BULLETIN DE LA S. M. F.

E. CAHEN

Sur les substitutions fondamentales du groupe modulaire

Bulletin de la S. M. F., tome 43 (1915), p. 69-88

<http://www.numdam.org/item?id=BSMF_1915__43__69_1>

SUR LES SUBSTITUTIONS FONDAMENTALES DU GROUPE MODULAIRE;

PAR M. E. CAHEN.

1. Il s'agit dans ce qui va suivre de substitutions linéaires, homogènes, à coefficients entiers, sur n variables $x_1, x_2, \ldots, x_n$.

Parmi ces substitutions, on distingue celles qui ont un déterminant égal à ± 1, et qu'on appelle *substitutions unités*. Elles forment un groupe.

En particulier, les substitutions unités de déterminant égal à $+1$, sont dites *modulaires*. Elles forment un groupe qui est un sous-groupe du précédent, et qu'on appelle *groupe modulaire*.

On appelle substitutions *fondamentales* ou *génératrices* d'un groupe, des substitutions $S_1, S_2, \ldots$ telles que toute substitution du groupe puisse se mettre sous la forme $S_1^{m_1} S_2^{m_2} \ldots$; $m_1, m_2, \ldots$ étant des entiers $\gtrless 0$.

Dans cette définition, on n'exige pas qu'une substitution du groupe ne puisse se mettre sous cette forme que d'une seule manière. On n'exige pas non plus que le nombre des substitutions fondamentales ne puisse se réduire.

Dans ce qui va suivre, la notation $x_h \parallel x_k$ désignera l'échange des deux variables x_h, x_k.

2. THÉORÈME. — *Le groupe des substitutions unités sur n variables $x_1, x_2, \ldots, x_n$ admet un système de substitutions fondamentales ainsi composé :*

1° *Le changement de x_1 en $-x_1$;*

2° *Les échanges de* x_1 *avec chacune des autres variables* $x_2, x_3, \ldots, x_n$;

3° *La substitution* $x_1 \mid x_1 + x_2$.

Soit Σ une substitution unité. Choisissons un système de n formes linéaires indépendantes à n variables et à coefficients entiers, d'ailleurs quelconques.

Appliquons-lui la substitution Σ ; nous obtenons un nouveau système de formes, équivalent au premier. On sait (1) qu'on ne peut passer du premier système au second que par une seule substitution, laquelle est Σ. D'autre part (2), si l'on examine le procédé par lequel on passe d'un système à un système équivalent, on voit qu'il consiste en une suite de substitutions des formes suivantes :

1° Substitutions de la forme

$$x_h \mid q_1 x_1 + q_2 x_2 + \ldots + x_h + \ldots + q_n x_n$$

(le coefficient de x_h au second membre étant 1) ;

2° Échanges de deux variables : $x_h \parallel x_i$;

3° Changements de signe de variables : $x_h \mid -x_h$.

Donc la substitution Σ est égale à un produit de substitutions telles que les précédentes.

Maintenant une substitution de la première forme :

$$x_h \mid q_1 x_1 + q_2 x_2 + \ldots + x_h + \ldots + q_n x_n$$

est égale au produit des $n - 1$ suivantes :

$$x_h \mid q_i x_i + x_h \qquad (i \neq h).$$

Prenons l'une d'elles, $x_h \mid q_i\, x_i + x_h$. Si $q_i > 0$, elle est égale au produit de q_i substitutions $x_h \mid x_i + x_h$.

Si $q_i < 0$, elle est égale au produit de $-q_i$ substitutions

$$x_h \mid -x_i + x_h.$$

Or cette dernière est égale au produit

$$(x_i \mid -x_i) \times (x_h \mid x_i + x_h) \times (x_i \mid -x_i).$$

---

(1) *Voir* notre *Théorie des Nombres* (Paris, A. Hermann et fils, 1914), t. I, n° 288. Cet Ouvrage sera désigné dans ce qui va suivre par *T. d. N.*

(2) *T. d. N.*, n°s 285 et suiv.

Nous avons donc ramené la substitution Σ à un produit de substitutions des trois formes suivantes :

(1^a) $\qquad x_h \mid x_i + x_h ;$

(2^a) $\qquad x_h \parallel x_i ;$

(3^a) $\qquad x_h \mid - x_h .$

Maintenant, la substitution $x_h \mid x_i + x_h$ est égale au produit

$$(x_1 \parallel x_h) \times (x_2 \parallel x_i) \times (x_1 \mid x_1 + x_2) \times (x_2 \parallel x_i) \times (x_1 \parallel x_h),$$

sauf si $i = 1$.

Si $1 = 1$ et $h \neq 2$, la substitution $x_h \mid x_1 + x_h$ est égale au produit

$$(x_2 \parallel x_h) \times (x_1 \parallel x_2) \times (x_1 \mid x_1 + x_2) \times (x_1 \parallel x_2) \times (x_2 \parallel x_h).$$

Si $i = 1$ et $h = 2$, la substitution $x_2 \mid x_1 + x_2$ est égale au produit

$$(x_1 \parallel x_2) \times (x_1 \mid x_1 + x_2) \times (x_1 \parallel x_2).$$

Donc, dans tous les cas, toutes les substitutions (1^a) se ramènent à la substitution $x_1 \mid x_1 + x_2$ et à des substitutions (2^a).

Ensuite une substitution de la forme (2^a), soit $x_h \parallel x_i$, est égale au produit

$$(x_1 \parallel x_h) \times (x_1 \parallel x_i) \times (x_1 \parallel x_h).$$

Et enfin une substitution de la forme (3^a), soit $x_h \mid - x_h$, peut se remplacer par le produit

$$(x_1 \parallel x_h) \times (x_1 \mid - x_1) \times (x_1 \parallel x_h).$$

Finalement, le théorème est démontré.

On a ainsi $n + 1$ substitutions fondamentales du groupe unité.

