ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

X. STOUFF

Théorie des formes à coefficients entiers décomposables en facteurs linéaires

Annales de la faculté des sciences de Toulouse 2^e série, tome 5, n° 2 (1903), p. 129-155

<http://www.numdam.org/item?id=AFST_1903_2_5_2_129_0>

THÉORIE DES FORMES A COEFFICIENTS ENTIERS

DÉCOMPOSABLES EN FACTEURS LINÉAIRES,

PAR M. X. STOUFF,

Professeur à la Faculté des Sciences de Besançon.

Théorie des formes à coefficients entiers où le degré est égal au nombre des variables et qui peuvent être décomposées en facteurs linéaires (1).

I.

Soit d'abord une forme de degré n, à m variables, dont les coefficients ne sont pas tous nuls. On peut trouver un système de valeurs entières des variables, premières entre elles, pour lequel cette forme a une valeur différente de zéro. En effet, attribuons à chaque variable, indépendamment des autres, $n+1$ valeurs entières distinctes, ce qui donne en tout $(n+1)^m$ systèmes de valeurs des variables. Parmi les $(n+1)^m$ valeurs correspondantes de la forme, l'une au moins n'est pas nulle. Supposons, en effet, pour un instant que le contraire ait lieu, et envisageons les valeurs de la forme relatives aux différents systèmes qui ne se distinguent entre eux que par la valeur de l'une des indéterminées; la forme ordonnée par rapport à cette variable est un polynome d'ordre n, qui a $n+1$ racines, et dont, par conséquent, tous les coefficients sont nuls. Les coefficients de la forme ainsi ordonnée, qui sont des formes d'ordre n au plus par rapport aux $m-1$ variables restantes, sont nuls pour les $(n+1)^{m-1}$ systèmes de valeurs que l'on peut attribuer à ces variables. On ordonnera chacun d'eux par rapport à l'une des variables qu'il contient, et l'on répétera le même raisonnement. Finalement, on prouve ainsi de proche en proche que tous les coefficients de la forme

(1) L'objet de cet article est de faciliter la lecture des Mémoires de M. Hermite (t. 47 du *Journal de Crelle*). M. Minkowski a souvent complété les travaux de M. Hermite avec des méthodes qui lui sont propres. Je me suis proposé ici d'interpréter autant que possible la pensée de M. Hermite.

proposée sont nuls, ce qui est contre l'hypothèse. Ayant obtenu un système de valeurs entières des variables qui n'annulent pas la forme, en les divisant par leur plus grand commun diviseur, nous obtiendrons un système de valeurs entières des variables premières entre elles qui n'annulent pas cette forme.

Nous nommons *équivalentes* deux formes lorsque la seconde s'obtient en soumettant la première à une substitution linéaire de déterminant *un*

$$x_i = \sum_{j=1}^{j=m} \alpha_{ij} x'_j \qquad (i = 1, 2, \ldots, m), \tag{1}$$

où les coefficients α_{ij} sont entiers.

On sait, d'après M. Hermite, que l'on peut toujours former un déterminant à éléments entiers et de valeur *un*, dont une colonne soit constituée par des nombres entiers donnés, premiers entre eux; on sait également que, si une forme est soumise à la substitution (1), le coefficient de $x_j'^n$ est le résultat obtenu en substituant respectivement à $x_1, x_2, \ldots, x_m$ dans la forme primitive $\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{mj}$. De ces deux propositions et de celle que nous avons démontrée en commençant il résulte que toute forme dont les coefficients ne sont pas tous nuls a une équivalente dans laquelle le coefficient de x_j^n n'est pas nul, j étant l'un des m indices à volonté.

Le problème que nous nous proposons maintenant d'étudier est le suivant :

On donne une forme à coefficients entiers de degré n, à m variables, et l'on sait a priori *que cette forme peut être décomposée en n facteurs linéaires; on demande d'obtenir ces facteurs.*

Le problème sera résolu pour la forme donnée s'il l'est pour l'une quelconque des formes équivalentes. Parmi celles-ci, soit $F(x_1, x_2, \ldots, x_m)$ une forme où le coefficient de x_1^n, qui est un nombre entier A, est différent de zéro, et

$$F(x_1, x_2, \ldots, x_m) = \prod_{j=1}^{j=n} U_j,$$

$$U_j = \sum_{h=1}^{h=m} a_{jh} x_h,$$

on aura

$$A = \prod_{j=1}^{j=n} a_{j1},$$

et, par hypothèse, A n'étant pas nul, aucun des coefficients a_{j1} n'est nul.

Le problème devra être considéré comme résolu si l'on connaît dans chaque

facteur linéaire les rapports des coefficients de $x_2, x_3, \ldots, x_m$ au coefficient de x_1. En effet, les données ne permettent pas de déterminer davantage ces facteurs. Prenons

$$x_2 = 1;$$

posons

$$x_1 = z,$$

$$\frac{a_{j2}}{a_{j1}} = -z_j \qquad (j = 1, 2, 3, \ldots, n),$$

$$v_j = \sum_{h=3}^{h=m} \frac{a_{jh}x_h}{a_{j1}} \qquad (j = 1, 2, 3, \ldots, n)$$

et

$$\frac{\mathrm{F}(z, 1, x_3, \ldots, x_m)}{\mathrm{A}} = f(z, x_3, \ldots, x_m),$$

nous aurons

$$f(z, x_3, \ldots, x_m) = \prod_{j=1}^{j=n} (z - z_j + v_j), \tag{2}$$

le polynome f a ses coefficients rationnels. Il doit être considéré comme connu. Le problème sera résolu si l'on connaît les quantités z_j et les expressions linéaires v_j qui ne contiennent que les $m - 2$ dernières variables $x_3, \ldots, x_m$.

Soit $\varphi(z)$ la somme des termes de $f(z, x_3, \ldots, x_m)$ où ne figurent pas les $m - 2$ dernières variables, et $\varphi_k(z, x_3, \ldots, x_m)$ la somme des termes de f dont le degré total par rapport aux $m - 2$ variables $x_3, \ldots, x_m$ est égal à k. On aura donc

$$f(z, x_3, \ldots, x_m) = \varphi + \varphi_1 + \varphi_2 + \ldots + \varphi_n.$$

En faisant

$$x_3 = \ldots = x_m = 0,$$

l'identité (2) donne

$$\varphi(z) = \prod_{j=1}^{j=n} (z - z_j);$$

les quantités z_j sont donc les n racines de l'équation à coefficients rationnels

$$\varphi(z) = 0, \tag{3}$$

à chacune des racines de cette équation correspond un facteur linéaire de f. Soit z_1 une racine simple de l'équation (3), je dis que les coefficients de la fonction linéaire v_1 s'expriment rationnellement en fonction de z_1. En effet, si l'on développe le produit qui figure dans le second membre de (2), on voit que l'on a

$$\varphi_1 = \sum_{j=1}^{j=n} \left[v_j \prod{}' (z - z_h) \right], \tag{4}$$

où le signe $\prod'$ indique le produit des facteurs binomes $z - z_h$ en exceptant la valeur $h = j$. Si, dans les deux membres de l'identité (4), on fait $z = z_1$, il vient

$$\varphi_1(z_1, x_3, \ldots, x_m) = v_1 \prod_{h=2}^{h=n} (z_1 - z_h) = v_1 \varphi'(z_1).$$

Ainsi *le facteur linéaire qui correspond à une racine simple* z_1 est

$$\frac{\varphi_1(z_1, x_3, \ldots, x_m) + (z - z_1)\varphi'(z_1)}{\varphi'(z_1)},$$

on voit qu'il est connu rationnellement dès que z_1 est connu.

Je dis encore que, si z_1 est une racine multiple d'ordre k de l'équation (3), le produit des facteurs linéaires de f qui correspondent à z_1 est connu rationnellement quand z_1 est connu. Soit, en effet,

$$P_1 = (z - z_1 + v_1)(z - z_1 + v_2)\ldots(z - z_1 + v_k)$$

ce produit. On a

$$\varphi_k(z, x_3, \ldots, x_m) = \sum \left(\prod_{h=1}^{h=k} v_{j_h} \right) \left[\prod' (z - z_l) \right];$$

dans chaque terme de la somme $\sum$, l'ensemble des indices j_h forme une combinaison des indices 1, 2, ..., n, k à k. Le signe $\prod'$ indique que l prend les valeurs qui ne sont pas comprises parmi celles des indices j_h. Si nous faisons $z = z_1$, tous les termes de la somme $\sum$ s'annulent, sauf un seul, et l'on a

$$\varphi_k(z_1, x_3, \ldots, x_m) = v_1 v_2 \ldots v_k (z_1 - z_{k+1})(z_1 - z_{k+2})\ldots(z_1 - z_n) = v_1 v_2 \ldots v_k \frac{1}{k!} \varphi^{(k)}(z_1).$$

Plus généralement, on a

$$\varphi_{k-l}(z, x_3, \ldots, x_m) = \sum \left(\prod_{h=1}^{h=k-l} v_{j_h} \right) \left[\prod' (z - z_r) \right]. \tag{5}$$

Dans le second membre, $z - z_1$ figure avec l'exposant l dans les termes qui contiennent les produits $k - l$ à $k - l$ des expressions $v_1, v_2, \ldots, v_k$; $z - z_1$ figure avec un exposant supérieur à l dans tous les autres termes du second membre. Prenons les dérivées d'ordre l des deux membres de l'identité (5), puis

faisons $z = z_1$, il viendra

$$\varphi_{k-l}^{(l)}(z_1, x_3, \ldots, x_m) = \frac{l!}{k!}\varphi^{(k)}(z_1)\sum\left(\prod_{h=1}^{h=k-l} v_{j_h}\right),$$

où, cette fois, les indices j_h sont pris parmi les nombres 1, 2, ..., k.

