JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

CAMILLE JORDAN

Mémoire sur les formes quadratiques, suivant un module premier p, invariantes par une substitution linéaire donnée

Journal de mathématiques pures et appliquées 6e série, tome 1 (1905), p. 217-284.

<http://www.numdam.org/item?id=JMPA_1905_6_1__217_0>

Mémoire sur les formes quadratiques, suivant un module premier p, invariantes par une substitution linéaire donnée;

PAR M. CAMILLE JORDAN.

Introduction.

1. Dans un précédent Mémoire (*Journal de Liouville*, 1888) nous avons indiqué les conditions nécessaires et suffisantes pour qu'une substitution linéaire S étant donnée, il existe des formes quadratiques (de discriminant non nul) que S n'altère pas.

Nous avons en outre montré que ces formes invariantes Φ appartiennent à un type unique, car on peut les transformer les unes dans les autres par des substitutions linéaires qui n'altèrent pas l'expression de S.

Si les coefficients de la substitution et de la forme, au lieu d'être des quantités quelconques, sont des entiers réduits à leur reste suivant un module premier p, on pourra se poser un problème analogue au précédent, mais de nature arithmétique. Il se résout à l'aide des mêmes principes; il est toutefois plus compliqué et les résultats sont sensiblement différents.

Avant de l'aborder, il conviendra de rappeler brièvement quelques résultats connus dont nous aurons à faire usage. Nous les empruntons en partie à notre *Traité des Substitutions*, en partie au bel Ouvrage dans lequel M. Dickson a récemment élargi et complété, sur plusieurs points essentiels, l'étude des groupes linéaires ([1]).

2. Deux entiers congrus suivant le module p seront considérés comme égaux pour abréger le langage. Deux substitutions linéaires (ou deux formes) seront regardées comme identiques si tous leurs coefficients sont égaux.

Elles seront dites *équivalentes* (ou du même type), si l'on peut passer de l'une à l'autre par une transformation linéaire opérée sur les variables. Si la substitution transformante appartient à un sous-groupe Γ du groupe linéaire, elles seront dites *équivalentes dans ce sous-groupe*.

3. Les substitutions linéaires de déterminant $\gtrless 0 \bmod p$ entre n variables $x_1, \ldots, x_n$ dérivent toutes de la combinaison des substitutions fondamentales suivantes, qui n'altèrent chacune qu'une variable

$$|x_i \quad \lambda x_i|,$$

$$|x_i \quad x_i + x_k|.$$

Leur nombre $\mathcal{A}_n^p$ est donné par la formule

$$\mathcal{A}_n^p = p^{\frac{n(n-1)}{2}} \prod_1^n (p^k - 1).$$

Si les coefficients, au lieu d'être réels, sont des entiers complexes formés avec une racine d'une congruence irréductible de degré ν, on devra, dans la formule précédente, changer p en p^ν; on aura ainsi

$$\mathcal{A}_{n,\nu}^p = p^{\nu\frac{n(n-1)}{2}} \prod_1^n (p^{\nu k} - 1).$$

([1]) Dickson, *Linear Groups*. Teubner, Leipzig, 1901.

4. Une substitution linéaire

$$S = |x_i \quad \Sigma a_{ik} x_k| \qquad \begin{pmatrix} i = 1, \ldots, n \\ k = 1, \ldots, n \end{pmatrix}$$

peut être ramenée par un changement de variables à une expression canonique que nous allons indiquer.

Formons la congruence caractéristique

$$\Delta = \begin{vmatrix} a_{11} - \rho & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - \rho & \ldots & a_{2n} \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - \rho \end{vmatrix} \equiv 0 \qquad (\bmod p),$$

et décomposons Δ en facteurs irréductibles suivant le module p. Soient P l'un de ces facteurs, ν son degré, μ son ordre de multiplicité. La congruence $P \equiv 0 \bmod p$ admettra ν racines conjuguées,

$$\rho, \quad \rho^p, \quad \ldots, \quad \rho^{p^{\nu-1}}.$$

Parmi les nouvelles variables qui donnent à S sa forme canonique, il y en aura précisément $\mu\nu$ correspondant au facteur P.

Ce système de $\mu\nu$ variables se partage en ν classes correspondant aux diverses racines conjuguées. Les μ variables x', x'', ... de la première classe C_0 (correspondant à la racine ρ) seront de la forme

$$x^i = X_0^i + \rho X_1^i + \ldots + \rho^{\nu-1} X_{\nu-1}^i \qquad (i = 1, \ldots, \mu),$$

les X étant des fonctions linéaires réelles des variables primitives. Elles forment une ou plusieurs séries s_1, s_2, ... La substitution S remplace les variables x_0, x_1, ..., x_m de l'une de ces séries respectivement par

$$\rho x_0, \quad \rho(x_1 + x_0), \quad \ldots, \quad \rho(x_m + x_{m-1}).$$

Les μ variables de la classe C_0 peuvent donc être représentées par le symbole x_i^α, l'indice supérieur α variant d'une série à l'autre, et l'indice i représentant le *rang* qu'occupe la variable considérée dans la série s_α.

Les variables de la classe C_k qui correspond à la racine ρ^{p^k} ont des expressions qui se déduisent des précédentes en y remplaçant ρ par sa conjuguée ρ^{p^k}. Les altérations que S leur fait subir sont de même conjuguées des altérations qu'elle fait éprouver aux variables correspondantes de la classe C_0. Elles se partagent donc en séries, s_1^k, s_2^k, ... respectivement conjuguées des séries s_1, s_2, ...

5. Si l'on exécute sur les variables de la classe C_0 une substitution linéaire quelconque T_0 dont les coefficients soient des entiers complexes formés avec ρ et si l'on effectue en même temps sur chacune des séries conjuguées la substitution conjuguée T_k, l'opération résultante

$$T = T_0 \ldots T_k \ldots$$

sera une substitution réelle.

Celles de ces substitutions qui transforment S en elle-même forment un groupe Γ qui peut être construit comme il suit :

1° Groupons les séries s_1, s_2, ... de la classe C_0 en sous-classes, en réunissant celles qui contiennent le même nombre $m+1$ de variables; soit

$$(x'_0, \ldots, x'_m), \quad (x''_0, \ldots, x'_m), \quad \ldots, \quad (x^l_0, \ldots, x^l_m)$$

une de ces sous-classes contenant l séries.

Opérons simultanément sur les $m+1$ systèmes de variables cogrédientes

$$(x'_0, x''_0, \ldots, x^l_0), \quad \ldots, \quad (x^l_m, \ldots, x^l_m),$$

une même substitution linéaire quelconque

$$|x', x'', \ldots, x^l \quad a_1 x' + b_1 x'' + \ldots + a_2 x' + b_2 x'' + \ldots + a_l x' + b_l x'' + \ldots|$$

En prenant pour T_0 cette opération, T sera l'une des substitutions du groupe Γ.

2° On en obtiendra une autre en prenant pour T_0 la substitution

$$|x^\alpha_m, x^\alpha_{m-1}, \ldots, x^\alpha_{m-r}, \ldots, x^\alpha_0 \quad x^\alpha_m + \lambda x^\beta_r, x^\alpha_{m-1} + \lambda x^\beta_{r-1}, \ldots, x^\alpha_{m-r} + \lambda x^\beta_0, \ldots, x^\alpha_0|,$$

où λ est une indéterminée et x_r^β l'une quelconque des variables de C_0 dont le rang r est $< m$.

Réciproquement toutes les substitutions de Γ résulteront de la combinaison des deux sortes de substitutions ci-dessus.

6. Les formes quadratiques Φ à n variables dont le discriminant D n'est pas congru à o mod p appartiennent, si p est impair, à deux types différents, correspondant aux deux valeurs ± 1 du caractère quadratique $\left(\frac{D}{p}\right)$.

La forme Φ peut en effet se réduire à la suivante :

$$x_1^2 + x_2^2 + \ldots + x_{n-1}^2 + a x_n^2,$$

où le nombre a est arbitrairement choisi parmi ceux qui satisfont à la relation

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^n \left(\frac{D}{p}\right).$$

Il est d'ailleurs évident que le caractère $\left(\frac{D}{p}\right)$ est un invariant, qu'aucun changement de variables ne peut altérer.

Le nombre $\Omega_n^p(D, c)$ des solutions de la congruence

$$\Phi \equiv c \pmod p$$

est égal, si $n = 2m+1$, à

$$p^m\left[p^m + \left(\frac{-1}{p}\right)^m \left(\frac{2c}{p}\right)\left(\frac{D}{p}\right)\right],$$

et si $n = 2m$, à

$$p^{m-1}\left[p^m - \left(\frac{-1}{p}\right)^m \left(\frac{D}{p}\right)\right] \quad \text{si} \quad c \gtrless 0,$$

$$p^{m-1}\left[p^m + (p-1)\left(\frac{-1}{p}\right)^m \left(\frac{D}{p}\right)\right] \quad \text{si} \quad c \equiv 0.$$

Ces formules nous serviront à déterminer le signe du caractère $\left(\frac{D}{p}\right)$

lorsque Φ est exprimée de telle sorte que le calcul de son discriminant offre quelque difficulté.

Si $p = 2$, il n'existera de forme quadratique de discriminant impair que si n est un nombre pair $2m$. On aura dans ce dernier cas deux types de formes, correspondant aux deux valeurs du caractère invariant $\left(\frac{2}{D}\right)$.

