NOUVELLES ANNALES DE MATHÉMATIQUES

MATHIEU

Des fonctions algébriques de plusieurs quantités, de leur formation, et des permutations qui les laissent invariables

Nouvelles annales de mathématiques 2e série, tome 1 (1862), p. 227-242

<http://www.numdam.org/item?id=NAM_1862_2_1__227_1>

DES FONCTIONS ALGÉBRIQUES DE PLUSIEURS QUANTITÉS, de leur formation, et des permutations qui les laissent invariables;

PAR M. MATHIEU,
Professeur.

Supposons une fonction de n quantités $a, b, c, \ldots, l$,

$$F(a, b, c, \ldots, k, l);$$

et remplaçons-y les lettres a, b, c, ..., k, l respectivement par les lettres a', b', c', ..., k', l' qui sont supposées être les mêmes lettres dans un ordre différent, la fonction deviendra

$$F\ (a',\ b',\ c',\ \ldots,\ k',\ l'),$$

et l'on dit que l'on a fait sur la fonction donnée la substitution

$$\begin{pmatrix} a & b & c & d & \ldots & k & l \\ a' & b' & c' & d' & \ldots & k' & l' \end{pmatrix} (*).$$

Considérons, par exemple, la fonction des quatre quantités a, b, c, d,

$$ab^2 + cd^2;$$

faisons sur cette fonction la substitution

$$\begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix},$$

cette fonction sera changée en celle-ci :

$$da^2 + bc^2,$$

et la fonction a changé de valeur. Faisons encore sur la fonction $ab^2 + cd^2$ la substitution

$$\begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix},$$

(*) Il serait plus naturel de donner aux expressions

$$a\ b\ c\ d \ldots l \quad \text{et} \quad a'\ b'\ c'\ d' \ldots l'$$

le nom de *dispositions* ou un autre nom analogue, afin de réserver le nom de *permutation* à l'opération qui consiste à permuter les lettres de la fonction; car le mot de *substitution* ne rappelle pas que les lettres primitives et les lettres substituées soient les mêmes à l'ordre près.

nous aurons la fonction

$$cd^2 + ab^2,$$

et l'on voit que par cette seconde substitution la fonction n'a pas changé de valeur.

Disposons les lettres a, b, c, ..., l sur un cercle, et dans l'ordre suivant lequel elles sont énoncées; puis mettons chacune d'elles à la place de celle qui la précède, nous aurons fait sur ces lettres une substitution qui est dite *circulaire;* d'après ce qui vient d'être dit, on représenterait cette substitution par l'expression

$$\begin{pmatrix} a & b & c & d & \ldots & l \\ b & c & d & e & & a \end{pmatrix},$$

mais on l'écrit plus simplement dans une seule ligne

$$(a\ b\ c\ d\ \ldots\ l).$$

Soit par exemple la fonction

$$ab + cd,$$

faisons la substitution circulaire

$$\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} \quad \text{ou} \quad (a\ b\ c\ d),$$

et nous aurons la nouvelle valeur

$$bc + da;$$

faisons ensuite sur $ab + cd$ la substitution circulaire

$$\begin{pmatrix} a & c & b & d \\ c & b & d & a \end{pmatrix} \quad \text{ou} \quad (a\ c\ b\ d),$$

et nous trouvons la valeur

$$cd + ba$$

qui est identique à la valeur considérée.

Toute substitution, si elle n'est pas circulaire, peut être décomposée en un certain nombre de substitutions circulaires.

En effet, soit S une substitution quelconque et a une lettre qui en fait partie; cette substitution remplacera la lettre a par une certaine autre lettre que nous appellerons b; cette substitution remplace la lettre b elle-même par une autre; si cette lettre est a, la substitution S renferme la substitution circulaire (ab). Si au contraire S remplace b par une lettre c différente de a, mais qu'elle substitue à c la lettre a, la substitution S contient la substitution circulaire (abc). Imaginons que l'on poursuive cette manière d'opérer, et il est évident que la lettre a fait partie d'une substitution circulaire contenue dans la substitution S. Soit f une lettre qui n'appartienne pas à cette substitution circulaire et qui soit permutée par S; on trouvera de même la substitution circulaire dont f fait partie. Et ainsi de suite.