On aura, par suite,

$$(6)\quad P_1 = \frac{\varphi_k(z_1, x_3, \ldots, x_m) + \frac{z-z_1}{1}\varphi'_{k-1}(z_1, x_3, \ldots, x_m) + \frac{(z-z_1)^2}{2!}\varphi''_{k-2}(z_1, x_3, \ldots, x_m) + \ldots + \frac{(z-z_1)^k}{k!}\varphi^{(k)}(z_1)}{\frac{1}{k!}\varphi^{(k)}(z_1)},$$

P_1 est donc connu rationnellement par z_1.

Supposons que l'équation ait s racines de l'ordre de multiplicité k, $z_1, z_2, \ldots, z_s$, et soit

$$\psi(z) = (z - z_1)(z - z_2)\ldots(z - z_s),$$

on sait que le polynome $\psi(z)$ est connu rationnellement; aux racines $z_1, z_2, \ldots, z_s$ correspondent des facteurs $P_1, P_2, \ldots, P_s$ de f tous de degré k donnés par la formule (6), et le produit effectué $P_1 P_2 \ldots P_s$ est un polynome de degré sk dont les coefficients sont des fonctions symétriques de $z_1, z_2, \ldots, z_s$. Ce polynome est donc connu rationnellement.

Supposons maintenant que la forme à coefficients entiers $F(x_1, x_2, \ldots, x_m)$ soit irréductible. Nous entendons par là qu'elle n'est le produit d'aucune autre forme à coefficients entiers par une forme aussi à coefficients entiers. D'après la théorie de la division des polynomes, F ne pourra être non plus le produit de deux formes de degré moindre que n à coefficients rationnels, et f n'admettra pas non plus de diviseur de degré moindre à coefficients rationnels. Or, si l'équation (3) admet s racines du degré k de multiplicité, et, en outre, d'autres racines d'un degré de multiplicité différent de k, f admet le facteur $P_1 P_2 \ldots P_s$ qui est connu rationnellement, et, par conséquent, F ne peut être irréductible. Donc, si F est irréductible, toutes les racines de (3) sont nécessairement du même ordre de multiplicité.

Quand $F(x_1, x_2, \ldots, x_m)$ *est irréductible, on peut, d'ailleurs, en tout cas, faire dépendre la décomposition complète de cette forme en facteurs linéaires d'une équation d'ordre n qui n'a que des racines simples.*

U_j désignant, comme il a été dit plus haut, l'un des facteurs linéaires de F, on peut écrire

$$U_j = a_{j1}x_1 + \sum_{h=2}^{h=m} a_{jh}x_h;$$

comme aucun des coefficients a_{j1} n'est nul, nous pouvons poser

$$L_j = \frac{1}{a_{j1}} \sum_{h=2}^{h=m} a_{jh} x_h.$$

Les n fonctions linéaires homogènes L_j contiennent seulement les $m-1$ dernières variables $x_2, x_3, \ldots, x_m$. Attribuons à chacune de ces variables indépendamment des autres $\frac{n(n-1)}{2}+1$ valeurs entières distinctes, ce qui donnera en tout $\left[\frac{n(n-1)}{2}+1\right]^{m-1}$ systèmes de valeurs de ces variables. Je dis que l'un au moins de ces systèmes fait acquérir aux n fonctions linéaires L_j des valeurs toutes différentes entre elles. Supposons, en effet, que le contraire ait lieu, c'est-à-dire que, pour chaque système, deux au moins des fonctions L_j prennent la même valeur. Il y a $\left[\frac{n(n-1)}{2}+1\right]^{m-2}$ groupes chacun de $\frac{n(n-1)}{2}+1$ systèmes, tels que les systèmes de chaque groupe ne diffèrent que par la valeur attribuée à x_2. Envisageons les systèmes d'un même groupe, pour chacun d'eux il existe une combinaison L_j, $L_{j'}$, pour laquelle les valeurs de L_j et de $L_{j'}$ sont égales, et, comme le nombre des systèmes de ce groupe surpasse d'une unité le nombre des combinaisons de n objets deux à deux, l'une au moins des combinaisons L_j, $L_{j'}$ doit se présenter deux fois. On a donc, pour les mêmes valeurs de $x_3, x_4, \ldots, x_m$ et pour deux valeurs différentes de x_2,

$$L_j = L_{j'};$$

d'où l'on déduit

$$\frac{a_{j2}}{a_{j1}} = \frac{a_{j'2}}{a_{j'1}}, \qquad \frac{a_{j3}x_3 + \ldots + a_{jm}x_m}{a_{j1}} = \frac{a_{j'3}x_3 + \ldots + a_{j'm}x_m}{a_{j'1}}.$$

Posons

$$L'_j = \frac{1}{a_{j1}} \sum_{h=3}^{h=m} a_{jh} x_h,$$

nous avons donc $\left[\frac{n(n-1)}{2}+1\right]^{m-2}$ systèmes de valeurs de $x_3, \ldots, x_m$ tels que dans chaque système une des combinaisons L'_j, $L'_{j'}$, présente des valeurs égales et que de plus $\frac{a_{j2}}{a_{j1}} = \frac{a_{j'2}}{a_{j'1}}$. Ces systèmes peuvent être répartis en $\left[\frac{n(n-1)}{2}+1\right]^{m-3}$ groupes où les systèmes d'un même groupe ne diffèrent que par la valeur de x_3; le nombre des systèmes d'un même groupe étant $\frac{n(n-1)}{2}+1$, l'une des combinaisons L'_j, $L'_{j'}$ présentant des valeurs égales doit se présenter au moins deux fois,

et l'on en déduit

$$\frac{a_{j2}}{a_{j1}} = \frac{a_{j'2}}{a_{j'1}}, \qquad \frac{a_{j3}}{a_{j1}} = \frac{a_{j'3}}{a_{j'1}}, \qquad \frac{a_{j1}x_1 + \ldots + a_{jm}x_m}{a_{j1}} = \frac{a_{j'1}x_1 + \ldots + a_{j'm}x_m}{a_{j'1}}$$

et ainsi de suite. De proche en proche on prouverait ainsi qu'il existerait dans F deux facteurs linéaires U_j, $U_{j'}$ dont les coefficients seraient proportionnels. F aurait donc des facteurs multiples, et le produit des facteurs d'un même degré de multiplicité donnerait un diviseur de F qui pourrait être trouvé rationnellement. F ne serait donc pas irréductible.

Envisageons maintenant un système de valeurs de $x_2, x_3, \ldots, x_m$ pour lesquelles les fonctions L_j sont toutes différentes. Divisons ces valeurs par leur plus grand commun diviseur, nous aurons des valeurs entières premières entre elles de x_2, $x_3, \ldots, x_m$ pour lesquelles les valeurs des L_j sont toutes différentes; ces valeurs peuvent être prises pour éléments de la première colonne d'un déterminant à éléments entiers et de valeur *un*. Dans F, sans changer la variable x_1, soumettons les $m-1$ dernières variables à la substitution dont les coefficients sont les éléments de ce déterminant; les différents quotients $\frac{a_{j2}}{a_{j1}}$ relatifs aux facteurs linéaires de la nouvelle forme seront précisément les valeurs des fonctions L_j toutes différentes entre elles. Par suite l'équation $\varphi(z) = 0$, relative à la nouvelle forme, n'aura que des racines simples; et chacune de ces racines étant connue, on connaît par cela même le facteur linéaire correspondant.

Soit $n = sk$, et supposons que l'équation $\varphi(z) = 0$ relative à la forme primitive ait s racines de degré k de multiplicité. Par la résolution d'une équation de degré s, la forme se trouvera décomposée en s autres formes de degré k; si l'on fait ensuite dans chacune de ces formes la substitution linéaire à coefficients entiers qui vient d'être indiquée, on voit que chaque forme d'ordre k pourra être décomposée en facteurs linéaires à l'aide d'une équation de degré k.

On peut encore remarquer que *si la fonction* F *est irréductible et si l'équation* $\varphi(z) = 0$ *n'a que des racines simples, cette dernière équation est nécessairement irréductible.* Car si $\varphi(z)$ avait un facteur rationnel, le produit des facteurs correspondants de F serait aussi connu rationnellement.

II.

Considérons plus particulièrement les formes irréductibles décomposables en facteurs linéaires et où le nombre des variables égale l'ordre n de la forme

$$\begin{aligned} F(x_1, x_2, \ldots, x_n) = {} & (a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n) \\ & \times (a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n)\ldots(a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n). \end{aligned}$$

M. Hermite nomme *invariant de* F le carré du déterminant des coefficients a_{jh} $(j, h = 1, 2, \ldots, n)$. L'invariant est une quantité rationnelle.

