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

J. LIOUVILLE

Sur un point de la théorie des équations binômes

Journal de mathématiques pures et appliquées 2^e série, tome 2 (1857), p. 413-423.
<http://www.numdam.org/item?id=JMPA_1857_2_2__413_0>

SUR

UN POINT DE LA THÉORIE DES ÉQUATIONS BINOMES;

PAR M. J. LIOUVILLE.

Le 20 avril dernier j'ai communiqué à l'Académie des Sciences une Note sous ce même titre : elle a été insérée dans les *Comptes rendus*, tome XLIV, page 798. Je la reproduis d'abord textuellement, puis j'ajoute quelques remarques qui la complètent.

I.

« Soit p un nombre premier impair, et

$$X = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

l'équation binôme de degré p débarrassée de la racine réelle 1 et réduite à n'avoir plus que des racines imaginaires

$$\alpha, \quad \alpha^2, \quad \alpha^3, \ldots, \quad \alpha^{p-1},$$

représentées par les puissances de la quantité

$$\alpha = e^{\frac{2\pi}{p}\sqrt{-1}} = \cos\frac{2\pi}{p} + \sqrt{-1}\sin\frac{2\pi}{p}.$$

On sait qu'en désignant chacun des exposants 1, 2, 3,..., $p-1$ par a ou b, suivant que cet exposant est ou n'est pas résidu quadratique de p, on décompose l'équation

$$X = 0$$

en deux autres, dont les coefficients sont des fonctions rationnelles de $\sqrt{\pm p}$, et qui ont pour racines, l'une les puissances α^a, l'autre les puissances α^b. Posons

$$2\Pi(x - \alpha^b) = Y + Z\sqrt{\pm p},$$

et

$$2\Pi(x-\alpha^a)=Y-Z\sqrt{\pm p},$$

en affectant p, sous le radical, du signe + ou du signe —, suivant que p est de la forme $4n+1$ ou de la forme $4n-1$, le signe Π indiquant à l'ordinaire un produit. Y et Z seront des polynômes à coefficients entiers; le premier Y, de degré $\frac{p-1}{2}$ et commençant par le terme $2x^{\frac{p-1}{2}}$; le second Z, de degré inférieur. On aura

$$4X=Y^2\mp pZ^2;$$

l'équation $X=0$ se décomposera donc en ces deux-ci :

$$Y+Z\sqrt{\pm p}=0,\quad Y-Z\sqrt{\pm p}=0.$$

Ce beau théorème est dû à Gauss.

» Pour qu'il n'y ait rien d'indécis relativement à nos notations, je prendrai la valeur de $\sqrt{p}$ toujours positivement, et j'entendrai par $\sqrt{-p}$ le produit $\sqrt{p}\sqrt{-1}$. Cela posé, je me hasarde à dire, après Gauss, Legendre, etc., quelques mots à mon tour sur les moyens que l'on peut employer pour déterminer les deux polynômes Y et Z, ou, ce qui revient au même, le polynôme unique

$$U=Y+Z\sqrt{\pm p},\quad \text{ou}\quad V=Y-Z\sqrt{\pm p}.$$

» En désignant par U′ la dérivée $\frac{dU}{dx}$ de U, et de même par X′ la dérivée de X, et en représentant par $\varphi(x)$ un certain polynôme à coefficients entiers dont j'écrirai plus bas la valeur, je trouve que l'on a

$$\frac{2U'}{U}=\frac{X'-\varphi(x)\sqrt{\pm p}}{X}.$$

Or l'équation $X=0$ n'ayant pas de racines égales, l'équation $U=0$ n'en a pas non plus. La fraction

$$\frac{2U'}{U}$$

est donc irréductible, et on devra l'obtenir en réduisant à sa plus simple expression la fraction placée au second membre. D'après cela : Cherchez le plus grand commun diviseur des deux polynômes X et $X' - \varphi(x)\sqrt{\pm p}$, et multipliez-le par une constante de manière que son premier terme soit $2x^{\frac{p-1}{2}}$. Vous formerez ainsi le polynôme $V = Y - Z\sqrt{\pm p}$. Le polynôme U s'en déduira en changeant le signe du radical, comme en divisant $4X$ par V; et l'on en conclura Y et Z en séparant les termes rationnels de ceux qui sont multipliés par $\sqrt{\pm p}$.

