l'aide de son dispositif mécanique, la cause d'adhérence des roues motrices sur la voie peut être trouvée dans la résistance même du convoi. Il fait aussi remarquer que le même principe de construction permet d'établir un frein aussi puissant que sûr, agissant de lui-même ou à la volonté d'un garde-frein, toutes les fois que cela est nécessaire. M. Seguier croit avoir ainsi pratiquement justifié les propositions qu'il avait eu l'honneur de formuler devant l'Académie, dans ses précédentes communications à l'occasion des chemins de fer.

ANALYSE MATHÉMATIQUE. — *Démonstration générale du théorème de Fermat, sur l'impossibilité, en nombres entiers, de l'équation* $x^n + y^n = z^n$; *par* M. LAMÉ.

« On sait qu'il suffit de démontrer cette impossibilité pour les cas où l'exposant n est un nombre premier. On possède des démonstrations particulières, relatives aux exposants 3, 5, 7; elles sont fondées sur la décomposition en deux facteurs du premier membre de l'équation. Mais quand on passe aux exposants 11, 13, 17, 19, etc., on se trouve arrêté par la trop grande inégalité des deux facteurs. Je cherchais depuis longtemps un genre de démonstration, applicable à tous les cas, et qui fût en quelque sorte indépendant de la grandeur de l'exposant, lorsque, il y a quelques mois, j'en causai avec M. Liouville; il me parut convaincu que la propriété négative, énoncée par Fermat, devait dépendre de certains facteurs complexes, récemment étudiés par les géomètres qui s'occupent de la théorie des nombres. C'était une nouvelle voie que je n'avais pas explorée; je l'ai suivie, et je suis parvenu au mode de démonstration que je vais exposer, et qui me paraît justifier la prévision de M. Liouville.

§ I.

» Les nombres complexes qu'il faut considérer, pour chaque exposant, ou nombre premier n, sont de la forme

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

$\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, sont des nombres entiers, r est une des racines imaginaires de l'équation $r^n - 1 = 0$, ou de celle-ci

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

Les autres racines sont, comme l'on sait, $r^2, r^3, \ldots, r^{n-1}$; si l'on pose généralement

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

les $\frac{n-1}{2}$ valeurs de z_i sont les racines réelles d'une équation $\varphi(z)=0$, que l'on compose facilement.

» Si l'on retranche du nombre A(1) le second membre de l'équation (2) multiplié par l'un des coefficients $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, on fera disparaître tel terme qu'on voudra. Plus généralement, on peut augmenter ou diminuer à la fois d'un même nombre d'unités ces coefficients entiers; toutes ces transformations ne changeront que l'expression du nombre complexe A. Cette indétermination dans la forme cesse, quand on fait disparaître un des termes, le dernier par exemple; mais on détruit la symétrie. Quand on conserve le nombre complexe sous la forme (1), pour qu'il ne soit pas divisible par un entier, il faut, et il suffit, que les restes de la division de tous les coefficients, par cet entier, ne soient pas égaux.

» Si l'on multiplie successivement A par $r, r^2, r^3, \ldots, r^{n-1}$, en réduisant à chaque fois les puissances de r, on obtient la série de n nombres, A, Ar, A$r^2, \ldots,$ Ar^{n-1}, que nous désignerons par A, A′, A″, …, A$^{(n-1)}$. Les $n^{ièmes}$ puissances de tous ces nombres sont égales.

» Si l'on substitue successivement à la racine r, dans A ou A(r), les autres racines $r^2, r^3, r^4, \ldots, r^{n-1}$, en réduisant aussi, à chaque fois, les puissances de r, on obtient une autre série de $(n-1)$ nombres, A(r), A(r^2), A$(r^3), \ldots,$ A(r^{n-1}), que nous désignerons par $A_1, A_2, A_3, \ldots, A_{n-1}$. Le produit $A_1 A_2 A_3 \ldots A_{n-1}$ est une fonction symétrique des racines de l'équation (2); ce produit sera donc une fonction entière, et du degré $(n-1)$, des coefficients $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, et, par conséquent, un nombre entier; nous le désignerons sous le nom de *module* du nombre A. Ce module est essentiellement de la forme quadratique $Y^2 \pm nZ^2$: le signe + ayant lieu, si le nombre premier n est de la forme $4i+3$, et le signe −, s'il est de la forme $4i+1$. Nous appellerons les nombres $A_1, A_2, \ldots, A_{n-1}$, les *sous-facteurs du module;* A est un de ces sous-facteurs. Quand le module est un nombre premier, A est un *sous-facteur premier*. Quand le module est un nombre composé de plusieurs facteurs premiers, A est le produit d'autant de sous-facteurs premiers correspondants, ou bien ce produit multiplié par un nombre complexe dont le module soit l'unité.

