BULLETIN DE LA S. M. F.

DE POLIGNAC

Sur la représentation analytique des substitutions

Bulletin de la S. M. F., tome 9 (1881), p. 59-67

<http://www.numdam.org/item?id=BSMF_1881__9__59_0>

Sur la représentation analytique des substitutions;

par M. DE POLIGNAC.

(Séance du 18 février 1881.)

Pour qu'une fonction entière $\psi(x)$ soit apte à représenter une substitution $[x, \psi(x)]$ entre p lettres, elle doit satisfaire à certaines conditions. Quand p est un nombre premier, M. Hermite a donné le critérium de ce caractère. Il consiste en ce que le coefficient de x^{p-1} soit divisible par p dans les $p-2$ premières puissances de la fonction, lorsque les exposants y ont été abaissés au-dessous de p au moyen de la congruence $x^p \equiv x \pmod{p}$.

Inversement, une substitution entre k lettres, étant donnée la formule d'interpolation de Lagrange, peut servir à la représenter analytiquement, ainsi que le fait remarquer M. Jordan dans le *Traité des substitutions* (Chap. II). Le but de cette Note est de donner une forme générale pour toutes les fonctions entières jouissant de la propriété en question.

J'observe d'abord qu'au moyen du théorème de Fermat on pourra, p étant premier, abaisser dans toute fonction entière les exposants de x au-dessous de $p-1$.

Soit donc

$$\psi(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{p-2} x^{p-2}.$$

Pour que cette fonction puisse représenter une substitution, il faut et il suffit que les nombres $\psi(0), \psi(1), \ldots, \psi(p-1)$ donnent à l'ordre près les résidus $0, 1, 2, \ldots, p-1$ suivant le module p.

Posons

$$\psi(x) = a_0 + \varphi(x);$$

on aura

$$\varphi(0) = 0.$$

a_0 doit être supposé premier avec p; il en résulte, pour les conditions du problème,

$$\varphi(1) \equiv r_1, \ \varphi(2) \equiv r_2, \ \ldots, \ \varphi(p-1) \equiv r_{p-1},$$

les quantités r ne différant que par l'ordre des nombres

$$1, 2, 3, \ldots, p-1.$$

Nous arrivons donc, en apparence, à un système de $p-1$ congruences entre $p-2$ inconnues $a_1, a_2, \ldots, a_{p-2}$; mais ce système se réduit à $p-2$ congruences distinctes, attendu que la somme de toutes les congruences est nulle suivant le module p. Cela résulte, pour les premiers membres, de ce que la somme des puissances semblables des $p-1$ premiers nombres entiers est divisible par p, jusqu'à la puissance $p-2$ inclusivement, et, pour les seconds membres, de la convention même relative aux quantités r.

Les conditions générales du problème sont donc exprimées par le système suivant de $p-2$ congruences :

$$\left.\begin{array}{l} a_1 + a_2 + \ldots + a_{p-2} \equiv r_1 \\ 2a_1 + 2^2 a_2 + \ldots + 2^{p-2} a_{p-2} \equiv r_2 \\ 3a_1 + 3^2 a_2 + \ldots + 3^{p-2} a_{p-2} \equiv r_3 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (p-2)a_1 + (p-2)^2 a_2 + \ldots + (p-2)^{p-2} a_{p-2} \equiv r_{p-2} \end{array}\right\} \pmod{p}.$$

Le déterminant de ce système a une valeur connue, différente de zéro; les coefficients $a_1, a_2, \ldots, a_{p-2}$ seront donc exprimables en fonction des quantités $r_1, r_2, \ldots, r_{p-2}$.

Soient ces valeurs

$$a_1 \equiv \rho_1, \quad a_2 \equiv \rho_2, \quad \ldots, \quad a_{p-2} \equiv \rho_{p-2};$$

on aura

$$\psi(x) = a_0 + \rho_1 x + \rho_2 x^2 + \ldots + \rho_{p-2} x^{p-2}.$$

Dans cette forme symbolique, a_0 est un nombre quelconque non divisible par p. Les symboles ρ sont des fonctions entières linéaires des quantités $r_1, r_2, \ldots, r_{p-2}$, dont les coefficients sont numériques et dépendent du nombre premier p. Les quantités r elles-mêmes sont des indéterminées assujetties à la condition d'être toutes *distinctes et différentes de zéro suivant le module p*.

Exemple. — Pour $p = 5$, on a

$$\psi(x) = a + (3r_1 + r_2 + 2r_3)x + 2(r_2 + r_3)x^2 + (3r_1 + 2r_2 + r_3)x^3,$$

forme analytique générale d'une substitution de cinq lettres.

En y faisant $a = 0$, $r_1 = 1$, $r_2 = 2$, $r_3 = 3$, on doit retomber sur la substitution identique $[x, x]$: c'est ce qu'il est facile de vérifier.