» Mais une élégante proposition de Gauss que je rappellerai en terminant cette Note permettait déjà de former U par la division, et a conduit Legendre à une méthode plus simple encore dans la pratique et fondée sur la considération des sommes de puissances semblables des racines. Le procédé sur lequel je veux appeler surtout l'attention de l'Académie est d'un genre différent, et il a pour caractère essentiel de permettre de former à priori un terme isolé quelconque de U.

» L'équation

$$\frac{2U'}{U} = \frac{X' - \varphi(x)\sqrt{\pm p}}{X},$$

dont je tire en passant ce résultat curieux

$$ZY' - YZ' = 2\varphi(x),$$

où Y' et Z' marquent les dérivées de Y et Z, fournit en effet par l'intégration une valeur de U très-remarquable qui mène au but indiqué.

» Donnons d'abord la valeur du polynôme $\varphi(x)$. Pour cela, faisons usage d'un signe de Legendre, et désignons comme lui par

$$\left(\frac{m}{p}\right)$$

l'unité prise avec le signe + ou avec le signe −, suivant que l'entier m, premier à p, est ou n'est pas résidu quadratique de p. Alors on a, sous la forme la plus concise,

$$\varphi(x) = \frac{1}{x-1}\left[\left(\frac{1}{p}\right)x^{p-2} + \left(\frac{2}{p}\right)x^{p-3} + \ldots + \left(\frac{p-2}{p}\right)x + \left(\frac{p-1}{p}\right)\right].$$

Le numérateur

$$\left(\frac{1}{p}\right)x^{p-2}+\left(\frac{2}{p}\right)x^{p-3}+\ldots+\left(\frac{p-1}{p}\right)$$

est divisible par $x-1$ en vertu de la formule connue

$$\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\ldots+\left(\frac{p-1}{p}\right)=0.$$

En effectuant la division, on trouve

$$\varphi(x)=\left(\frac{1}{p}\right)x^{p-3}+\left[\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)\right]x^{p-4}+\left[\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)\right]x^{p-3}+\ldots$$
$$-\left[\left(\frac{p-2}{p}\right)+\left(\frac{p-1}{p}\right)\right]x-\left(\frac{p-1}{p}\right),$$

où l'on a simplifié la dernière moitié des coefficients au moyen de l'équation citée

$$\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\ldots+\left(\frac{p-1}{p}\right)=0.$$

» Nous sommes assurés par là que $\varphi(x)$ est bien une fonction entière; mais la première expression est la plus commode. On en conclut facilement que

$$\int_x^\infty \frac{\varphi(x)\,dx}{X}=\left(\frac{1}{p}\right)\frac{1}{x}+\left(\frac{2}{p}\right)\frac{1}{2x^2}+\ldots=\sum\left(\frac{m}{p}\right)\frac{1}{mx^m},$$

le signe $\sum$ s'appliquant à tous les entiers m premiers à p. Si donc on effectue l'intégration dont j'ai parlé plus haut, et qu'on pose, pour abréger,

$$\lambda=\frac{1}{2}\sum\left(\frac{m}{p}\right)\frac{1}{mx^m},$$

on aura

$$U=2\sqrt{X}\cdot e^{\lambda\sqrt{\pm p}}.$$

» Maintenant, puisque U est un simple polynôme, il est clair qu'on l'obtiendra en développant le second membre suivant les puissances

