha_1-\alpha_2)-(\alpha_0-\alpha_3)z_2], & A_2'' - A_3''' = r^4\lambda_2[(\alpha_1-\alpha_2)-(\alpha_0-\alpha_3)z_1], \\ A_1'' - A_4''' = r^2\lambda_1[(\alpha_0-\alpha_1)-(\alpha_4-\alpha_2)z_2], & A_2^{iv} - A_3' = r^4\lambda_2[(\alpha_0-\alpha_1)-(\alpha_4-\alpha_2)z_1], \\ A_1''' - A_4'' = r^2\lambda_1[(\alpha_4-\alpha_0)-(\alpha_3-\alpha_1)z_2], & A_2' - A_3^{iv} = r^4\lambda_2[(\alpha_4-\alpha_0)-(\alpha_3-\alpha_1)z_1], \\ A_1^{iv} - A_4' = r^2\lambda_1[(\alpha_3-\alpha_4)-(\alpha_2-\alpha_0)z_2], & A_2''' - A_3'' = r^4\lambda_2[(\alpha_3-\alpha_4)-(\alpha_2-\alpha_0)z_1]; \end{cases}$$

d'où l'on conclut

$$(40)\qquad A_1^5 - A_4^5 = \lambda_1^5 Z_2, \quad A_2^5 - A_3^5 = \lambda_2^5 Z_1,$$

en désignant par Z_2 et Z_1 deux produits réels et conjugués.

Les entiers (37), et ceux que donneraient les produits des facteurs conjugués de Z_2 et Z_1, sont des nombres qui se déduisent de A, et que l'on pourrait appeler ses *normes latérales*. Ils ne sont plus essentiellement positifs, ni toujours de la forme $(5i+1)$. Leur étude conduit à des remarques importantes, mais qui sont étrangères à l'objet du Mémoire actuel.

DEUXIÈME PARTIE.

§ I.

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

$$(1)\qquad A^5 + B^5 + C^5 = 0.$$

On peut supposer que A, B, C sont premiers entre eux ; car si un même sous-facteur δ, d'un nombre premier dont la norme n'est pas l'unité, divise à la fois A, B, C, on pourra diviser l'équation par δ^5, et le quotient sera encore la somme de trois cinquièmes puissances. On agira de même pour tout diviseur complexe commun aux trois nombres A, B, C. Ces trois nombres n'étant plus divisibles tous les trois par un même sous-facteur, deux quelconques sont aussi premiers entre eux ; car si A et B avaient un sous-facteur commun δ, δ^5 diviserait $A^5 + B^5$, et par suite C^5 : donc C serait aussi divisible par δ ; A, B, C ne seraient donc pas premiers entre eux.

Un des trois nombres A, B, C est nécessairement divisible par

$(1-r)=\lambda_1$ sous-facteur de 5. En effet, on a généralement

$$(2)\quad\begin{cases}(A+B+C)^5=A^5+B^5+C^5\\ +5(A+B)(B+C)(C+A)[(A+B+C)^2-(AB+CA+BC)],\end{cases}$$

et l'on aura, en vertu de l'équation proposée,

$$(3)\quad\begin{cases}(A+B+C)^5\\ =5(A+B)(B+C)(C+A)[(A+B+C)^5-(AB+CA+BC)].\end{cases}$$

Or 5 égale $r^3z_2^2\lambda_1^4$; le second membre de l'équation (3) est donc divisible par λ_1, le premier doit donc l'être: étant une cinquième puissance, il sera divisible par λ_1^5; le second devant l'être aussi, et 5 n'étant divisible que par λ_1^4, il faudra que l'un des quatre autres facteurs soit divisible par λ_1. Si c'est le dernier, puisque $(A+B+C)$ est divisible par λ_1, il faudra que $(AB+CA+BC)$ le soit, et par suite aussi $(A^2+B^2+C^2)$; les sommes des coefficients de A, B, C, divisées par 5, donneront les résidus ± 1, ± 2, et les sommes des coefficients de leurs carrés les résidus $+1$, -1: or la somme de trois résidus $+1$ et -1 ne peut être nulle, ni égale à 5; donc il faudra qu'une des sommes des coefficients de A, de B, de C, donne le résidu zéro, c'est-à-dire que l'un des trois nombres A, B, C soit divisible par λ_1. Sinon, le dernier facteur du second membre de l'équation précédente n'admettant pas le diviseur λ_1, il faudra que ce soit un des trois facteurs $(A+B)$, $(C+A)$, $(B+C)$, qui l'admette; alors, puisque $(A+B+C)$ est divisible par λ_1, C, B ou A le sera aussi. Ainsi un des trois nombres A, B, C est nécessairement divisible par λ_1; nous supposerons que ce soit C.