3. *Autre système de substitutions fondamentales.* — En remarquant que

$$x_1 \parallel x_h = \begin{pmatrix} x_1 & x_h \\ x_h & - x_1 \end{pmatrix} \times (x_1 \mid - x_1),$$

on voit qu'on peut prendre comme substitutions fondamentales du groupe unité :

(1^b) $\qquad x_1 \mid - x_1 ;$

(2^b) les $n-1$ substitutions

$$\begin{pmatrix} x_1 \\ x_h \end{pmatrix} \left| \begin{matrix} x_h \\ -x_1 \end{matrix} \right. \qquad (h = 2, 3, \ldots, n);$$

(3^b) $$x_1 \,|\, x_1 + x_2.$$

L'avantage qu'il y a à considérer ce nouvel ensemble de substitutions fondamentales est le suivant. La première de ces substitutions seule a comme déterminant -1 ; toutes les autres ont comme déterminant $+1$. Alors, si on laisse la première de côté, il reste n substitutions qui sont fondamentales du groupe modulaire. Ainsi :

4. Théorème. — *Le groupe modulaire à n variables x_1, x_2, ..., x_n admet un système de substitutions fondamentales ainsi composées :*

Les $n-1$ substitutions

(1^c) $$\begin{pmatrix} x_1 \\ x_h \end{pmatrix} \left| \begin{matrix} x_h \\ -x_1 \end{matrix} \right. \qquad (h = 2, 3, \ldots, n);$$

(2^c) $$x_1 \,|\, x_1 + x_2.$$

Pour le démontrer, nous démontrerons que : *une substitution unité étant décomposée en un produit de substitutions fondamentales comme au n° 3, on peut toujours supposer que le facteur $x_1 \,|\, -x_1$ soit unique et placé à la fin du produit.*

En effet, si cette substitution se trouve à l'intérieur du produit et suivie d'une substitution

$$\begin{pmatrix} x_1 \\ x_h \end{pmatrix} \left| \begin{matrix} x_h \\ -x_1 \end{matrix} \right.,$$

on pourra la faire passer après en faisant usage de l'égalité

$$(x_1 \,|\, -x_1) \times \begin{pmatrix} x_1 \\ x_h \end{pmatrix} \left| \begin{matrix} x_h \\ -x_1 \end{matrix} \right. = \begin{pmatrix} x_1 \\ x_h \end{pmatrix} \left| \begin{matrix} x_h \\ -x_1 \end{matrix} \right.^2 \times (x_1 \,|\, -x_1);$$

si cette substitution est suivie de la substitution $x_1 \,|\, x_1 + x_2$, on la fera passer après en faisant usage de l'égalité

$$(x_1 \,|\, -x_1) \times (x_1 \,|\, x_1 + x_2) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \left| \begin{matrix} x_2 \\ -x_1 \end{matrix} \right. \times (x_1 \,|\, x_1 + x_2) \times \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \left| \begin{matrix} x_1 \\ -x_1 \end{matrix} \right.$$
$$\times (x_1 \,|\, x_1 + x_2) \times \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \left| \begin{matrix} x_2 \\ -x_1 \end{matrix} \right. \times (x_1 \,|\, -x_1).$$

Les substitutions $(x_1 | -x_1)$ ayant été ainsi toutes rejetées à la fin du produit, se réunissent en un produit $(x_1 | -x_1)^m$; mais par suite de l'égalité $(x_1 | -x_1)^2 = 1$, on peut réduire l'exposant m à zéro ou à un.

Une substitution unité ayant été mise ainsi sous forme de produit de substitutions (1^c), (2^c) (lesquelles sont de déterminant $+1$) suivi ou non d'une substitution $x_1 | -x_1$ (laquelle est le déterminant -1), il est évident que la substitution est modulaire ou non suivant que cette dernière substitution ne figure pas, ou figure dans le produit. Le théorème est donc démontré.

En conséquence, à partir de maintenant, nous ne considérerons plus que des substitutions modulaires.

5. La décomposition qu'on vient de trouver d'une substitution modulaire en substitutions fondamentales est possible d'une infinité de manières, car il y a des relations entre ces substitutions.

En posant, pour abréger,

$$x_1 | x_1 + x_2 = \mathrm{S}, \qquad \begin{matrix} x_1 \\ x_h \end{matrix} \Big| \begin{matrix} x_h \\ -x_1 \end{matrix} = \mathrm{T}_h \qquad (h = 2, 3, \ldots, n),$$

on a

$$(1) \quad (\mathrm{T}_h)^4 = 1, \qquad (\mathrm{S}\mathrm{T}_2)^3 = 1, \qquad (\mathrm{T}_h \mathrm{T}_i \mathrm{T}_h)^2 = 1, \qquad \mathrm{T}_h^2 \mathrm{T}_i^2 = \mathrm{T}_i^2 \mathrm{T}_h^2.$$

Ces relations, qui ne sont pas d'ailleurs toutes distinctes, permettent de changer la forme d'un produit sans changer sa valeur. Par exemple,

$$\mathrm{T}_2 \mathrm{S}^2 \mathrm{T}_3 = \mathrm{T}_2^2 \mathrm{S}\mathrm{T}_2 \mathrm{S}\mathrm{T}_2 \mathrm{S}^3 \mathrm{T}_3.$$

La forme de la seconde relation (1) suggère de prendre

$$\mathrm{V} = \mathrm{S}\mathrm{T}_2 = \begin{matrix} x_1 \\ x_2 \end{matrix} \Big| \begin{matrix} -x_1 + x_2 \\ -x_1 \end{matrix}$$

comme substitution fondamentale au lieu de S. C'est possible, car on peut, dans tout produit, remplacer S par $\mathrm{V}\mathrm{T}_2^{-1} = \mathrm{V}\mathrm{T}_2^3$.