En effet, d'après ce qui précède, dans chaque facteur linéaire de F, les rapports des $n-1$ derniers coefficients au premier peuvent toujours s'exprimer comme nous l'avons vu par des fonctions rationnelles des diverses racines d'une équation d'ordre n à coefficients rationnels. L'invariant est, par suite, égal à une fonction symétrique des racines de cette équation, multipliée par le carré du produit

$$a_{11}a_{21}\ldots a_{n1}$$

qui est lui-même égal au coefficient de x_1^n dans la forme; donc, c'est une quantité rationnelle.

Si l'invariant n'est pas nul, aucun des coefficients a_{jh} n'est nul, ni dans la forme F, ni dans aucune forme équivalente.

En effet, d'après ce qui précède, il existe une équation à coefficients rationnels qui n'a que des racines simples $z_1, z_2, \ldots, z_n$ et telle que l'on ait

$$a_{1h} = \pi(z_1), \quad a_{2h} = \pi(z_2), \quad \ldots, \quad a_{jh} = \pi(z_j), \quad \ldots, \quad a_{nh} = \pi(z_n),$$

$\pi(z)$ étant une fonction rationnelle. De plus, cette équation est irréductible, sans quoi F ne pourrait être irréductible. Si donc on avait

$$\pi(z_j) = 0,$$

l'équation $\pi(z) = 0$, à coefficients rationnels, admettant la racine z_j, devrait admettre toutes les racines $z_1, z_2, \ldots, z_n$; on aurait alors

$$a_{1h} = a_{2h} = \ldots = a_{jh} = \ldots = a_{nh} = 0,$$

et le déterminant dont le carré donne l'invariant ayant une colonne de zéros serait nul.

Le coefficient de x_h^n dans la forme F est égal à $\prod_{j=1}^{j=n} a_{jh}$. Ainsi dans F et dans toutes ses équivalentes les coefficients des puissances $n^{\text{ièmes}}$ des variables sont des entiers qui ne sont jamais nuls.

D'après ce qui précède, deux des rapports $\frac{a_{lh}}{a_{l1}}, \frac{a_{l'h}}{a_{l'1}}$, ne peuvent devenir égaux que si les n rapports $\frac{a_{jh}}{a_{j1}}$ $(j = 1, 2, \ldots, n)$ se partagent en un certain nombre s de groupes différents contenant chacun le même nombre k de rapports tous égaux entre eux. La décomposition de F en facteurs linéaires peut encore être consi-

dérée comme dépendant d'une équation E d'ordre n, à coefficients rationnels, et qui n'a que des racines simples. Mais comme cette décomposition peut aussi être effectuée par la résolution d'une équation d'ordre s suivie de celle d'une équation d'ordre k, *le groupe de Galois de l'équation* E *est alors nécessairement imprimitif.*

Si les facteurs de F ne sont pas tous réels, on peut supposer les facteurs imaginaires deux à deux conjugués. Soit μ le nombre des facteurs réels, ν le nombre de couples de facteurs imaginaires conjugués, de sorte que $\mu + 2\nu = n$. Représentons par U_j ($j = 1, 2, \ldots, \mu$) les facteurs réels, et par U_j pour $j = \mu + 1$, $\mu + 2$, $\ldots$, n les facteurs imaginaires conjugués. Supposons de plus que $U_{\mu+2}$ soit conjugué de $U_{\mu+1}$, $U_{\mu+4}$ conjugué de $U_{\mu+3}$, et ainsi de suite. Considérons le déterminant

$$D = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{\mu+1,1} & a_{\mu+1,2} & \ldots & a_{\mu+1,n} \\ a_{\mu+2,1} & a_{\mu+2,2} & \ldots & a_{\mu+2,n} \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ a_{n-1,1} & a_{n-1,2} & \ldots & a_{n-1,n} \\ a_{n,1} & a_{n,2} & \ldots & a_{n,n} \end{vmatrix},$$

en combinant les lignes on reconnaît aisément que ce déterminant est égal à

$$D = \frac{1}{2^\nu} \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{\mu+1,1} + a_{\mu+2,1} & a_{\mu+1,2} + a_{\mu+2,2} & \ldots & a_{\mu+1,n} + a_{\mu+2,n} \\ a_{\mu+2,1} - a_{\mu+1,1} & a_{\mu+2,2} - a_{\mu+1,2} & \ldots & a_{\mu+2,n} - a_{\mu+1,n} \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots & \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots & \ldots\ldots\ldots\ldots \\ a_{n-1,1} + a_{n,1} & a_{n-1,2} + a_{n2} & \ldots & a_{n-1,n} + a_{n,n} \\ a_{n,1} - a_{n-1,1} & a_{n,2} - a_{n-1,2} & \ldots & a_{nn} - a_{n-1,n} \end{vmatrix}.$$

Tous les éléments de ce déterminant autres que ceux des lignes de rangs $\mu + 2$, $\mu + 4$, $\ldots$, n sont réels; les éléments de ces lignes sont des imaginaires pures. Donc D est égal à $(\sqrt{-1})^\nu$ multiplié par une quantité réelle. L'invariant étant égal à D^2, on en conclut que l'invariant a le signe de $(-1)^\nu$.

III.

Soit

$$F(x_1, x_2, \ldots, x_n) = \prod_{j=1}^{j=n} U_j,$$

$$U_j = \sum_{h=1}^{h=n} a_{jh} x_h,$$

une forme à coefficients entiers, irréductible, décomposable en n facteurs linéaires et dont l'invariant n'est pas nul. On se propose de déterminer les substitutions linéaires à coefficients entiers

$$(S) \qquad x_i = \sum_{j=1}^{j=n} \alpha_{ij} x'_j,$$

qui changent cette forme en elle-même.

Par la substitution S, chaque forme linéaire U_j se change en une autre forme linéaire que l'on peut représenter par $U_j S$, et comme on doit avoir identiquement

$$\prod_{j=1}^{j=n} U_j = \prod_{j=1}^{j=n} U_j S,$$

et que d'après la théorie de la division des polynomes chaque facteur linéaire du premier membre doit se retrouver dans le second, à chaque indice j doit correspondre un indice h_j tel que l'on ait identiquement

$$(7) \qquad U_j S = \varepsilon_j U h_j,$$

lorsque j parcourt les valeurs $1, 2, \ldots, n$, l'indice correspondant h_j prend successivement une fois et une seule chacune de ces mêmes valeurs, de plus il faut évidemment que

$$(8) \qquad \prod_{j=1}^{j=n} \varepsilon_j = 1.$$

Nous distinguons maintenant deux cas.

Premier cas. — L'un des facteurs U_j se reproduit par la substitution S à une constante multiplicative près, ce qui s'exprime par les équations

$$(9) \qquad \frac{a_{j1}}{\sum_{i=1}^{i=n} a_{ji}\alpha_{i1}} = \frac{a_{j2}}{\sum_{i=1}^{i=n} a_{ji}\alpha_{i2}} = \ldots = \frac{a_{jn}}{\sum_{i=1}^{i=n} a_{ji}\alpha_{in}}.$$

Or, à chacun des facteurs de F correspond, d'après ce qui précède, une racine z_j d'une équation irréductible par laquelle les rapports $\frac{a_{jh}}{a_{j1}}$ $(h = 2, 3, \ldots, n)$ s'expriment rationnellement. En vertu de l'irréductibilité de cette équation, les relations (9) subsistent quand on y remplace z_j par une autre quelconque des racines de cette équation, ou, ce qui revient au même, les coefficients de U_j par ceux de l'un quelconque des autres facteurs linéaires. Donc, si l'un des facteurs se reproduit à une constante multiplicative près, il en est de même de tous les autres. On a donc, pour $j = 1, 2, \ldots, n$,

$$U_j S = \varepsilon_j U_j,$$

Le déterminant de la substitution S est toujours égal à $+1$.

En effet, on peut regarder cette substitution comme résultant de trois autres :

1° Substitution des variables $U_1, U_2, \ldots, U_n$ aux variables $x_1, x_2, \ldots, x_n$;

2° Substitution aux variables $U_1, U_2, \ldots, U_n$ des variables $U'_1, U'_2, \ldots, U'_n$ définies par les relations

$$U_j = \varepsilon_j U'_j.$$

3° Substitution aux variables $U'_1, U'_2, \ldots, U'_n$ des variables $x'_1, x'_2, \ldots, x'_n$.

Le déterminant de la première substitution est l'inverse du déterminant Δ des coefficients des fonctions linéaires U_j. Le déterminant de la seconde est $\prod \varepsilon_j = 1$. Le déterminant de la troisième est Δ. Le déterminant de S est nécessairement égal au produit de ces trois substitutions et, par conséquent, à l'unité.

La valeur commune des rapports (9) est $\frac{1}{\varepsilon_j}$. Donc ε_j s'exprime rationnellement par z_j; elle appartient au corps algébrique déterminé par cette racine.

ε_j est une unité complexe. Soit, en effet,

$$L = \sum_{i=1}^{i=n} \lambda_i x_i,$$

une fonction linéaire qui se reproduit multipliée par une constante ω quand on la soumet à la substitution S, de telle sorte que l'on ait identiquement

$$\sum_{i=1}^{i=n} \lambda_i \sum_{j=1}^{j=n} \alpha_{ij} x'_j = \omega \sum_{j=1}^{j=n} \lambda_j x'_j,$$

ce qui donne les relations

$$\sum_{i=1}^{i=n} \lambda_i \alpha_{ij} = \omega \lambda_j,$$

et par suite, en éliminant les quantités λ,

$$\begin{vmatrix} \alpha_{11}-\omega & \alpha_{21} & \dots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22}-\omega & \dots & \alpha_{n2} \\ \dots & \dots\dots & \dots & \dots \\ \alpha_{1n} & \dots\dots & \dots & \alpha_{nn}-\omega \end{vmatrix} = 0,$$

équation à coefficients entiers où le coefficient de ω^n est égal à *un*. Or ε_j est nécessairement une racine de cette équation. Donc ε_j est un entier complexe, et, d'après l'équation (8), ε_j *est une unité*.