Si $\left(\frac{2}{D}\right) = +1$, Φ sera réductible à une somme de rectangles

$$\sum_1^m x_k y_k.$$

Si $\left(\frac{2}{D}\right) = -1$, elle sera réductible à la forme

$$x_1^2 + y_1^2 + \sum_1^m x_k y_k.$$

Le nombre $\Omega_{2m}^2(D, c)$ des solutions de la congruence $\Phi \equiv c$ sera donné par les formules

$$\begin{aligned}
\Omega_{2m}^2(D, c) &= 2^{2m-1} + 2^{m-1}(-1)^m\left(\frac{2}{D}\right) \qquad \text{si} \qquad c = 0, \\
&= 2^{2m-1} - 2^{m-1}(-1)^m\left(\frac{2}{D}\right) \qquad \text{si} \qquad c = 1.
\end{aligned}$$

7. Les substitutions linéaires qui laissent invariable une forme quadratique donnée Φ (de discriminant $\gtrless 0 \bmod p$) forment un groupe G, dit *groupe de la forme* Φ.

A deux formes équivalentes Φ, Φ' correspondent deux groupes G, G′ transformables l'un dans l'autre par une substitution linéaire et appartenant par suite au même type.

Si le nombre n des variables est pair, on aura ainsi deux types de groupes répondant aux deux types de formes Φ.

Si n est impair (d'où p impair), ces deux types se confondent en un seul, car toute substitution qui laisse invariante une forme Φ de discriminant D laissera aussi invariante la forme $a\Phi$ de discriminant a^nD, laquelle est d'un autre type que Φ, si a est un non résidu de p.

L'ordre $O_n^p(D)$ du groupe G qui laisse invariante une forme Φ de discriminant D s'obtient aisément, si p est impair, par la formule récurrente

$$O_n^p(D) = \Omega_n^p(D, c)\, O_{n-1}^p(2cD),$$

où c est un entier quelconque $\gtrless 0 \bmod p$.

On trouve ainsi, si n est impair $= 2m+1$,

$$O_{2m+1}^p(D) = 2p^{m^2}\prod_1^m (p^{2k}-1)$$

et, si $n = 2m$,

$$O_{2m}^p(D) = 2p^{m(m-1)}\left[p^m - \left(\frac{-1}{p}\right)^m\left(\frac{D}{p}\right)\right]\prod_1^{m-1}(p^{2k}-1).$$

Si $p = 2$, auquel cas n est toujours pair $= 2m$, on aura

$$O_{2m}^2(D) = 2^{m(m-1)+1}\left[2^m - (-1)^m\left(\frac{2}{D}\right)\right]\prod_1^{m-1}(2^{2k}-1).$$

Le nombre $\mathcal{N}_n^p(D)$ des formes distinctes équivalentes à Φ s'obtient évidemment en divisant le nombre total $\mathcal{A}_n^p$ des substitutions linéaires par le nombre $O_n^p(D)$ de celles qui laissent Φ invariante. On aura par suite, si p est impair,

$$\mathcal{N}_{2m+1}^p(D) = \frac{1}{2}p^{m(m+1)}\prod_1^m(p^{2k-1}-1)$$

$$\mathcal{N}_{2m}^p\;(D) = \frac{1}{2}p^{m^2}\left[p^m + \left(\frac{-1}{p}\right)^m\left(\frac{D}{p}\right)\right]\prod_1^m(p^{2k-1}-1)$$

et, si $p = 2$,

$$\mathcal{N}_{2m}^2(D) = 2^{m^2-1}\left[2^m + (-1)^m\left(\frac{2}{D}\right)\right]\prod_1^m(2^{2k-1}-1).$$

8. Les formes bilinéaires gauches

$$\sum c_{ik} x_i X_k \qquad (c_{ik} = -c_{ki})$$

à deux séries de variables cogrédientes

$$x_1, \quad \dots, \quad x_n; \qquad X_1, \quad \dots, \quad X_n$$

n'ont leur déterminant différent de zéro que si n est un nombre pair $2m$. Elles sont toutes équivalentes à une même forme type

$$\sum_1^m (x_{2k-1} X_{2k} - x_{2k} X_{2k-1}).$$

L'ordre ω_{2m}^p du groupe formé par les substitutions qui laissent invariante l'une d'elles est donné par la formule

$$\omega_{2m}^p = p^{m^2} \prod_1^m (p^{2k} - 1)$$

et le nombre ϖ_{2m}^p des formes distinctes du système sera

$$\varpi_{2m}^p = \frac{\mathfrak{A}_{2m}^p}{\omega_{2m}^p} = p^{m(m-1)} \prod_1^m (p^{2k-1} - 1).$$

9. Ces préliminaires posés, nous donnerons, dans les trois premières Sections de ce Mémoire, la solution des questions suivantes :

1° Une substitution $S \pmod p$ étant donnée, quelles sont les conditions nécessaires et suffisantes pour qu'il existe des formes quadratiques $\Phi \pmod p$, de discriminant $\gtrless 0 \pmod p$, que S laisse invariantes ?

2° Quelle est l'expression générale de ces formes invariantes ?

3° A quels types simples peut-on les réduire par les changements de variables qui n'altèrent pas l'expression de S ?

4° Quel est le nombre de ces types ?

5° Quel est le nombre des formes invariantes distinctes réductibles à chacun d'eux ?

6° Quel est pour chacun d'eux le signe du caractère quadratique $\left(\frac{D}{p}\right)$ ou $\left(\frac{2}{D}\right)$?

Nous établissons en particulier les théorèmes suivants :

Théorème I. — *Les conditions nécessaires et suffisantes pour l'existence de formes invariantes* Φ *sont les suivantes* :

1° *A chaque racine* ρ *de la congruence caractéristique de* S, *autre que* $\pm 1 \bmod p$, *est associée une racine* ρ^{-1} *de la même congruence, réciproque de* ρ;

2° *Les deux classes* C, C′ *correspondant à ces deux racines contiennent le même nombre de variables, dont la répartition en séries est identique dans les deux classes;*

3° *Si la congruence caractéristique admet une racine égale à* $\pm 1 \bmod p$, *la classe correspondante* C *sera dite* singulière. *Groupons ses séries en sous-classes, en réunissant ensemble celles où le nombre des variables est le même.*

Si p est impair, chaque sous-classe dont les séries contiennent un nombre pair de variables sera formée d'un nombre pair de séries.

Si $p = 2$, *chaque sous-classe dont les séries contiennent un nombre impair de variables sera formée d'un nombre pair de séries.*

Théorème II. — *Les formes invariantes* Φ *appartiennent toutes au même type, si la congruence caractéristique de* S *n'a pas de racine égale à* $\pm 1 \bmod p$.

Si elle admet de semblables racines, p étant impair, le nombre des types distincts sera 2^k, *k désignant le nombre des sous-classes contenues dans les classes singulières et dont les séries sont formées d'un nombre impair de variables.*

Si, p étant égal à 2, *la congruence caractéristique admet la racine* 1, *soient, dans la classe singulière, k le nombre total des sous-classes, k′ celui des sous-classes formées d'un nombre pair de séries, contenant chacune un nombre pair de variables : le nombre des types distincts sera* $2^{k-k'}3^{k'}$.

Pour la solution des autres questions posées ci-dessus, qu'il serait plus difficile de résumer, nous renverrons à la suite du Mémoire.

10. La quatrième Section a pour objet la question suivante :

Le groupe G des substitutions linéaires qui laissent invariante une forme quadratique à $2n$ variables réductible à une somme de rectangles

$$\Phi = \sum_1^n x_k y_k,$$

est dérivé, comme on sait, des substitutions fondamentales suivantes

$$\begin{aligned} L_i &= | x_i, y_i \quad y_i, x_i |, \\ M_{ik} &= | x_i, y_k \quad x_i + x_k, y_k + y_i |. \end{aligned}$$

Si la forme Φ est du second type

$$\Phi = x_1^2 + y_1^2 + \sum_1^n x_k y_k,$$

les substitutions fondamentales seront les suivantes

$$\begin{aligned} &L_i, \\ &M_{ik} \qquad (i > 1, k > 1), \\ N &= | x_1, y_1 \quad y_1, x_1 + y_1 |, \\ P &= | x_1, y_1, y_2 \quad x_1 + y_1 + x_2, x_1, x_1 + x_2 + y_2 |. \end{aligned}$$

Une substitution de G sera dite *paire* ou *impaire* suivant que, dans son expression en produit de substitutions fondamentales, le nombre des facteurs de l'espèce L est pair ou impair.

Nous avons établi autrefois par des considérations indirectes que les substitutions paires de G forment un sous-groupe invariant Γ d'ordre moitié moindre. Mais nous avions inutilement cherché à établir un caractère, plus simple que la définition précédente, et qui permette de discerner les substitutions paires. M. Dickson a réussi à combler cette lacune dans le bel Ouvrage auquel nous avons déjà renvoyé. Il y donne, au n° 205, l'expression d'un invariant dont la parité ou l'imparité sert à fixer le genre d'une substitution quelconque de G.

Ce critérium suppose, pour être appliqué, que la forme Φ a été réduite préalablement à l'un des deux types normaux

$$\sum x_k y_k, \quad x_1^2 + y_1^2 + \sum x_k y_k.$$

Nous montrerons que l'on peut se dispenser de cette opération, en assignant un nouveau critérium très simple et complètement indépendant de la forme Φ que l'on considère. Il peut s'énoncer ainsi :

THÉORÈME. — *Soit* S *une substitution linéaire qui laisse invariante une forme quadratique* Φ mod 2. *Elle sera paire ou impaire, suivant que dans sa forme canonique le nombre des séries formées par les variables est pair ou impair.*

Analyse.

11. Supposons la substitution S ramenée à sa forme canonique

$$S = \left| \begin{array}{ll} x_0, \ \ldots, \ x_i, \ \ldots & \rho\, x_0, \ \ldots, \ \rho\,(x_i + x_{i-1}), \ \ldots \\ y_0, \ \ldots, \ y_k, \ \ldots & \rho_1 y_0, \ \ldots, \ \rho_1 (y_k + y_{k-1}), \ \ldots \\ \ldots \ \ldots \ \ldots \ \ldots & \ldots \ \ldots \ \ldots \ \ldots \end{array} \right|.$$

Soient

$$s_0 = (x_0, x_1, \ldots, x_m), \qquad s_1 = (y_0, y_1, \ldots, y_m), \quad \ldots$$

les diverses séries entre lesquelles se répartissent les variables; $\rho, \rho_1, \ldots$ les multiplicateurs correspondants.