De même, la troisième relation (1) suggère de prendre

$$\mathrm{U}_h = \mathrm{T}_2 \mathrm{T}_h \mathrm{T}_2 = \begin{matrix} x_1 \\ x_2 \\ x_h \end{matrix} \Big| \begin{matrix} -x_1 \\ -x_h \\ -x_2 \end{matrix} \qquad \text{au lieu de } \mathrm{T}_h \qquad (h = 3, 4, \ldots, n).$$

On n'a qu'à remplacer T_h par

$$T_2^{-1} U_h T_2^{-1} = T_2^2 U_h T_2^2.$$

6. On a ainsi un nouveau système de substitutions fondamentales pour le groupe modulaire, à savoir (en écrivant T au lieu de T_2) :

(1^d) $$T = \begin{matrix} x_1 \\ x_2 \end{matrix} \Big| \begin{matrix} x_2 \\ -x_1 \end{matrix};$$

(2^d) Les $n-2$ substitutions

$$U_h = \begin{matrix} x_1 \\ x_2 \\ x_h \end{matrix} \Big| \begin{matrix} -x_1 \\ -x_h \\ -x_2 \end{matrix} \qquad (h = 3, 4, \ldots, n);$$

(3^d) $$V = \begin{matrix} x_1 \\ x_2 \end{matrix} \Big| \begin{matrix} -x_1 + x_2 \\ -x_1 \end{matrix},$$

avec les relations

$$(2) \quad \begin{cases} T^4 = 1, \quad U_h^2 = 1, \quad V^3 = 1, \\ (T^3 U_h T^3)^4 = 1, \quad (U_h T^2)^2 = (T^2 U_h)^2, \\ (T_h T_2 T_h)^2 = 1, \quad T_h^2 T_l^2 = T_l^2 T_h^2. \end{cases}$$

En particulier, les trois premières relations permettent de réduire dans tout produit l'exposant de T à 1, 2, ou 3; celui de V à 1 ou 2, celui de chaque U_h à 1.

Ainsi la substitution prise plus haut comme exemple $T_2 S^2 T_3$ s'écrit

$$T.VT^3VT^3.T^3U_3T^3 \qquad \text{ou} \qquad TVT^3VT^2U_3T^3.$$

7. Avant d'aller plus loin, nous remarquerons que les résultats qui viennent d'être obtenus peuvent se transporter aux tableaux formés par les coefficients des substitutions et répondent à une question qui se pose en théorie des nombres (1) : *On part du déterminant dont les éléments de la diagonale principale sont égaux à* 1, *tous les autres étant égaux à* 0; *on ajoute entre elles des lignes ou des colonnes, on échange des lignes ou des colonnes, on répète ces opérations autant de fois qu'on le veut; peut-on obtenir ainsi tous les déterminants à éléments entiers, égaux à* $+1$?

(1) *T. d. N.*, t. I, n° 210.

La réponse à la question ainsi posée est d'ailleurs évidemment: « non », car on n'obtient de cette façon que des déterminants à éléments tous positifs ; or on voit immédiatement qu'il y a des déterminants égaux à + 1, et dont les éléments ne sont pas tous positifs.

Mais il suffit de modifier légèrement le procédé indiqué plus haut pour que la réponse devienne: « oui ». Il suffit d'adjoindre aux opérations indiquées celle qui consiste à changer de signe tous les éléments d'une ligne. Et l'on peut alors supprimer l'opération qui consiste à ajouter des lignes (en gardant celle qui consiste à ajouter des colonnes). On obtient ainsi tous les déterminants égaux à + 1 ou — 1.

Plus particulièrement :

Tout déterminant égal à + 1 *peut s'obtenir en partant du déterminant*

$$\begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & \dots & 1 \end{vmatrix}$$

et faisant un certain nombre de fois les deux opérations suivantes : 1° *échange d'une colonne avec la première suivie du changement de signe des éléments de la première colonne ainsi obtenue;* 2° *addition des éléments de la première colonne à ceux de la seconde. Tout déterminant égal à* — 1 *peut s'obtenir en faisant les opérations précédentes et en les faisant suivre du changement de signe des éléments de la première ligne.*

Ce n'est pas autre chose que les théorèmes des nos 3 et 4.

8. Maintenant la question suivante se pose : *La décomposition d'une substitution modulaire en substitutions fondamentales* T, U_h et V, *les exposants de* T *étant réduits à* 1, 2, *ou* 3, *ceux des* T_h *à* 1, *et ceux de* V *à* 1 *ou* 2, *n'est-elle possible que d'une seule manière?*

On sait en effet de quelle importance est, pour les nombres

entiers positifs, le fait qu'ils sont décomposables en facteurs premiers positifs *d'une seule manière.*

De même, pour tout groupe abélien, chaque élément est décomposable en un produit d'éléments fondamentaux, et cette décomposition n'est possible que d'une seule manière, lorsqu'on réduit l'exposant de chaque facteur à son reste. Donc, pour tout groupe dont les éléments se décomposent en produits d'éléments fondamentaux, on devra chercher, si c'est possible, des éléments fondamentaux jouissant de cette même propriété.

Cette propriété *n'a pas lieu* pour le groupe modulaire, relativement aux substitutions T, U_h et V, *lorsque* $n > 3$. Il suffit, en effet, de considérer les relations (2) autres que les trois premières pour avoir des exemples de substitutions modulaires décomposées de deux façons différentes.

Mais pour $n = 2$, comme il n'y a pas de substitutions U_h, de pareilles relations n'existent pas et l'on doit se demander si la propriété a lieu pour $n = 2$. Avant d'aborder cette question, parlons des *substitutions homographiques.*

9. Considérons une substitution linéaire homogène à n variables (faisons $n = 3$ pour simplifier les notations)

$$(3)\qquad \begin{array}{c|l} x_1 & a_{11}x_1 + a_{12}x_2 + a_{13}x_3, \\ x_2 & a_{21}x_1 + a_{22}x_2 + a_{23}x_3, \\ x_3 & a_{31}x_1 + a_{32}x_3 + a_{33}x_3, \end{array}$$

puis considérons les rapports des variables à l'une d'elles, par exemple à x_n, soit

$$\frac{x_1}{x_3} = z_1, \qquad \frac{x_2}{x_3} = z_2.$$

On voit que de la substitution (3) résulte pour z_1 et z_2 la substitution homographique

$$(4)\qquad \begin{array}{c|l} z_1 & \dfrac{a_{11}z_1 + a_{12}z_2 + a_{13}}{a_{31}z_1 + a_{32}z_2 + a_{33}}, \\ z_2 & \dfrac{a_{21}z_1 + a_{22}z_2 + a_{23}}{a_{31}z_1 + a_{32}z_2 + a_{33}}. \end{array}$$

Nous représenterons cette substitution par le tableau des coefficients a, et les calculs sur les substitutions homographiques

seront identiques à ceux sur les substitutions linéaires, c'est-à-dire au calcul des tableaux, avec cette différence cependant, que la substitution (3) dépend des coefficients a eux-mêmes, tandis que la substitution (4) ne dépend que de leurs rapports. On peut dans cette dernière remplacer tous les a par λa sans qu'elle change.

