HEINE

Théorèmes d'Eisenstein sur les séries qui sont les développements de fonctions algébriques

Nouvelles annales de mathématiques 1re série, tome 13 (1854), p. 245-253

<http://www.numdam.org/item?id=NAM_1854_1_13__245_1>

THÉORÈMES D'EISENSTEIN SUR LES SÉRIES QUI SONT LES DÉVELOPPEMENTS DE FONCTIONS ALGÉBRIQUES;

DÉMONTRÉS PAR M. HEINE,
Professeur à Bonn.

(Journal de M. Crelle, t. XLV, p. 285; 1853.)

---

1. *Lemme.* g et h étant deux nombres donnés, *premiers entre eux*, p un nombre *premier* donné, n un

nombre *entier* donné, les racines de la congruence

$$g - hx = (\dot{p}^n),$$

sont comprises entre o et $p^n - 1$; p^n, $2p^n - 1$; $2p^n$, $3p^n - 1$, etc.

Observation. Le point Leibnitzien placé sur une lettre indique un multiple.

2. *Lemme.* m étant un nombre entier, $m!$ un produit continuel et p un nombre *premier*, faisons

$$m = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \ldots + a_r p^r,$$

les a sont des nombres positifs tous moindres que p et pouvant être nuls; posons

$$\begin{aligned}
a_1 + a_2 + a_3 + \ldots + a_r &= A_1,\\
a_2 + a_3 + \ldots\ldots\ldots + a_r &= A_2,\\
a_3 + a_4 + \ldots\ldots\ldots + a_r &= A_3,\\
&\vdots\\
a_{r-1} + a_r &= A_{r-1},\\
a_r &= A_r;
\end{aligned}$$

et faisons

$$A_1 + A_2 p + A_3 p^2 + \ldots + A_{r-1} p^{r-2} + A_r p^{r-1} = B,$$

alors B est la plus haute puissance de p qui divise le produit continuel $m!$ (LEGENDRE, *Théorie des nombres*, tome I, page 10.)

Observation. Il est évident que a_0, a_1, a_2, etc., sont les chiffres avec lesquels on écrirait le nombre m dans le système de numération dont la base est p.

3. *Lemme.* g et h étant deux nombres *premiers entre eux*; m un nombre entier; si l'on simplifie, autant que possible, le coefficient binomial

$$\frac{g(g-h)(g-2h)\ldots[g-(m-1)h]}{m!},$$

le dénominateur de la fraction ainsi simplifiée ne renferme plus aucun facteur *premier non diviseur* de h, mais uniquement des diviseurs de h.

Démonstration. Si $m!$ renferme avant la simplification un diviseur de h, il ne peut s'en aller par cette opération, car, g et h étant *premiers entre eux*, un tel diviseur ne peut diviser aucun facteur du numérateur. Soit donc p un *nombre premier non diviseur* de h, et supposons que p^n se trouve au dénominateur comme facteur. Partageons le numérateur en groupes, renfermant chacun p^n facteurs successifs. Dans le dernier groupe, il pourra se trouver moins de p^n facteurs. Chaque groupe (le dernier excepté), renfermera un nombre divisible par p^n (lemme 1); soit s le nombre de ces groupes. Le numérateur est donc divisible par p^{ns} ou bien par p^{ns+n} si le dernier groupe renferme ainsi un nombre divisible par p^n; opérant de même sur le dénominateur; le premier groupe est $1, 2, 3, \ldots, p^n$ et le deuxième $p^n + 1, p^n + 2, \ldots, p^n + 2p^n$, etc., le dernier groupe, s'il est incomplet, ne peut pas renfermer un diviseur de p^n; donc, après les simplifications, le numérateur renferme au plus p^n comme facteur et le dénominateur aucun facteur divisible par p^n.

C. Q. F. D.

4. Théorème. *Dans le développement de* $(1 + x)^{\frac{g}{h}}$, *suivant les puissances croissantes de* x, g *et* h *étant des nombres premiers entre eux, les dénominateurs des coefficients, simplification faite, ne contiennent que des facteurs diviseurs de* h.

Démonstration. C'est une conséquence du lemme précédent; le coefficient binomial affecte $\left(\frac{x}{h}\right)^m$.

Observation. $\frac{g}{h}$ peut être négatif; la conclusion reste la même.