On peut obtenir les symboles ρ sous forme explicite. Soient Δ le déterminant du système caractéristique de congruences, $M_{n,1}$, $M_{n,2}$, ... les déterminants mineurs des éléments successifs de la $n^{\text{ième}}$ colonne. On a

$$\Delta a_n = M_{n,1} r_1 + M_{n,2} r_2 + \ldots + M_{n,h} r_h + \ldots + M_{n,p-2} r_{p-2}.$$

Adoptons les signes conventionnels suivants

$$1.2.3\ldots k = \Pi(k),$$
$$\Pi(k)\ \Pi(k+1)\ \Pi(k+2)\ldots\Pi(N) = \overline{\Pi\Pi}(k, N),$$

$\sum_1^N (h, m)$ = *somme des produits m à m des nombres entiers depuis* 1 *jusqu'à* N, *défalcation faite de h,* autrement dit des nombres $1, 2, \ldots, h-1, h+1, \ldots, N$,

et rappelons que l'on a

$$\begin{vmatrix} a_1 & a_1^2 & \ldots & a_1^{n-1} & a_1^{n+1} & a_1^{n+2} & \ldots & a_1^m \\ a_2 & a_2^2 & \ldots & a_2^{n-1} & a_2^{n+1} & a_2^{n+2} & \ldots & a_2^m \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m-2} & a_{m-2}^2 & \ldots & a_{m-2}^{n-1} & a_{m-2}^{n+1} & a_{m-2}^{n+2} & \ldots & a_{m-2}^m \\ a_{m-1} & a_{m-1}^2 & \ldots & a_{m-1}^{n-1} & a_{m-1}^{n+1} & a_{m-1}^{n+2} & \ldots & a_{m-1}^m \end{vmatrix} = a_1 a_2 \ldots a_{m-1} \times (a_{m-1} - a_{m-2}) \times (a_{m-2} - a_{m-3}) \ldots \times (a_2 - a_1) \sum (m-n),$$

expression dans laquelle le dernier facteur désigne la somme des produits $m-n$ à $m-n$ des quantités $a_1, a_2, \ldots$. Les déterminants mineurs M seront du type de celui-ci, présentant une lacune dans la suite naturelle des exposants, et l'on trouvera, tout calcul fait,

$$\Delta = \overline{\Pi\Pi}(1, p-2),$$
$$M_{n,h} = (-1)^{n+h} \frac{\overline{\Pi\Pi}(1, h-3)}{\Pi(h)\,\Pi(p-2-h)} \sum_1^{p-2} (h, p-2-n).$$

Si l'on observe qu'en vertu du théorème de Wilson on a

$$\Pi(p-2) \equiv 1 \pmod{p},$$

il en résultera

$$\Delta \equiv \overline{\Pi\Pi}(1, p-3);$$

par suite, posant

$$A_{n,h} = \frac{M_{n,h}}{\Delta},$$

il viendra

$$A_{n,h} \equiv (-1)^{n+h} \frac{\overset{p-2}{\underset{1}{S}}(h, p-2-n)}{\Pi(h)\,\Pi(p-2-h)}$$

et

$$a_n \equiv \sum_{h=1}^{h=p-2} (-1)^{n+h} \frac{\overset{p-2}{\underset{1}{S}}(h, p-2-n)}{\Pi(h)\,\Pi(p-2-h)}\, r_h,$$

formule susceptible d'une notable simplification, ainsi qu'on le verra plus loin.

Quand une substitution est donnée, les valeurs particulières de $a_0, r_1, r_2, \ldots$ s'en déduisent immédiatement, par suite la fonction $\psi(x)$ qui la représente. Inversement, si la fonction $\psi(x)$ est donnée, le système de congruences ci-dessus déterminera les quantités r_1, $r_2, \ldots, r_{p-2}$ en fonction des coefficients, et la validité du caractère consiste en ce que les valeurs trouvées soient toutes différentes entre elles et différentes de zéro.

L'hypothèse

$$a_0 = 0, \quad r_1 = 1, \quad r_2 = 2, \quad \ldots, \quad r_{n-1} = n-1$$

correspond à une substitution ne déplaçant pas les n premières lettres. On peut donc appliquer l'analyse précédente aux substitutions composées d'un nombre quelconque de lettres non premier. Il suffira de prendre p égal au nombre premier immédiatement supérieur au nombre considéré.

Dans ce mode de représentation, la somme de deux substitutions ne donne pas, en général, une substitution, mais toute substitution peut s'exprimer linéairement en fonction de $p-2$ substitutions convenablement choisies.

