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

EDMOND MAILLET

Sur la détermination du groupe des équations numériques

Journal de mathématiques pures et appliquées 5^e série, tome 5 (1899), p. 205-216.
<http://www.numdam.org/item?id=JMPA_1899_5_5__205_0>

Sur la détermination du groupe des équations numériques;

PAR M. EDMOND MAILLET.

I.

Nous nous proposons ici :

1° De déterminer toute une série d'équations numériques de degré premier dont le groupe est symétrique ou alterné;

2° De montrer que l'équation $x^{2p} \pm qx \pm q = 0$, où $2p-1$ et q sont premiers, a son groupe deux fois transitif quand q est supérieur à une certaine limite fonction de p.

II.

THÉORÈME I. — *Soit l'équation algébrique irréductible*

$$f(x) = x^p + qA_1 x^{p-1} + \ldots + qA_{p-1}x \pm q = 0 \qquad (1)$$

(*p et q nombres premiers différents ou non, p impair*, $A_1, \ldots, A_{p-1}$ *entiers*). *On peut toujours déterminer une infinité de systèmes de valeurs des coefficients* $A_1, \ldots, A_{p-1}$ *de* (1), *de façon que l'équation* (1) *ait au moins* $2l+1$ *racines réelles et deux racines imaginaires, et, par suite, que son groupe contienne le groupe alterné si*

$l = 1$ quand $p = 5$ et si $p - 1 - 2l < \varphi(p)$, $\varphi(p)$ étant une fonction u de p, telle que (1)

$$p = \frac{(4+u)\left(4 + u\log\frac{u}{2}\right)}{4},$$

quand $p > 5$.

En effet, on sait (2) que l'équation (1) est irréductible et que son groupe G est primitif. Si cette équation a $2\lambda + 1$ racines réelles, avec $2\lambda + 1 < p$, elle aura $p - 2\lambda - 1 = 2\mu$ racines imaginaires $x_1, x_2, \ldots, x_{2\mu-1}, x_{2\mu}$, et si x_{2i-1} et x_{2i} sont conjuguées ($i \leq \mu$), G contiendra la substitution (3)

$$U = (x_1 x_2)\ldots(x_{2\mu-1} x_{2\mu}),$$

en sorte que la classe de G est $\leq 2\mu$: d'après un théorème connu (4), la classe de G étant $\geq \varphi(p)$, si G ne contient pas le groupe alterné de p éléments, G contiendra ce groupe alterné si $1 < 2\mu < \varphi(p)$.

Cherchons à déterminer $A_1, A_2, \ldots, A_{p-1}$, de façon que 2μ soit $< \varphi(p)$, en remarquant que $\varphi(p) > 2$, quand $p > 5$. La méthode à employer pour $p = 5$ sera la même, on fera $l = \mu = 1$.

Soient

$$(2) \qquad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_{2l} \quad \text{avec} \quad p - 1 - \varphi(p) < 2l \leq p - 3$$

des nombres entiers réels donnés $\neq 0$, avec

$$\alpha_1 < \alpha_2 < \ldots < \alpha_{2l}.$$

Si

$$(3) \qquad \beta_1, \quad \beta_2, \quad \ldots, \quad \beta_{2l}$$

---

(1) JORDAN, *Journal für Math.*, p. 248; 1875.

(2) SERRET, *Algèbre supérieure*, t. I, p. 244; 1885.

(3) *Voir* notre Note des *Mémoires du Congrès de Saint-Étienne*, 1897 (*Association française pour l'avancement des Sciences*, p. 196).

(4) JORDAN, *loc. cit.*

sont des nombres entiers réels > 0, posons :

$$(4)\qquad f(\alpha_1) = +\beta_1, \qquad f(\alpha_2) = -\beta_2, \qquad \ldots \qquad f(\alpha_{2l}) = -\beta_{2l},$$

les seconds membres étant alternativement positifs et négatifs.

Si les quantités $A_1, \ldots, A_{p-1}$ sont déterminées de façon à être des entiers satisfaisant à (4), l'équation (1) aura au moins $2l+1$ racines réelles, puisque p est impair.