5. Théorème. *a_0, a_1, a_2,..., a_m étant des nombres rationnels ; si l'on développe suivant les puissances croissantes de x l'expression $(a_0 + a_1 x + a_2 x^2 \ldots a_m x^m)^{\frac{g}{h}}$, où g et h sont des nombres premiers entre eux, chaque coefficient simplifié est le quotient de deux nombres entiers ; le dénominateur est un produit formé par des puissances de h, des puissances des dénominateurs de a_1, a_2,..., a_m et des puissances des numérateurs de a_0.*

Démonstration.

$$(a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m)^{\frac{g}{h}}$$

$$= (a^0)^{\frac{g}{h}} \left[1 + \frac{a_1}{a_0} x + \frac{a_2}{a_0} x^2 + \ldots + \frac{a_m}{a_0} x^m \right]^{\frac{g}{h}}.$$

Chaque coefficient renferme : 1° les coefficients binomiaux ; 2° des puissances positives de a_1, a_2,..., a_m ; 3° des puissances négatives de a_0 ; donc, etc.

Observation. Les dénominateurs renferment donc des puissances d'un nombre *limité* de certains nombres entiers. Il est donc toujours possible de remplacer x par un multiple kx tel, que tous les coefficients deviennent des nombres entiers.

6. Théorème. *Si une fonction algébrique d'une variable x peut se développer suivant les puissances croissantes de cette variable, alors les coefficients étant simplifiés peuvent être représentés par des fractions dont les dénominateurs sont des produits de puissance d'un nombre limité de nombres entiers.*

Démonstration. L'addition, la soustraction et la multiplication de deux séries ou de deux fonctions entières n'introduisent pas de nouveaux nombres premiers dans les dénominateurs ; l'élévation à une puissance positive ou négative d'une fonction ordonnée suivant les puissances de x n'introduit dans les dénominateurs qu'un nombre *limité* de nombres premiers (5); or toute fonction algébrique d'une variable x est le résultat d'un certain nombre desdites opérations; donc, etc.

Observation. On ne parle pas de la division, car elle équivaut à l'élévation à la puissance — 1.

IRRATIONNELS.

7. *Définitions.* Un nombre *irrationnel* résulte des quatre opérations et de l'élévation à des puissances fractionnaires positives, faites sur des nombres rationnels *entiers*.

Nous appelons *irrationnel entier,* lorsque la division n'est pas indiquée. *Exemple :*

$$\sqrt[3]{3+\sqrt{7}} \text{ est un } \textit{irrationnel entier.}$$

Observation. Un nombre irrationnel quelconque peut se ramener à la forme d'une fraction dont les deux termes sont des *irrationnels entiers.* Exemple :

$$\sqrt{1-\sqrt{\frac{2}{3}}}=\frac{\sqrt{\sqrt{3}-\sqrt{2}}}{\sqrt[4]{3}},$$

$\sqrt{\sqrt[3]{3}-\sqrt{2}}$ est le numérateur entier et $\sqrt[4]{3}$ le dénominateur entier. Un *irrationnel entier* est dit divisible par un *deuxième irrationnel entier* lorsqu'il existe un troisième irrationnel entier qui, multiplié par le deuxième, reproduise le premier.

Observation. Lorsqu'on élève un nombre irrationnel entier à une puissance positive, le résultat est un irrationnel entier; de même lorsqu'on combine deux irrationnels entiers par voie d'addition, soustraction et multiplication.

8. Ces définitions admises, le théorème 6 subsiste même lorsque les a sont des nombres *irrationnels entiers*. Toutefois, il faut encore démontrer que lorsque, par combinaisons de quatre opérations, on obtient des irrationnels qui, en se simplifiant, deviennent rationnels, ces simplifications n'amènent pas aux dénominateurs des facteurs premiers en nombre *illimité*. M. Heine donne cette démonstration qui repose sur la classification *abélienne* des irrationnels; classification trop peu connue pour que nous puissions donner cette belle démonstration. (*).

ÉQUATIONS ALGÉBRIQUES.