Second cas. — Chacun des facteurs U_j soumis à la substitution S se transforme en un facteur U_{h_j} différent de U_j, multiplié par une constante ε_j.

Comme les rapports des coefficients de U_j s'expriment rationnellement par la racine z_j d'une équation d'ordre n qui n'a que des racines simples, on peut poser

$$(10)\qquad \begin{cases} a_{j1} = k_j(b_{10} + b_{11}z_j + b_{12}z_j^2 + \dots + b_{1,n-1}z_j^{n-1}), \\ a_{j2} = k_j(b_{20} + b_{21}z_j + b_{22}z_j^2 + \dots + b_{2,n-1}z_j^{n-1}), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots, \\ a_{jn} = k_j(b_{n0} + b_{n1}z_j + b_{n2}z_j^2 + \dots + b_{n,n-1}z_j^{n-1}), \end{cases}$$

les quantités b_{10}, b_{11}, ..., $b_{1,n-1}$, b_{20}, ..., b_{n0}, ..., $b_{n,n-1}$ sont des nombres rationnels, k_j est une quantité différente de zéro; pour avoir les expressions des coefficients d'un autre facteur linéaire U_h, il suffira de remplacer, dans les formules (10), k_j par une autre constante k_h, et z_j par la racine z_h qui correspond au facteur u_h, les nombres b restant les mêmes.

Il est évident que, pour que l'invariant de F ne soit pas nul, il faut que le déterminant des quantités b soit différent de zéro.

Mettons, pour simplifier, h au lieu de h_j. L'identité (7) donne alors

$$\sum_{i=1}^{i=n} a_{ji} \sum_{r=1}^{r=n} \alpha_{ir}x'_r = \varepsilon_j \sum_{r=1}^{r=n} a_{hr}x'_r,$$

et, en égalant les coefficients de x'_r dans les deux membres

$$(11)\qquad \sum_{i=1}^{i=n} a_{ji}\alpha_{ir} = \varepsilon_j a_{hr} \qquad (r = 1, 2, \dots, n).$$

Les équations (11) sont au nombre de n; comme le déterminant des quantités α_{ir} est égal à *un*, on pourra en tirer les coefficients a_{ji} comme fonctions linéaires des coefficients a_{hr}. Enfin en remplaçant a_{j1}, a_{j2}, ..., a_{jn} par les valeurs (10) et en

résolvant les équations ainsi obtenues, il vient

$$\begin{aligned}
1 &= \frac{\varepsilon_j k_h}{k_j}(c_{00} + c_{01} z_h + \ldots + c_{0,n-1} z_h^{n-1}),\\
z_j &= \frac{\varepsilon_j k_h}{k_j}(c_{10} + c_{11} z_h + \ldots + c_{1,n-1} z_h^{n-1}),\\
z_j^2 &= \frac{\varepsilon_j k_h}{k_j}(c_{20} + c_{21} z_h + \ldots + c_{2,n-1} z_h^{n-1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
z_j^{n-1} &= \frac{\varepsilon_j k_h}{k_j}(c_{n-1,0} + c_{n-1,1} z_h + \ldots + c_{n-1,n-1} z_h^{n-1}),
\end{aligned}$$

où les quantités c sont des coefficients rationnels; en divisant membre à membre la seconde équation par la première, on aura z_j exprimé rationnellement en fonction de z_h. On pourra toujours mettre cette relation sous la forme

$$z_j = \mu_0 + \mu_1 z_h + \mu_2 z_h^2 + \ldots + \mu_{n-1} z_h^{n-1} = \psi(z_h),$$

les coefficients $\mu_0, \mu_1, \ldots, \mu_{n-1}$ étant rationnels. z_h étant la racine de l'équation irréductible

$$\varphi(z) = 0, \tag{12}$$

les deux équations à coefficients rationnels

$$\varphi(z) = 0, \qquad \varphi[\psi(z)] = 0,$$

admettent z_h comme racine, et, par suite, toutes les racines de la première vérifient la seconde. Ainsi, en prenant pour z l'une quelconque des racines de (12), $\psi(z)$ est encore une racine de cette équation.

Si l'on considère l'équation

$$z_j = \psi(z),$$

il n'existe d'ailleurs qu'une seule racine de (12), $z = z_h$, qui vérifie cette équation. En effet, si l'on substitue à z, dans $\psi(z)$, les n racines de (12), on obtient n quantités qui, d'après la théorie des fonctions symétriques, sont les racines d'une équation E rationnelle d'ordre n. Si deux racines de (12) substituées dans $\psi(z)$ donnaient toutes deux z_j, z_j serait au moins racine double de l'équation E, et E serait réductible, z_j étant racine d'une équation rationnelle de degré moindre que n, l'équation (12) serait réductible, ce qui est contre l'hypothèse.

IV.

Le développement de la méthode indiquée par M. Hermite dans son Mémoire *Sur la théorie des formes quadratiques* (*Journal de Crelle*, t. 47, II^e^ Partie, V) permet : 1° *de démontrer que pour un invariant donné il n'existe qu'un nombre fini de classes distinctes de formes* F ; 2° *de déterminer la nature des substitutions qui transforment en elle-même une forme* F *décomposable en facteurs linéaires.*

Soient

$$U_1, \quad U_2, \quad \ldots, \quad U_p$$

les facteurs réels de F,

$$V_1, \quad W_1; \quad V_2, \quad W_2; \quad \ldots; \quad V_q, \quad W_q$$

les couples de facteurs imaginaires conjugués, de sorte que $p + 2q = n$. Nous poserons

$$(13)\qquad \begin{cases} U_j = \sum_{h=1}^{h=n} a_{jh} x_h \qquad (j = 1, 2, \ldots, p), \\ V_j = \sum_{h=1}^{h=n} (b_{jh} + i c_{jh}) x_h \qquad (j = 1, 2, \ldots, q) \qquad (i = \sqrt{-1}), \\ W_j = \sum_{h=1}^{h=n} (b_{jh} - i c_{jh}) x_h \qquad (j = 1, 2, \ldots, q), \end{cases}$$

les lettres a, b, c désignant des quantités réelles. On a identiquement

$$(14)\qquad F(x_1, x_2, \ldots, x_n) = \prod_{j=1}^{j=p} U_j \prod_{j=1}^{j=q} V_j W_j.$$

Envisageons, d'après M. Hermite, la forme quadratique

$$(15)\quad \varphi(x_1, x_2, \ldots, x_n) = \lambda_1^2 U_1^2 + \lambda_2^2 U_2^2 + \ldots + \lambda_p^2 U_p^2 + 2\mu_1^2 V_1 W_1 + \ldots + 2\mu_q^2 V_q W_q,$$

pour toutes les valeurs des paramètres λ et μ. Comme entre plusieurs formes φ qui ne diffèrent que par un facteur constant, il n'y a intérêt qu'à en considérer une seule, nous pouvons, sans porter atteinte à la généralité, supposer

$$(16)\qquad \lambda_1 \lambda_2 \ldots \lambda_p \mu_1^2 \mu_2^2 \ldots \mu_q^2 = 1,$$

D'après cela, en désignant par I l'invariant de F, le déterminant de φ est $(-1)^\nu I$.

Soit

$$(17)\quad (S)\qquad x_j = \sum_{h=1}^{h=n} \alpha_{jh} x'_h,$$

la substitution à coefficients entiers et de déterminant *un* propre à réduire φ pour des valeurs particulières des quantités λ et μ. Par cette substitution F devient

$$F'(x'_1, x'_2, \ldots, x'_n);$$

$$(18)\qquad F'(x'_1, x'_2, \ldots, x'_n) = \prod_{j=1}^{j=p} U'_j \prod_{j=1}^{j=q} V'_j W'_j,$$

U'_j est ce que devient U_j par la substitution S. D'une manière générale, nous représentons par des lettres accentuées les quantités relatives à la forme F'. Dans la forme φ', réduite de φ, le coefficient de x'^2_h est

$$(19)\quad \lambda_1^2 a'^2_{1h} + \lambda_2^2 a'^2_{2h} + \ldots + \lambda_p^2 a'^2_{ph} + \mu_1^2 (b'^2_{1h} + c'^2_{1h}) + \mu_1^2 (b'^2_{1h} + c'^2_{1h}) + \mu_2^2 (b'^2_{2h} + c'^2_{2h}) + \mu_2^2 (b'^2_{2h} + c'^2_{2h}) + \ldots + \mu_q^2 (b'^2_{qh} + c'^2_{qh}) + \mu_q^2 (b'^2_{qh} + c'^2_{qh}),$$

il résulte de la relation (16) que le produit des termes de l'expression (19) donne précisément le coefficient de x'^n_h dans F'. Or, nous avons démontré que, F étant irréductible, les coefficients de x'^n_1, x'^n_2, ..., x'^n_n ne peuvent être nuls, et comme ils sont entiers, leur valeur absolue est au moins égale à *un*. D'après le théorème relatif à une somme de termes positifs dont le produit est constant, la somme (19) est au moins égale à n. Or, d'après le théorème de M. Hermite sur les formes définies réduites, le produit des coefficients des carrés des indéterminées dans φ' est moindre que $\rho(-1)^\nu I$, ρ étant un coefficient numérique qui ne dépend que de n. Le coefficient de x'^2_h dans φ' est donc moindre que $\frac{\rho(-1)^\nu I}{n^{n-1}}$, puisque chacun des autres facteurs est au moins égal à n.