Si l'on a à résoudre l'équation

$$A^5+B^5=z_1^2C^5,$$

il est facile de voir que C doit être divisible par λ_1: en effet, l'équation (2) devient alors

$$(4)\quad\begin{cases}(A+B+C)^5=(z_1^2+1)C^5\\ +5(A+B)(B+C)(C+A)[(A+B+C)^2-(AB+CA+BC)],\end{cases}$$

et l'on a

$$5 = r^3 z_2^2 \lambda_1^4, \quad z_1^2 + 1 = 2 - z_1 = (1 - r)(1 - r^4) = - r^4 \lambda_1^2 ;$$

donc le second membre de l'équation (4) est divisible par λ_1^2 ; (A+B+C) doit donc être divisible par λ_1, le second membre par λ_1^5, d'où C par λ_1, et par suite aussi (A+B).

Si l'on se propose l'équation

$$A^5 + B^5 = z_1 C^5,$$

il faut encore que C soit divisible par λ_1 : en effet, on a généralement

$$(A + B - 2C)^2 = A^5 + B^5 - 32C^5$$
$$+ 5(A + B)(A - 2C)(B - 2C)[(A + B - 2C)^2 + 2C(A + B) - AB],$$

et, d'après l'équation à résoudre, on aura

$$(A + B - 2C)^2 = (z_1 - 2) C^5$$
$$+ 5\{(A + B)(A - 2C)(B - 2C)[(A + B - 2C)^2 + 2C(A + B) - AB] - 6C^5\};$$

or $5 = r^3 z_2^2 \lambda_1^4$, $z_1 - 2 = r^4 \lambda_1^2$, donc le second membre de l'équation précédente est divisible par λ_1^2 ; (A + B − 2C) doit donc être divisible par λ_1, le second membre par λ_1^5, d'où C, et par suite (A + B) par λ_1.

On démontre de la même manière que les équations

$$A^5 + B^5 = z_2^2 C^5, \quad A^5 + B^5 = z_2 C^5$$

ne peuvent exister si C n'est pas divisible par λ_1. Ainsi les cinq équations

$$(5) \qquad \begin{cases} A^5 + B^5 = (-C)^5, \\ A^5 + B^5 = z_1 C^5, \quad A^5 + B^5 = z_2 C^5, \\ A^5 + B^5 = z_1^2 C^5, \quad A^5 + B^5 = z_2^2 C^5, \end{cases}$$

sont telles, que le second membre est nécessairement divisible par λ_1^5, A et B étant premiers avec λ_1.

§ II.

On démontre que C, dans les équations (5), est nécessairement divisible par λ_1^2 ; en effet, ni A, ni B ne sont divisibles par λ_1, et l'on

pourra poser

$$A = p\lambda_1 + q, \quad B = p'\lambda_1 + q',$$

p et p' étant des quotients complexes, q et q' des nombres entiers, respectivement égaux aux sommes des coefficients de A et B. On aura alors

$$A^5 = \lambda_1^5 p^5 + 5\lambda_1^4 p^4 q + 10\lambda_1^3 p^3 q^2 + 10\lambda_1^2 p^2 q^3 + 5\lambda_1 p q^4 + q^5,$$
$$B^5 = \lambda_1^5 p'^5 + 5\lambda_1^4 p'^4 q' + 10\lambda_1^3 p'^3 q'^2 + 10\lambda_1^2 p'^2 q'^3 + 5\lambda_1 p' q'^4 + q'^5 ;$$