En effet, soit une substitution donnée

$$\psi'(x) = A + \Phi(x).$$

Formons avec $p-2$ autres substitutions la fonction

$$f(x) = \alpha_0 + \alpha_1 \psi_1(x) + \alpha_2 \psi_2(x) + \ldots + \alpha_{p-2}\, \psi_{p-2}(x),$$

qui peut s'écrire

$$f(x) = a + \alpha_1 \varphi_1(x) + \alpha_2 \varphi_2(x) + \ldots + \alpha_{p-2} \varphi_{p-2}(x).$$

L'identification de $f(x)$ avec $\Psi(x)$ donnera d'abord

$$\Phi(n) \equiv \alpha_1 \varphi(n) + \alpha_2 \varphi_2(n) + \ldots + \alpha_{p-2} \varphi_{p-2}(n) \pmod{p},$$
$$n = 1, 2, \ldots, p-2,$$

système de $p-2$ congruences qui fera connaître $\alpha_1, \alpha_2, \ldots, \alpha_{p-2}$, à la seule condition que le déterminant formé avec les quantités φ ne soit pas congru à p. Ensuite

$$a \equiv A,$$

congruence qui déterminera α_0.

Si l'on se donne les quantités φ, les quantités Φ restant, au contraire, indéterminées, on aura l'expression générale d'une substitution en fonction linéaire de $p-2$ autres.

Reprenons la formule

$$A_{n,h} = (-1)^{n+h} \frac{\sum_1^{p-2} (h, p-2-n)}{\Pi(h)\,\Pi(p-2-h)}.$$

Il est facile de voir qu'en vertu du théorème de Wilson on a généralement

$$\Pi(h+1)\,\Pi(p-2-h) \equiv (-1)^h \pmod{p};$$

il en résulte

$$A_{n,h} = (-1)^n (h+1) \sum_1^{p-2} (h, p-2-n).$$

On peut encore simplifier cette formule.

En vertu de l'identité

$$x^{p-1} - 1 = (x-1)(x-2)\ldots\overline{(x-p-1)} + p\,F(x)$$

qui résulte du théorème de Fermat, on a

$$\sum_{1}^{p-1}(m) \equiv 0 \pmod{p},$$

excepté pour $m = p - 1$. Ici le symbole S désigne la somme des produits m à m des nombres entiers $1, 2, \ldots, p-1$.

D'ailleurs, on a évidemment

$$\sum_{1}^{p-1}(m) = \sum_{1}^{p-2}(m) + (p-1)\sum_{1}^{p-2}(m-1),$$

d'où il résulte

$$\sum_{1}^{p-2}(m) \equiv \sum_{1}^{p-2}(m-1) \pmod{p},$$

et de cette congruence on déduit, en faisant décroître m,

$$\sum_{1}^{p-2}(m) \equiv 1 \pmod{p}.$$

D'autre part, la définition de nos symboles S donne lieu à l'identité

$$\sum_{1}^{p-2}(m) = \sum_{1}^{p-2}(h, m) + h\sum_{1}^{p-2}(h, m-1);$$

on a donc finalement

$$\sum_{1}^{p-2}(h, m) + h\sum_{1}^{p-2}(h, m-1) \equiv 1.$$

Désignons, pour abréger, cette congruence par

$$U_0 \equiv 1 \pmod{p},$$

et changeons-y m successivement en $m-1$, $m-2$, ..., 1, h restant constant. Nous aurons de nouvelles congruences

$$U_1 \equiv 1, \quad U_2 \equiv 1, \quad \ldots, \quad U_{m-1} \equiv 1 \pmod{p}.$$

Multipliant généralement U_i par $(-1)^i h^i$ et ajoutant, il viendra

$$\sum_{i=0}^{i=m-1} (-1)^i h^i U_i = \sum_{1}^{p-2} (h, m) + (-1)^{m-1} h^m \equiv \sum_{i=0}^{i=m-1} (-1)^i h^i$$

ou

$$\sum_{1}^{p-2} (h, m) \equiv \sum_{i=0}^{i=m} (-1)^i h^i.$$

Le second membre est la différence des deux progressions géométriques $1 + h^2 + h^4 + \ldots$ et $h + h^3 + h^5 + \ldots$, qui est égale à $\frac{1 + (-1)^m h^{m+1}}{1 + h}$. On a donc

$$\sum_{1}^{p-2} (h, m) \equiv \frac{1 + (-1)^m h^{m+1}}{1 + h} \pmod{p},$$

et la valeur trouvée en dernier lieu pour $A_{n,h}$ devient, en posant $m = p - 2 - n$ et toutes réductions faites,

$$A_{n,h} \equiv (-1)^n - h^{p-1-n} \pmod{p},$$

formule qui peut aussi s'écrire

$$A_{n,h} \equiv (-1)^n - \frac{1}{h^n} \pmod{p},$$

à cause du théorème de Fermat.