descendantes de x, sans s'inquiéter des termes affectés d'un exposant négatif qui doivent disparaître d'eux-mêmes. Ceci rappelle le beau Mémoire sur l'élimination que Lagrange a donné dans le Recueil de l'Académie de Berlin. Je n'ai pas à insister ici sur les simplifications de détail dont le calcul est susceptible, ni sur les formes diverses qu'on peut lui faire prendre. On poura évidemment réduire la suite infinie λ à ceux de ses termes qui ont de l'influence sur la valeur de U, ou plutôt sur les termes de U qu'on veut former. On pourra aussi remplacer $\sqrt{X}$ par

$$x^{\frac{p-1}{2}}\left(1-\frac{1}{x}\right)^{-\frac{1}{2}}$$

ou bien encore par

$$x^{\frac{p-1}{2}}.e^{-\frac{1}{2}\log\left(1-\frac{1}{x}\right)},$$

c'est-à-dire par

$$x^{\frac{p-1}{2}}.e^{\frac{1}{2x}+\frac{1}{4x^2}+\cdots},$$

en ne prenant, comme pour λ, qu'un nombre limité de termes dans la série qui sert d'exposant. Si donc on demande le terme de U, qui est multiplié par

$$x^{\frac{p-1}{2}-\mu},$$

on n'aura qu'à développper des exponentielles de la forme

$$e^{\frac{g}{x^s}}$$

s ne surpassant pas μ, et à chercher dans leur produit le terme qui répond à l'exposant $-\mu$ de x.

» Notre fonction $\varphi(x)$ a une liaison intime avec celle-ci :

$$f(x)=\left(\frac{1}{p}\right)x+\left(\frac{2}{p}\right)x^2+\left(\frac{3}{p}\right)x^3+\ldots+\left(\frac{p-1}{p}\right)x^{p-1},$$

qui entre dans la belle formule de Gauss

$$f(\alpha^m) = \left(\frac{m}{p}\right)\sqrt{\pm p}, \quad \text{ou} \quad = 0,$$

suivant que l'entier m est ou non premier à p. J'ai fait allusion plus haut à cette formule : elle montre que U est aussi le plus grand commun diviseur des deux polynômes X et $f(x) + \sqrt{\pm p}$. »

II.

L'équation fondamentale

$$\frac{2\,U'}{U} = \frac{X' - \varphi(x)\sqrt{\pm p}}{X}$$

peut être établie de différentes manières, et, par exemple, comme il suit :

La fonction que nous désignons ici par $\varphi(x)$ est liée à la fonction $f(x)$ de la formule de Gauss, de telle sorte qu'on a

$$(x-1)\varphi(x) = x^{p-1} f\left(\frac{1}{x}\right).$$

Si donc on fait $x = \alpha^m$, m désignant un des nombres $1, 2, 3, \ldots, p-1$, et par suite α^m étant une quelconque des racines de l'équation $X = 0$, il viendra

$$(\alpha^m - 1)\varphi(\alpha^m) = \alpha^{mp-m} f(\alpha^{-m}) = \alpha^{-m} f(\alpha^{-m}).$$

Mais on a

$$f(\alpha^{-m}) = \left(\frac{-m}{p}\right)\sqrt{\pm p},$$

d'où

$$f(\alpha^{-m}) = \pm\left(\frac{m}{p}\right)\sqrt{\pm p},$$

en prenant partout les signes supérieurs ou partout les signes inférieurs, suivant que p est de la forme $4n+1$ ou de la forme $4n-1$.

Donc

$$(\alpha^m - 1)\,\varphi(\alpha^m) = \pm\left(\frac{m}{p}\right)\alpha^{-m}\sqrt{\pm p},$$

et, par conséquent,

$$\frac{\alpha^m}{p}(\alpha^m - 1)\,\varphi(\alpha^m)\sqrt{\pm p} = \left(\frac{m}{p}\right).$$

Cela posé, décomposons la fraction rationnelle

$$\frac{\varphi(x)\sqrt{\pm p}}{\mathrm{X}}$$

en fractions simples, de manière à avoir

$$\frac{\varphi(x)\sqrt{\pm p}}{\mathrm{X}} = \sum\frac{\mathrm{C}_m}{x - \alpha^m},$$

ou, ce qui revient au même,

$$\frac{(x-1)\,\varphi(x)\sqrt{\pm p}}{x^p - 1} = \sum\frac{\mathrm{C}_m}{x - \alpha^m}.$$