Or les équations (4) s'écrivent

$$(5)\qquad \begin{cases} \alpha_1^p + qA_1\alpha_1^{p-1} + \ldots + qA_{p-1}\alpha_1 \pm q = +\beta_1, \\ \alpha_2^p + qA_1\alpha_2^{p-1} + \ldots + qA_{p-1}\alpha_2 \pm q = -\beta_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \alpha_{2l}^p + qA_1\alpha_{2l}^{p-1} + \ldots + qA_{p-1}\alpha_{2l} \pm q = -\beta_{2l}. \end{cases}$$

Elles permettront, en principe, de déterminer $2l$ des quantités $A_1, \ldots, A_{p-1}$ en fonction des $p-1-2l \geq 2$ autres. Si l'on choisit ces dernières de façon que (1) ait 2μ racines imaginaires ($\mu > 0$) et que $A_1, \ldots, A_{p-1}$ soient entiers, on aura $2\mu \leq p-2l-1 < \varphi(p)$, et G contiendra le groupe alterné.

Proposons-nous, par exemple, de déterminer les $2l$ premiers coefficients en fonction des autres : la méthode à employer dans les autres cas sera la même.

(5) donne

$$(6)\qquad \begin{cases} qA_1\alpha_1^{p-1} + \ldots + qA_{2l}\alpha_1^{p-2l} = M_1 + \beta_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ qA_1\alpha_{2l}^{p-1} + \ldots + qA_{2l}\alpha_{2l}^{p-2l} = M_{2l} - \beta_{2l}. \end{cases}$$

Le déterminant de ces équations est

$$\Delta = q^{2l}\begin{vmatrix} \alpha_1^{p-1}, & \alpha_1^{p-2}, & \ldots, & \alpha_1^{p-2l} \\ \alpha_2^{p-1}, & \alpha_2^{p-2}, & \ldots, & \alpha_2^{p-2l} \\ \ldots, & \ldots, & \ldots, & \ldots \\ \alpha_{2l}^{p-1}, & \alpha_{2l}^{p-2}, & \ldots, & \alpha_{2l}^{p-2l} \end{vmatrix} = q^{2l}(\alpha_1\alpha_2\ldots\alpha_{2l})^{p-2l}\Delta_2,$$

où

$$\Delta_2 = \begin{vmatrix} \alpha_1^{2l-1}, & \alpha_1^{2l-2}, & \ldots, & 1 \\ \alpha_2^{2l-1}, & \alpha_2^{2l-2}, & \ldots, & 1 \\ \ldots\ldots, & \ldots\ldots, & \ldots\ldots & \\ \alpha_{2l}^{2l-1}, & \alpha_{2l}^{2l-2}, & \ldots, & 1 \end{vmatrix}.$$

Δ_2 étant un déterminant de Vandermonde formé du produit des quantités $\alpha_i - \alpha_j$, avec $i > j$, $i = 1, 2, \ldots, 2l$, et $j = 1, 2, \ldots, 2l-1$, est $\neq 0$. Donc $\Delta \neq 0$.

Les équations (6) donnent alors

$$(7) \qquad A_1 = \frac{1}{\Delta}[(M_1 + \beta_1)\Delta'_1 - (M_2 - \beta_2)\Delta'_2 + \ldots],$$

et des expressions analogues pour $A_2, \ldots, A_{2l}$, $\Delta'_1, \Delta'_2, \ldots$ étant des déterminants mineurs de Δ.

On peut d'ailleurs, toujours, $A_{2l+1}, \ldots, A_{p-1}$ étant des entiers arbitrairement choisis, déterminer les quantités positives $\beta_1, \beta_2, \ldots, \beta_{2l}$ d'une infinité de manières, de façon que l'on ait

$$(8) \qquad M_1 + \beta_1 \equiv M_2 - \beta_2 \equiv \ldots \equiv M_{2l} - \beta_{2l} \equiv 0 \pmod{\Delta}.$$

moyennant quoi les équations (7) donneront pour $A_1, \ldots, A_{2l}$ des valeurs entières. A deux systèmes distincts des valeurs $\beta_1, \ldots, \beta_{2l}$ correspondront pour un même système de valeurs des quantités $\alpha_1, \ldots, \alpha_{2l}$, $A_{2l+1}, \ldots, A_{p-1}$ des équations (1) distinctes.