$(A^5 + B^5)$ devant être divisible par λ_1^5, il faudra que $(q^5 + q'^5)$, nombre entier, soit aussi divisible par λ_1^5 : il ne suffira pas alors que $(q^5 + q'^5)$ soit divisible par $5 = r^3 z_2^2 \lambda_1^4$, il faudra qu'il soit divisible par $25 = r z_2^4 \lambda_1^8$. Cela posé, $(A^5 + B^5)$ pourra s'écrire ainsi :

$$A^5 + B^5 = \lambda_1^5 \left[p^5 + p'^5 + r^3 z_2^2 (pq^4 + p'q'^4) \right] + Q \cdot \lambda_1^6,$$

Q étant un quotient complexe entier. Lorsqu'on substituera cette valeur dans l'une quelconque des équations (5), on pourra remplacer le second membre par $\lambda_1^5 z_h^i R^5$, diviser par λ_1^5, et il faudra que la somme

$$\left[p^5 + q^5 + r^3 z_2^2 (pq^4 + p'q'^4) - z_h^i R^5 \right]$$

soit divisible par λ_1, ou qu'elle s'annule pour $r = 1$; c'est-à-dire que, si l'on substitue, dans cette expression, aux nombres complexes les sommes de leurs coefficients, et aux entiers leurs résidus relatifs au module 5, le résidu total doit être nul : or soient a, a', ρ les résidus des sommes des coefficients dans p, p', R, 2 étant celui de z_2 et de z_1, on a

$$\rho^5 \equiv \rho, \ a^5 \equiv a, \ a'^5 \equiv a', \ q^4 \equiv 1, \ q'^4 \equiv 1, \ 2^2 \equiv -1 \pmod 5,$$

et le résidu total de l'expression précédente devient $[a + a' - (a + a') - 2^i \rho]$ ou simplement $[-2^i \rho]$; or ce résidu doit être nul, donc $\rho \equiv 0 \pmod 5$, c'est-à-dire que R est divisible par λ_1, et R^5 par λ_1^5 ; donc C est divisible par λ_1^2, et C^5 par λ_1^{10}.

§ III.

Ainsi, dans l'une quelconque des équations (5), le premier membre

$(A^5 + B^5)$ est divisible par λ_1^{10}, A et B étant premiers avec λ_1. Ce premier membre étant décomposé en deux facteurs, qui sont, lorsqu'on pose $A + B = t$, d'où $B = t - A$,

$$t.(t^4 - 5t^3 A + 10t^2 A^2 - 10t A^3 + 5A^4),$$

les deux facteurs de ce produit ne peuvent admettre de diviseur commun qu'une puissance de λ_1; alors, le second ne peut être divisible que par λ_1^4, ou 5, et t par λ_1^6, sans quoi A devrait être aussi divisible par λ_1, et t et A, par suite A et B, ne seraient pas premiers entre eux.

Donc, dans la décomposition du second facteur en quatre autres, ainsi qu'il suit :

$$A^5 + B^5 = (A + B)(Ar + Br^4)(Ar^2 + Br^3)(Ar^3 + Br^2)(Ar^4 + Br),$$

$A + B$ sera divisible par λ_1^6, et les autres facteurs seront chacun divisibles par λ_1 seulement. De là suit que, pour satisfaire à l'une des équations (5), si l'on pose

$$A + B = \lambda_1 M,\ Ar + Br^4 = \lambda_1 M',\ Ar^2 + Br^3 = \lambda_1 M'',$$
$$Ar^3 + Br^2 = \lambda_1 M''',\ Ar^4 + Br = \lambda_1 M^{IV},\ C = \lambda_1 R,$$

on aura à vérifier l'équation

$$M.M'.M''.M'''.M^{IV} = z_h^j R^5, \tag{6}$$

M et R^5 étant divisibles par λ_1^5, et aucun des facteurs M', M'', M''', M^{IV} ne l'étant par λ_1. L'indice h est 1 ou 2; alors l'exposant j est 0, 1, ou 2: car, dans le cas où j surpasse 2, on peut remplacer $z_1^j R^5$ ou $z_2^j R^5$ par $z_2^{5-j}[(-1)^j z_1 R]^5$ ou $z_1^{5-j}[(-1)^j z_2 R]^5$, et prendre $(5-j)$ pour j, et $[(-1)^j z_1 R]$ ou $[(-1)^j z_2 R]$ pour R.