Bornons-nous aux substitutions linéaires homogènes unités. Alors tous les a sont entiers ; de plus, tous les a d'une même ligne sont premiers dans leur ensemble (puisque le déterminant de la substitution est égal à ± 1). Nous supposerons que cette condition est remplie aussi dans les substitutions homographiques. Alors $\lambda = \pm 1$. Il en résulte qu'à deux substitutions linéaires homogènes unités, ne différant que par les signes de tous les coefficients, ne correspond qu'une substitution homographique et réciproquement.

On voit aussi que, si n est impair, il n'y a pas lieu de distinguer les substitutions homographiques modulaires d'entre les substitutions unités, puisqu'un changement de signe de tous les coefficients qui ne change pas la substitution change cependant le signe de son déterminant. Au contraire, si n est pair, la distinction est à faire.

10. A partir de maintenant, nous supposons $n = 2$.

Les substitutions linéaires homogènes modulaires sont les substitutions

$$\begin{matrix} x \\ y \end{matrix} \left| \begin{matrix} \alpha x + \beta y, \\ \gamma x + \delta y, \end{matrix} \right.$$

et les substitutions homographiques modulaires sont les substitutions

$$z \left| \frac{\alpha z + \beta}{\gamma z + \delta} \right.$$

avec, dans les deux cas, $\alpha\delta - \beta\gamma = 1$.

Le groupe modulaire homogène admet pour substitutions fondamentales

$$\mathrm{T} = \begin{matrix} x \\ y \end{matrix} \left| \begin{matrix} y, \\ -x, \end{matrix} \right. \qquad \mathrm{V} = \begin{matrix} x \\ y \end{matrix} \left| \begin{matrix} -x + y, \\ -x, \end{matrix} \right.$$

avec les relations

$$\mathrm{T}^4 = 1, \qquad \mathrm{V}^3 = 1.$$

Le groupe modulaire homographique admet pour substitutions fondamentales

$$T = z\left|-\frac{1}{z}\right., \qquad V = z\left|\frac{z-1}{z}\right.,$$

avec les relations

$$T^2 = 1, \qquad V^3 = 1.$$

Il n'y a pas de confusion à craindre par la désignation des substitutions fondamentales homogènes et homographiques par les mêmes lettres T et V, mais il faut remarquer la différence entre les relations à laquelle satisfait T dans chacun des cas. Pour les substitutions homogènes, on a

$$T^2 = \begin{matrix} x \\ y \end{matrix}\left|\begin{matrix} -x, \\ -y. \end{matrix}\right.$$

11. Nous allons nous occuper des substitutions modulaires homographiques. Une telle substitution se met sous forme d'un produit de substitutions T et V, l'exposant des facteurs T étant 1, celui des facteurs V à 1 ou 2 (1). Et nous allons montrer que *cette décomposition n'est possible que d'une seule manière.*

Pour cela nous allons démontrer que deux produits différents ne peuvent être identiques.

Examinons la forme d'un tel produit. Il se compose de facteurs V ou V^2 ou T, et il y a toujours un facteur T sur deux consécutifs. Par exemple :

$$TV^2, \quad TVTVTV^2TVT, \quad TVTV^2, \quad VTV^2TV^2TV^2TVTVTV.$$

Réunissons dans une parenthèse les facteurs VT et les facteurs V^2T ; de plus, quand m facteurs VT se suivent, réunissons-les en $(VT)^m$, de même pour les facteurs V^2T ; nous pourrons écrire ces produits :

$$TV^2, \quad T(VT)^2(V^2T)(VT), \quad T(VT)V^2, \quad (VT)(V^2T)^3(VT)^2V.$$

En définitive, tout produit est de l'une des quatre familles

(1) La substitution unité fait exception. Il en est de même dans la décomposition des entiers positifs en facteurs premiers. Si l'on n'admet pas le nombre 1 parmi les facteurs premiers, la décomposition en facteurs premiers ne s'applique pas au nombre 1. Et si on l'admet, la décomposition est possible d'une infinité de façons.

suivantes :

$A = (V\,T)^{m_1}(V^2T)^{n_1}\ldots(V^2T)^{n_i}$ commençant par VT et finissant par V^2T,
$B = (V\,T)^{m_1}(V^2T)^{n_1}\ldots(V\,T)^{m_i}$ » VT » VT,
$C = (V^2T)^{n_1}(V\,T)^{m_1}\ldots(V\,T)^{m_i}$ » V^2T » VT,
$D = (V^2T)^{n_1}(V\,T)^{m_1}\ldots(V^2T)^{n_i}$ » V^2T » V^2T,

ou de l'une des quatre familles précédentes suivies de V ou de V^2, c'est-à-dire de l'une des huit familles

$$AV,\ BV,\ CV,\ DV,\ AV^2,\ BV^2,\ CV^2,\ DV^2,$$

ou enfin de l'une des douze familles précédentes, précédée de T, c'est-à-dire de l'une des douze familles

$$TA,\ TB,\ TC,\ TD,\ TAV,\ TBV,\ TCV,\ TDV,$$
$$TAV^2,\ TBV^2,\ TCV^2,\ TDV^2,$$

en tout vingt-quatre familles. Nous allons montrer que :

1° *Deux produits appartenant à une même famille ne peuvent être égaux que s'ils sont composés des mêmes facteurs, dans le même ordre ;*