Ainsi prenons pour exemple la substitution

$$\begin{pmatrix} a & b & c & d & e \\ c & e & a & b & d \end{pmatrix};$$

elle peut se décomposer en les deux substitutions circuculaires

$$(a\ c), \quad (b\ e\ d).$$

Considérons encore la substitution

$$(\alpha) \qquad \begin{pmatrix} a & b & c & d & e & f & g & h & i & k \\ b & d & h & c & g & e & k & a & f & i \end{pmatrix};$$

elle peut se décomposer en les deux substitutions circulaires

$$(a\ b\ d\ c\ h) \quad (e\ g\ k\ i\ f).$$

Les substitutions circulaires en lesquelles se décompose une substitution quelconque sont appelées les *cycles* de la substitution. Si le nombre des lettres de chacun des cycles d'une substitution est le même, la substitution est dite *régulière;* ainsi la substitution (α) est régulière, parce qu'elle se décompose en deux cycles qui renferment tous deux cinq lettres.

Il est clair que si une fonction est invariable par deux substitutions A et B, elle est invariable par la substitution que l'on obtient en faisant d'abord la substitution A, ensuite B; ainsi, par exemple, la fonction $ab + cd$ est invariable par chacune des deux substitutions

$$(a\ b),\qquad (a\ c\ b\ d);$$

si on effectue la première, puis la seconde, on se trouve avoir fait la substitution

$$\begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} \quad \text{ou} \quad (a\ d)\ (b\ c),$$

qui laisse invariable la fonction $ab + cd$.

Soient

$$\mathrm{A},\ \mathrm{B},\ \mathrm{C},\ \ldots,\ \mathrm{G}$$

différentes substitutions effectuées sur les n lettres d'une fonction

$$\mathrm{F}(a,\ b,\ c,\ \ldots,\ l),$$

et qui laissent cette fonction invariable; si nous faisons successivement dans un ordre quelconque quelques-unes de ces substitutions, nous obtiendrons en général d'autres substitutions, qui laisseront la fonction F invariable; toutes les substitutions ainsi formées sont appelées les *dérivées* des substitutions A, B, ..., G. On considère

$$\begin{pmatrix} a & b & c & \ldots & l \\ a & b & c & \ldots & l \end{pmatrix}$$

comme faisant partie de ces substitutions dérivées.

Ainsi, par exemple, soient les deux substitutions

$$(\beta) \qquad (ab)\,(cd), \quad (ad)\,(bc),$$

qui laissent invariable la fonction

$$(a-b)\,(c-d).$$

On voit facilement que toutes les dérivées des substitutions (β) sont les quatre substitutions

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \ (ab)(cd), \quad (ad)(bc), \quad (ac)(bd)$$

et ces quatre substitutions laissent invariable la fonction $(a-b)\,(c-d)$.

Si sur la fonction

$$(\gamma) \qquad F(a,\, b,\, c,\, \ldots,\, l)$$

on fait les M substitutions qui la laissent invariable, on obtient M valeurs égales de cette fonction, savoir F, F_1, $F_2, \ldots, F_{M-1}$.

Faisons ensuite sur la fonction (γ) la substitution

$$\begin{pmatrix} a & b & c & \ldots & l \\ a' & b' & c' & \ldots & l' \end{pmatrix}$$

qui change cette fonction; a', b', c', ..., l' sont par conséquent les lettres a, b, c, ..., l prises dans un autre ordre; nous aurons la fonction

$$(\delta) \qquad F(a',\, b',\, c',\, \ldots,\, l');$$

changeons dans les M substitutions qui laissent la fonction (γ) invariable les lettres a, b, c, ..., l, respectivement en a', b', c', ..., l' et nous aurons M substitutions qui laissent la fonction (δ) invariable, et si on les effectue sur la fonction (δ), on obtient M autres valeurs égales

F', F'_1, F'_2, ..., F'_{M-1}. On voit d'après cela que les $1.2.3...n$ valeurs que l'on obtient en permutant les n lettres a, b, c, ..., l dans la fonction (γ) de toutes les manières possibles sont égales M à M, et que le nombre des valeurs distinctes de la fonction (γ) est égal à $\frac{1.2.3..n}{M}$, et, par conséquent, à un diviseur du produit $1.2.3...n$.

Des fonctions transitives.

On appelle fonction *transitive* une fonction dans laquelle on peut faire occuper à une lettre quelconque telle place que l'on veut, sans que la fonction change de valeur, à la condition de faire occuper à toutes les autres des positions convenablement choisies.

Une fonction qui n'est pas transitive est dite *intransitive*.

Prenons pour exemple la fonction de quatre lettres

$$ab + cd^2;$$

on voit immédiatement que cette fonction est intransitive; car il est clair que si l'on met a à la place de c, quelles que soient les places occupées par les trois autres lettres, la fonction changera de valeur.

On voit encore que

$$ab^2 + cd^2$$

est une fonction intransitive, car on ne peut amener a à la place de b sans changer sa valeur.