Les facteurs $M^{(i)}$, de l'équation (6), doivent vérifier les dix équations (première partie, § VIII) :

$$(7)\quad \begin{cases} (1)\ M'' + M''' = z_2 M, & (6)\ M^{IV} + M' = z_1 M, \\ (2)\ M''' + M^{IV} = z_2 M', & (7)\ M + M'' = z_1 M', \\ (3)\ M^{IV} + M = z_2 M'', & (8)\ M' + M''' = z_1 M'', \\ (4)\ M + M' = z_2 M''', & (9)\ M'' + M^{IV} = z_1 M''', \\ (5)\ M' + M'' = z_2 M^{IV} & (10)\ M''' + M = z_1 M^{IV}. \end{cases}$$

On peut supposer que les facteurs $M^{(i)}$ n'ont plus aucun diviseur complexe commun dont la norme ne serait pas l'unité, puisque les équations (7) démontrent qu'un tel diviseur δ, commun à deux de ces facteurs, le sera à tous, et conséquemment à R; on pourra donc diviser par δ^5 les deux membres de l'équation (6), qui conservera la même forme; et les quotients des $M^{(i)}$ par δ vérifieront toujours les équations (7). Alors, à chaque diviseur complexe et premier f, de R, correspondra un diviseur f^5 du second membre de l'équation (6), lequel devra entrer tout entier dans la composition d'un des facteurs $M^{(i)}$, et non se partager entre eux; de là résulte enfin que les facteurs $M^{(i)}$ seront tous des cinquièmes puissances de nombres complexes, multipliées par des sous-facteurs de l'unité, et qu'on satisfera à l'équation (6), en posant

$$(8)\quad M=\nu\mu^5,\quad M'=\nu'\mu'^5,\quad M''=\nu''\mu''^5,\quad M'''=\nu'''\mu'''^5,\quad M^{IV}=\nu^{IV}\mu^{IV5}.$$

Les coefficients $\nu^{(i)}$, ayant pour norme l'unité, seront tous de la forme $r^k z_1^i$, ou $r^k z_2^i$; z_1 ou z_2 excluant z_2 ou z_1, en vertu de la relation

$$z_2 z_1 = -1.$$

L'exposant k de r est moindre que 5, puisque $r^{k+5l}=r^k$; l'exposant i peut aussi être regardé comme moindre que 5, car on peut remplacer $z_h^{i+5l}\mu^{(j)5}$ par $z_h^i[z_h^l\mu^{(j)}]^5$ et prendre $z_h^l\mu^{(j)}$ pour $\mu^{(j)}$.

On peut réduire à l'unité l'un des coefficients $\nu^{(j)}$, qui est égal à $r^k z_1^i$ ou $r^k z_2^i$, dans les valeurs (8), en multipliant, dans l'équation (6), chacun des nombres $M^{(i)}$ et R, par $r^{5-k}z_2^i$ ou $r^{5-k}z_1^i$, ce qui ne troublera pas l'équation (6), et ce qui n'empêchera pas les nouvelles valeurs de $M^{(i)}$ de vérifier les équations (7). Nous supposerons qu'on ait ainsi réduit à l'unité le coefficient ν^{IV} dans M^{IV}, qui n'est pas divisible par λ_1. On aura ainsi les valeurs

$$(8\,bis)\quad M=\nu\mu^5,\quad M'=\nu'\mu'^5,\quad M''=\nu''\mu''^5,\quad M'''=\nu'''\mu'''^5,\quad M^{IV}=\mu^{IV5},$$

§ IV.