2° *Deux produits appartenant à deux familles différentes ne peuvent être égaux.*

1° Comparons deux produits de la *première famille :*

$$A = (VT)^{m_1}(V^2T)^{n_1}\ldots(V^2T)^{n_i},$$
$$A' = (VT)^{m'_1}(V^2T)^{n'_1}\ldots(V^2T)^{n'_j}.$$

On a

$$VT = z\,|\,z+1, \qquad \text{donc} \qquad (VT)^m = z\,|\,z+m;$$
$$V^2T = z\left|\frac{1}{\frac{1}{z}+1}\right., \qquad \text{donc} \qquad (V^2T)^n = z\left|\frac{1}{\frac{1}{z}+n}\right..$$

Donc

$$A = z\left|\, m_1 + \cfrac{1}{n_1 + \cfrac{1}{m_2} + \ldots + \cfrac{1}{n_i + \cfrac{1}{z}}}\right. \qquad \text{ou} \qquad z\,|\,[m_1, n_1, \ldots, n_i, z]$$

en employant la notation des fractions continuelles.

On peut écrire

$$A = z \left| \frac{Pz + R}{Qz + S} \right.$$

en posant $\frac{P}{Q}$ et $\frac{R}{S}$ respectivement pour la dernière et l'avant-dernière réduite de la fraction continuelle

$$[m_1, n_1, \ldots, m_i, n_i].$$

On aurait de même

$$A' = z' \left| \frac{P'z + R'}{Q'z + S'} \right.$$

en posant $\frac{P'}{Q'}$ et $\frac{R'}{S'}$ pour la dernière et l'avant-dernière réduite de

$$[m'_1, n'_1, \ldots, m'_i, n'_i].$$

Les entiers P, P', ..., S, S' étant tous positifs, les deux substitutions ne peuvent être identiques que si

$$P = P', \quad \ldots, \quad S = S'.$$

D'après la théorie des fractions continuelles, cela ne peut avoir lieu que si les entiers $m_1, n_1, \ldots, n_i$ sont identiques aux entiers $m'_1, n'_1, \ldots, n'_i$, ce qui démontre le théorème pour les substitutions de la première famille.

Comparons maintenant deux produits de la *seconde famille :*

$$B = (VT)^{m_1}(V^2T)^{n_1}\ldots(VT)^{m_i},$$
$$B' = (VT)^{m'_1}(V^2T)^{n'_1}\ldots(VT)^{m'_i}.$$

On trouve de même

$$B = z \,|\, [m_1, n_1, \ldots, n_{i-1}, m_i + z],$$

qu'on peut écrire

$$B = z \left| \frac{Rz + P}{Sz + Q} \right.$$

en posant $\frac{P}{Q}$ et $\frac{R}{S}$ respectivement pour la dernière et l'avant-dernière réduite de

$$[m_1, n_1, \ldots, n_{i-1}, m_i].$$

La démonstration se continue comme plus haut.

Les démonstrations sont analogues pour la troisième et la

quatrième famille. Quant aux vingt autres familles, le théorème pour celles-là résulte immédiatement du théorème pour les quatre premières. En effet, si deux produits de la cinquième famille, par exemple AV et A′V, sont identiques, c'est que A et A′ le sont. On est donc ramené au théorème démontré pour deux produits de la première famille.

2° Nous allons démontrer maintenant que deux produits appartenant à deux familles différentes ne peuvent être égaux. Pour cela, refaisons pour chacune des familles le calcul qui vient d'être fait pour les deux premières. Nous avons trouvé par exemple qu'une substitution de la première famille est de la forme

$$\begin{pmatrix} P & R \\ Q & S \end{pmatrix}.$$

On trouve ainsi, pour les vingt-quatre familles, respectivement les vingt-quatre formes :

$$\begin{pmatrix} P & R \\ Q & S \end{pmatrix} \quad \begin{pmatrix} R & P \\ S & Q \end{pmatrix} \quad \begin{pmatrix} S & Q \\ R & P \end{pmatrix} \quad \begin{pmatrix} Q & S \\ P & R \end{pmatrix}$$

$$\begin{pmatrix} P+R & -P \\ Q+S & -Q \end{pmatrix} \quad \begin{pmatrix} R+P & -R \\ S+Q & -S \end{pmatrix} \quad \begin{pmatrix} S+Q & -S \\ R+P & -R \end{pmatrix} \quad \begin{pmatrix} Q+S & -Q \\ P+R & -P \end{pmatrix}$$

$$\begin{pmatrix} R & -P-R \\ S & -Q-S \end{pmatrix} \quad \begin{pmatrix} P & -R-P \\ Q & -S-Q \end{pmatrix} \quad \begin{pmatrix} Q & -S-Q \\ P & -R-P \end{pmatrix} \quad \begin{pmatrix} S & -Q-S \\ R & -P-R \end{pmatrix}$$

$$\begin{pmatrix} Q & S \\ -P & -R \end{pmatrix} \quad \begin{pmatrix} S & Q \\ -R & -P \end{pmatrix} \quad \begin{pmatrix} R & P \\ -S & -Q \end{pmatrix} \quad \begin{pmatrix} P & R \\ -Q & -S \end{pmatrix}$$

$$\begin{pmatrix} Q+S & -Q \\ -P-R & P \end{pmatrix} \quad \begin{pmatrix} S+Q & -S \\ -R-P & R \end{pmatrix} \quad \begin{pmatrix} R+P & -R \\ -S-Q & S \end{pmatrix} \quad \begin{pmatrix} P+R & -P \\ -Q-S & Q \end{pmatrix}$$

$$\begin{pmatrix} S & -Q-S \\ -R & P+R \end{pmatrix} \quad \begin{pmatrix} Q & -S-Q \\ -P & R+P \end{pmatrix} \quad \begin{pmatrix} P & -R-P \\ -Q & S+Q \end{pmatrix} \quad \begin{pmatrix} R & -P-R \\ -S & Q+S \end{pmatrix}$$

$\frac{P}{Q}$ et $\frac{R}{S}$ désignent, dans chacune de ces formes, respectivement la dernière et l'avant-dernière réduite d'une fraction continuelle de valeur plus grande ou égale à 1.