Le coefficient C_m s'obtiendra, d'après la règle ordinaire, en faisant $x = \alpha^m$ dans l'expression

$$\frac{(x-1)\,\varphi(x)\sqrt{\pm p}}{px^{p-1}}.$$

Dès lors on trouvera facilement

$$\mathrm{C}_m = \frac{\alpha^m}{p}(\alpha^m - 1)\,\varphi(\alpha^m)\sqrt{\pm p} = \left(\frac{m}{p}\right),$$

c'est-à-dire

$$\mathrm{C}_m = 1,$$

quand m est un des nombres a, résidus quadratiques de p, et

$$\mathrm{C}_m = -1,$$

quand m est un des non-résidus b.

Nous voyons par là que

$$\frac{\varphi(x)\sqrt{\pm p}}{\mathrm{X}} = \sum \frac{1}{x-\alpha^a} - \sum \frac{1}{x-\alpha^b}.$$

Mais déjà

$$\frac{\mathrm{X}'}{\mathrm{X}} = \sum \frac{1}{x-\alpha^a} + \sum \frac{1}{x-\alpha^b}.$$

Donc

$$\frac{\mathrm{X}' - \varphi(x)\sqrt{\pm p}}{\mathrm{X}} = 2\sum \frac{1}{x-\alpha^b} = \frac{2\,\mathrm{U}'}{\mathrm{U}},$$

ce qu'il fallait démontrer.

III.

Nous devons en second lieu expliquer comment on arrive à l'équation

$$\int_x^\infty \frac{\varphi(x)\,dx}{\mathrm{X}} = \left(\frac{1}{p}\right)\frac{1}{x} + \left(\frac{2}{p}\right)\frac{1}{2x^2} + \ldots = \sum \left(\frac{m}{p}\right)\frac{1}{mx^m},$$

où le signe $\sum$ s'applique à tous les entiers m premiers à p, en sorte que l'on a une suite infinie, qui sera convergente si l'on suppose avec nous $x > 1$.

D'après l'expression de $\varphi(x)$, on a

$$\frac{\varphi(x)}{\mathrm{X}} = \frac{(x-1)\,\varphi(x)}{x^p-1} = \frac{1}{x^p-1}\left[\left(\frac{1}{p}\right)x^{p-2} + \left(\frac{2}{p}\right)x^{p-3} + \ldots + \left(\frac{p-1}{p}\right)\right].$$

Mais, dans l'hypothèse de $x > 1$,

$$\frac{1}{x^p-1} = \frac{1}{x^p} + \frac{1}{x^{2p}} + \frac{1}{x^{3p}} + \ldots.$$

La fraction

$$\frac{\varphi(x)}{\mathrm{X}}$$

est donc la somme des quantités suivantes :

$$\left(\frac{1}{p}\right)\frac{1}{x^2}+\left(\frac{2}{p}\right)\frac{1}{x^3}+\ldots+\left(\frac{p-1}{p}\right)\frac{1}{x^p},$$
$$\left(\frac{1}{p}\right)\frac{1}{x^{p+2}}+\left(\frac{2}{p}\right)\frac{1}{x^{p+3}}+\ldots+\left(\frac{p-1}{p}\right)\frac{1}{x^{2p}},$$
$$\left(\frac{1}{p}\right)\frac{1}{x^{2p+2}}+\left(\frac{2}{p}\right)\frac{1}{x^{2p+3}}+\ldots+\left(\frac{p-1}{p}\right)\frac{1}{x^{3p}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

et si l'on remplace, comme on en a le droit,

$$\left(\frac{1}{p}\right),\ \left(\frac{2}{p}\right),\ldots,\ \left(\frac{p-1}{p}\right)$$