Donc, dans la forme φ' chaque coefficient du carré d'une indéterminée est compris entre une limite inférieure et une limite supérieure, toutes deux positives et qui ne dépendent que de I.

On sait d'ailleurs, d'après M. Hermite, que les formes binaires quadratiques obtenues en annulant dans φ', $n - 2$ quelconques des indéterminées sont toutes réduites; il résulte de cette remarque et de ce qui précède que, dans φ', les coefficients des rectangles des indéterminées ont tous des limites supérieures qui ne dépendent que de I.

De là résulte aussi que tous les coefficients de F' ont des limites supérieures qui ne dépendent que de I. En effet, la somme (19) ne comprenant que des termes positifs et ayant une limite supérieure qui ne dépend que de I, il en est de même

de chacun de ses termes, par conséquent, les quantités

$$\text{val. abs. } \lambda_j a'_{jh} \qquad (j=1, 2, \ldots, p;\ h=1, 2, \ldots, n)$$

$$\mu_j \mod(b'_{jh}+ic'_{jh}), \quad (j=1, 2, \ldots, q;\ h=1, 2, \ldots, n),$$

ont toutes des limites supérieures qui ne dépendent que de I.

Or, en effectuant le produit des quantités U', V', W', on voit que chaque coefficient de F' est une somme de produits de la forme

$$a'_{1j_1}a'_{2j_2}\ldots a'_{pj_p}(b'_{1j_1}+ic'_{1j_1})\ldots(b'_{qj_q}+ic'_{qj_q})(b'_{1h_1}-ic'_{1h_1})\ldots(b'_{qh_q}-ic'_{qh_q}),$$

on ne changera pas la valeur de cette expression en la multipliant par le produit (16) qui est égal à l'unité, ce qui donne

$$\lambda_1 a'_{1j_1}.\lambda_2 a'_{2j_2}\ldots\lambda_p a'_{pj_p}.\mu_1(b'_{1j_1}+ic'_{1j_1})\ldots\mu_q(b'_{qj_q}+ic'_{qj_q}).\mu_1(b'_{1h_1}-ic'_{1h_1})\ldots\mu_q(b'_{qh_q}-ic'_{qh_q}).$$

Dans ce dernier produit, chaque facteur ayant une limite supérieure, il en est de même du produit.

Les formes F' ayant des coefficients entiers dont les valeurs absolues sont limitées, sont donc en nombre fini. Nous obtenons donc le théorème de M. Hermite.

Pour un invariant donné, il n'existe qu'un nombre fini de classes distinctes.

La même méthode donne les transformations semblables de F (¹).

Soit

$$(20) \qquad \frac{\log\lambda_1^2}{r_1}=\frac{\log\lambda_2^2}{r_2}=\ldots=\frac{\log\lambda_p^2}{r_p}=\frac{\log\mu_1^2}{s_1}=\ldots=\frac{\log\mu_q^2}{s_q}=k,$$

$$(21) \qquad r_1+r_2+\ldots+r_p+2s_1+\ldots+2s_q=0,$$

k est un paramètre que l'on fait croître d'une valeur k_0 à $+\infty$, et ensuite décroître de k_0 à $-\infty$. Les quantités positives ou négatives r et s sont considérées comme fixes; $p+q-1$ d'entre elles peuvent être prises arbitrairement; la dernière est alors déterminée par la relation (21) qui est une conséquence de (16) et de (20). Nous dirons qu'une forme F est *réduite* quand elle correspond à une forme quadratique réduite pour des valeurs convenables des quantités λ et μ. Pour un invariant donné I, le nombre des formes réduites est limité, comme nous l'avons vu, et *a fortiori* il est limité pour une même classe.

En général, les corps algébriques qui correspondent aux divers facteurs de F

(¹) *Comparer* MINKOWSKI, *Geometrie der Zahlen*, p. 137.

sont distincts; nous supposerons que l'on adopte arbitrairement pour ces corps un ordre déterminé. On décomposera les formes réduites F en leurs facteurs linéaires, et l'on rangera ces facteurs dans l'ordre des corps auxquels ils correspondent. On ne considère pas comme distincts deux systèmes de facteurs qui ne différeraient respectivement que par des constantes multiplicatives.

Dans le cas où les corps algébriques correspondant aux divers facteurs de F ne sont pas distincts, on rangera d'abord les corps distincts dans un ordre déterminé, d'où il résultera un certain ordre entre les groupes de facteurs linéaires qui appartiennent aux différents corps. Pour disposer les facteurs linéaires à l'intérieur d'un même groupe, on adoptera d'abord un ordre arbitraire que l'on soumettra ensuite aux permutations du groupe de Galois de l'équation

$$\varphi(z) = 0. \tag{3}$$

Ainsi, dans ce cas, nous considérons comme distincts certains systèmes de facteurs qui ne diffèrent que par l'ordre des facteurs. Mais nous faisons toujours abstraction des constantes multiplicatives.

Soit dans tous les cas N le nombre des systèmes de formes linéaires ainsi obtenues.

Soit F_0 une certaine forme de la classe considérée. On décomposera F_0 en facteurs, et l'on rangera ces facteurs

$$u_1, \quad u_2, \quad \ldots, \quad u_p, \quad v_1, \quad \ldots, \quad v_q, \quad w_1, \quad \ldots, \quad w_q$$

dans l'ordre convenu pour les corps algébriques correspondants, si ces corps sont tous distincts; dans le cas contraire, on choisira un arrangement qui, vis-à-vis des précédents, ne soit pas en opposition avec le groupe de Galois de l'équation (3).

Envisageons la forme quadratique (15), $\varphi(x_1, x_2, \ldots, x_n)$ qui correspond à F_0, les valeurs des paramètres λ et μ étant obtenues d'après les équations (20). Soit P un nombre dont nous nous réservons de disposer. Donnons à k les valeurs

$$\mathrm{P}, \quad 2\mathrm{P}, \quad 3\mathrm{P}, \quad \ldots, \quad (\mathrm{N}+1)\mathrm{P},$$

réduisons chaque fois la forme quadratique φ, et faisons subir en même temps aux facteurs de F_0 la substitution propre à réduire φ; nous obtiendrons ainsi $N+1$ systèmes de formes linéaires dont le produit donne une forme réduite. Or, il n'y a que N pareils systèmes qui soient distincts. Donc un système au moins

$$\mathrm{U}_1, \quad \mathrm{U}_2, \quad \ldots, \quad \mathrm{U}_p, \quad \mathrm{V}_1, \quad \ldots, \quad \mathrm{V}_q, \quad \mathrm{W}_1, \quad \ldots, \quad \mathrm{W}_q$$

se présentera deux fois, abstraction faite de multiplicateurs constants, pour

$k = l\mathrm{P}$ et pour $k = m\mathrm{P}$, l et m étant deux valeurs différentes prises dans la suite 1, 2, 3, ..., N + 1. Soient

$$(22)\quad \begin{cases} \lambda_1^2\varepsilon_1^2\,\mathrm{U}_1^2 + \lambda_2^2\,\varepsilon_2^2\,\mathrm{U}_2^2 + \ldots + \lambda_p^2\varepsilon_p^2\,\mathrm{U}_p^2 + 2\mu_1^2\,\eta_1^2\,\mathrm{V}_1\mathrm{W}_1 + \ldots + 2\mu_q^2\,\eta_q^2\,\mathrm{V}_q\mathrm{W}_q, \\ \lambda_1^2\varepsilon_1'^2\,\mathrm{U}_1^2 + \lambda_2'^2\,\varepsilon_2'^2\,\mathrm{U}_2^2 + \ldots + \lambda_p^2\varepsilon_p'^2\,\mathrm{U}_p^2 + 2\mu_1'^2\,\eta_1'^2\,\mathrm{V}_1\mathrm{W}_1 + \ldots + 2\mu_q'^2\,\eta_q'^2\,\mathrm{V}_q\mathrm{W}_q, \end{cases}$$

les deux formes quadratiques réduites correspondantes, S et S′ les substitutions qui ont servi respectivement à les réduire.