Dans chacune de ces formes de substitution, le premier coefficient est positif. Deux substitutions dans lesquelles cela a lieu ne peuvent

être égales que si leurs coefficients sont identiques. Or il y a entre deux formes des différences incompatibles dans les signes des coefficients ou dans leurs grandeurs respectives. Elles sont indiquées dans le Tableau suivant, où α, β, γ, δ désignent les coefficients d'une substitution.

Remarquons encore une fois, que la substitution identique est à part ; elle ne fait partie d'aucune des familles ci-dessous :

1re famille...	$\alpha > 0$	$\beta > 0$	$\gamma > 0$	$\delta > 0$	$\alpha > \beta$	$\alpha > \gamma$
2e » ...	$\alpha > 0$	$\beta > 0$	$\gamma \geqq 0$	$\delta > 0$	$\alpha \leqq \beta$	$\alpha > \gamma$
3e » ...	$\alpha > 0$	$\beta > 0$	$\gamma > 0$	$\delta > 0$	$\alpha < \beta$	$\alpha < \gamma$
4e » ...	$\alpha > 0$	$\beta \geqq 0$	$\gamma > 0$	$\delta > 0$	$\alpha > \beta$	$\alpha \leqq \gamma$
5e » ...	$\alpha > 0$	$\beta < 0$	$\gamma > 0$	$\delta < 0$	$-\beta < \alpha < -2\beta$	$\alpha > \gamma$
6e » ...	$\alpha > 0$	$\beta < 0$	$\gamma > 0$	$\delta \leqq 0$	$\alpha \geqq -2\beta$	$\alpha > \gamma$
7e » ...	$\alpha > 0$	$\beta < 0$	$\gamma > 0$	$\delta < 0$	$\alpha > -2\beta$	$\alpha < \gamma$
8e » ...	$\alpha > 0$	$\beta < 0$	$\gamma > 0$	$\delta < 0$	$-\beta \leqq \alpha < -2\beta$	$\alpha < \gamma$
9e » ...	$\alpha > 0$	$\beta < 0$	$\gamma > 0$	$\delta < 0$	$-\beta > 2\alpha$	$-\beta > \delta$
10e » ...	$\alpha > 0$	$\beta < 0$	$\gamma > 0$	$\delta < 0$	$\alpha < -\beta \leqq 2\alpha$	$-\beta > -\delta$
11e » ...	$\alpha > 0$	$\beta < 0$	$\gamma > 0$	$\delta < 0$	$\alpha < -\beta < 2\alpha$	$-\beta < -\delta$
12e » ...	$\alpha \geqq 0$	$\beta < 0$	$\gamma > 0$	$\delta < 0$	$-\beta > 2\alpha$	$-\beta < -\delta$
13e » ...	$\alpha > 0$	$\beta > 0$	$\gamma < 0$	$\delta < 0$	$\alpha > \beta$	$\alpha < -\gamma$
14e » ...	$\alpha \geqq 0$	$\beta > 0$	$\gamma < 0$	$\delta < 0$	$\alpha < \beta$	$\alpha < -\gamma$
15e » ...	$\alpha > 0$	$\beta > 0$	$\gamma < 0$	$\delta < 0$	$\alpha < \beta$	$\alpha > -\gamma$
16e » ...	$\alpha > 0$	$\beta > 0$	$\gamma < 0$	$\delta \leqq 0$	$\alpha \geqq \beta$	$\alpha \geqq -\gamma$
17e » ...	$\alpha > 0$	$\beta < 0$	$\gamma < 0$	$\delta > 0$	$-\beta < \alpha < -2\beta$	$\alpha < -\gamma$
18e » ...	$\alpha > 0$	$\beta \leqq 0$	$\gamma < 0$	$\delta > 0$	$\alpha > -2\beta$	$\alpha < -\gamma$
19e » ...	$\alpha > 0$	$\beta < 0$	$\gamma < 0$	$\delta > 0$	$\alpha > -2\beta$	$\alpha > -\gamma$
20e » ...	$\alpha > 0$	$\beta < 0$	$\gamma < 0$	$\delta > 0$	$-\beta < \alpha < -2\beta$	$\alpha > -\gamma$
21e » ...	$\alpha > 0$	$\beta < 0$	$\gamma < 0$	$\delta > 0$	$-\beta > 2\alpha$	$-\beta < \delta$
22e » ...	$\alpha > 0$	$\beta < 0$	$\gamma < 0$	$\delta > 0$	$\alpha \leqq -\beta < 2\alpha$	$-\beta < \delta$
23e » ...	$\alpha > 0$	$\beta < 0$	$\gamma < 0$	$\delta > 0$	$\alpha < -\beta < 2\alpha$	$-\beta > \delta$
24e » ...	$\alpha > 0$	$\beta < 0$	$\gamma \leqq 0$	$\delta > 0$	$-\beta > 2\alpha$	$-\beta > \delta$

L'exactitude de ce Tableau se vérifie sans peine. Considérons par exemple la première famille :

$$\alpha = P, \quad \beta = R, \quad \gamma = Q, \quad \delta = S,$$

où

$$\frac{P}{Q} = [m_1, n_1, \ldots, n_i] \qquad \text{et} \qquad \frac{R}{S} = [m_1, n_1, \ldots, m_i].$$

On a à vérifier

$$P > o, \quad Q > o, \quad R > o, \quad S > o, \quad P > R, \quad P > Q,$$

toutes inégalités évidentes d'après les propriétés des fractions continuelles.