Ceci posé, il restera à déterminer les entiers arbitraires $A_{2l+1}, \ldots, A_{p-1}$, en nombre $p - 1 - 2l \geq 2$, de façon que (1) ait au moins deux racines imaginaires, moyennant quoi G contiendra le groupe alterné de p éléments.

Pour effectuer cette détermination de la manière la plus générale, on pourra recourir au théorème de Sturm. Nous nous contenterons (1)

(1) *Voir*, par exemple, NIEWENGLOWSKI, *Algèbre*, t. II, 2e édition, p. 383-385, et p. 410.

de remarquer que, d'après des théorèmes connus, l'équation (1) aura des racines imaginaires :

1° Si le polynome

$$(9) \qquad A_{2l}x^{p-2l} + A_{2l+1}x^{p-2l-1} + \ldots + A_{p-1}x \pm 1$$

est tel que la somme du nombre des variations que lui et son transformé en $-x$ présentent (théorème de Descartes) soit $< p - 2l$;

2° Si dans le premier membre de (9) il manque un terme entre deux termes de même signe, ou plus d'un terme entre deux termes de signe quelconque (théorème des lacunes);

3° Si le polynome (9) a au moins trois coefficients consécutifs, dont le premier ne fait pas partie, et qui sont en progression géométrique;

4° Si le polynome (9) a au moins quatre coefficients consécutifs, dont le premier ne fait pas partie, et qui sont en progression arithmétique.

Et ainsi de suite.

Dans tous ces cas, (1) jouit, en effet, des mêmes propriétés, et G contient le groupe alterné.

III.

LEMME I. — *Soit* V *une fonction symétrique entière à coefficients entiers des racines* $x_1, \ldots, x_n$ *d'une équation algébrique*

$$X = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0,$$

dont les coefficients, sauf le premier qui est égal à 1, *sont des entiers tous divisibles par le nombre premier* q. *Si* V *ne contient aucun terme indépendant de* $x, \ldots, x_n$, *on a*

$$V \equiv 0 \pmod{q}.$$

En effet, appliquons, pour le calcul de V en fonction des coefficients $a_1, \ldots, a_n$ la méthode de Waring. On aura, en conservant les

notations de Serret (¹),

$$\left\{\begin{array}{l} V = V_1 + A(-1)^{\alpha+\beta+\ldots+\lambda} a_1^{\alpha-\beta} a_2^{\beta-\gamma} \ldots a_n^{\lambda} = V_1 + P_1, \\ V_1 = V_2 + P_2, \\ \ldots\ldots\ldots\ldots, \\ V_{\mu-1} = V_\mu + P_{\mu-1}, \end{array}\right.$$

où V_μ est indépendant de $x_1, \ldots, x_n$.

Le terme qui occupe le premier rang dans V est $Ax_1^\alpha x_2^\beta \ldots x_n^\lambda$, et, d'après l'hypothèse faite sur V, $\alpha + \beta + \ldots + \lambda > 0$. Donc

$$V - V_1 \equiv 0 \pmod{q}.$$

De plus, $V - V_1$ ne contenant aucun terme indépendant de $x_1, \ldots, x_n$, V_1 n'en contiendra également aucun.

En continuant le raisonnement, on voit qu'il en est de même de $V_2, \ldots, V_{\mu-1}$, et que $P_2, P_3, \ldots$ sont $\equiv 0 \pmod{q}$. Donc $V_\mu = 0$.

V sera donc une fonction entière à coefficients entiers des coefficients $a_1, \ldots, a_n$ ne contenant aucun terme indépendant de ces coefficients, et, par suite, sera $\equiv 0 \pmod{q}$.

Lemme II. — *Soit*

$$X = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

un polynome de degré quelconque dont les coefficients, sauf le premier qui est égal à 1, *sont des entiers divisibles par* q (q *étant premier*), *et où* $a_n = \pm q^\mu (\mu \geq 1)$. X *a pour facteurs irréductibles des polynomes entiers à coefficients entiers où le terme de degré le plus élevé en* x *a pour coefficient l'unité, et où le terme indépendant de* x *est* $\pm q^\alpha$, *avec* $\alpha > 0$.