La substitution S transforme $u_1, u_2, \ldots, u_p, v_1, \ldots, v_q, w_1, \ldots, w_q$ respectivement en

$$\varepsilon_1\mathrm{U}_1,\quad \varepsilon_2\mathrm{U}_2,\quad \ldots,\quad \varepsilon_p\mathrm{U}_p,$$
$$\eta_1 e^{i\theta_1}\mathrm{V}_1,\quad \ldots,\quad \eta_q e^{i\theta_q}\mathrm{V}_q,\quad \eta_1 e^{-i\theta_1}\mathrm{W}_1,\quad \ldots,\quad \eta_q e^{-i\theta_q}\mathrm{W}_q,$$

où $\theta_1, \theta_2, \ldots, \theta_q$ désignent des arguments réels et S′ transforme les mêmes formes linéaires respectivement en

$$\varepsilon_1'\mathrm{U}_1,\quad \varepsilon_2'\mathrm{U}_2,\quad \ldots,\quad \varepsilon_p'\mathrm{U}_p,$$
$$\eta_1' e^{i\theta_1'}\mathrm{V}_1,\quad \ldots,\quad \eta_q' e^{i\theta_q'}\mathrm{V}_q,\quad \eta_1' e^{-i\theta_1'}\mathrm{W}_1,\quad \ldots,\quad \eta_q' e^{-i\theta_q'}\mathrm{W}_q.$$

Donc S^{-1} transforme $\mathrm{U}_1, \mathrm{U}_2, \ldots, \mathrm{U}_p, \mathrm{V}_1, \ldots, \mathrm{V}_q, \mathrm{W}_1, \ldots, \mathrm{W}_q$ respectivement en

$$\varepsilon_1^{-1}u_1,\quad \varepsilon_2^{-1}u_2,\quad \ldots,\quad \varepsilon_p^{-1}u_p,$$
$$\eta_1^{-1}\varepsilon^{-i\theta_1}v_1,\quad \ldots,\quad \eta_q^{-1}\varepsilon^{-i\theta_q}v_q,\quad \eta_1^{-1}e^{i\theta_1}w_1,\quad \ldots,\quad \eta_q^{-1}e^{i\theta_q}w_q,$$

et par conséquent la substitution $\mathrm{S}'\mathrm{S}^{-1}$ change respectivement $u_1, u_2, \ldots, u_p$, $v_1, \ldots, v_q, w_1, \ldots, w_q$ en

$$\varepsilon_1'\varepsilon_1^{-1}u_1,\quad \varepsilon_2'\varepsilon_2^{-1}u_2,\quad \ldots,\quad \varepsilon_p'\varepsilon_p^{-1}u_p,$$
$$\eta_1'\eta_1^{-1}e^{i(\theta_1'-\theta_1)}v_1,\quad \ldots,\quad \eta_q'\eta_q e^{i(\theta_q'-\theta_q)}v_q,\quad \eta_1'\eta_1^{-1}e^{i(\theta_1-\theta_1')}w_1,\quad \ldots,\quad \eta_q'\eta_q^{-1}e^{i(\theta_q-\theta_q')}w_q.$$

Posons pour abréger

$$\varepsilon_j'\varepsilon_j^{-1} = \mathrm{E}_j,\qquad \eta_j'\eta_j^{-1} = \mathrm{H}_j,\qquad \theta_j' - \theta_j = \Theta_j.$$

Le déterminant de la substitution $\mathrm{S}'\mathrm{S}^{-1}$ est égal à *un*. Si l'on adopte comme variables les n fonctions linéaires indépendantes u_j, v_j, w_j, à $\mathrm{S}'\mathrm{S}^{-1}$ correspond sur ces variables une substitution qui en est la transformée et qui a, par suite, même déterminant. Ce déterminant est égal au produit des multiplicateurs E_j, $\mathrm{H}_j e^{\pm i\Theta_j}$. Donc

$$\mathrm{E}_1\mathrm{E}_2\ldots\mathrm{E}_p\,\mathrm{H}_1^2\mathrm{H}_2^2\ldots\mathrm{H}_q^2 = 1,$$

et, par suite, $\mathrm{S}'\mathrm{S}^{-1}$ est une transformation semblable de F_0. Elle change chacun des facteurs de F_0 en lui-même, à un multiplicateur constant près. C'est une sub-

stitution appartenant à la première catégorie considérée au § III. Tous les multiplicateurs sont des unités.

Une pareille substitution peut évidemment être caractérisée par les multiplicateurs correspondants.

Si S et T sont deux substitutions de cette catégorie, les substitutions ST et TS sont évidemment identiques et les multiplicateurs relatifs à ST sont les produits respectifs des multiplicateurs de S et de T. Nous utiliserons maintenant la remarque suivante :

Considérant toujours la même forme F_0, si l'on attribue aux quantités λ et μ des valeurs satisfaisant à la relation (16) et en dehors de cela absolument quelconques, les produits

$$\lambda_1^2\varepsilon_1^2, \quad \lambda_2^2\varepsilon_2^2, \quad \ldots, \quad \lambda_p^2\varepsilon_p^2, \quad \mu_1^2\eta_1^2, \quad \ldots, \quad \mu_q^2\eta_q^2$$

sont chacun compris entre une limite supérieure et une limite inférieure positives (la limite inférieure n'est jamais nulle).

En effet, en représentant les facteurs U_j, V_j, W_j d'après les formules (13), le coefficient de x_1^2 par exemple, dans la forme (22) sera

$$\lambda_1^2\varepsilon_1^2 a_{11}^2 + \lambda_2^2\varepsilon_2^2 a_{21}^2 + \ldots + \lambda_p^2\varepsilon_p^2 a_{p1}^2 + 2\mu_1^2\eta_1^2(b_{11}^2 + c_{11}^2) + \ldots + 2\mu_q^2\eta_q^2(b_{q1}^2 + c_{q1}^2),$$

nous savons que cette somme a une limite supérieure. Donc il en est de même *a fortiori* de $\lambda_1^2\varepsilon_1^2 a_{11}^2$. D'ailleurs, a_{11} n'est pas nul et ne peut prendre qu'un nombre limité de valeurs; car les facteurs U_j, V_j, W_j résultent de la décomposition des formes réduites en nombre limité. Donc $\gamma_1^2\varepsilon_1^2$ a une limite supérieure. Le même raisonnement s'applique à $\lambda_2^2\varepsilon_2^2$, ..., $\mu_1^2(b_{11}^2 + c_{11}^2)$, ...

On voit, en tenant compte de (16), que le produit

$$\lambda_1^2\varepsilon_1^2 a_{11}^2 . \lambda_2^2\varepsilon_2^2 a_{21}^2 \ldots \mu_1^4\eta_1^4(b_{11}^2 + c_{11}^2)^2 \ldots \mu_q^4\eta_q^4(b_{q1}^2 + c_{q1}^2)^2$$

est égal au carré du coefficient de x_1^n dans une forme réduite F_1. Ce coefficient n'est pas nul, et il est entier; donc il est au moins égal à *un*. Donc $\lambda_1^2\varepsilon_1^2 a_{11}^2$ est supérieur à l'unité divisée par les limites inférieures des autres facteurs, et comme a_{11} n'a qu'un nombre limité de valeurs $\lambda_1^2\varepsilon_1^2$ a une limite inférieure, et il en est de même des quantités analogues. On a donc

$$\log(\lambda_j^2\varepsilon_j^2) = Z_j, \qquad \log(\mu_j^2\eta_j^2) = \Lambda_j,$$

Z_j et Λ_j étant des quantités comprises dans des intervalles finis, d'où

$$\log\varepsilon_j^2 = -\log\lambda_j^2 + Z_j, \qquad \log\eta_j^2 = -\log\mu_j^2 + \Lambda_j$$

ou en se reportant aux équations (20) :

$$\log\varepsilon_j^2 = -l\,\mathrm{P}r_j + \mathrm{Z}_j, \qquad \log\eta_j^2 = -l\,\mathrm{P}s_j + \Lambda_j,$$
$$\log\varepsilon_j'^2 = -m\mathrm{P}r_j + \mathrm{Z}_j', \qquad \log\eta_j'^2 = -m\mathrm{P}s_j + \Lambda_j',$$

d'où

$$(23)\qquad \log\mathrm{E}_j^2 = (l-m)\mathrm{P}r_j + \mathrm{Z}_j' - \mathrm{Z}_j, \qquad \log\mathrm{H}_j^2 = (l-m)\mathrm{P}s_j + \Lambda_j' - \Lambda_j,$$

De là résulte que les substitutions de la première catégorie qui transforment F_0 en elle-même ne peuvent dériver de moins de $p+q-1$ substitutions fondamentales. Supposons, en effet, pour un instant qu'il y en ait un nombre ν inférieur à $p+q-1$. Désignons par $\sum', \sum'', \ldots, \sum^{(\alpha)}, \ldots, \sum^{(\nu)}$ ces substitutions fondamentales et par

$$\mathrm{E}_j^{(\alpha)} \quad (j=1, 2, \ldots, p), \qquad \mathrm{H}_j^{(\alpha)} e^{\pm i\Theta_j^{(\alpha)}},$$

les multiplicateurs relatifs à $\sum^{(\alpha)}$.