» La fonction de $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$, qui forme le module, reste la même 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 surpasseraient n, ou ceux qui leur seraient inférieurs; c'est-à-dire que le module de A n'est pas affecté par toutes les transformations

qu'on peut faire subir à l'expression (1), et que ce module est aussi celui de $A^{(i)}$. En outre, $A^{(i)}$ ou Ar^i correspond au même sous-facteur que A, le multiplicateur r^i ayant pour module l'unité.

» Le nombre A sera *divisible* par un autre nombre complexe $D = \partial_0 + \partial_1 r + \partial_2 r^2 + \ldots + \partial_{n-1} r^{n-1}$, dont les coefficients entiers sont donnés, s'il est possible de satisfaire à l'équation

$$\alpha_0 + \alpha_1 r + \alpha_2 r^2 + \ldots + \alpha_{n-1} r^{n-1}$$
$$= (\partial_0 + \partial_1 r + \partial_2 r^2 + \ldots + \partial_{n-1} r^{n-1})(\varepsilon_0 + \varepsilon_1 r + \varepsilon_2 r^2 + \ldots + \varepsilon_{n-1} r^{n-1})$$

par des valeurs entières de $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-1}$; il le sera encore, s'il peut suffire, pour remplir cette condition, d'augmenter d'un même nombre tous les coefficients α, ou tous les coefficients ∂. Dans ce cas de divisibilité, le nombre complexe $E = \varepsilon_0 + \varepsilon_1 r + \varepsilon_2 r^2 + \ldots + \varepsilon_{n-1} r^{n-1}$ sera le quotient de A par D; A sera aussi divisible par $D^{(i)}$, et le quotient sera $E^{(n-i)}$. Le module de A sera le produit des modules de D et de E.

§ II.

» Soient maintenant un autre nombre complexe

$$B = \beta_0 + \beta_1 r + \beta_2 r^2 + \ldots + \beta_{n-1} r^{n-1},$$

et la série de n nombres B, B′, B″, ..., $B^{(n-1)}$ qui lui correspond. La somme $(A^n + B^n)$ des $n^{ièmes}$ puissances de A et B est divisible par $(A + B)$; cette somme est identiquement égale à $[(A^{(i)})^n + B]$, quel que soit i; elle est donc pareillement divisible par $A' + B$, par $A'' + B$, ..., par $A^{(n-1)} + B$. D'ailleurs, elle n'est autre que le produit de ces n diviseurs : en effet, la série des nombres A, A′, A″, ..., $A^{(n-1)}$ se forme en multipliant successivement A par les n racines $r^{(0)}, r', r'', \ldots, r^{(n-1)}$ de l'équation $r^n - 1 = 0$; et si l'on désigne généralement par S_k la somme des produits de k facteurs, qu'on peut former avec ces racines, on aura

$$(B + A)(B + A')\ldots[B + A^{(n-1)}]$$
$$= [B + Ar^{(0)}](B + Ar')(B + Ar'')\ldots[B + Ar^{(n-1)}]$$
$$= B^n + S_1 AB^{n-1} + S_2 A^2 B^{n-2} + \ldots + S_n A^n = B^n + A^n;$$

car, d'après la composition de l'équation aux racines $r^{(0)}, r', \ldots, r^{(n-1)}$, on a

$$S_1 = 0,\ S_2 = 0, \ldots,\ S_{n-1} = 0,\ S_1 = 1.$$

» Or on peut mettre ce produit sous une autre forme, et poser

$$(5)\quad A^n + B^n = (A + B)[A' + B^{(n-1)}][A'' + B^{(n-2)}]\ldots[A^{(i)} + B^{(n-i)}]\ldots[A^{(n-1)} + B'].$$

En effet, on reconnaît facilement que

$$\begin{aligned}
&A' + B^{(n-1)} = r^{n-1}(B + A''),\\
&A'' + B^{(n-2)} = r^{n-2}(B + A^{IV}),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&A^{\left(\frac{n-1}{2}\right)} + B^{\left(\frac{n+1}{2}\right)} = r^{\frac{n+1}{2}}\left[B + A^{(n-1)}\right],\\
&A^{\left(\frac{n+1}{2}\right)} + B^{\left(\frac{n-1}{2}\right)} = r^{\frac{n-1}{2}}(B + A'),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&A^{(n-2)} + B'' = r^2\left[B + A^{(n-4)}\right],\\
&A^{(n-1)} + B' = r\left[B + A^{(n-2)}\right];
\end{aligned}$$

d'où il résulte que le second membre de l'équation (5) est égal à

$$(A^n + B^n)\, r^p = A^n + B^n,$$

car l'exposant p, égal à la somme $1 + 2 + 3 + \ldots + (n-1)$, ou à $\frac{n(n-1)}{2}$, est un multiple de n.