par

$$\left(\frac{p+1}{p}\right),\ \left(\frac{p+2}{p}\right),\ldots,\ \left(\frac{2p-1}{p}\right)$$

dans la seconde de ces quantités, puis par

$$\left(\frac{2p+1}{p}\right),\ \left(\frac{2p+2}{p}\right),\ldots,\ \left(\frac{3p-1}{p}\right)$$

dans la troisième, et ainsi de suite, on verra facilement que la somme dont il s'agit peut s'écrire

$$\sum\left(\frac{m}{p}\right)\frac{1}{x^{m+1}},$$

en prenant successivement pour m les nombres naturels $1, 2, 3,\ldots, p-1, p+1,\ldots$, à l'infini, à l'exclusion des multiples de p.

Ayant ainsi

$$\frac{\varphi(x)}{\mathrm{X}}=\sum\left(\frac{m}{p}\right)\frac{1}{x^{m+1}},$$

on en conclura, en intégrant, la formule

$$\int_x^\infty\frac{\varphi(x)\,dx}{\mathrm{X}}=\sum\left(\frac{m}{p}\right)\frac{1}{mx^m},$$

qu'il s'agissait d'établir, et où le signe $\sum$ s'applique, je le répète, à tous les entiers m premiers à p.

IV.

Après les développements dans lesquels nous venons d'entrer, tout devient facile, et les indications données au § 1 montrent suffisamment à nos lecteurs comment on peut trouver sous diverses formes le coefficient de tel terme qu'on voudra de la fonction entière

$$U = 2x^{\frac{p-1}{2}} + A_1 x^{\frac{p-1}{2}-1} + \ldots,$$

par exemple le coefficient A_μ du terme où figure

$$x^{\frac{p-1}{2}-\mu}.$$

Bornons-nous à transcrire ici une des expressions auxquelles on arrive pour ce coefficient A_μ.

Désignons par $k_1, k_2, \ldots, k_m, \ldots, k_\mu$ un quelconque des groupes de nombres entiers non négatifs pour lesquels on a

$$k_1 + 2k_2 + \ldots + mk_m + \ldots + \mu k_\mu = \mu,$$

Pour chaque groupe $k_1, k_2, \ldots, k_m, \ldots, k_\mu$ remplissant la condition voulue, formons le produit

$$\Pi \left[\frac{1 + \left(\frac{m}{p}\right)\sqrt{\pm p}}{2}\right]^{k_m} \frac{1}{m^{k_m}\Gamma(k_m+1)},$$

où le signe de multiplication Π se rapporte à m qui doit prendre les valeurs 1, 2, 3, ..., μ, et où le signe Γ est employé avec la signification que lui a donnée Legendre. Le double de la somme de ces produits sera égal à A_μ.

Nous écrirons donc

$$A_\mu = 2\sum \Pi \left[\frac{1 + \left(\frac{m}{p}\right)\sqrt{\pm p}}{2}\right]^{k_m} \frac{1}{m^{k_m}\Gamma(k_m+1)}.$$

Pour $\mu = 1$, on ne peut prendre que $k_1 = 1$, et notre formule fournit

$$A_1 = 1 + \sqrt{\pm p};$$

pour $\mu = 2$, on a les deux groupes $k_1 = 2$, $k_2 = 0$, et $k_1 = 0$, $k_2 = 1$: notre formule donne donc

$$A_2 = \frac{1}{4}(3 \pm p) + \frac{1}{2}\left[1 + \left(\frac{2}{p}\right)\right]\sqrt{\pm p}.$$

Et ainsi de suite.

Indépendamment des développements algébriques qui donnent pour A_μ des expressions de formes très-diverses dont la comparaison ne serait pas sans intérêt, on pourrait aussi exprimer A_μ par une intégrale définie.

Nous avons supposé le nombre p premier. Il y a, comme on sait, des théorèmes analogues pour les équations binômes de degré composé, et notre méthode se prête très-bien à une telle extension.