On aurait

$$\log\mathrm{E}_j^2 = \sum_{\alpha=1}^{\alpha=\nu} p_\alpha \log\mathrm{E}_j^{(\alpha)2} \qquad (j=1, 2, \ldots, p),$$
$$\log\mathrm{H}_j^2 = \sum_{\alpha=1}^{\alpha=\nu} p_\alpha \log\mathrm{H}_j^{(\alpha)2} \qquad (j=1, 2, \ldots, q),$$

où les quantités p_α sont ν entiers positifs ou négatifs, ces équations étant au nombre de $p+q$, tandis que les nombres p_α sont au plus au nombre de $p+q-2$, les $p+q-1$ premières équations suffiront pour que l'on puisse éliminer entre elles les quantités p_α. On obtiendra ainsi une relation de la forme

$$(24)\qquad \sum_{j=1}^{j=p} \mathrm{C}_j \log\mathrm{E}_j^2 + \sum_{=1}^{j=q-1} \mathrm{K}_j \log\mathrm{H}_j^2 = 0,$$

où les quantités C_j et K_j sont des coefficients qui ne sont pas tous nuls. En remplaçant dans la relation (24) les logarithmes par les valeurs (23), il vient en divisant par $(l-m)\mathrm{P}$

$$\sum_{j=1}^{j=p} \mathrm{C}_j r_j + \sum_{j=1}^{=q-1} \mathrm{K}_j s_j + \frac{\sum_{j=1}^{j=p} \mathrm{C}_j(\mathrm{Z}_j' - \mathrm{Z}_j) + \sum_{j=1}^{j=q-1} \mathrm{K}_j(\Lambda_j' - \Lambda_j)}{(l-m)\mathrm{P}} = 0,$$

l et m étant entiers et différents, $(l-m)\mathrm{P}$ est au moins égal à P en valeur

absolue. D'ailleurs le numérateur de la fraction est essentiellement limité, et comme P peut être supposé aussi grand que l'on veut, il faudrait que l'on eût

$$\sum_{j=1}^{j=p} C_j r_j + \sum_{j=1}^{j=q-1} K_j s_j = 0, \tag{25}$$

mais une relation de la forme (25) est impossible puisque $p+q-1$ des quantités r_j, s_j peuvent être prises arbitrairement.

Les substitutions semblables de la première catégorie dérivent donc au moins de $p+q-1$ substitutions fondamentales. Le nombre des substitutions fondamentales qui correspondent à des unités dont le module analytique est différent de *un* n'est d'ailleurs pas plus grand, comme on le reconnaît aisément d'après les considérations développées par M. Hermite dans sa quatrième lettre à Jacobi.

V.

Il s'agit maintenant d'étudier de plus près les transformations semblables des formes décomposables en facteurs linéaires. A ce point de vue, certaines de ces formes se prêtent à une recherche facile. Nous utiliserons ici une notion très employée, celle du *système de modules minimum*.

Nous considérons un corps algébrique K comme l'ensemble des quantités qui s'expriment rationnellement à l'aide d'une racine z_1 d'une équation Γ à coefficients rationnels :

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

Soit n le degré de cette équation.

D'après la définition générale des entiers complexes, les entiers du corps K sont des quantités qui s'expriment rationnellement par l'une des racines de Γ et qui, en même temps, satisfont à des équations à coefficients entiers dont le plus haut coefficient est égal à l'unité.

On sait que la somme, le produit de plusieurs entiers complexes, et toute racine d'une équation algébrique entière dont le plus haut coefficient est l'unité et dont tous les autres coefficients sont des entiers complexes, sont aussi des entiers complexes. Ces propositions se démontrent aisément par la théorie des fonctions symétriques.

Soient n entiers complexes du corps K :

$$\omega_1, \quad \omega_2, \quad \ldots, \quad \omega_n,$$

il résulte de ce qui précède que

$$m_1\omega_1 + m_2\omega_2 + \ldots + m_n\omega_n$$

est un entier complexe du même corps en désignant par $m_1, m_2, \ldots, m_n$ des entiers non-complexes quelconques.

Soient

$$\omega_1', \quad \omega_2', \quad \ldots, \quad \omega_n'; \quad \omega_1'', \quad \ldots, \quad \omega_n''; \quad \ldots; \quad \omega_1^{(n-1)} \quad \ldots, \quad \omega_n^{(n-1)}$$

les entiers conjugués de $\omega_1, \ldots, \omega_n$. Le carré du déterminant

$$D = \begin{vmatrix} \omega_1 & \omega_2 & \ldots & \omega_n \\ \omega_1' & \ldots & \ldots & \omega_n' \\ \ldots & \ldots & \ldots & \ldots \\ \omega_1^{(n-1)} & \ldots & \ldots & \omega_n^{(n-1)} \end{vmatrix}$$

est un entier non-complexe. En effet, ce carré est une quantité rationnelle, car il ne change pas quand on permute d'une manière quelconque les racines de l'équation Γ. Comme il satisfait d'ailleurs à la définition générale des entiers complexes, c'est un entier de l'arithmétique élémentaire. Car une équation à coefficients entiers dont le plus haut coefficient est l'unité, n'a pas d'autres racines rationnelles que des racines entières. D^2 est positif ou négatif suivant que le nombre des couples de racines imaginaires de l'équation Γ est pair ou impair.

Nous appellerons *système de modules minimum* un système d'entiers complexes $\omega_1, \omega_2, \ldots, \omega_n$ appartenant au corps K et tel que la valeur absolue de D^2 soit la plus petite possible, sans être nulle. Ce minimum existe certainement, puisque D^2 ne peut prendre que des valeurs entières.

Tout entier complexe E du corps K peut se mettre sous la forme

$$m_1\omega_1 + m_2\omega_2 + \ldots + m_n\omega_n,$$

$m_1, m_2, \ldots, m_n$ étant des entiers non complexes. En effet, soient $E', E'', \ldots, E^{(n-1)}$, les conjugués de E; déterminons les quantités $m_1, m_2, \ldots, m_n$ par les équations

$$\begin{aligned} E &= m_1\omega_1 + m_2\omega_2 + \ldots + m_n\omega_n, \\ E' &= m_1\omega_1' + \ldots\ldots + m_n\omega_n', \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ E^{(n-1)} &= m_1\omega_1^{(n-1)} + \ldots\ldots + m_n\omega_n^{(n-1)}; \end{aligned}$$

les quantités $m_1, m_2, \ldots, m_n$ seront rationnelles, car leurs valeurs ne changent évidemment pas quand on permute d'une manière quelconque les racines de Γ. Supposons que l'une au moins de ces quantités soit fractionnaire, par exemple,

$$m_1 = m_1' + r_1,$$

m_1' étant un nombre entier et r_1 une fraction moindre que 1. $E_1 - m_1'\omega_1$ est donc

un entier complexe égal à $r_1\omega_1 + m_2\omega_2 + \ldots + m_n\omega_n$. Or le déterminant

$$\begin{vmatrix} r_1\omega_1 + m_2\omega_2 + \ldots + m_n\omega_n & \omega_2 & \ldots & \omega_n \\ r_1\omega'_1 + m_2\omega'_2 + \ldots + m_n\omega'_n & \omega'_2 & \ldots & \omega'_n \\ \ldots\ldots\ldots\ldots\ldots\ldots & \ldots & \ldots & \ldots \\ r_1\omega_1^{(n-1)} + m_2\omega_2^{(n-1)} + \ldots + m_n\omega_n^{(n-1)} & \omega_2^{(n-1)} & \ldots & \omega_n^{(n-1)} \end{vmatrix}$$

a pour valeur $r_1 D$. Donc $\omega_1, \omega_2, \ldots, \omega_n$ ne constitueraient pas un système de modules minimum, ce qui est contre l'hypothèse (1).

Soit $F(x_1, x_2, \ldots, x_n)$ une forme d'ordre n irréductible et décomposable en facteurs linéaires. Nous avons vu que la décomposition de cette forme dépend de la résolution d'une équation irréductible

$$\Gamma \qquad \varphi(z) = 0,$$

qui n'a que des racines simples. Ces racines déterminent n corps algébriques conjugués K, K', ..., $K^{(n-1)}$. Soit $\omega_1, \omega_2, \ldots, \omega_n$ un système de modules minimum, la forme

$$\Phi(y_1, y_2, \ldots, y_n) = \prod_{j=0}^{j=n-1} (\omega_1^{(j)} y_1 + \omega_2^{(j)} y_2 + \ldots + \omega_n^{(j)} y_n)$$

a évidemment ses coefficients entiers. Quant à $F(x_1, x_2, \ldots, x_n)$, dans la majorité des cas il ne sera pas possible de la décomposer en facteurs linéaires dont les coefficients sont des entiers de K. Mais on peut toujours écrire

$$F_1(x_1, x_2, \ldots, x_n) = A^{n-1} F(x_1, x_2, \ldots, x_n) = \prod_{j=1}^{j=n} T_j,$$

en désignant par A le coefficient de x_1^n dans F et par T_j des facteurs linéaires à coefficients complexes entiers. En effet on voit aisément que ces coefficients sont déterminés par des équations où le coefficient du plus haut terme est l'unité.

Les transformations semblables de F et de F_1 sont évidemment les mêmes. Il suffira donc d'étudier celles de F_1.

Considérons d'abord les transformations semblables de la première catégorie. Nous avons déjà démontré que, à une pareille transformation, correspond toujours une unité complexe.

Réciproquement, je dis que, à toute unité complexe de K, correspond une transformation semblable de Φ.

---

(1) *Voir* au sujet des théorèmes que je rappelle ici l'*Arithmétique* de DIRICHLET ou MINKOWSKI, *Geometrie der Zahlen*.