X *a au plus* μ *facteurs irréductibles.*

(¹) Serret, *Algèbre supérieure*, t. I, p. 385 et suiv.; 1885.

Nous nous contentons d'énoncer ce lemme qui généralise un lemme connu et s'établit comme lui (¹).

THÉORÈME II. — *L'équation irréductible*

$$x^{2\rho} \pm qx \pm q = 0 \qquad (q \text{ premier}) \tag{10}$$

a son groupe G *d'ordre* $g \equiv 0 \pmod{2\rho(2\rho-1)}$, *sauf peut-être pour des valeurs de* q *limitées en fonction de* ρ. *Si* $2\rho - 1$ *est premier,* G *est deux fois transitif, sauf peut-être pour les mêmes valeurs de* q.

Soient l'équation

$$f(x) = x^n + a_{n-1}x + a_n = 0, \tag{11}$$

$$\text{avec } n = 2\rho,\ a_{n-1} = \pm q,\ a_n = \pm q,$$

$$x_1, \quad x_2, \quad \ldots, \quad x_n, \tag{12}$$

ses racines. Considérons l'équation

$$\varphi(z) = 0, \tag{13}$$

de degré $\nu = C_n^2 = \frac{n(n-1)}{2}$ ayant pour racines les C_n^2 quantités $z_{i,j} = x_i + x_j (i \neq j)$. Les deux équations (11) et (13) sont équivalentes.

En effet, la résolution de (11) entraîne évidemment celle de (13); réciproquement, les égalités

$$x_2 + x_3 = z_{2,3}, \quad x_1 + x_2 = z_{1,2}, \quad x_1 + x_3 = z_{1,3}, \quad \ldots, \quad x_1 + x_n = z_{1,n}$$

(¹) SERRET, *Algèbre supérieure*, t. I, p. 244; 1885.

Une démonstration semblable montrera encore que si

$$X = x^n + A_1 x^{n-1} + \ldots + A_i x^{n-i} + \ldots \pm q^\mu (\mu > 0)$$

est tel que $A_j \equiv 0 \pmod{q}$ quand $j > i$, X n'a de diviseur rationnel $x^\nu + \ldots \pm 1$ que si $\nu \leq i$. Si, par exemple, $i = 1$, il faudra $\nu = 1$; alors si X n'a pas la racine ± 1, c'est-à-dire *a fortiori* si $A_1 \neq \pm 1 + nq$, X est irréductible.

Comp. NETTO, *Math. Ann.*, t. XLVIII, 1896, p. 82 et suiv.

permettant de déterminer les racines (12) en fonction linéaire rationnelle des $z_{i,j}$, la résolution de (13) entraîne celle de (11).

Ceci posé, je dis que l'on a

$$(14)\qquad \begin{cases} \varphi(z) = z^{\nu} + \ldots + A_k z^{\nu-k} + \ldots \pm q^{\rho}, \\ \text{avec } A_k \equiv 0 \pmod{q}, \quad \text{quand } 0 < k < \nu. \end{cases}$$

En effet, l'équation (13) est le résultat de l'élimination (1) de x entre les équations (11) et

$$(15)\quad \Phi(x, z) = f'(x) + \frac{z - 2x}{1.2} f''(x) + \ldots + \frac{(z-2x)^{n-1}}{n!} f^{n}(x) = 0.$$

Si l'on pose

$$(16)\qquad |\Psi(z)|^2 = \Phi(x_1, z)\Phi(x_2, z)\ldots\Phi(x_n, z),$$

on pourra prendre

$$(17)\qquad \varphi(z) = \Psi(z).$$

Alors, pour prouver que (14) a lieu, je dis qu'il suffit de montrer que

$$(18)\qquad \begin{cases} |\Psi(z)|^2 = z^{2\nu} + \ldots + B_k z^{2\nu-k} + \ldots + q^{2\rho}, \\ \text{avec } B_k \equiv 0 \pmod{q}, \quad \text{quand } 0 < k < 2\nu. \end{cases}$$