Considérons, comme second exemple, la sixième famille :

$$\alpha = P + R, \quad \beta = -R, \quad \gamma = Q + S, \quad \delta = -S,$$

avec

$$\frac{P}{Q} = [m_1, n_1, \ldots, m_i] \qquad \text{et} \qquad \frac{R}{S} = [m_1, n_1, \ldots, n_{i-1}] \quad \text{si } i > 1$$

et

$$\frac{R}{S} = \frac{1}{o} \qquad \text{si} \qquad i = 1.$$

On a à vérifier

$$P + R > o, \quad -R < o, \quad Q + S > o, \quad -S \leqq o,$$
$$P + R \geqq 2R, \quad P + R > Q + S,$$

toutes inégalités évidentes encore. Les cas particuliers $S = o$, $P + R = 2R$ se présentent, le premier quand $i = 1$, alors

$$P = m_1, \quad Q = 1, \quad R = 1, \quad S = o,$$

et la substitution est

$$\begin{pmatrix} m_1 + 1 & -1 \\ 1 & o \end{pmatrix};$$

le second quand $i = 1$, et $m_1 = 1$, alors

$$P = 1, \quad Q = 1, \quad R = 1, \quad S = o,$$

et la substitution est

$$\begin{pmatrix} 2 & -1 \\ 1 & o \end{pmatrix}.$$

La vérification se fait de même pour chacune des familles.

Le théorème de l'univocité de la décomposition est donc démontré. La démonstration donne d'ailleurs le moyen d'effectuer la décomposition (¹).

Exemples. — 1° Soit la substitution

$$\Sigma = z \left| \frac{19z + 12}{49z + 31} \right.$$

On a

$$\alpha, \beta, \gamma, \delta > 0, \qquad \alpha > \beta, \qquad \alpha < \gamma,$$

ce qui caractérise la *quatrième famille*. La substitution S se met donc sous la forme

$$\Sigma = (V^2T)^{n_1}(VT)^{m_1} \dots (VT)^{m_{i-1}}(V^2T)^{n_i}$$

ou

$$z \,|\, [0, n_1, m_1, \dots, n_{i-1}, n_i, z],$$

ou, en posant la dernière réduite de $[n_1, m_1, \dots, n_i]$ égale à $\frac{P}{Q}$ et l'avant-dernière égale à $\frac{R}{S}$,

$$z \left| \frac{Qz + S}{Pz + R} \right.$$

Donc

$$\frac{P}{Q} = \frac{49}{19} = [2, 1, 1, 2, 1, 2];$$

mais, comme le nombre des éléments $n_1, m_1, \dots, n_i$ est impair (pour que $QR - PS = +1$), nous écrivons

$$\frac{P}{Q} = [2, 1, 1, 2, 1, 1, 1]$$

et

$$\begin{aligned}\Sigma &= (V^2T)^2(VT)(V^2T)(VT)^2(V^2T)(VT)(V^2T) \\ &= V^2TV^2TVTV^2TVTVTV^2TVTV^2T.\end{aligned}$$

2° Soit la substitution

$$\Sigma' = z \left| \frac{7z - 9}{-10z + 13} \right.$$

(¹) Ce résultat se trouve contenu, pour les quatre premières familles, dans l'article de M. CHATELET, *Contribution à la théorie des fractions continues arithmétiques* (*Bulletin de la Société mathématique*, t. XL, 1912, p. 9).

On a

$$\alpha, \delta > 0, \qquad \beta, \gamma < 0, \qquad \alpha < -\beta < 2\alpha, \qquad -\beta < \delta,$$

ce qui caractérise la vingt-deuxième famille. Donc

$$\Sigma' = T(VT)^{m_1}(V^2T)^{n_1}\dots(V^2T)^{n_{i-1}}(VT)^{m_i}V^2.$$

Formons la substitution

$$T^{-1}\Sigma' V^{-2} = T\Sigma' V = (VT)^{m_1}\dots(VT)^{m_i} = z \,\Big|\, \left[m_1, n_1, \dots, m_i, \frac{1}{z}\right]$$

qui est la deuxième famille. On trouve

$$T\Sigma' V = \frac{3z+10}{2z+7} = \frac{Rz+P}{Sz+Q}.$$

Or

$$\frac{10}{7} = [1, 2, 3]$$

(on doit avoir un nombre impair d'éléments). Donc

$$T\Sigma' V = (VT)(V^2T)^2(VT)^3$$

et

$$\Sigma' = T(VT)(V^2T)^2(VT)^3V^2 = TVTV^2TV^2TVTVTVTV^2.$$

12. Plusieurs substitutions étant décomposées en substitutions premières, on a immédiatement leur produit. Mais il n'est pas vrai que le produit soit composé de toutes les substitutions premières des deux facteurs, comme cela a lieu pour les nombres entiers. Car des réductions peuvent s'opérer. Par exemple, le produit des deux substitutions Σ et Σ' prises plus haut comme exemples

$$\Sigma\Sigma' = V^2TV^2TVTV^2TVTVTV^2TVTV^2T \times TVTV^2TV^2TVTVTVTV^2$$

se réduit à

$$V^2TV^2TVTV^2TVTVTVTVTVTVTV^2.$$

L'inverse d'une substitution décomposée en substitutions premières s'obtient en renversant l'ordre des substitutions, et remplaçant V par V^2 et V^2 par V. Il en résulte que l'inverse d'une substitution de la première famille appartient à la vingt et unième

ou à la vingt-deuxième, l'inverse d'une substitution de la seconde à la vingt-troisième ou la vingt-quatrième, etc., l'inverse d'une substitution de la vingt-quatrième à la première ou à la seconde.

Remarque. — *Le produit de deux substitutions de la première famille appartient lui-même à la première famille. De plus, ces deux substitutions étant décomposées en leurs facteurs premiers, si l'on forme leur produit comme il vient d'être expliqué, il ne se fait pas de réduction.*

C'est évident.

Mais *l'inverse d'une substitution de la première famille n'appartient pas à la première famille.*

Il y a là quelque chose d'analogue à ce qui se passe dans l'ensemble des nombres entiers. Car le produit de deux d'entre eux appartient à l'ensemble, mais non l'inverse de l'un d'entre eux. On sait qu'il se pose alors une question de la divisibilité. Un entier peut être, ou non, divisible par un autre.