Soit Φ une forme invariante : elle sera une somme de formes partielles, les unes $B_{\alpha\beta}$ bilinéaires par rapport à deux séries différentes s_α, s_β; les autres Q_α quadratiques par rapport aux variables d'une seule série s_α. Chacune de ces formes partielles devra être invariante séparément.

Soit d'ailleurs $a x_i y_k$ un terme quelconque de l'une de ces formes partielles, telle que B_{01}. Nous dirons que x_i, y_k sont des variables de rang i et k respectivement et que le terme $a x_i y_k$ est de rang $i + k$.

La substitution S le transforme en

$$\rho\rho_1 a(x_i + x_{i-1})(y_k + y_{k-1}),$$

somme de quatre termes dont le premier est $\rho\rho_1 a x_i y_k$; les deux suivants $\rho\rho_1 a x_{i-1} y_k$, $\rho\rho_1 a x_i y_{k-1}$ sont de rang $i+k-1$ et le dernier $\rho\rho_1 a x_{i-1} y_{k-1}$ de rang $i+k-2$. (Si i ou k était égal à zéro, ceux de ces termes où figureraient des variables à indice négatif sont à supprimer.)

Il résulte évidemment de là que, dans la transformée $B_{01} + \Delta B_{01}$ de B_{01} par S, l'ensemble des termes de rang maximum s'obtiendra en multipliant par $\rho\rho_1$ l'ensemble des termes de rang maximum dans B_{01}.

Pour que ces deux formes soient égales il est donc nécessaire, ou que B_{01} soit identiquement nul, ou qu'on ait $\rho\rho_1 \equiv 1$.

Mais le discriminant de Φ serait nul si les variables d'une série, telle que s_0, disparaissaient de son expression. Il faut donc qu'il y ait au moins une série (différente ou non de s_0) dont le multiplicateur soit égal à ρ^{-1}.

Il peut y avoir plusieurs séries s_0, s_1, ... correspondant au même multiplicateur ρ; elles formeront une classe C; les séries au multiplicateur ρ^{-1} formeront une classe C′ *associée* à la précédente; et Φ sera de la forme

$$\Phi = [CC'] + \Psi,$$

$[CC']$ désignant une forme bilinéaire par rapport aux variables de C et de C′ et Ψ ne les contenant plus.

1° Si $\rho \equiv \rho^{-1}$, d'où $\rho \equiv \pm 1 \pmod p$ (ces deux hypothèses se confondent si $p=2$), la classe C′ se confond avec la classe C, et l'on aura

$$\Phi = [C] + \Psi,$$

$[C]$ étant quadratique par rapport aux variables de C, et Ψ ne les contenant plus;

2° Si ρ n'est pas égal à ρ^{-1}, les classes C et C′ sont différentes et l'on aura

$$\Phi = [CC'] + \Phi',$$

$[CC']$ étant bilinéaire par rapport aux variables de C et de C′ et Φ' ne les contenant plus.

Dans ce cas ρ pourra ne pas être réel, mais racine d'une congruence irréductible de degré >1; C fera alors partie d'un système s de classes conjuguées

$$C, \quad C_1, \quad \ldots, \quad C_k, \quad \ldots$$

ayant pour multiplicateurs respectifs

$$\rho, \quad \rho^p, \quad \ldots, \quad \rho^{p^k}, \quad \ldots.$$

Si ρ^{-1} fait partie de cette suite, soit pour fixer les idées

$$\rho^{p^\nu} \equiv \rho^{-1}, \qquad \text{d'où} \qquad \rho^{p^\nu+1} \equiv 1.$$

Les classes

$$C, \quad C_1, \quad \ldots, \quad C_k$$

auront respectivement pour associées les classes

$$C_\nu, \quad C_{\nu+1}, \quad \ldots, \quad C_{\nu+k}$$

et C_ν aura pour associée $C_{2\nu}$. Mais cette associée est C. Donc s contient 2ν classes distinctes, et l'on aura

$$\Phi = [CC_\nu] + [C_1 C_{\nu+1}] + \ldots + [C_{\nu-1} C_{2\nu-1}] + \Psi = [s] + \Psi,$$

$[s]$ ne contenant que les variables du système s et Ψ les autres variables.

D'ailleurs la forme Φ étant réelle ne doit pas changer si l'on y remplace ρ par ρ^p. Donc Ψ a ses coefficients réels; d'autre part, par ce changement, les formes partielles $[CC_\nu]$, $[C_1 C_{\nu+1}]$, ... devront se transformer chacune dans la suivante; elles sont donc conjuguées; enfin la dernière $[C_{\nu-1} C_{2\nu-1}]$ devra se changer dans la première; ce qui revient à dire que $[CC_\nu]$ ne doit pas être altérée par le changement de ρ en ρ^{p^ν}. Cette condition implique une certaine restriction pour les coefficients de cette forme bilinéaire. En outre leur déterminant ne doit pas être nul.

3° Supposons enfin que C′ ne fasse pas partie de la suite des conjuguées de C. Soit ν le nombre de celles-ci. Elles auront respectivement pour associées les conjuguées de C',

$$C', \quad C'_1, \quad \ldots, \quad C'_{\nu-1},$$

lesquelles formeront un système s' associé à s et Φ sera de la forme

$$\Phi = [CC'] + [C_1 C'_1] + \ldots + [C_\nu C'_\nu] + \Psi,$$

$[CC']$, $[C_1 C'_1]$, ... étant des fonctions bilinéaires conjuguées et Ψ ne contenant plus les variables de s ni de s'.

Les formes partielles $[CC'] + [C_1 C'_1] + \ldots + [C_\nu C'_\nu]$ constituent par leur réunion une forme réelle $[ss']$ bilinéaire par rapport aux variables des deux systèmes associés s et s'. Dans chacun de ces systèmes les variables complexes peuvent être remplacées par les variables réelles dont elles dépendent.

On remarquera que le déterminant de la forme bilinéaire $[CC']$, entrant en facteur dans le discriminant de Φ, ne doit pas être nul. Il faut pour cela que les classes associées C, C' contiennent le même nombre μ de variables. Il en était évidemment de même dans le cas précédent où l'on supposait ces deux classes conjuguées.

Nous pouvons donc énoncer une première condition nécessaire pour qu'il existe des formes Φ (de déterminant non nul) invariantes par la substitution S. C'est qu'à chaque racine ρ de sa congruence caractéristique, autre que ± 1, corresponde une racine associée ρ^{-1} du même ordre de multiplicité; autrement dit :

La congruence caractéristique de S *doit être réciproque.*

Il résulte d'ailleurs de l'analyse précédente que, si l'on joint à chaque classe ses conjuguées et leurs associées pour les réunir en une même famille, toute forme invariante Φ sera une somme de formes partielles Φ_1, Φ_2, ... contenant chacune les variables d'une seule famille. Chacune de ces formes partielles sera :

1° Ou une fonction bilinéaire

$$[ss'] = \sum_0^{\nu-1} [C_k C'_k]$$

par rapport aux variables de deux systèmes associés;

2° Ou une fonction

$$[s]=[\mathrm{C}\mathrm{C}_\nu]+[\mathrm{C}_1\mathrm{C}_{\nu+1}]+\ldots+[\mathrm{C}_{\nu-1}\mathrm{C}_{2\nu-1}]$$

des variables d'un seul système contenant un nombre pair 2ν de séries associées deux à deux;

3° Ou enfin une fonction $[\mathrm{C}]$ quadratique par rapport aux variables d'une série au multiplicateur ± 1, laquelle sera associée à elle-même.

La substitution S de son côté est le produit de substitutions partielles S_1, S_2, ... effectuées chacune sur les variables d'une seule famille. Il en est de même des substitutions qui la transforment en elle-même.

La détermination des formes Φ invariantes par la substitution S revient donc à celle des formes partielles Φ_1, Φ_2, ... respectivement invariantes par les substitutions partielles S_1, S_2, ...

Pour les réduire à des formes types, il faudra réduire séparément ces formes partielles.

Le nombre des formes distinctes réductibles à chaque type sera le produit des nombres de formes distinctes pour Φ_1, pour Φ_2, etc.

Enfin, le caractère quadratique du discriminant D de la forme Φ est le produit des caractères des discriminants des formes partielles Φ_1, Φ_2, ...

Les problèmes que nous nous sommes posés se trouvent ainsi réduits au cas où les variables ne forment qu'une seule famille.

Trois cas seront à considérer :

I.

12. Supposons d'abord qu'il existe deux systèmes associés mais différents s, s'.

La forme

$$\Phi_1=[ss']=\sum_0^{\nu-1}[\mathrm{C}_k\mathrm{C}'_k]$$

est une somme de ν formes bilinéaires complexes $[\mathrm{C}\mathrm{C}']$, $[\mathrm{C}_1\mathrm{C}'_1]$, ..., conjuguées les unes des autres, et invariantes séparément. Il suffira de déterminer l'expression de l'une d'elles $[CC']$. Celle de Φ_1 s'obtiendra en y ajoutant ses conjuguées.

Soient $s_1, s_2, \ldots$ les séries qui constituent la classe C; $s'_1, s'_2, \ldots$ celles qui constituent la classe C'; on aura évidemment

$$[CC'] = \sum_{\alpha,\beta} [\alpha\beta],$$

$[\alpha\beta]$ désignant l'ensemble des termes de $[CC']$ qui contiennent les produits des variables de s_α par celles de s_β. Chacune de ces formes partielles doit évidemment être invariante. Il suffira donc de construire l'une d'elles $[\alpha\beta]$.