Si l'on substitue ces valeurs (8 *bis*) dans les équations (7), qui n'en comportent réellement que trois distinctes, les deuxième, troisième et

cinquième de ces équations deviennent

$$(9)\qquad \begin{cases} \nu'''\mu'''^5 + \mu^{IV5} = z_2\nu'\mu'^5, \\ \mu^{IV5} + \nu\mu^5 = z_2\nu''\mu''^5, \\ \nu'\mu'^5 + \nu''\mu''^5 = z_2\mu^{IV5}. \end{cases}$$

Si l'on prend tous les nombres complexes compris dans ces trois équations comme premiers conjugués, en leur donnant l'accent $_1$ en bas, et qu'on change r en r^4, on obtiendra les quatrièmes conjugués, lesquels serviraient à résoudre l'équation $A_4^5 + B_4^5 = z_h^i C_4^5$, et l'on aura les six équations

$$\begin{aligned} \nu'''_1\mu'''^5_1 + \mu^{IV5}_1 &= z_2\nu'_1\mu'^5_1, & \nu'''_4\mu'''^5_4 + \mu^{IV5}_4 &= z_2\nu'_4\mu'^5_4, \\ \mu^{IV5}_1 + \nu_1\mu^5_1 &= z_2\nu''_1\mu''^5_1, & \mu^{IV5}_4 + \nu_4\mu^5_4 &= z_2\nu''_4\mu''^5_4, \\ \nu'_1\mu'^5_1 + \nu''_1\mu''^5_1 &= z_2\mu^{IV5}_1, & \nu'_4\mu'^5_4 + \nu''_4\mu''^5_4 &= z_2\mu^{IV5}_4, \end{aligned}$$

lesquelles donnent par soustraction

$$(10)\qquad \begin{cases} (\nu'''_1\mu'''^5_1 - \nu'''_4\mu'''^5_4) + (\mu^{IV5}_1 - \mu^{IV5}_4) = z_2(\nu'_1\mu'^5_1 - \nu'_4\mu'^5_4), \\ (\mu^{IV5}_1 - \mu^{IV5}_4) + (\nu_1\mu^5_1 - \nu_4\mu^5_4) = z_2(\nu''_1\mu''^5_1 - \nu''_4\mu''^5_4), \\ (\nu'_1\mu'^5_1 - \nu'_4\mu'^5_4) + (\nu''_1\mu''^5_1 - \nu''_4\mu''^5_4) = z_2(\mu^{IV5}_1 - \mu^{IV5}_4). \end{cases}$$

Or la différence $(\mu^{IV5}_1 - \mu^{IV5}_4)$ des cinquièmes puissances de deux conjugués directs d'un même nombre complexe est divisible par λ_1^5 (première partie, § VIII), de plus μ_1^5 et μ_4^5 sont tous les deux divisibles par λ_1^5, puisque M l'est; alors la deuxième (10) exige que $(\nu''_1\mu''^5_1 - \nu''_4\mu''^5_4)$ le soit; la troisième, qu'il en soit de même de $(\nu'_1\mu'^5_1 - \nu'_1\mu'^5_4)$; enfin, la première, que $(\nu'''_1\mu'''^5_1 - \nu'''_4\mu'''^5_4)$ soit aussi divisible par λ_1^5.

On peut écrire ces trois différences de la manière suivante :

$$(11)\qquad \begin{cases} (\nu'_1 - \nu'_4)\mu'^5_1 + \nu'_4(\mu'^5_1 - \mu'^5_4), \\ (\nu''_1 - \nu''_4)\mu''^5_1 + \nu''_4(\mu''^5_1 - \mu''^5_4), \\ (\nu'''_1 - \nu'''_4)\mu'''^5_1 + \nu'''_4(\mu'''^5_1 - \mu'''^5_4). \end{cases}$$

Les dernières parties sont divisibles par λ_1^5, d'après ce qu'on vient de dire; μ', μ'', μ''' sont premiers avec λ_1 : donc il faudra que les trois dif-

férences

$$(\nu'_1 - \nu'_4), \quad (\nu''_1 - \nu''_4), \quad (\nu'''_1 - \nu'''_4)$$

soient divisibles par λ_1^5. Chacun des coefficients $\nu^{(i)}$ est de la forme $r^h z_h$; en y changeant r en r^4, il devient $r^{4h} z_h^i$, et l'une quelconque des trois différences précédentes est de la forme $z_h^i r^k (1 - r^{3k})$. Or, si k n'est pas nul, cette quantité n'est divisible que par λ_1, et non par λ_1^5; donc il faut que $k = 0$.