En effet, on aura

$$(19)\qquad \begin{cases} |\Psi(z)|^2 = z^{2\nu} + 2A_1 z^{2\nu-1} + (A_1^2 + 2A_2) z^{2\nu-2} + \ldots \\ \qquad + (A_i^2 + 2A_{i-1}A_{i+1} + \ldots + 2A_{2i}) z^{2\nu-2i} \\ \qquad + (2A_iA_{i+1} + 2A_{i-1}A_{i+2} + \ldots + 2A_{2i+1}) z^{2\nu-2i-1} + \ldots + A_\nu^2 \end{cases}$$

et

$$\Psi(z) = z^{\nu} + A_1 z^{\nu-1} + \ldots + A_\nu.$$

(1) SERRET, *Algèbre supérieure*, t. I, p. 208; 1885.

D'abord $A_1, \ldots, A_\nu$ sont entiers, d'après un lemme connu (¹), puisque $B_1, \ldots, B_{2\nu-1}$ le sont. Identifiant (18) et (19), on obtient

$$(20)\qquad \begin{cases} 2A_1 = B_1 \equiv 0 \pmod q, \\ A_1^2 + 2A_2 = B_2 \equiv 2A_2 \pmod q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ A_\nu^2 = q^{2\rho}, \end{cases}$$

c'est-à-dire que (14) a lieu si $q > 2$.

Établissons donc (18).

D'après (16), le coefficient de la plus haute puissance $z^{2\nu}$ de z dans (18) est $\left[\frac{f^n(x)}{n!}\right]^n = 1$. Les coefficients des termes de (18), autres que le premier, sont une somme de termes provenant du terme $(z-2x_1)^{n-1}\ldots(z-2x_n)^{n-1}$, ou des autres termes du produit (16). Les seuls qui ne contiennent aucune des racines $x_1, \ldots, x_n$ sont, en remarquant que

$$\frac{f^j(x)}{j!} = \frac{1}{j!}\left[n(n-1)\ldots(n-j+1)x^{n-j} + \ldots + j!\,a_{n-j}\right],$$

$$\text{avec } a_0 = 1, \quad a_{n-j} = 0, \quad \text{si } n > j > 1,$$

des produits de quantités a_{n-j}, dont une au moins est telle que $j < n$, et, par suite, sont divisibles par q. Ces coefficients sont donc de la forme V + multiple de q, V étant une fonction symétrique entière à coefficients entiers des racines $x_1, \ldots, x_n$, ne contenant aucun terme indépendant de $x_1, \ldots, x_n$; d'après le lemme I, V est divisible par q, et, par suite, ces coefficients sont divisibles par q.

Enfin, le terme A_ν^2 indépendant de z dans (18) est

$$A_\nu^2 = \prod_1^n {}^i N_i = \prod_1^n {}^i \left[f'(x_i) - \frac{2x_i}{2!}f''(x_i) + \ldots + \frac{(-2x_i)^{n-1}}{n!}f^n(x_i)\right],$$

avec

$$N_i = a_{n-1} + x_i^{n-1}\left[C_n^1 - 2C_n^2 + 2^2C_n^3 + \ldots + (-1)^{n-1}2^{n-1}C_n^n\right].$$

(¹) SERRET, *Algèbre supérieure*, t. I, p. 243; 1885.

Or

$$(1-2)^n = 1 - 2C_n^1 + 2^2 C_n^2 - \ldots + (-1)^n 2^n C_n^n = (-1)^n = 1,$$

puisque n est pair : il en résulte de suite que le coefficient de x_i^{n-1} dans X_i est nul et

$$A_i^2 = a_{n-1}^n = q^{2p},$$

puisque $a_{n-1} = \pm q$.

Les équations (14) et (18) sont ainsi établies.