Soient

$$x_0^\alpha, \quad x_1^\alpha, \quad \ldots, \quad x_{m_\alpha}^\alpha$$

les variables de la série s_α,

$$y_0^\beta, \quad y_1^\beta, \quad \ldots, \quad y_{m_\beta}^\beta$$

celles de la série s'_β.

Soit enfin

$$t = c_{ik} x_i^\alpha y_k^\beta$$

l'un quelconque des termes de la forme $[\alpha\beta]$; il aura pour rang $i+k$.

En lui appliquant la substitution S il sera changé en

$$c_{ik}(x_i^\alpha + x_{i-1}^\alpha)(y_k^\beta + y_{k-1}^\beta).$$

Son accroissement Δt se composera de trois termes, dont deux, $c_{ik} x_{i-1}^\alpha y_k^\beta$, $c_{ik} x_i^\alpha y_{k-1}^\beta$, sont de rang $i+k-1$ et le dernier, $c_{ik} x_{i-1}^\alpha y_{k-1}^\beta$, de rang $i+k-2$.

La forme $[\alpha\beta]$ étant invariante, son accroissement total $\Delta[\alpha\beta] = \Sigma \Delta t$ devra être identiquement nul.

Cela posé, considérons ceux des termes de $[\alpha\beta]$ dont le rang est le plus élevé; soit r ce maximum. L'ensemble de ces termes sera

$$c_{0r} x_0^\alpha y_r^\beta + c_{1,r-1} x_1^\alpha y_{r-1}^\beta + \ldots + c_{r0} x_r^\alpha y_0^\beta.$$

(On devra toutefois considérer *a priori* comme nuls tous ceux des coefficients c qui multiplieraient soit des variables x d'indice $> m_\alpha$, soit des variables y d'indice $> m_\beta$, puisqu'il n'existe pas de semblables variables.)

Les termes de rang le plus élevé dans $\Delta[\alpha\beta]$ seront de rang $r-1$ et exclusivement fournis par les termes de rang r écrits ci-dessus. Leur ensemble est le suivant :

$$(c_{0r}+c_{1,r-1})x_0^\alpha y_{r-1}^\beta+(c_{1,r-1}+c_{2,r-2})x_1^\alpha y_{r-2}^\beta+\ldots+(c_{r-1,1}+c_{r0})x_{r-1}^\alpha y_0^\beta.$$

Il doit être identiquement nul; les coefficients c sont donc égaux et de signes alternatifs. Mais ils ne peuvent être tous nuls, puisqu'on admet l'existence dans $[\alpha\beta]$ de termes de rang r. Donc aucun d'eux ne le sera.

On en conclut que r ne peut surpasser le plus petit des deux nombres m_α, m_β; car s'il était $> m_\alpha$, par exemple, la variable x_r étant inexistante, c_{r0} serait nul.

L'ensemble des termes de rang maximum sera donc

$$a_r^{\alpha\beta}[x_0^\alpha y_r^\beta - x_1^\alpha y_{r-1}^\beta+\ldots+(-1)^r x_r^\alpha y_0^\beta],$$

$a_r^{\alpha\beta}$ étant un entier complexe constant.

On voit par là que la forme $[\alpha\beta]$, si elle n'est pas identiquement nulle, contient nécessairement les variables x_0^α, y_0^β au moins dans ses termes de rang maximum. Elle sera donc complètement déterminée par la connaissance de ceux de ses termes qui contiennent x_0^α en facteur. L'ensemble de ces termes sera de la forme

$$x_0^\alpha \sum_r a_r^{\alpha\beta} y_r^\beta,$$

r variant depuis o jusqu'au plus petit des deux nombres m_α, m_β.

Or on vérifie aisément que la forme

$$\begin{aligned} f_{\alpha\beta r} = {} & x_0^\alpha y_r^\beta - x_1^\alpha y_{r-1}^\beta + (x_2^\alpha + x_1^\alpha) y_{r-2}^\beta + \ldots \\ & + (-1)^k [x_k^\alpha + C_{k-1}^1 x_{k-1}^\alpha + C_{k-1}^2 x_{k-2}^\alpha + \ldots + x_1^\alpha] y_{r-k}^\beta + \ldots \\ & + (-1)^r (x_r^\alpha + C_{r-1}^1 x_{r-1}^\alpha + \ldots + x_1^\alpha) y_0^\beta, \end{aligned}$$

où le multiplicateur de x_0^α se réduit à y_r^β, est invariante. En effet, par la substitution S, le coefficient du terme en y^β_{r-k} se trouve accru de

$$\begin{aligned}
&(-1)^k \quad [x^\alpha_{k-1} + C^1_{k-1} x^\alpha_{k-2} + \ldots + x^\alpha_0] \\
&+ (-1)^{k-1} [x^\alpha_{k-1} + C^1_{k-2} x^\alpha_{k-2} + \ldots + x^\alpha_1] \\
&+ (-1)^{k-1} [x_{k-2} + C^1_{k-2} x_{k-3} + \ldots + x^\alpha_0],
\end{aligned}$$

quantité identiquement nulle, car, en remplaçant les indices des x^α par des exposants, elle prend la forme symbolique

$$(-1)^k (1 + x^\alpha)^{k-1} + (-1)^{k-1} x^\alpha (1 + x^\alpha)^{k-2} + (-1)^{k-1} (1 + x^\alpha)^{k-2} = 0.$$

La forme la plus générale des fonctions $[\alpha\beta]$ invariantes sera donc

$$[\alpha\beta] = \sum_r a^{\alpha\beta}_r f_{\alpha\beta r}$$

et celle des fonctions $[CC']$ invariantes sera

$$\sum_{\alpha,\beta} \sum_r a^{\alpha\beta}_r f_{\alpha\beta r},$$

les a étant des entiers complexes arbitraires assujettis à la seule restriction que le déterminant de la forme bilinéaire $[CC']$ ne soit pas nul.

13. Nous allons montrer que toutes les formes invariantes ainsi obtenues peuvent être ramenées à un type unique par les substitutions du groupe Γ (formé des substitutions échangeables à S), et du même coup nous déterminerons leur nombre.

Continuons à désigner par $s_1, s_2, \ldots, s_\alpha, \ldots$ les séries qui constituent la classe C; et soient

$$x^\alpha_0, \quad \ldots, \quad x^\alpha_{m_\alpha}$$

les variables en nombre $m_\alpha + 1$ de la série s_α.

Soient de même $s'_1, \ldots, s'_\beta, \ldots$ les séries de la classe C′ et

$$y^\beta_0, \quad \ldots, \quad y^\beta_{m'_\beta}$$

les variables de la série s'_β.

On peut admettre que les séries aient été ordonnées de telle sorte qu'on ait

$$m_1 \overline{\overline{>}} m_2 \overline{\overline{>}} m_3 \ldots$$

et

$$m'_1 \overline{\overline{>}} m'_2 \overline{\overline{>}} m'_3 \ldots.$$

Admettons, pour fixer les idées, que l'on ait

$$m_1 = m_2 = \ldots = m_l = m, \qquad \text{mais} \qquad m_\alpha < m \quad \text{si} \quad \alpha > l,$$
$$m'_1 = m'_2 = \ldots = m'_{l'} = m', \qquad \text{mais} \qquad m'_\beta < m' \quad \text{si} \quad \beta > l'.$$

On aura nécessairement

$$m = m', \qquad l = l'.$$

Supposons en effet $m > m'$; $[CC']$ ne contenant aucun terme de rang $> m'$ ne pourrait contenir aucune des variables $x'_m, \ldots, x^l_m$ et son déterminant serait nul.

Si m était $< m'$, on n'aurait qu'à permuter les x et les y dans ce raisonnement.

Soit donc $m = m'$; $[CC']$ pourra contenir des termes de rang m, mais seulement dans celles des formes partielles $[\alpha\beta]$, où $\alpha \overline{\overline{<}} l$, $\beta \overline{\overline{<}} l'$; et dans celles-ci $x'_m, \ldots, x^l_m$ ne figurent que multipliées par les variables $y'_0, \ldots, y^{l'}_0$. Si donc l était $> l'$, les dérivées de $[CC']$ par rapport aux l variables $x'_m, \ldots, x^l_m$, ne dépendant que de l' variables ne seraient pas linéairement distinctes, et le déterminant serait encore nul. (De même si l était $< l'$, les dérivées par rapport aux l' variables $y'_m, \ldots, y^{l'}_m$ ne seraient pas distinctes.)

14. Cela posé, les termes de $[CC']$ qui contiennent les l variables y^β_m $(\beta = 1, \ldots, l)$ seront ceux de la forme binaire

$$\varphi = \sum a^{\alpha\beta}_m x^\alpha_0 y^\beta_m \qquad \begin{pmatrix} \alpha = 1, \ldots, l \\ \beta = 1, \ldots, l \end{pmatrix}.$$

Il faudra, pour que les dérivées par rapport à ces variables soient linéairement distinctes, que le déterminant de cette forme ne soit pas nul.

Il existe (n° 3) $\mathcal{A}^p_{l,\nu}$ systèmes de valeurs des entiers complexes $a^{\alpha\beta}_m$ qui satisfont à cette condition.

Nous allons vérifier que tous ces systèmes de valeurs sont également admissibles.

Le groupe Γ contient une substitution T qui remplace les variables $y'_m, \ldots, y^l_m$ respectivement par

$$\sum_\beta a^{1\beta}_m y^\beta_m, \quad \sum_\beta a^{2\beta} y^\beta_m, \quad \ldots$$

sans altérer les variables x (n° 5).