» Ainsi, la somme des $n^{ièmes}$ puissances de deux nombres complexes de la forme (1) est décomposable en n facteurs complexes de la même forme. Ces n facteurs ont entre eux des relations nécessaires. Si l'on adopte pour ce produit la forme du second membre de l'équation (5), dont la loi est facile à saisir, et que l'on désigne généralement ces facteurs par $M^{(i)}$, l'indice i étant le même que celui de A, on démontre facilement que la somme de deux quelconques de ces facteurs est égale à un troisième de ces mêmes facteurs, multiplié par l'une des valeurs de z_i (3); car on trouve

$$M^{(i)} + M^{(i')} = z_{\left(\frac{i'-i}{2}\right)} \cdot M^{\left(\frac{i'+i}{2}\right)}, \tag{6}$$

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

» Les n nombres complexes $M, M', M'', \ldots, M^{(n-1)}$ vérifient donc $\frac{n(n-1)}{2}$ équations, semblables à l'équation (6), ou à celle-ci, citée pour exemple,

$$M' + M''' = z_1 M''. \tag{7}$$

Toutes ces relations peuvent être groupées de deux manières.

» Chaque nombre $M^{(i)}$ est facteur du second membre, dans $\frac{n-1}{2}$ équations, dont le premier membre est la somme de deux des $(n-1)$ autres nombres, associés de telle sorte que la somme de leurs indices soit la même. De là, et de la définition que nous avons donnée pour la divisibilité, on déduit cette conséquence, que, si un nombre complexe δ divise deux des n nombres $M, M', M'', \ldots, M^{(n-1)}$, il divisera nécessairement tous les autres.

» Chaque racine z_i est facteur du second membre dans n équations, dont le premier membre est la somme de deux des n nombres $M, M', M'', \ldots, M^{(n-1)}$, associés de telle sorte que la différence de leurs indices soit la même. De là suit cette autre conséquence, qu'un nombre complexe z_i, ou z_1 par exemple, (ou même l'un des sous-facteurs de z_i s'il en avait), ne peut diviser un seul des n facteurs $M, M', \ldots, M^{(n-1)}$, sans diviser aussi tous les autres.

» Il résulte enfin de ces deux conséquences, que la somme des $n^{ièmes}$ puissances de deux nombres complexes est égale à un produit de cette forme

$$A^n + B^n = k^n m m' m'' \ldots m^{(n-1)}, \tag{8}$$

k étant un nombre formé du produit de tous les nombres complexes qui pouvaient diviser à la fois deux des nombres $M, M', \ldots, M^{(n-1)}$, et, par suite, tous les autres; $m, m', m'', \ldots, m^{(n-1)}$, étant des nombres complexes, non divisibles, deux à deux par un même facteur complexe, ni seul à seul par aucune des valeurs de z_i; et ces nombres $m^{(i)}$ vérifient toutes les équations (6), en sorte qu'on a, par exemple,

$$m' + m'' = z_1 m''. \tag{9}$$

» Ainsi, la somme des $n^{ièmes}$ puissances de deux nombres complexes de la forme (1) ne saurait être divisible par une puissance de z_i (3), de z_1 par exemple, dont l'exposant ne serait pas un multiple de n.

§ III.

» Actuellement, si l'on veut rendre le produit

$$k^n m m' m'' \ldots m^{(n-1)}$$

égal à la $n^{ième}$ puissance d'un nombre complexe C, il faudra que les nombres $m, m', m'', \ldots, m^{(n-1)}$, qui n'admettent plus de diviseur commun, même deux à deux, soient respectivement égaux à des $n^{ièmes}$ puissances; c'est-à-dire qu'il faudra poser

$$\begin{cases} C = k \mu \mu' \mu'' \ldots \mu^{(n-1)}, \\ m = \mu^n, \ m' = \mu'^n, \ m'' = \mu''^n, \ \ldots, \ m^{(n-1)} = \mu^{(n-1)n}. \end{cases} \tag{10}$$

Mais les relations, telles que (9), ne permettent pas de prendre $\mu, \mu', \ldots, \mu^{(n-1)}$ arbitrairement; il faudra, entre autres conditions, que les nombres complexes μ'^n, μ''^n, μ'''^n vérifient l'équation

$$\mu'^n + \mu'''^n = z_i \mu''^n. \tag{11}$$

Or, pour que cette équation (11) fût possible, il faudrait nécessairement que la somme des $n^{ièmes}$ puissances des nombres complexes μ' et μ''' fût divisible par z_i^{in+1}, ce qui est impossible. On démontre d'ailleurs que $z_i = r + r^{(n-1)}$ ne peut être la $n^{ième}$ puissance d'un nombre complexe.