Montrons maintenant des fonctions transitives. Toute fonction symétrique est évidemment transitive; ainsi, par exemple, la fonction symétrique

$$a + b + c + d$$

est transitive; mais il existe d'autres fonctions transitives que celles qui sont symétriques. Une fonction est en effet transitive toutes les fois qu'elle est invariable par une substitution circulaire effectuée sur toutes ses lettres.

Ainsi, par exemple, soit la fonction

$$(1) \qquad ab^2c^3d^4 + bc^2d^3a^4 + cd^2a^3b^4 + da^2b^3c^4,$$

qui est invariable par la substitution circulaire

$$(abcd);$$

faisons cette substitution sur cette fonction une fois, deux fois, trois fois, nous obtiendrons trois valeurs égales à la fonction (1) et qui se présenteront de la manière suivante :

$$bc^2d^3a^4 + cd^2a^3b^4 + da^2b^3c^4 + ab^2c^3d^4,$$
$$cd^2a^3b^4 + da^2b^3c^4 + ab^2c^3d^4 + bc^2d^3a^4,$$
$$da^2b^3c^4 + ab^2c^3d^4 + bc^2d^3a^4 + cd^2a^3b^4.$$

Or, en agissant ainsi, on amène dans la fonction (1) à la place de la lettre a successivement b, c, d; et à la place de b successivement c, d, a, et ainsi de suite. Il est donc évident que la fonction (1) est transitive.

Du reste, une fonction peut être transitive sans être invariable par une substitution circulaire effectuée sur toutes les quantités qu'elle renferme. Par exemple, il est aisé de voir que la fonction

$$(a-b)(c-d)$$

est changée par toute substitution circulaire effectuée sur les quatre quantités a, b, c, d, et cependant elle est transitive.

Mais, lorsque le nombre des quantités renfermées dans une fonction transitive est premier, cette fonction est nécessairement invariable par une substitution circulaire effectuée sur toutes les quantités. Nous avons démontré ce théorème dans le *Journal de M. Liouville*, année 1861, p. 304.

Il est facile de reconnaître que le nombre des valeurs distinctes d'une fonction transitive de n lettres est le même que si cette fonction était considérée comme fonction de $n - 1$ lettres, c'est-à-dire que si l'on supposait une lettre immobile. Considérons, en effet, une fonction transitive de n lettres

$$F(a, b, c, d, \ldots, k, l),$$

et supposons que l'on ait fait sur ses lettres toutes les permutations possibles. Nous pourrons ensuite, dans toutes les fonctions ainsi obtenues, et dans lesquelles la lettre a ne sera pas à la première place, l'amener à cette place, pourvu que nous déplacions convenablement les autres. Toutes les valeurs se réduisant à des fonctions dans lesquelles a occupe la première place, il est clair que la fonction F, acquiert toutes ses valeurs, considérée comme fonction des $n - 1$ lettres $b, c, d, \ldots, l$.

Reprenons la fonction transitive de quatre lettres

$$(a - b)(c - d); \tag{2}$$

cette fonction acquiert toutes ses valeurs distinctes, si on laisse a immobile et si l'on permute les trois quantités b, c, d. D'ailleurs les $1 \cdot 2 \cdot 3 = 6$ permutations que l'on peut faire sur b, c, d donnent toutes des valeurs distinctes; donc la fonction (2) a six valeurs.

Des fonctions plusieurs fois transitives.

Il arrive quelquefois qu'une fonction transitive de n lettres est encore transitive par rapport à $n - 1$ de ces lettres, et l'on dit alors que la fonction est deux fois transitive. Si cette fonction est encore transitive, considérée comme fonction de $n - 2$ lettres prises parmi les $n - 1$ précédentes, on dit que la fonction est trois fois transitive, et ainsi de suite.

On voit par là qu'une fonction μ fois transitive acquiert toutes ses valeurs considérée comme fonction de $n - \mu$ lettres seulement. Considérons la fonction des cinq lettres a, b, c, d, e :

(3) $(ad + bc)(ab + ce)(ac + bd)(ac + de)(af + be)$;

on vérifie qu'elle est invariable par la substitution circulaire

$$(abcde);$$

donc cette fonction est transitive et acquiert toutes ses valeurs par les permutations des quatre lettres a, b, c, d. On peut ensuite vérifier que cette fonction est invariable par la substitution circulaire

$$(abdc);$$

donc elle est encore transitive par rapport aux quatre lettres a, b, c, d. Cette fonction est deux fois transitive, et elle acquiert toutes ses valeurs par les permutations des trois lettres a, b, c. On constate ensuite facilement que les permutations des trois lettres a, b, c donnent $1.2.3 = 6$ résultats distincts; donc cette fonction deux fois transitive a six valeurs.