En résumé, toute substitution pourra se mettre sous la forme $a + \varphi(x)$, le coefficient de x^n dans $\varphi(x)$ étant

$$\sum_{h=1}^{h=p-2} \left[(-1)^n - \frac{1}{h^n} \right] r_h.$$

Voici quelques conséquences immédiates des dernières formules :

1° Le coefficient de r_1 dans chaque terme de $\varphi(x)$ est nul si n est pair et égal à -2, ou, ce qui est la même chose, à $p - 2$, si n est impair.

2° Le coefficient de x^{p-2} est immédiatement donné. On a

$$a_{p-2} \equiv -[2r_1 + 3r_2 + \ldots + (p-1) r_{p-2}].$$

3° Pour $n = \frac{p-1}{2}$, on a

$$A_{\frac{p-1}{2},h} = (-1)^{\frac{p-1}{2}} - h^{\frac{p-1}{2}};$$

on en conclut, pour le terme du milieu de $\varphi(x)$,

$$a_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \cdot 2(r_{\alpha_1} + r_{\alpha_2} + r_{\alpha_3} + \dots),$$

expression dans laquelle $\alpha_1, \alpha_2, \dots$ seront les *résidus quadratiques* si p est de la forme $4N - 1$ et les *non-résidus* si p est de la forme $4N + 1$.

Il existe une loi de récurrence entre les termes $A_{n,h}$ correspondant à une même valeur de n, qui réduit de moitié les calculs à faire.

On a, d'après la formule générale,

$$\begin{aligned} A_{n,2+k} &= (-1)^n - (2+k)^{p-1-n}, \\ A_{n,p-(2+k)} &= (-1)^n - [p-(2+k)]^{p-1-n} \\ &\equiv (-1)^n + (-1)^{p-n}(2+k)^{p-1-n}, \end{aligned}$$

d'où il résulte immédiatement pour n pair

$$A_{n,2+k} \equiv A_{n,p-(2+k)},$$

pour n impair

$$A_{n,2+k} + A_{n,p-(2+k)} \equiv -2.$$

Si l'on observe que $A_{n,1} = 0$ quand n est pair, on pourra énoncer ainsi ces deux relations :

Pour n pair, les termes à égale distance des extrêmes sont égaux.

Pour n impair, abstraction faite du premier terme $A_{n,1}$ *qui est toujours* -2, *la somme des termes à égale distance des extrêmes est égale à* -2 (*suivant le module p*).

Par un calcul tout semblable on trouvera pour le terme du milieu, qui correspond à $h = \frac{p-1}{2}$,

$$A_{n,\frac{p-1}{2}} \equiv (-1)^n(1 - 2^n).$$

Grâce à ces remarques, on trouvera aisément : pour $p = 7$,

$$\begin{aligned}\psi(x) = a &+ (5r_1 + 2r_2 + r_3 + 4r_4 + 3r_5)\,x \\ &- (r_2 + 3r_3 + 3r_4 + r_5)\,x^2 \\ &- 2(r_1 + r_2 + r_4)\,x^3 + (4r_2 - r_3 - r_4 + 4r_5)x^4 \\ &+ (5r_1 + 4r_2 + 3r_3 + 2r_4 + r_5)\,x^5;\end{aligned}$$

pour $p = 11$,

$$\begin{aligned}\psi(x) = a &+ (9r_1 + 4r_2 + 6r_3 + 7r_4 + r_5 + 8r_6 + 2r_7 + 3r_8 + 5r_9)\,x \\ &+ (9r_2 + 7r_3 + 3r_4 - 3r_5 - 3r_6 + 3r_7 + 7r_8 + 9r_9)\,x^2 \\ &+ (9r_1 + 3r_2 + r_3 + 5r_4 - 4r_5 + 2r_6 + 4r_7 - 3r_8 - 5r_9)\,x^3 \\ &+ (3r_2 - 2r_3 - 3r_4 - 4r_5 - 4r_6 - 3r_7 - 2r_8 + 3r_9)\,x^4 \\ &- 2(r_1 + r_3 + r_4 + r_5 + r_9)\,x^5 \\ &- (4r_2 + 3r_3 + 2r_4 - 3r_5 - 3r_6 + 2r_7 + 3r_8 + 4r_9)\,x^6 \\ &+ (9r_1 + 2r_2 + 5r_3 + r_4 + 6r_5 + 3r_6 - 3r_7 + 4r_8 - 4r_9)\,x^7 \\ &- (3r_2 - 3r_3 + 4r_4 + 2r_5 + 2r_6 + 4r_7 - 3r_8 + 3r_9)\,x^8 \\ &+ (9r_1 + 8r_2 + 7r_3 + 6r_4 + 5r_5 + 4r_6 + 3r_7 + 2r_8 + r_9)\,x^9.\end{aligned}$$