En transformant $[CC']$ par T^{-1}, on réduira φ à la forme plus simple

$$\varphi = \sum_\alpha x^\alpha_0 y^\alpha_m \qquad (\alpha = 1, \ldots, l).$$

15. Après cette première opération, les termes en $x'_0, \ldots, x^l_0$ que contient $[CC']$ seront de la forme

$$x'_0[y'_m + \varphi_1] + \ldots + x^l_0[y^l_m + \varphi_l],$$

$\varphi_1, \ldots, \varphi_l$ étant des fonctions linéaires de celles des variables y dont le rang est $< m$, lesquelles sont en nombre $\mu - l$ si μ est le nombre des variables de la classe C'. Leurs coefficients, au nombre de $l(\mu - l)$, pourront prendre chacun p^ν valeurs, soit en tout $p^{\nu l(\mu - l)}$ systèmes de valeurs également admissibles.

On pourra en effet, quels que soient ces coefficients, les faire disparaître successivement en commençant par ceux dont le rang est le plus élevé, en opérant sur $[CC']$ les substitutions de Γ.

Soit en effet cy^β_r un des termes de φ_1 dont le rang r soit maximum; il sera $< m$. Donc Γ contient une substitution T qui remplace y'_m, $y'_{m-1}, \ldots, y'_{m-r}$ par $y'_m - cy^\beta_r$, $y'_{m-1} - cy^\beta_{r-1}, \ldots, y'_{m-r} - cy^\beta_0$ sans altérer ni les autres variables y ni les variables x. Par cette substitution on fera disparaître de φ_1 le terme cy^β_r. On pourra, à la vérité, en introduire d'autres, tant dans φ_1 que dans $\varphi_2, \ldots, \varphi_l$, mais tous seront de rang moins élevé que celui qu'on a détruit.

En répétant cette réduction, on fera disparaître totalement les fonctions φ, de manière à réduire ceux des termes de $[CC']$ qui contiennent $x'_0, \ldots, x^l_0$ en facteur à

$$x'_0 y'_m + \ldots + x^l_0 y^l_m.$$

On aura par suite, à ce moment de la réduction,

$$[CC'] = f_{11m} + f_{22m} + \ldots + f_{llm} + \Psi,$$

Ψ étant une forme invariante qui ne contient plus $x'_0, \ldots, x^l_0$, ni, par suite, aucune des variables des séries $s_1, \ldots, s_l$.

Les termes en $y'_0, \ldots, y^l_0$ dans

$$f_{11m} + \ldots + f_{llm}$$

sont

$$(-1)^m [x'_m y'_0 + x''_m y''_0 + \ldots + x^l_m y^l_0],$$

et dans Ψ ils seront de la forme

$$\varphi_1 y'_0 + \varphi_2 y''_0 + \ldots + \varphi_l y^l_0,$$

$\varphi_1, \ldots, \varphi_l$ étant des fonctions linéaires des $\mu' = \mu - l(m+1)$ variables x qui appartiennent aux séries $s_{l+1}, \ldots$.

Leurs coefficients seront susceptibles de $p^{\nu l[\mu - l(m+1)]}$ systèmes de valeurs également admissibles. On pourra, en effet, quels que soient ces coefficients, les faire disparaître progressivement par le même procédé que tout à l'heure, en altérant les x de la même manière que nous l'avions fait pour les y.

16. Reste à réduire la fonction Ψ qui, à l'heure actuelle, ne contient plus ni les variables des séries $s_1, \ldots, s_l$, ni celles des séries $s'_1, \ldots, s'_l$. C'est un problème tout semblable à celui de la réduction de $[CC']$, mais le nombre des variables est diminué. Soient $s_{l+1}, \ldots, s_{l+l'}$ les séries les plus longues parmi celles qui restent dans la classe C; $m'+1$ le nombre des variables de chacune d'elles : on verra que C′ doit contenir aussi l' séries $s'_{l+1}, \ldots, s'_{l+l'}$ de $m'+1$ variables, et que Ψ peut se réduire à la forme

$$\Psi = f_{l+1,l+1,m'} + \ldots + f_{l+l',l+l',m'} + \Psi',$$

Ψ' ne contenant plus les variables des séries

$$s_{l+1}, \quad \ldots, \quad s_{l+l'}; \qquad s'_{l+1}, \quad \ldots, \quad s'_{l+l}.$$

Poursuivant cette réduction on voit que $[CC']$ peut se réduire à la forme parfaitement définie

$$\sum_1^l f_{kkm} + \sum_l^{l+l'} f_{kkm'} + \ldots,$$

et nous trouvons cette nouvelle condition pour l'existence de formes invariantes par la substitution S.

Dans deux classes associées C, C' *les séries entre lesquelles se répartissent les variables doivent être en même nombre et de même longueur.*

Cette nouvelle condition, dont nous venons d'établir la nécessité en supposant que les deux classes associées C, C' appartiennent à des systèmes différents, est satisfaite d'elle-même dans les deux cas qui nous restent à examiner, à savoir ceux où les séries C, C' sont conjuguées ou coïncidentes.

17. Soient, d'ailleurs, $O(m, l; m', l'; \ldots)$ le nombre des formes invariantes $[CC']$; $O(m', l'; \ldots)$ celui des formes invariantes de l'espèce Ψ; il résulte évidemment de notre analyse qu'on aura la formule récurrente

$$\begin{aligned} O(m, l; m', l'; \ldots) &= \mathfrak{A}_{l,\nu}^{p}\, p^{\nu l(\mu-1)} p^{\nu l[\mu-l(m+1)]}\, O(m', l'; \ldots) \\ &= \mathfrak{A}_{l,\nu}^{p}\, p^{\nu l[2\mu-l(m+2)]}\, O(m', l'; \ldots). \end{aligned}$$

18. Il reste enfin à déterminer le caractère des formes $[SS']$ que nous venons de construire et de réduire. La chose ne présente aucune difficulté; car $[SS']$ est bilinéaire par rapport aux variables x et à leurs conjuguées en nombre $\mu\nu$ d'une part, aux variables y et à leurs conjuguées d'autre part. Elle restera bilinéaire si l'on remplace les deux systèmes de variables complexes par les variables réelles $X_1, \ldots, X_{\mu\nu}$; $Y_1, \ldots, Y_{\mu\nu}$ dont elles dépendent. Par un changement de variables qui n'altère pas son caractére on la ramènera à la forme

$$\sum_1^{\mu\nu} X_k Y_k,$$

dont le discriminant est $(-1)^{\mu\nu}$.

On aura donc, si p est impair,

$$\left(\frac{D}{p}\right) = \left(\frac{-1}{p}\right)^{\mu\nu},$$

et, si $p = 2$,

$$\left(\frac{2}{D}\right) = (-1)^{\mu\nu}.$$

II.

19. Supposons maintenant qu'il existe un système S formé de 2ν classes, $C, C_1, \ldots, C_{2\nu-1}$ associées deux à deux. La forme correspondante $[S]$ sera encore ici la somme de ν formes partielles conjuguées

$$[CC_\nu] + [C_1 C_{\nu+1}] + \ldots + [C_{\nu-1} C_{2\nu-1}],$$

et il suffira de construire la première.

Soient $s_1, s_2, \ldots$ les séries qui constituent C; $s'_1, s'_2, \ldots$ les séries conjuguées contenues dans C_ν; et désignons par $x_0^\alpha, x_1^\alpha, \ldots, x_{m_\alpha}^\alpha$ les variables de s_α, par $y_0^\alpha, \ldots, y_{m_\alpha}^\alpha$ les variables correspondantes de s'_α.

On verra comme dans le cas discuté précédemment que $[CC_\nu]$ est une somme de formes partielles contenant respectivement les produits des variables d'une des séries de C, telle que s_α, par celle d'une des séries de C_ν, telle que s_β. Chacune de ces fonctions partielles $[\alpha\beta]$ sera séparément invariante.

La fonction $[\alpha\beta]$ ne peut contenir aucun terme de rang supérieur au plus petit des deux nombres m_α, m_β, et l'ensemble des termes de rang r maximum sera ici encore de la forme

$$a_r^{\alpha\beta}[x_0^\alpha y_r^\beta - x_1^\alpha y_{r-1}^\beta + \ldots + (-1)^r x_r^\alpha y_0^\beta].$$

On pourrait en conclure que $[\alpha\beta]$ peut être mis sous la forme

$$\sum_r a_r^{\alpha\beta} f_{\alpha\beta r}.$$

Mais les formes invariantes élémentaires $f_{\alpha\beta r}$ n'étant pas symétriques par rapport aux variables x, y, la condition que $[\mathrm{CC}_\nu]$ ne soit pas altérée par le changement de ρ en ρ^{p^ν} s'exprimerait par des relations linéaires assez complexes entre les coefficients $a_r^{\alpha\beta}$. Il est donc préférable de substituer aux $f_{\alpha\beta r}$ de nouvelles fonctions élémentaires qui échappent à ce défaut.

20. Soit d'abord r pair $= 2n$. Considérons la fonction

$$\mathrm{F}_{\alpha\beta,2n} = \left\{\begin{array}{l}
\quad\left\{\begin{array}{l} x_n^\alpha y_n^\beta - x_{n-1}^\alpha y_{n+1}^\beta + x_{n-2}^\alpha y_{n+2}^\beta - \ldots + (-1)^n x_0^\alpha y_{2n}^\beta \\ \qquad - y_{n-1}^\beta x_{n+1}^\alpha + y_{n-2}^\beta x_{n+2}^\beta - \ldots + (-1)^n y_0^\beta x_{2n}^\alpha \end{array}\right\} \\
- \left\{\begin{array}{l} b_0\, x_{n-1}^\alpha y_n^\beta - b_1\, x_{n-2}^\alpha y_{n+1}^\beta + b_2\, x_{n-3}^\alpha y_{n+2}^\beta - \ldots \\ + b_0^{p^\nu} y_{n-1}^\beta x_n^\alpha - b_1^{p^\nu} y_{n-2}^\beta x_{n+1}^\alpha + b_2^{p^\nu} y_{n-3}^\beta x_{n+2}^\alpha - \ldots \end{array}\right\} \\
+ \left\{\begin{array}{l} c_0\, x_{n-2}^\alpha y_n^\beta - c_1\, x_{n-3}^\alpha y_{n+1}^\beta + c_2\, x_{n-4}^\alpha y_{n+2}^\beta - \ldots \\ + c_0^{p^\nu} y_{n-2}^\beta x_n^\alpha - c_1^{p^\nu} y_{n-3}^\beta x_{n+1}^\alpha + c_2^{p^\nu} y_{n-4}^\beta x_{n+2}^\alpha - \ldots \end{array}\right\} \\
- \left\{\begin{array}{l} d_0\, x_{n-3}^\alpha y_n^\beta - \ldots\ldots\ldots\ldots\ldots\ldots \\ + d_0^{p^\nu} y_{n-3}^\beta x_n^\alpha - \ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right\} \\
+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}\right.$$

Par le changement de ρ en ρ^{p^ν}, qui permute les x avec les y, elle se change en $\mathrm{F}_{\beta\alpha,2n}$. Cherchons à déterminer les coefficients b, c, ... de telle sorte qu'elle soit invariante par la substitution S.