Considérons encore la fonction des six lettres a, b, c, d, e, f :

$$(4)\quad \begin{bmatrix} (ad + bc + ef)(ab + ce + df)(ae + bd + cf) \\ (ac + de + bf)(af + be + cd), \end{bmatrix},$$

que l'on déduit facilement de la fonction (3); on vérifie que cette fonction est invariable par la substitution circulaire

$$(acbfed);$$

donc cette fonction est transitive par rapport à ses six lettres a, b, c, d, e, f; ensuite elle est invariable comme la fonction (3) par les substitutions

$$(abcde),\quad (abdc);$$

donc elle est aussi transitive par rapport aux cinq lettres a, b, c, d, e, et par rapport aux quatre lettres a, b, c, d. C'est donc une fonction trois fois transitive, et comme la fonction (3) elle a $1.2.3 = 6$ valeurs.

(Cette fonction trois fois transitive de six lettres est la plus simple des fonctions trois fois transitives dont le nombre des lettres est un nombre premier augmenté d'une unité et dont l'existence se trouve démontrée dans le *Journal de M. Liouville*, année 1860, p. 24).

Pour se faire une idée parfaitement exacte des fonctions plusieurs fois transitives, il convient de démontrer le théorème suivant :

« Si une fonction de n lettres est μ fois transitive, elle est transitive par rapport à $n-1$ lettres quelconques; elle est transitive par rapport à $n-2$ lettres quelconques, etc.; enfin elle est transitive par rapport à $n-\mu+1$ lettres quelconques. »

Ainsi, supposons une fonction transitive par rapport à ses n lettres

$$a,\ b,\ c,\ d,\ldots,\ k,\ l,$$

puis par rapport aux lettres

$$b,\ c,\ d,\ldots,\ k,\ l,$$

puis par rapport aux lettres

$$c,\ d,\ldots,\ k,\ l,$$

et ainsi de suite. Je dis que la fonction est transitive par rapport à $n-\mu+1$ lettres quelconques

$$(5) \qquad e_1, f_1, \ldots, k_1, l_1.$$

Désignons par a', b'', c''',... les $\mu-1$ lettres de la fonction qui ne font pas partie des lettres (5). Puisque la fonction est transitive par rapport aux lettres $a, b, c, \ldots, k, l$, nous pouvons amener la lettre a' à la place de la lettre a, et les $n-1$ autres $b', c', \ldots, k', l'$ remplaceront respectivement $b, c, \ldots, k, l$. Or ces $n-1$ lettres $b', c', \ldots, k', l'$ remplaçant respectivement $b, c, \ldots, k, l$, la fonction sera transitive par rapport aux lettres

$$b', c', d', \ldots, k', l',$$

puis par rapport aux lettres

$$c', d', \ldots, k', l',$$

et ainsi de suite. Parmi les $n-1$ lettres $b', c', \ldots, k', l'$, nous pouvons prendre b'' et l'amener à la place de b', pourvu que nous déplacions convenablement les autres, et les lettres $c', d' \ldots, k', l'$ seront remplacées respectivement par $c'', d'', \ldots, k'', l''$. Les lettres $c'', d'', \ldots, k'', l''$ se trouvent dans les mêmes conditions que les lettres $c', d' \ldots, k', l'$ et par suite que les lettres $c, d, \ldots, k, l$. On peut imaginer que l'on continue ce raisonnement et la proposition à démontrer devient évidente.

On reconnaît aussi, d'après le raisonnement même qui vient d'être fait, qu'on peut, dans une fonction μ fois transitive, amener μ lettres quelconques à telles places que l'on veut.

Dans une fonction transitive de n lettres, chacune des lettres remplit le même rôle. Ce qui précède prouve que dans une fonction μ fois transitive de n lettres, l'ensemble de μ lettres remplit toujours le même rôle dans la fonction, quelles que soient les μ lettres que l'on considère, et quel que soit l'ordre dans lequel on les prend.

Ainsi dans la fonction trois fois transitive

$$(ad+bc+ef)(ab+ce+df)(ae+bd+cf)$$
$$(ac+de+bf)(af+be+cd)$$

que nous avons considérée tout à l'heure, l'ensemble de trois des six lettres remplit le même rôle, quelles que soient les trois lettres considérées, et l'on peut amener trois quelconques des six lettres à trois quelconques des six places, pourvu que l'on assigne aux trois autres lettres des places convenables.

On ne connaît pas de fonctions qui soient transitives plus de cinq fois. L'existence d'une fonction cinq fois transitive de douze lettres se trouve démontrée dans le *Journal de M. Liouville* (année 1861, p. 270).