Ainsi les coefficients ν', ν'', ν''' se réduisent essentiellement à des puissances de z_1 ou de z_2, et ne contiennent pas de facteur r isolé. Restera le coefficient ν de μ^5; mais étant le seul qui puisse contenir r^k, il faudra nécessairement que $k = 0$, ou 5, pour que l'équation (6) soit vérifiée.

§ V.

Ainsi, μ étant divisible par λ_1, $\mu', \mu'', \mu''', \mu^{IV}$ ne l'étant pas, le coefficient de μ^{IV^5} étant réduit à l'unité, les coefficients des autres $\mu^{(i)^5}$ seront seulement des puissances de z_1 ou de z_2. Les cas de $h = 1$ et de $h = 2$ se traitant de la même manière, il suffit de considérer l'un d'eux; soit donc $h = 1$. On peut réduire les coefficients à ne contenir que des puissances de z_1, en remplaçant $z_2^i \mu^{(j)^5}$ par $z_1^{5-i}[(-1)^i z_2 \mu^{(j)}]^5$, et prenant $[(-1)^i z_2 \mu^{(j)}]$ pour $\mu^{(j)}$. On aura ainsi, pour vérifier l'équation (6), le tableau définitif

$$(12) \quad \begin{cases} M = z_1^i \mu^5, \ M' = z_1^{i'} \mu'^5, \ M'' = z_1^{i''} \mu''^5, \ M''' = z_1^{i'''} \mu'''^5, \ M^{IV} = \mu^{IV^5}, \\ i + i' + i'' + i''' = j + 5l, \ R = \mu \mu' \mu'' \mu''' \mu^{IV} z_1^l. \end{cases}$$

Chacun des exposants i, i', i'', i''' est au plus égal à 4, j au plus égal à 2; donc l sera au plus égal à 3, et l'on aura un nombre limité de valeurs de ces exposants, correspondants à $j = 0, 1, 2$, à $l = 0, 1, 2, 3$.

Or, en examinant avec attention tous ces systèmes, les valeurs (12) qui correspondent à chacun d'eux étant substituées dans les équations (7), on trouve toujours qu'au moins une de ces équations se réduit à la forme

$$(13) \qquad m''^5 + m'''^5 = z_h^{j'} . m'^5,$$

h étant 1 ou 2, j' étant 0, ou 1, ou 2.

En effet, tous ces systèmes se groupent en trois cas généraux :

1°. Ou l'un des exposants est nul, soit $i' = 0$; alors la sixième équation (7) donne

$$\mu^{\text{IV}5} + \mu'^5 = z_1^{i+1}\mu^5;$$

2°. Ou deux des quatre exposants sont égaux, soit $i''' = i''$; alors la première équation (7) donne

$$\mu''^5 + \mu'''^5 = z_1^{i-i''-1}(-\mu)^5;$$

3°. Ou enfin les quatre exposants sont inégaux et aucun n'est nul, ce qui ne peut avoir lieu que pour $j' = 0$, $l = 2$, ces exposants étant 1, 2, 3, 4, dans un ordre quelconque; alors, soit $i''' = 1$, la dixième équation (7) donne

$$\mu'''^5 + (-\mu^{\text{IV}})^5 = z_1^{i-1}(-\mu)^5.$$

Si, dans l'équation (13), j' n'est pas nul, et si m' n'est pas μ, qui est seul divisible par λ_1, cette équation est impossible, et le système correspondant de valeurs des exposants i, i', i'', i''' est inadmissible. Il en est de même encore quand, j' étant nul, μ n'est pas un des trois nombres m', m'', m'''. Ces cas d'impossibilité immédiate sont nombreux, et il ne reste qu'un petit nombre de systèmes admissibles, c'est-à-dire tels que, j' étant nul, μ est l'un des trois nombres m', m'', m'''; ou tels que, j' n'étant pas nul, m' est précisément μ.

Alors, si l'équation (13) est semblable à celle des équations (5) d'où l'on est parti, l'impossibilité de l'équation primitive sera établie de suite, puisqu'une solution supposée de cette équation conduit à une solution en nombres beaucoup plus petits; la grandeur d'un nombre complexe se mesurant par celle de sa norme.