9. Soit

$$f(x, y) = 0$$

une équation algébrique en x, y; si les coefficients sont irrationnels, on peut toujours la ramener à une autre équation où les coefficients sont rationnels et entiers. L'équation peut alors se mettre sous la forme

$$(1)\quad f(x, y) = \mathrm{A}_0 y^m + \mathrm{A}_1 y^{m-1} + \ldots + \mathrm{A}_{m-1} y + \mathrm{A}_m = 0,$$

les A sont des fonctions entières à coefficients entiers de x; soient a_0, $a_1, \ldots, a_m$ les valeurs de ces diverses fonctions A en y faisant $x = 0$, valeurs qui sont des nombres entiers, ainsi :

$$(2)\quad f(0, y) = a_0 y^m + a_1 y^{m-1} + a_2 y^{m-2} \ldots a_{m-1} y + a_m,$$

l'équation (1) résolue par rapport à y, donne m racines, chacune fonction de x; supposons qu'une de ces racines, que nous désignons par y_1, puisse se développer suivant des puissances croissantes de x, à coefficients rationnels, de

(*) On trouvera cette classification dans la nouvelle édition de l'*Algèbre supérieure*.

sorte que

(3) $$y_1 = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n + \ldots,$$

les c sont des nombres rationnels en nombre infini.

10. Théorème. *Les dénominateurs des nombres c_0, c_1, etc., ne renferment qu'un nombre limité de diviseurs premiers.*

Démonstration. Faisons

$$x = 0,$$

nous aurons

$$y_1 = c_0;$$

donc, d'après l'équation (2),

(4) $$f(y_1, 0) = a_0 c_0^m + a_1 c_0^{m-1} + \ldots + a_m = 0.$$

Substituant la valeur de y_1 dans l'équation (1), on a

$$\left.\begin{array}{l} f(x, y_1) = A_0 (c_0 + c_1 x + \ldots + c_n x^n + \ldots)^m \\ \quad + A_1 (c_0 + c_1 x + \ldots + c_n x^n + \ldots)^{m-1} \\ \quad \vdots \\ \quad + A_{m-1} (c_0 + c_1 x + \ldots + c_n x^n + \ldots) \\ \quad + A_m \end{array}\right\} = 0,$$

comme c'est une identité, les coefficients des puissances de x doivent s'anéantir. Supposons n plus grand que le degré de x dans A_m; alors le coefficient de x^n renferme deux parties :

1re partie. $c_n \left[m a_0 c_0^{m-1} + m - 1 . a_1 c_0^{m-2} + \ldots 2 a_{m-2} c_0 + a_{m-1} \right]$,

car A_m ne fournit rien;

2e partie. Les termes fournis par les divers A combinés avec les c depuis c_0 jusqu'à c_{n-1}.

Supposons que le nombre premier p paraisse pour la *première fois* dans le dénominateur de c_n; la somme des deux parties devant être nulle, la deuxième partie ne peut pas renfermer p au dénominateur, car elle ne contient pas de c_n; il s'ensuit que p doit aussi disparaître dans la première partie, donc p doit diviser

$$ma_0 c_0^{m-1} + m - 1 . a_1 c_0^{m-2} \ldots . a_{m-1}.$$

Or cette expression est la dérivée de l'équation (4). Si donc cette équation n'a pas de racines égales, la dérivée n'est pas nulle et a une valeur finie; donc tous les facteurs premiers qu'on rencontre dans les dénominateurs à partir de c_n, divisent une même expression finie. Ils sont donc en nombre *limité*. Il faut y joindre les diviseurs qui sont fournis par les dénominateurs qui précèdent c_n et qui sont évidemment en nombre limité; donc les dénominateurs en nombre infini c_0, c_1, etc., étant simplifiés, ne renferment qu'un nombre limité de facteurs premiers. C. Q. F. D.

Eisenstein dit que, lorsque l'équation (4) a des racines égales, le développement en séries suivant des puissances croissantes de x est impossible. M. Heine fait voir que cette assertion n'est pas exacte et que le théorème subsiste encore lorsque l'équation (4) a des racines égales.

11. Il s'ensuit que toute série ordonnée suivant les puissances croissantes de x qui renferme dans les dénominateurs un nombre indéfini de facteurs premiers, ne saurait être ni le développement d'une fonction algébrique, ni même la racine d'une équation algébrique; or, $\log x$, $\operatorname{arc tang} x$, $\sin x$, e^x, etc., se développent en séries, où les dénominateurs renferment un nombre illimité de facteurs premiers; donc ces fonctions ne sont ni algébriques, ni racines d'une fonction algébrique.

Remarque. Une mort prématurée a empêché Eisenstein de donner la démonstration de ces importants théorèmes, surtout en ce qui concerne les équations.