Soit Δ l'accroissement qu'elle éprouve par cette substitution. Les termes de rang $2n-1$ s'y détruisent d'eux-mêmes. Pour annuler ceux de rang $2n-2$ on aura les équations de condition

$$1 - b_0 - b_0^{p^\nu} \equiv 0, \qquad -1 - b_0 + b_1 \equiv 0, \qquad 1 + b_1 - b_2 \equiv 0, \qquad \ldots,$$
$$-1 - b_0^{p^\nu} + b_1^{p^\nu} \equiv 0, \qquad 1 + b_1^{p^\nu} - b_2^{p^\nu} \equiv 0, \qquad \ldots.$$

La première de ces congruences admet p^ν racines qui sont des polynomes en ρ, car $b_0^{p^\nu}+b_0-1$ est un diviseur de $b_0^{p^{2\nu}}-b_0$. Prenons pour b_0 l'une d'elles choisie arbitrairement. Les autres relations de la première ligne donneront généralement

$$b_k \equiv b_{k-1}+1 \equiv \ldots \equiv b_0+k,$$

et celles de la seconde ligne, conjuguées des précédentes, seront satisfaites en même temps.

Pour annuler les termes de rang $2n-3$, on aura les relations

$$\begin{array}{llll} -b_0+c_0\equiv 0, & b_1+c_0-c_1\equiv 0, & -b_2-c_1+c_2\equiv 0, & \ldots, \\ & b_1^{p^\nu}+c_0^{p^\nu}-c_1^{p^\nu}\equiv 0, & -b_2^{p^\nu}-c_1^{p^\nu}+c_2^{p^\nu}\equiv 0, & \ldots, \end{array}$$

d'où

$$c_k\equiv c_{k-1}+b_k\equiv\ldots\equiv b_0+b_1+\ldots+b_k\equiv(k+1)b_0+\frac{k(k+1)}{2}.$$

On trouvera de même

$$d_k\equiv c_0+\ldots+c_k\equiv\frac{(k+1)(k+2)}{2}b_0+\frac{k(k+1)(k+2)}{2.3},$$

etc.

21. Supposons maintenant $r=2n-1$. La congruence $e^{p^\nu}+e\equiv 0$ admettra comme racines des polynomes en ρ, car son premier membre divise $e^{p^{2\nu}}-e$. Soit e l'une d'elles choisie à volonté et formons l'expression

$$F_{\alpha\beta,2n-1}=e\left\{\begin{array}{l} \left\{\begin{array}{l} x_{n-1}^\alpha y_n^\beta - x_{n-2}^\alpha y_{n+1}^\beta+\ldots+(-1)^{n-1}x_0^\alpha y_{2n-1}^\beta \\ -y_{n-1}^\beta x_n^\alpha + y_{n-2}^\beta x_{n+1}^\alpha - \ldots -(-1)^{n-1} y_0^\beta x_{2n-1}^\alpha \end{array}\right\} \\ -\left\{\begin{array}{l} b_0 x_{n-2}^\alpha y_n^\beta - b_1 x_{n-3}^\alpha y_{n+1}^\beta+\ldots+(-1)^{n-2}b_{n-2}x_0^\alpha y_{2n-2}^\beta \\ -b_0^{p^\nu} y_{n-2}^\beta x_n^\alpha + b_1^{p^\nu} y_{n-3}^\beta x_{n+1}^\alpha - \ldots -(-1)^{n-2} b_{n-2}^{p^\nu} y_0^\beta x_{2n-2}^\alpha \end{array}\right\} \\ +[\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots] \\ -\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right.$$

Par le changement de ρ en ρ^{p^ν}, elle se transforme en $F_{\beta\alpha,2n-1}$. Elle sera d'ailleurs invariante par la substitution S si l'on y détermine les coefficients b, c, ... par les relations

$$\begin{array}{lll} 1 - b_0 = 0, & -1 - b_0 + b_1 = 0, & \ldots, \\ -b_0 + c_0 = 0, & b_1 + c_0 - c_1 = 0, & \ldots, \\ \ldots\ldots\ldots\ldots, & \ldots\ldots\ldots\ldots\ldots, & \ldots, \end{array}$$

d'où l'on tire

$$\begin{array}{l} b_k = k+1, \\ c_k = b_0 + \ldots + b_k = \dfrac{(k+1)(k+2)}{2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

22. L'expression la plus générale de la fonction invariante $[\alpha\beta]$ que nous cherchons sera évidemment

$$[\alpha\beta] = \sum_r a_r^{\alpha\beta} F_{\alpha\beta r},$$

les a étant des entiers complexes constants; et celle de $[CC_\nu]$ sera, par suite,

$$[CC_\nu] = \sum_{\alpha,\beta} \sum_r a_r^{\alpha\beta} F_{\alpha\beta r}.$$

D'ailleurs, le changement de ρ en ρ^{p^ν} dans cette expression la transforme en

$$\sum_{\alpha,\beta} \sum_r (a_r^{\alpha\beta})^{p^\nu} F_{\beta\alpha r} = \sum_{\alpha,\beta} \sum_r (a_r^{\beta\alpha})^{p^\nu} F_{\alpha\beta r}.$$

Comme elle doit rester invariable, on aura les relations de condition

(1) $$(a_r^{\beta\alpha})^{p^\nu} = a_r^{\alpha\beta}.$$

En particulier, si $\beta = \alpha$, on voit que les coefficients de la forme $[\alpha\alpha]$ sont assujettis à la relation

(2) $$(a_r^{\alpha\alpha})^{p^\nu} = a_r^{\alpha\alpha}.$$

Ceux des formes $[\alpha\beta]$ où $\beta < \alpha$ sont déterminés complètement par les relations précédentes en fonction de ceux des formes où $\beta > \alpha$; ces derniers restent indéterminés, à la seule condition que le discriminant de $[CC_\nu]$ ne soit pas nul.

23. L'expression de $[CC_\nu]$ étant ainsi déterminée, proposons-nous de la réduire à une forme normale en la transformant par les substitutions de Γ, et de déterminer du même coup le nombre des formes distinctes de discriminant non nul, comprises sous cette expression générale.

Supposons, pour fixer les idées, que, parmi les séries $s_1, s_2, \ldots$, il y ait l, à savoir $s_1, \ldots, s_l$, qui contiennent $m+1$ variables, les autres séries $s_{l+1}, \ldots$ étant moins longues.

Les variables de rang maximum, $x'_m, \ldots, x^l_m$; $y'_m, \ldots, y^l_m$ ne figureront dans $[CC_\nu]$ que dans les termes de la forme bilinéaire

$$(3) \qquad \varphi = A\sum_{\alpha,\beta} a_m^{\alpha\beta}[x_0^\alpha y_m^\beta + (-1)^m x_m^\alpha y_0^\beta] \qquad \begin{pmatrix} \alpha = 1, \ldots, l \\ \beta = 1, \ldots, l \end{pmatrix},$$

le coefficient A ayant une valeur constante, égale à $(-1)^n$ si $m=2n$, et à $(-1)^{n-1}e$ si $m = 2n-1$.

D'ailleurs, les dérivées de $[CC_\nu]$ par rapport à $y'_m, \ldots, y^l_m$ devant être linéairement distinctes, le déterminant des coefficients $a_m^{\alpha\beta}$ ne sera pas nul. En particulier, les coefficients de la première ligne, $a_m^{11}, \ldots, a_m^{l1}$ ne seront pas nuls à la fois.

Si le coefficient a_m^{11} est nul, supposons, pour fixer les idées, que a_m^{21} ne le soit pas. Transformons $[CC_\nu]$ par la substitution T qui remplace

$$x''_m, \quad x''_{m-1}, \quad \ldots \qquad \text{par} \qquad x''_m + \lambda x'_m, \quad x''_{m-1} + \lambda x'_{m-1}, \quad \ldots,$$

et leurs $\nu^{\text{ièmes}}$ conjuguées

$$y''_m, \quad y''_{m-1}, \quad \ldots \qquad \text{par} \qquad y''_m + \lambda^{p^\nu} y'_m, \quad y''_{m-1} + \lambda^{p^\nu} y'_{m-1}, \quad \ldots.$$

Le coefficient a_m^{11} sera remplacé dans la transformée par un nouveau coefficient

$$a_m^{11} + \lambda a_m^{21} + \lambda^{p^\nu} a_m^{12} + \lambda^{p^\nu+1} a_m^{22}$$

qui ne pourra s'annuler que pour $p^\nu + 1$ valeurs de λ. Cette indéterminée étant susceptible de $p^{2\nu}$ valeurs distinctes pourra être choisie de telle sorte que le premier coefficient ne s'annule pas.