Si l'équation (13) est une des équations (5) autre que la première d'où l'on est parti, on traitera de nouveau cette seconde équation (13), qui conduira à une troisième de la même forme générale; si cette troisième est semblable à la seconde ou à la première, leur impossibilité sera encore établie. Si elle est encore différente, on en déduira une quatrième équation, toujours de la forme (13).

En continuant ainsi, on retombera nécessairement, après cinq transformations au plus, sur une équation semblable à l'une de celles qui la précèdent, dans la série de ces équations dépendantes; d'où résultera leur impossibilité.

Les équations (5) ne sont donc possibles qu'en nombres complexes dont la norme est infinie.

§ VI.

Toutefois, il existe un cas singulier qu'il est nécessaire de traiter à part: car la démonstration qui précède suppose implicitement que les nombres $\mu^{(i)}$ contiennent d'autres facteurs complexes que ceux dont la norme est l'unité; et l'on doit se demander si les valeurs (8) ne pourraient pas vérifier l'équation (6), en supposant que μ', μ'', μ''', μ^{IV} aient pour norme l'unité, et que μ, contenant λ_1 facteur indispensable, fût un nombre complexe ayant la même norme que R.

Or on peut démontrer, plus généralement, qu'il n'est pas possible que deux facteurs, par exemple M'' et M''', n'aient pour norme que l'unité. En effet, soit

$$(14) \qquad M = m\lambda_1^5, \quad M'' = \nu'', \quad M''' = \nu''',$$

m étant un nombre complexe, et ν'', ν''' étant de la forme $r^k z_h^i$, k inférieur à 5, mais i n'ayant plus de limite. La première des équations (7) et sa quatrième conjuguée deviennent

$$(14\ bis) \qquad \begin{cases} \nu_1'' + \nu_1''' = z_2 m_1 \lambda_1^5, \\ \nu_4'' + \nu_4''' = -z_2 m_4 \lambda_1^5; \end{cases}$$

car $\lambda_4^5 = -\lambda_1^5$, et, en retranchant la seconde de la première, il viendra

$$(15) \qquad (\nu_1'' - \nu_4'') + (\nu_1''' - \nu_4''') = z_2 (m_1 + m_4) \lambda_1^5.$$

Soit en général $n_1 = r^k z_h^i$, d'où $n_4 = r^{4k} z_h^i$, et $n_1 - n_4 = r^k (1 - r^{3k}) z_h^i$; on reconnaît facilement que $r^k (1 - r^{3k})$ est toujours égal à $\pm \lambda_1$, multiplié par $z_2 r^2$, ou par r^2 seulement: car

$$\begin{aligned} \text{Si } k = 1, \quad \text{on a} \quad & r(1 - r^3) = -r^2 z_2 \lambda_1, \\ k = 2, \quad & r^2 (1 - r) = r^2 \lambda_1, \\ k = 3, \quad & r^3 (1 - r^4) = -r^2 \lambda_1, \\ k = 4, \quad & r^4 (1 - r^2) = r^2 z_2 \lambda_1. \end{aligned}$$

Ainsi, si les exposants de r dans ν'' et ν''' ne sont pas nuls, l'équation (15), divisée par λ_1 et multipliée par r^3, sera de la forme

$$Z + Z' = r^3 z_2 (m_1 + m_4) \lambda_1^4, \tag{16}$$

Z et Z' étant deux puissances de z_1 ou de z_2.

Il ne se peut, d'ailleurs, que les exposants de r dans ν'' et ν''' soient nuls; en effet, si l'un d'eux seulement est nul, l'équation (15) exigera qu'une puissance de z_1 ou de z_2 soit divisible par λ_1^4, ce qui ne peut être; si ces deux exposants sont nuls, le premier membre de l'équation (15) s'évanouit, et l'on a nécessairement $(m_1 + m_4) = 0$, ce qui exige que l'on ait, ou $m_1 = 0$, cas inadmissible, ou $m_1 = \lambda_1^5$, cas facile à traiter, et que nous écartons pour le moment.