En effet, ε étant une unité du corps K, $\varepsilon\omega_1, \varepsilon\omega_2, \ldots, \varepsilon\omega_n$ sont des entiers du même corps; donc on a

$$(26)\qquad \begin{cases} \varepsilon\omega_1 = \omega_1\alpha_{11} + \omega_2\alpha_{21} + \ldots + \omega_n\alpha_{n1}, \\ \varepsilon\omega_2 = \omega_1\alpha_{12} + \ldots\ldots\ldots + \omega_n\alpha_{n2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \varepsilon\omega_n = \omega_1\alpha_{1n} + \ldots\ldots\ldots + \omega_n\alpha_{nn}, \end{cases}$$

où nous désignons par α_{jh} des entiers non-complexes. A cause de l'irréductibilité de Γ, les relations précédentes subsistent si l'on y remplace $\omega_1, \omega_2, \ldots, \omega_n, \varepsilon$ respectivement par les quantités conjuguées $\omega_1^{(h)}, \omega_2^{(h)}, \ldots, \omega_n^{(h)}, \varepsilon^{(h)}$. $y_1, y_2, \ldots, y_n$ étant des variables arbitraires, on déduit des relations (26) :

$$\begin{aligned} &\varepsilon(\omega_1 y_1 + \omega_2 y_2 + \ldots + \omega_n y_n) \\ &\quad = \omega_1(\alpha_{11}y_1 + \alpha_{12}y_2 + \ldots + \alpha_{1n}y_n) + \ldots + \omega_n(\alpha_{n1}y_1 + \ldots + \alpha_{nn}y_n); \end{aligned}$$

donc, en posant

$$(27)\qquad x_j = \sum_{h=1}^{h=n} \alpha_{jh} y_h,$$

$\omega_1 x_1 + \omega_2 x_2 + \ldots + \omega_n x_n$ devient, par la substitution (27),

$$\varepsilon(\omega_1 y_1 + \omega_2 y_2 + \ldots + \omega_n y_n).$$

Le déterminant de la substitution (27) est égal à *un*. En effet, considérons les variables $u^{(l)}$, $z^{(l)}$ définies par les équations

$$(28)\qquad \begin{cases} u^{(l)} = \sum_{j=1}^{j=n} \omega_j^{(l)} y_j, \qquad z^{(l)} = \sum_{j=1}^{j=n} \omega_j^{(l)} x_j \\ (l = 0, 1, \ldots, n-1). \end{cases}$$

La substitution (27) a pour transformée la substitution définie par les équations suivantes :

$$(29)\qquad z^{(l)} = u^{(l)}\varepsilon^{(l)} \qquad (l = 0, 1, \ldots, n-1).$$

Or, le déterminant de la substitution (29) est égal au produit des quantités $\varepsilon^{(l)}$, c'est-à-dire à l'unité. D'ailleurs il est égal au déterminant de la substitution (27), donc ce déterminant est égal à *un*.

Revenons à la forme $F_1(x_1, x_2, \ldots, x_n)$. Les facteurs T_j sont de la forme

$$T_j = \sum_{h=1}^{h=n} \psi_h^{(j)} x_h,$$

et comme les nombres $\psi_h^{(j)}$ sont des entiers complexes, on pourra poser

$$\psi_h^{(j)} = \sum_{k=1}^{k=n} b_{hk} \omega_k^{(j)},$$

où les quantités b_{hk} sont des entiers non-complexes.

La fonction $F_1(x_1, x_2, \ldots, x_n)$ se déduit donc de $\Phi(y_1, y_2, \ldots, y_n)$ par la substitution

$$y_j = \sum_{h=1}^{h=h} b_{hj} x_h. \tag{30}$$

La transformée de la substitution (27) par la substitution (30) est en général une substitution à coefficients fractionnaires. Donc, à toute unité ne correspond pas nécessairement une transformation semblable de F à coefficients entiers et à déterminant *un*.

Supposons d'abord que le corps K ne contienne pas d'unité dont le module analytique soit égal à *un*.

Soient $S_1, S_2, \ldots, S_\nu$ les substitutions fondamentales qui transforment Φ en elle-même.

A $S_1, S_2, \ldots, S_\nu$ répondent des multiplicateurs $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\nu$ qui forment un système d'unités fondamentales. D'après la théorie générale exposée précédemment, nous savons aussi que F possède une infinité de transformations semblables de la première catégorie dérivant de ν substitutions fondamentales $S'_1, S'_2, \ldots, S'_\nu$, qui correspondent aussi, comme nous l'avons vu, à des unités $\varepsilon'_1, \varepsilon'_2, \ldots, \varepsilon'_\nu$, et l'on a nécessairement

$$\begin{aligned}
\varepsilon'_1 &= \varepsilon_1^{m_{11}} \varepsilon_2^{m_{12}} \ldots \varepsilon_\nu^{m_{1\nu}}, \\
\varepsilon'_1 &= \varepsilon_1^{m_{21}} \ldots\ldots \varepsilon_\nu^{m_{2\nu}}, \\
&\ldots\ldots\ldots\ldots\ldots, \\
\varepsilon'_\nu &= \varepsilon_1^{m_{\nu 1}} \ldots\ldots \varepsilon_\nu^{m_{\nu\nu}},
\end{aligned}$$

les exposants m étant des nombres entiers. S'_j est une substitution à coefficients entiers et de déterminant *un*, et elle est la transformée par la substitution (30) de la substitution obtenue en multipliant par ε'_1 le facteur correspondant de Φ. Ainsi, *à toute transformation semblable de* F *correspond une transformation sem-*

blable de Φ. De plus, toute unité étant de la forme

$$\mathrm{E} = \varepsilon_1^{k_1}\varepsilon_2^{k_2}\ldots\varepsilon_\nu^{k_\nu},$$

on peut toujours déterminer des nombres entiers au nombre de $\nu+1$, $\lambda, \mu_1, \ldots, \mu_\nu$, de manière à satisfaire aux ν relations homogènes :

$$\begin{aligned}
\lambda k_1 &= \mu_1 m_{11} + \mu_2 m_{21} + \ldots + \mu_\nu m_{\nu 1},\\
\lambda k_2 &= \mu_1 m_{12} + \mu_2 m_{22} + \ldots + \mu_\nu m_{\nu 2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\lambda k_\nu &= \mu_1 m_{1\nu} + \mu_2 m_{2\nu} + \ldots + \mu_\nu m_{\nu\nu},
\end{aligned}$$

On aura alors

$$\mathrm{E}^\lambda = \varepsilon_1'^{\mu_1}\varepsilon_2'^{\mu_2}\ldots\varepsilon_\nu'^{\mu_\nu}.$$

Donc à E^λ correspond une transformation semblable de F de la première catégorie.

La discussion du cas où le corps K présente des unités dont le module analytique est *un* est un peu plus compliquée, sans offrir de difficultés particulières. Nous nous permettrons de l'omettre. Dans tous les cas, on arrive à la conclusion suivante :

Il existe toujours une puissance d'une transformation semblable quelconque de Φ *de la première catégorie dont la transformée par la substitution* (3o) *est une transformation semblable de* F.

On sait, d'après M. Hermite, que tout entier complexe dont le module analytique est *un,* est une racine aliquote de l'unité.

Par suite, les transformations semblables de F qui correspondent à de pareils multiplicateurs sont toutes périodiques et sont en nombre limité.

Reste à examiner les transformations semblables de la deuxième catégorie. Un facteur de F ne peut être transformé en un autre, à un multiplicateur constant près, qu'autant que les racines de Γ qui correspondent à ces deux facteurs s'expriment rationnellement l'une par l'autre. Si cette circonstance se présente, d'abord il est certain que la forme Φ se transformera en elle-même par des substitutions périodiques échangeant entre elles les facteurs de Φ.

En effet, les corps conjugués qui correspondent aux diverses racines de Γ ne sont pas tous distincts, et le nombre des corps conjugués distincts est un diviseur de n. Supposons que

$$\omega_1,\ \omega_2,\ \ldots,\ \omega_n;\ \omega_1',\ \omega_2',\ \ldots,\ \omega_n';\ \ldots;\ \omega_1^{(q-1)},\ \omega_2^{(q-1)},\ \ldots,\ \omega_n^{(q-1)}$$

appartiennent au même corps algébrique; comme $\omega_1, \omega_2, \ldots, \omega_n$ forment un système de modules minimum et que $\omega_1', \omega_2', \ldots, \omega_n'$ sont des entiers complexes,

on aura

$$\omega'_j = \sum_{h=1}^{h=n} \alpha_{jh}\omega_h \qquad (j = 1, 2, \ldots, n), \tag{31}$$

les quantités α_{jh} étant des coefficients entiers.

En remplaçant les quantités ω_h dans les seconds membres de (31) par un système quelconque de modules conjugués, on obtiendra encore un système de modules conjugués. Dès lors, si l'on opère sur les quantités ω'_j comme on a opéré sur les quantités ω_h et ainsi de suite, on devra finalement retomber sur le système de modules primitif. Il en résulte que les quantités α_{jh} sont les coefficients d'une substitution périodique.

Considérons maintenant la substitution

$$x_h = \sum_{j=1}^{j=n} \alpha_{jh} x'_j,$$

cette substitution ne fait que permuter les facteurs de Φ; c'est donc une transformation en elle-même de Φ appartenant à la seconde catégorie. Chacun des $q - 1$ systèmes appartenant au même groupe que $\omega_1, \ldots, \omega_n$ donnera de même lieu à une substitution transformant Φ en elle-même.

Réciproquement, on voit sans difficulté que toute transformation de Φ en elle-même résulte d'une transformation de la première catégorie suivie d'une transformation de la seconde catégorie permutant simplement entre eux les facteurs de Φ.

Quant aux transformations semblables de seconde catégorie des formes F, il existe une puissance de l'une quelconque d'entre elles qui appartient à la première catégorie; il existe aussi un nombre limité de transformations semblables de la seconde catégorie qui ramènent une transformation de la seconde catégorie à la première catégorie.