Appliquons le lemme II à l'équation (14) : $\varphi(z)$ a σ facteurs irréductibles $\varphi_1, \varphi_2, \ldots, \varphi_\sigma$ de degrés respectifs $d_1, d_2, \ldots, d_\sigma$, avec $\sigma \leq p$; les termes indépendants de z dans ces facteurs sont respectivement $q^{b_1}, q^{b_2}, \ldots, q^{b_\sigma}$ et tous > 1; l'on a

$$(21) \quad \begin{cases} d_1 + d_2 + \ldots + d_\sigma = \dfrac{n(n-1)}{2} = p(2p-1), \\ b_1 + b_2 + \ldots + b_\sigma = p. \end{cases}$$

Considérons les équations irréductibles

$$(22) \qquad \varphi_1 = 0, \qquad \varphi_2 = 0, \qquad \ldots, \qquad \varphi_\sigma = 0.$$

Soient $F_1, F_2, \ldots, F_\sigma$ leurs groupes de substitutions, d'ordres respectifs $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_\sigma$, divisibles par $d_1, d_2, \ldots, d_\sigma$ respectivement (1), G le groupe de (10), d'ordre $\mathcal{G}$.

La résolution de l'équation (10) réduit le groupe de $\varphi_i = 0$ à l'unité, puisqu'elle entraîne la résolution de (13), par suite celle des équations (22). Il en résulte (2) que la résolution de $\varphi_i = 0$ réduit le groupe de (13) à un groupe d'ordre $\frac{\mathcal{G}}{\mathcal{F}_i}$. Donc $\mathcal{G}$ est divisible par $\mathcal{F}_i$, par suite par d_i. La connaissance des quantités d_i peut donc donner des indications sur la valeur de $\mathcal{G}$.

---

(1) JORDAN, *Traité des subst.*, Liv. III, Chap. I, th. II.

(2) *Id.*, th. XIII.

Je dis que l'on a les inégalités

$$q^{b_i} \leq 2^{d_i}\left(1 + q^{\frac{1}{2\rho-1}}\right)^{d_i}. \tag{23}$$

En effet, soit α une limite supérieure du module des racines de (10); on aura, en désignant par $|\theta|$ le module d'une quantité quelconque θ

$$z_{i,j} = x_i + x_j,$$
$$|z_{i,j}| \leq |x_i| + |x_j| \leq 2\alpha;$$

or q^{b_i} est le produit des d_i racines de $\varphi_i = 0$ et, par suite,

$$q^{b_i} \leq (2\alpha)^{d_i}; \tag{24}$$

il reste à déterminer α.

(10) donne

$$|x_i^{2\rho}| \leq |a_{n-1}x_i + a_n| \leq q|x_i| + q,$$

et toute limite supérieure β des racines réelles positives de

$$x^{2\rho} - qx - q = 0$$

est telle que $|x_i| \leq \beta$, en sorte qu'on peut prendre $\beta = \alpha$.

Choisissons $\beta = 1 + q^{\frac{1}{2\rho-1}}$; (24) entraînera (23).

Ceci posé, les inégalités (23) ne seront toutes possibles, quand q est suffisamment grand, ρ étant donné, que si l'on a

$$d_i \geq (2\rho - 1)b_i \qquad (i = 1, 2, \ldots, \sigma). \tag{25}$$

Supposons qu'il en soit ainsi; on ne pourra avoir, pour une valeur particulière τ de i,

$$d_\tau > (2\rho - 1)b_\tau,$$

sans quoi les inégalités (25) additionnées membre à membre, en tenant compte de cette dernière, donneraient

$$d_1 + \ldots + d_\sigma = \rho(2\rho - 1) > (2\rho - 1)(b_1 + \ldots + b_\sigma) = \rho(2\rho - 1),$$

ce qui est absurde. Donc (25) entraîne

$$d_i = (2\rho - 1)\, b_i \qquad (i = 1, 2, \ldots, \sigma)$$

et

$$d_i \equiv 0 \pmod{2\rho - 1}.$$

On en conclut

$$g \equiv 0 \pmod{2\rho - 1}.$$

Le théorème proposé résulte alors immédiatement de ce que : 1° $g \not\equiv 0 \pmod{2\rho}$ puisque (10) est irréductible et G transitif; 2° quand $2\rho - 1$ est premier, G contient une substitution circulaire d'ordre $2\rho - 1$ et est deux fois transitif. C. Q. F. D.