Considérons encore la fonction de sept lettres

$$(6)\quad \left\{\begin{array}{l} (ab+cd+ef)(ac+bd+eg) \\ \times(ad+bc+gf)(ae+bf+cg) \\ \times(af+be+dg)(ag+ce+df)(bg+cf+de). \end{array}\right.$$

On vérifie facilement que cette fonction est invariable par les deux substitutions

$$(ace)(bdf), \qquad (ab)(cd),$$

et par suite que cette fonction est transitive par rapport aux six lettres a, b, c, d, e, f. On reconnaît de même qu'elle est invariable par la substitution

$$(ae)(cg);$$

or cette fonction étant transitive par rapport aux six lettres a, b, c, d, e, f, et étant invariable par cette dernière substitution, est évidemment transitive par rapport aux sept lettres a, b, c, d, e, f, g; donc elle est deux fois transitive, et elle acquiert toutes ses valeurs par les permutations de cinq quelconques de ses lettres, par exemple de a, b, c, d, e. La fonction est transitive aussi par rapport aux quatre lettres a, b, c, d; car on constate qu'elle est invariable par les deux substitutions

$$(7) \qquad (ab)(cd), \quad (ad)(bc);$$

mais considérée comme fonction des cinq lettres a, b, c, d, e, elle est changée par toute substitution qui remuerait la lettre e; car autrement la fonction étant transitive par rapport aux quatre lettres a, b, c, d, il est clair que la lettre e pourrait être permutée avec chacune des lettres a, b, c, d, et par conséquent que la fonction serait transitive aussi par rapport aux cinq lettres a, b, c, d, e; donc, considérée comme fonction de sept lettres, la fonction serait quatre fois transitive, et acquérant toutes ses valeurs par les permutations des trois lettres a, b, c, n'aurait pas plus de six valeurs; or la fonction a plus de six valeurs. En effet, transposons la lettre a avec chacune des six autres, nous aurons, en comptant la fonction (6), sept fonctions résultantes; et si la fonction n'avait que six valeurs, en transposant a en b' et ensuite a en c', on aurait deux valeurs égales F_1 et F_2. Représentons la fonction (6) par

$$F = F(a, b', c', \ldots),$$

on aurait

$$F_1 = F(b', a, c', \ldots),$$
$$F_2 = F(c', b', a, \ldots),$$

qui seraient deux valeurs égales; donc F_1 serait invariable par la substitution circulaire $(a, b' c')$, et par suite F invariable par $(b' a c')$, et comme à la place de b', a, c' on peut amener les trois lettres a, b, c, puisque la fonction est supposée quatre fois transitive, la fonction F ou (6) serait invariable par la substitution circulaire $(a\ b\ c)$, ce qui n'a pas lieu.

On constate que par les permutations des trois lettres a, b, c la fonction (6) acquiert six valeurs distinctes; donc les seules substitutions effectuées sur a, b, c, d, e, laissent invariable la fonction (6), sont les dérivées des substitutions (7), c'est-à-dire

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix},\ (ab)(cd),\quad (ad)(bc),\quad (ac)(bd).$$

Considérée comme fonction de ces cinq lettres, elle a donc quatre valeurs égales et par conséquent $\frac{1.2.3.4.5}{4}=30$ valeurs distinctes; c'est donc aussi le nombre de ses valeurs distinctes, quand on permute les sept lettres.

Prenons ensuite la fonction de huit lettres

$$(8)\quad \left\{\begin{aligned} &(ab+cd+ef+gh)(ac+bd+eg+fh)\\ &\times(ad+bc+eh+gf)(ae+bf+cg+dh)\\ &\times(af+be+ch+dg)(ag+bh+ce+df)\\ &\times(ah+bg+cf+de),\end{aligned}\right.$$

qui se déduit facilement de la fonction (6). Si dans la fonction (8) on suppose h immobile, cette fonction est *semblable* à la fonction (6), c'est-à-dire invariable par les mêmes substitutions. On reconnaît ensuite que cette fonction est invariable par la substitution

$$(ef)(gh);$$

d'ailleurs elle est transitive par rapport aux sept quantités a, b, c, d, e, f, g, donc cette fonction est transitive par rapport aux huit lettres a, b, c, d, e, f, g, h. Ainsi la fonction (8) est trois fois transitive, et comme la fonction (6) elle a 30 valeurs distinctes.

Cette fonction trois fois transitive de huit lettres appartient à une famille de fonctions dont le nombre des quantités est une puissance d'un nombre premier, et qui a été étudiée dans le *Journal de M. Liouville* (année 1861, p. 275).