» Il est donc impossible de satisfaire à l'équation

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

en prenant pour A, B, C des nombres complexes de la forme (1).

» Toutefois, le cas de $n = 3$ échappe à ce genre de démonstration, car alors il n'y a qu'une seule valeur de z_i, laquelle est -1, et tout le système des équations (6), exprimé en μ, μ', μ'', se réduit à l'équation unique

$$\mu^3 + \mu'^3 + \mu''^3 = 0; \tag{13}$$

en sorte que l'impossibilité de l'équation (12), dans le cas particulier de $n = 3$, exige que l'on ait recours à l'ancien mode de démonstration.

» Le théorème de Fermat, pour $n > 3$, n'est qu'un cas particulier de celui qui vient d'être démontré; car si A et B sont des entiers, ou s'ils se réduisent à α_0, β_0, M sera entier, ainsi que C, k, μ; mais $\mu', \mu'', \ldots, \mu^{(n-1)}$ seront toujours des nombres complexes : seulement, leur produit devra être un module entier, c'est-à-dire que $\mu, \mu', \ldots, \mu^{(n-1)}$ devront être les sous-facteurs d'un nombre entier de la forme $Y^2 \pm nZ^2$; enfin, les relations telles que (11) seront encore nécessaires, et la couclusion d'impossibilité sera la même. »

Observations de M. **Liouville**.

« Dans la communication qu'il vient de faire à l'Académie, M. Lamé a bien voulu déclarer qu'il a suivi une idée dont je lui avais fait part autrefois : celle d'introduire des nombres complexes dérivés de l'équation binôme $r^n - 1 = 0$ dans la théorie de l'équation $x^n - y^n = z^n$, pour essayer d'en conclure l'impossibilité de cette dernière équation, soit en nombres entiers ordinaires, soit même en nombres complexes de la forme indiquée. Une telle idée n'a rien de neuf en soi, et a dû se présenter naturel-

lement aux géomètres d'après la forme du binôme $x^n - y^n$. Je n'en ai d'ailleurs déduit aucune démonstration satisfaisante, et, à vrai dire, je ne me suis même jamais occupé sérieusement de l'équation $x^n - y^n = z^n$. Toutefois, quelques essais me portaient à croire qu'il faudrait d'abord chercher à établir pour les nouveaux nombres complexes un théorème analogue à la proposition élémentaire pour les nombres entiers ordinaires, qu'un produit ne peut être décomposé en facteurs premiers que d'une seule manière. L'analyse de M. Lamé me confirme dans ce sentiment; elle a besoin, ce me semble, du théorème dont je parle: et pourtant je ne vois pas que notre confrère soit entré, à ce sujet, dans les détails que la matière paraît exiger. N'y a-t-il pas là une lacune à remplir? Je soumets cette observation à notre confrère, mais en exprimant la ferme espérance qu'il viendra à bout de toutes les difficultés, et qu'il obtiendra un nouveau et plus éclatant triomphe dans cette question épineuse où il s'est déjà tant distingué. Je rappellerai, en terminant, que depuis M. Gauss, et même depuis Euler et Lagrange, les géomètres se sont souvent occupés de nombres complexes. Le tome XVII de nos Mémoires renferme un grand travail de M. Cauchy, où ceux de ces nombres qui se rattachent à l'équation $r^n - 1 = 0$, jouent un rôle important. Mais pour le point spécial que j'ai signalé tout à l'heure, c'est surtout dans un article de M. Jacobi (*Journal de Mathématiques*, tome VIII, page 268), que l'on pourra trouver des renseignements utiles. »

A la suite de la lecture faite par M. Lamé, M. Cauchy prend aussi la parole et rappelle un Mémoire qu'il a présenté à l'Académie dans une précédente séance (19 octobre 1846), et qui a été paraphé, à cette époque, par l'un de MM. les Secrétaires perpétuels. Dans ce Mémoire, M. Cauchy exposait une méthode et des formules qui étaient, en partie, relatives à la théorie des nombres, et qui lui avaient semblé pouvoir conduire à la démonstration du dernier théorème de Fermat. Détourné par d'autres travaux, M. Cauchy n'a pas eu le temps de s'assurer si cette conjecture était fondée. D'ailleurs, la méthode dont il s'agit était très-différente de celle que M. Lamé paraît avoir suivie, et pourra devenir l'objet d'un nouvel article.

PHYSIOLOGIE. — *Sur la découverte du siége distinct de la sensibilité et de la motricité; par* M. Flourens.

« M. Magendie m'a demandé d'exposer les raisons sur lesquelles je me suis appuyé pour ne citer que M. Charles Bell à propos de la découverte du siége distinct de la *sensibilité* et de la *motricité* dans la moelle épinière.