Une question analogue se pose pour les substitutions modulaires de la première famille. Seulement, ici, il y a deux espèces de divisibilité, celle *première manière* et celle *seconde manière*(1). Pour que A soit divisible, *première manière*, par B, il faut et il suffit que la décomposition de A en facteurs soit formée de celle de B *suivie* d'autres facteurs. Pour que A soit divisible, *seconde manière*, par B, il faut et il suffit que la décomposition de A en facteurs soit formée de celle de B *précédée* d'autres facteurs. D'où une théorie facile du plus grand commun diviseur, *première* ou *seconde manière*.

Tout ce que nous avons dit de la première famille s'applique d'ailleurs aussi à la quatrième.

Une autre conséquence de la décomposition univoque des substitutions modulaires en produit de substitutions V et T est la suivante, d'ailleurs connue : à savoir qu'il n'existe entre V et T aucune autre relation que les relations $T^2 = V^3 = 1$. Car une telle relation pourrait être mise sous la forme $T^{\alpha} V^{\beta} T^{\alpha'} \ldots = 1$, les

(1) *T. d. N.*, n° 368.

exposants α étant 0 ou 1, les exposants B étant 0, 1 ou 2, et ces exposants n'étant pas tous nuls. Mais cette relation donnerait l'expression d'une substitution décomposée de deux façons différentes en facteurs T et V.

Comme dernière application, proposons-nous de *trouver les substitutions* S *telles que* $S^m = 1$ (1). Soit $S = AB \dots KL$; A, B, ..., K, L étant des facteurs T, V, ou V^2. On doit avoir

$$(AB \dots KL)(AB \dots KL) \dots (AB \dots KL) = 1$$

(m parenthèses dans le premier membre).

A cause de l'univocité de la décomposition en facteurs premiers, il faut que des réductions se produisent dans le premier membre de manière à ce qu'il devienne identique à 1 ; et comme, par hypothèse, ces réductions ne se produisent pas à l'intérieur d'une même parenthèse, c'est qu'elles se produisent entre les extrémités de deux parenthèses consécutives.

On a donc $LA = 1$. Opérant cette réduction, on voit ensuite de même que $KB = 1$, etc., c'est-à-dire que les facteurs équidistants des extrêmes dans un même crochet sont inverses l'un de l'autre. Si le nombre de ces facteurs est pair, la substitution S se réduit à 1, ce qui est une première solution; si le nombre des facteurs est impair, S prend la forme $\Sigma A \Sigma^{-1}$, en désignant par A l'un des trois facteurs T, V ou V^2, et par Σ une substitution quelconque. Les substitutions $S = \Sigma T \Sigma^{-1}$ satisfont à $S^2 = 1$ et, par suite, à $S^{2k} = 1$; les substitutions $S = \Sigma V \Sigma^{-1}$ et $S = \Sigma V^2 \Sigma^{-1}$ satisfont à $S^3 = 1$ et, par suite, à $S^{3k} = 1$. Ainsi le problème proposé n'admet de solution autre que la substitution identique que si l'exposant m est divisible par 2 ou par 3. Dans le premier cas, il a comme solutions

$$\Sigma T \Sigma^{-1} \quad \text{ou} \quad \begin{pmatrix} \beta\delta + \alpha\gamma & -(\alpha^2 + \beta^2) \\ \gamma^2 + \delta^2 & -(\beta\delta + \alpha\gamma) \end{pmatrix}.$$

Dans le second cas, il a comme solutions

$$\Sigma V \Sigma^{-1} \quad \text{ou} \quad \begin{pmatrix} \alpha\delta + \beta\delta + \alpha\gamma & -\alpha\beta - \alpha^2 - \beta^2 \\ \gamma\delta + \gamma^2 + \delta^2 & -\beta\gamma - \beta\delta - \alpha\gamma \end{pmatrix}$$

(1) *Voir* par exemple SERRET, *Algèbre supérieure*, 3e édition, t. II, p. 332. La solution donnée s'applique aux substitutions à coefficients quelconques. La nôtre peut s'en déduire.

et

$$\Sigma V^2 \Sigma^{-1} \quad \text{ou} \quad \begin{pmatrix} \beta\delta + \alpha\gamma + \beta\gamma & -\alpha\beta - \alpha^2 - \beta^2 \\ \gamma\delta + \gamma^2 + \delta^2 & -\beta\delta - \alpha\gamma - \alpha\delta \end{pmatrix},$$

α, β, γ, δ étant, dans tous les cas, des entiers satisfaisant à la condition $\alpha\delta - \beta\gamma = 1$.

13. Revenons aux substitutions linéaires homogènes à deux variables.

A la substitution

$$A = \begin{matrix} x \\ y \end{matrix} \Big| \begin{matrix} \alpha x + \beta y, \\ \gamma x + \delta y \end{matrix}$$

correspond la substitution

$$\overline{A} = z \Big| \frac{\alpha z + \beta}{\gamma z + \delta}.$$

Soit alors

$$T = \begin{matrix} x \\ y \end{matrix} \Big| \begin{matrix} y, \\ -x, \end{matrix} \qquad V = \begin{matrix} x \\ y \end{matrix} \Big| \begin{matrix} -x + y, \\ -x. \end{matrix}$$

Alors

$$\overline{T} = z \Big| -\frac{1}{z}, \qquad \overline{V} = z \Big| \frac{z}{z-1}.$$

Soit Σ une substitution homogène, la substitution homographique Σ peut se décomposer, et d'une seule manière, en un produit de substitutions $\overline{T}$ et $\overline{V}$. Le produit correspondant de substitutions T et V donnera, soit Σ, soit la substitution Σ' qui se déduit de Σ par le changement de signe de tous les coefficients. Or $\Sigma = \Sigma' T^2$. Donc *toute substitution homogène* Σ *se décompose en un produit de substitutions* V *et* T, *les substitutions* V *ayant comme exposant* 1 *ou* 2, *les substitutions* T *ayant comme exposant* 1, *sauf que le dernier facteur peut être* T^2 *ou* T^3. *Cette décomposition n'est possible que d'une seule manière.*