Supposons donc $a_m^{11} \gtrless 0$. Opérons la substitution T qui multiplie $x'_m, x'_{m-1}, \ldots$ par λ, et leurs conjuguées $y'_m, y'_{m-1}, \ldots$ par λ^{p^ν}; le premier coefficient deviendra

$$\lambda^{p^\nu+1} a_m^{11}$$

et pourra être rendu égal à l'unité; car, en vertu de la relation (2), on aura $(a_m^{11})^{p^\nu-1} = 1$ et, par suite, la congruence

$$\lambda^{p^\nu+1} a_m^{11} - 1 \equiv 0$$

aura $p^\nu + 1$ racines, car son premier membre divise

$$(\lambda^{p^\nu+1} a_m^{11})^{p^\nu-1} - 1 = \lambda^{p^{2\nu}-1} - 1.$$

Le premier coefficient a_m^{11} étant ainsi réduit à l'unité, on fera disparaître les autres coefficients $a_m^{12}, \ldots$ de la première ligne par la substitution T qui remplace

$$\begin{array}{llll} x'_m, \quad x'_{m-1}, \quad \ldots & \text{par} & x'_m - a_m^{12} x''_m - \ldots, & x'_{m-1} - a_m^{12} x''_{m-1} - \ldots, \\ y'_m, \quad y'_{m-1}, \quad \ldots & \text{par} & y'_m - (a_m^{12})^{p^\nu} y''_m - \ldots, & \ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Les coefficients $a_m^{21}, \ldots$ de la première colonne, liés aux précédents par la relation (1), disparaîtront en même temps.

Par des opérations analogues, on réduira le second coefficient diagonal a_m^{22} à l'unité, et les autres coefficients de la seconde ligne et de la seconde colonne à zéro, et ainsi de suite. Finalement, φ se trouvera réduit à la forme canonique

$$\varphi = A \sum [x_0^\alpha y_m^\alpha + (-1)^m x_m^\alpha y_0^\alpha].$$

24. Le nombre $\omega_{l,\nu}^p$ des fonctions distinctes φ réductibles à cette forme type s'obtiendra évidemment en divisant le nombre total $\mathcal{N}_{l,2\nu}^p$ des substitutions de la forme

$$(4) \quad \left| \begin{array}{lll} x', \ x'', \ \ldots, & c_1 x' + d_1 x'' + \ldots, & c_2 x' + d_2 x'' + \ldots, \quad \ldots \\ y', \ y'', \ \ldots, & c_1^{p^\nu} y' + d_1^{p^\nu} y'' + \ldots, & c_2^{p^\nu} y' + d_2^{p^\nu} y'' + \ldots, \quad \ldots \end{array} \right|$$

par le nombre $N_{l,\nu}$ de celles de ces substitutions qui transforment l'expression canonique ci-dessus en elle-même.

Cherchons à déterminer ce dernier nombre.

Les coefficients c, d, ... devront satisfaire aux relations suivantes :

$$\begin{gathered}
c_1^{p^\nu+1}+c_2^{p^\nu+1}+\ldots+c_l^{p^\nu+1}\equiv 1,\\
c_1 d_1^{p^\nu}+c_1^{p^\nu}d_1+c_2 d_2^{p^\nu}+\ldots\equiv 0,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{gathered}$$

Déterminons d'abord le nombre $M_{l,\nu}$ des solutions de la première de ces congruences.

On peut y satisfaire de $M_{l-1,\nu}$ manières en posant

$$c_2^{p^\nu+1}+\ldots+c_l^{p^\nu+1}\equiv 1,\qquad c_1=0.$$

On aura d'autre part

$$p^{2\nu(l-1)}-M_{l-1,\nu}$$

manières de déterminer c_2, ..., c_l, de telle sorte que l'on ait

$$c_2^{p^\nu+1}+\ldots+c_l^{p^\nu+1}\lesssim 1.$$

A chacun de ces systèmes de valeurs correspondront $p^\nu+1$ valeurs de c_1 qui seront des polynomes en ρ; car la congruence proposée, élevée à la puissance p^ν, donnera, en remarquant que $c_2^{p^{2\nu}}\equiv c_2$, ..., $c_l^{p^{2\nu}}\equiv c_l$,

$$c_1^{p^{2\nu}+p^\nu}+c_2^{p^\nu+1}+\ldots+c_l^{p^\nu+1}\equiv 1$$

et, par suite,

$$c_1^{p^{2\nu}+p^\nu}\equiv c_1^{1+p^\nu},\qquad \text{ou}\qquad c_1^{p^{2\nu}}\equiv c_1.$$

On a donc la formule récurrente

$$M_{l,\nu}=M_{l-1,\nu}+[p^{2\nu(l-1)}-M_{l-1,\nu}](p^\nu+1)=p^{\nu(2l-1)}+p^{\nu(2l-2)}-p^\nu M_{l-1,\nu}.$$

D'ailleurs

$$M_{1,\nu}=p^\nu+1$$

et, par suite,

$$\begin{gathered}
M_{2,\nu}=p^{3\nu}-p^\nu,\\
M_{3,\nu}=p^{5\nu}+p^{2\nu},\\
\ldots\ldots\ldots\ldots,
\end{gathered}$$

et généralement

$$M_{l,\nu} = p^{\nu(2l-1)} + (-1)^{l-1} p^{\nu(l-1)} = p^{\nu(l-1)}[p^{\nu l} - (-1)^l].$$

25. Ce premier point établi, supposons qu'on ait assigné à $c_1, \ldots, c_\rho$ l'un quelconque des $M_{l,\nu}$ systèmes de valeurs précédents. Il existera des substitutions de l'espèce (4) où les c ont ce système de valeurs. Elles seront toutes le produit de l'une d'elles, T_1, par des substitutions de la forme

$$U = \begin{vmatrix} x', x'', x''' & x' + d_1 x'' + e_1 x''' + \ldots, & d_2 x'' + e_2 x''' + \ldots, & \ldots \\ y', y'', y''' & y' + d_1^{p^\nu} y'' + e_1^{p^\nu} y''' + \ldots, & d_2^{p^\nu} y'' + e_2^{p^\nu} x''' + \ldots, & \ldots \end{vmatrix}.$$

La substitution T_1 transforme φ en une fonction φ_1 où le coefficient du terme en $x'_0 y'_m$ n'a pas changé. On peut déterminer une substitution U_1 de la forme

$$U_1 = \begin{vmatrix} x' & x' + d_1 x'' + e_1 x''' \\ y' & y' + d_1^{p^\nu} y'' + e_1^{p^\nu} y''' \end{vmatrix},$$

qui transforme φ_1 en une nouvelle fonction φ_2 ne contenant plus de termes en $x'_0 y''_m$, $x'_0 y'''_m$, et par suite se réduisant à la forme

$$A[x'_0 y'_m + (-1)^m x'_m y'_0] + \Psi',$$

Ψ' ne contenant plus les variables x', y'. On peut déterminer une substitution U_2 de la forme

$$U_2 = \begin{vmatrix} x'', x''', \ldots & d_2 x'' + e_2 x''' + \ldots, & \ldots \\ y'', y''', \ldots & d_2^{p^\nu} y'' + e_2^{p^\nu} y''' + \ldots, & \ldots \end{vmatrix},$$

qui ramène Ψ' à sa forme normale

$$A \sum_2^l [x_0^\alpha y_m^\alpha + (-1)^m x_m^\alpha y_0^\alpha].$$

La substitution $T_1 U_1 U_2$ transforme ainsi φ en elle-même; et les substitutions de la forme $T_1 U$ qui jouissent de cette propriété seront le produit de cette substitution particulière par une nouvelle substitution U' de la forme U qui transforme φ en elle-même.

Or, pour que cette substitution opérée sur φ n'y introduise aucun terme en $x'_0 y''_m$, $x'_0 y'''_m$, ..., il faut évidemment que les coefficients d_1, e_1, ... soient nuls : U' se réduira donc à la forme

$$\begin{vmatrix} x'', & x''', & \ldots & d_2 x'' + e_2 x''' + \ldots, & \ldots \\ y'', & y''', & \ldots & d_2^{p^\nu} y'' + e_2^{p^\nu} y''' + \ldots, & \ldots \end{vmatrix},$$

et les coefficients d_2, e_2, ... devront être choisis de telle sorte que cette substitution n'altère pas la forme

$$A \sum_2^l [x_0^\alpha y_m^\alpha + (-1)^m x_m^\alpha y_0^\alpha].$$

Le nombre des systèmes de valeurs qu'on peut leur assigner sera donc $N_{l-1,\nu}$.

Nous obtenons donc la formule récurrente

$$N_{l,\nu} = M_{l,\nu} N_{l-1,\nu} = \prod_1^l M_{k,\nu} = p^{\nu \frac{l(l-1)}{2}} \prod_1^l [p^{\nu k} - (-1)^k],$$

et par suite

$$\omega_{l,\nu}^p = \frac{\mathfrak{N}_{l,2\nu}^p}{N_{l,\nu}} = p^{\nu \frac{l(l-1)}{2}} \prod_1^l [p^{\nu k} + (-1)^k].$$

26. La forme φ étant ainsi réduite, les termes de rang maximum dans la fonction $[CC_\nu]$ seront les suivants :

$$A \sum_\alpha [x_0^\alpha y_m^\alpha - x_1^\alpha y_{m-1}^\alpha + \ldots + (-1)^m x_m^\alpha y_0^\alpha] \qquad (\alpha = 1, 2, \ldots, l).$$

D'ailleurs $[CC_\nu]$ peut contenir des termes de la forme

$$c x_0^\alpha y_r^\beta, \qquad \text{où} \qquad \alpha \lesseqgtr l, \qquad \beta > \alpha, \qquad r < m.$$

Le nombre de ces termes possibles sera

$$l[\mu-(m+1)l]+\frac{l(l-1)}{2}m=\frac{l}{2}[2\mu-m-(m+2)l],$$

et le coefficient de chacun d'eux sera susceptible de $p^{2\nu}$ valeurs distinctes. Ces

$$p^{\nu l[2\mu-m-(m+2)l]}$$

systèmes de valeurs sont tous également admissibles. Car nous allons voir que, quelle que soit l'hypothèse adoptée, on pourra, par des substitutions qui n'altèrent pas l'expression de S, détruire successivement tous ces coefficients.