Il reste donc à chercher si l'équation (16) est possible, ou si la somme de deux puissances de z_1 ou de z_2 peut être divisible par λ_1^4. On ne peut avoir $Z + Z' = 0$, puisque, comme il vient d'être dit, le second membre de l'équation (16) n'est pas nul.

Dans tous les cas, on peut mettre $(Z+Z')$ sous la forme $\pm z_h^i (1 \pm z_h^j)$, en s'aidant de la formule

$$z_1 z_2 = -1;$$

le premier facteur ne saurait être divisible par λ_1, il faudra donc que le second $(1 \pm z_h^j)$ le soit par λ_1^4; ce qui exige d'abord que la somme des coefficients soit un multiple de 5, c'est-à-dire que l'on ait

$$(1 \pm 2^j) \equiv 0 \pmod 5,$$

d'où j de la forme $5i + 2$, lors du signe (+), et de la forme $(5i' + 4)$, lors du signe (−). Ainsi le facteur $(1 \pm z_h^j)$ doit être de la forme $(1 + z_h^{5i+2})$, ou de celle-ci $(1 - z_h^{5i'+4})$; ou bien, comme on a

$$z_h^5 = 5 z_h - 3 = 5 (z_h - 1) + 2,$$

il faut que $(1 + 2^i z_h^2)$ ou $(1 - 2^{i'} z_h^4)$ soit divisible par λ_1^4.

L'exposant i ou i' est inférieur à 4, puisque $2^4 \equiv 1 \pmod 5$; alors i ou i' ne peut être que zéro, afin que la somme des coefficients dans $(1 + 2^i z_h^2)$ ou $(1 - 2^{i'} z_2^4)$ soit toujours un multiple de 5. Donc enfin, $(1 + z_h^2)$ ou $(1 - z_h^4)$ doit être divisible par λ_1^4. Comme

$$(1 - z_h^4) = (1 - z_h^2)(1 + z_h^2) = z_h (1 + z_h^2),$$

les deux cas se confondent. Il faut et il suffit que $(1+z_h^2)$, ou son égal $(2-z_h)$, soit divisible par λ_1^4. Mais, si $h=1$,

$$2-z_1=(1-r)(1-r^4)=-r^4\lambda_1^2;$$

et si $h=2$,

$$2-z_2=(1-r^2)(1-r^3)=-r^4z_2^2\lambda_1^2;$$

donc $(1+z_h^2)$ est seulement divisible par λ_1^2.

L'équation (16) est donc impossible; à moins que l'on ait $m_1=\lambda_1^5$, d'où $m_4=\lambda_4^5=-\lambda_1^5$, et $(m_1+m_4)=0$. Or, pour cette valeur particulière de m_1, les équations (14 *bis*) deviennent

$$\nu_1''+\nu_1'''=z_2\lambda_1^{10},$$
$$\nu_4''+\nu_4'''=z_2\lambda_1^{10},$$

et, en les ajoutant, on a

$$(\nu_1''+\nu_4'')+(\nu_1'''+\nu_4''')=2z_2\lambda_1^{10}. \tag{17}$$

Soit en général $n_1=r^kz_h^i$, d'où $n_1+n_4=r^k(1+r^{3k})z_h^i$; on reconnaît facilement que $r^k(1+r^{3k})$ est égal à z_1, pour $k=1, 4$, à z_2 pour $k=2, 3$, à 2 pour $k=0$; d'où résulte que le premier membre de l'équation (17) sera la somme de deux puissances de z_1 ou de z_2: si ce ne sont pas deux cinquièmes puissances, il vient d'être démontré qu'une pareille somme ne peut être divisible que par λ_1^2; si le premier membre de l'équation (17) est $(z_2^{5j}-z_1^{5j})$, j étant premier avec 5, ce premier membre est divisible par λ_1^6, et non par λ_1^{10}; si $j=5$, $(z_2^{25}-z_1^{25})$ est divisible par λ_1^{10}, mais le quotient, outre des facteurs complexes dont la norme est 1, contient le facteur 3001, nombre premier, qui ne peut diviser le second membre. L'équation (17) est donc impossible.