En effet, supposons que nous nous soyons déjà débarrassé de tous ceux de ces termes dont le rang est $> r$.

Nous ferons disparaître à son tour l'un quelconque $cx_0^\alpha y_r^\beta$ des termes de rang r sans rétablir aucun des termes déjà détruits en opérant une substitution de la forme

$$\mathrm{T}=\begin{vmatrix} x_m^\alpha, & \ldots, & x_{m-r}^\alpha, & x_m^\alpha+\lambda x_r^\beta, & \ldots, & x_{m-r}^\alpha+\lambda x_0^\beta \\ y_m^\alpha, & \ldots, & y_{m-r}^\alpha, & y_m^\alpha+\lambda^{p^\nu} y_r^\beta, & \ldots, & y_{m-r}^\alpha+\lambda^{p^\nu} y_0^\beta \end{vmatrix}.$$

Cette opération accroîtra φ de certains termes tous de rang $< r$, sauf une partie de ceux qui proviennent des termes de rang m écrits ci-dessus. Parmi les nouveaux termes de rang r ainsi introduits, deux seulement

$$\mathrm{A}\lambda^{p^\nu} x_0^\alpha y_r^\beta \quad \text{et} \quad (-1)^{m-r}\mathrm{A}\lambda x_0^\beta y_r^\alpha,$$

provenant respectivement des deux termes

$$\mathrm{A}x_0^\alpha y_m^\alpha \quad \text{et} \quad (-1)^{m-r}\mathrm{A}x_{m-r}^\alpha y_r^\alpha,$$

contiendront une variable x avec l'indice zéro; le second n'est pas de ceux que nous cherchons à faire disparaître; et le premier viendra détruire le terme $cx_0^\alpha y_r^\beta$ si l'on détermine λ par la condition

$$\mathrm{A}\lambda^{p^\nu}+c\equiv 0, \qquad \text{d'où} \qquad \lambda\equiv(-\mathrm{A}^{-1}c)^{p^\nu}.$$

Après cette nouvelle réduction, celles des fonctions bilinéaires partielles $[\alpha\beta]$, où $\alpha = 1, \ldots, l$, et $\beta > \alpha$ ne contenant plus la variable x_0^α, seront identiquement nulles. Les fonctions conjuguées $[\beta\alpha]$ auront disparu en même temps, de sorte que l'expression de $[\mathrm{CC}_\nu]$ sera réduite à

$$[\mathrm{CC}_\nu] = \sum_1^l [\alpha\alpha] + \Psi,$$

Ψ étant une nouvelle fonction où ne figurent plus les variables $x', \ldots, x^l; y', \ldots, y^l$.

27. Achevons la réduction de la fonction partielle $[\alpha\alpha]$. Elle est de la forme

$$\sum_r a_r^{\alpha\alpha} \mathrm{F}_{\alpha\alpha r},$$

et le premier coefficient $a_m^{\alpha\alpha}$ a déjà été réduit à l'unité. Chacun des autres, en nombre m, satisfaisant à la relation $(a_r^{\alpha\alpha})^{p^\nu} \equiv a_r^{\alpha\alpha}$, sera susceptible de p^ν valeurs distinctes, et comme nous avons l fonctions $[\alpha\alpha]$, nous pourrons faire en tout $p^{\nu l m}$ hypothèses sur les valeurs de leurs coefficients. Elles sont également admissibles, car nous allons montrer qu'en toute hypothèse on pourra, en opérant sur $[\mathrm{CC}_\nu]$ une substitution convenable de l'espèce T, rendre nuls successivement tous les coefficients $a_r^{\alpha\alpha}$, où $r < m$.

Supposons, en effet, que nous ayons déjà réussi à annuler les coefficients $a_{m-1}^{\alpha\alpha}, \ldots, a_{r+1}^{\alpha\alpha}$ de telle sorte que $[\alpha\alpha]$ se réduise à la forme

$$\mathrm{F}_{\alpha\alpha m} + a_r^{\alpha\alpha} \mathrm{F}_{\alpha\alpha r} + \ldots.$$

Pour détruire le coefficient $a_r^{\alpha\alpha}$ opérons la substitution

$$\begin{vmatrix} x_m^\alpha, & \ldots, & x_{m-r}^\alpha & x_m^\alpha + \lambda x_r^\alpha, & \ldots, & x_{m-r}^\alpha + \lambda x_0^\alpha \\ y_m^\alpha, & \ldots, & y_{m-r}^\alpha & y_m^\alpha + \lambda^{p^\nu} y_r^\alpha, & \ldots, & y_{m-r}^\alpha + \lambda^{p^\nu} y_{m-r}^\alpha \end{vmatrix},$$

λ étant indéterminée.

L'accroissement Δ de $[\alpha\alpha]$ sera une nouvelle forme invariante dont aucun terme ne sera de rang $> r$; il sera donc de la forme

$$b_r \mathrm{F}_{\alpha\alpha r} + b_{r-1} \mathrm{F}_{\alpha\alpha, r-1} + \ldots$$

et la réduction demandée sera obtenue si $b_r = -a_r^{\alpha\alpha}$. Or on peut toujours arriver à ce résultat.

1° En effet, supposons en premier lieu m pair, $m = 2m'$ et r pair, $r = 2r'$, et comparons les coefficients de $x_r^\alpha y_r^\alpha$ dans $a_r^{\alpha\alpha} F_{\alpha\alpha r}$ et dans Δ. Le premier sera égal à $a_r^{\alpha\alpha}$; dans Δ nous aurons deux termes de ce genre, provenant de la variation des deux termes $(-1)^{m'-r'} x_r^\alpha y_{m-r}^\alpha$ et $(-1)^{m'-r'} y_r^\alpha x_{m-r}^\alpha$. La somme de leurs coefficients est

$$(-1)^{m'-r'}(\lambda^{p^\nu} + \lambda).$$

On aura donc à déterminer λ par la congruence

$$(-1)^{m'-r'}(\lambda^{p^\nu} + \lambda) + a_r^{\alpha\alpha} \equiv 0.$$

2° Si $m = 2m' - 1$ et $r = 2r'$, le terme en $x_r^\alpha y_r^\alpha$ dans Δ proviendra de la variation des deux termes

$$e(-1)^{m'-1-r'} x_r^\alpha y_{m-r}^\alpha \quad \text{et} \quad -e(-1)^{m'-1-r'} y_r^\alpha x_{m-r}^\alpha,$$

et l'on aura la congruence

$$(-1)^{m'-r'} e(\lambda^{p^\nu} - \lambda) + a_r^{\alpha\alpha} \equiv 0.$$

3° Si $r = 2r' - 1$, on comparera les coefficients des deux termes en $x_{r-1}^\alpha y_r^\alpha$. Dans $a_r^{\alpha\alpha} F_{\alpha\alpha r}$, il sera égal à $e a_r^{\alpha\alpha}$; et, dans Δ, le terme correspondant proviendra de la variation des deux termes en $x_{r-1}^\alpha y_{m-r+1}^\alpha$ et en $y_r^\alpha x_{m-r}^\alpha$, et aura pour coefficient, si $m = 2m'$,

$$(-1)^{m'-r'+1} \lambda^{p^\nu} + (-1)^{m'-r'} \lambda,$$

et, si $m = 2m' - 1$,

$$e(-1)^{m'-r'} \lambda^{p^\nu} + e(-1)^{m'-r'} \lambda.$$

On aura donc dans le premier cas la congruence

$$(-1)^{m'-r'+1}(\lambda^{p^\nu} + \lambda) + e a_r^{\alpha\alpha} \equiv 0,$$

et dans le second celle-ci :

$$(-1)^{m'-r'} e(\lambda^{p^\nu} + \lambda) + e a_r^{\alpha\alpha} \equiv 0.$$

Or, chacune des quatre congruences ci-dessus admet pour racines des entiers complexes formés avec ρ. En effet, considérons la dernière, par exemple; élevons-la à la puisssance p^ν; il viendra, en tenant compte des relations $e^{p^\nu} \equiv -e$, $a^{p^\nu} \equiv a$,

$$(-1)^{m'-r'-1} e(\lambda^{p^{2\nu}} + \lambda^{p^\nu}) - e a_r^{\alpha\alpha} = 0,$$

et, en ajoutant cette équation à la primitive et supprimant un facteur commun,

$$\lambda^{p^{2\nu}} - \lambda \equiv 0.$$

On opérera de même sur chacune des trois autres congruences.

28. Il est donc établi que $[CC_\nu]$ peut se réduire à la forme

$$[CC_\nu] = \sum_1^l F_{\alpha\alpha m} + \Psi,$$

Ψ étant une nouvelle forme ne contenant plus les variables des séries $s_1, \ldots, s_l$, ni leurs conjuguées. On la réduira de même; et si C contient l' séries à $m'+1$ variables, l'' séries à $m''+1$ variables, etc., on trouvera finalement

$$[CC_\nu] = \sum_1^l F_{\alpha\alpha m} + \sum_{l+1}^{l+l'} F_{\beta\beta m'} + \sum_{l+l'+1}^{l+l'+l''} F_{\gamma\gamma m''} + \ldots,$$

expression réduite entièrement déterminée. Toutes les formes $[CC_\nu]$ sont donc équivalentes dans le groupe Γ.

Leur nombre résulte d'ailleurs immédiatement de l'analyse précédente. En le désignant par $O(m, l; m', l'; \ldots)$ et appelant de même $O(m', l'; \ldots)$ celui des formes invariantes de l'espèce Ψ, on aura la formule récurrente :

$$O(m, l; m', l'; \ldots) = \omega_{l,\nu}^{\prime\prime} p^{\nu l[2\mu-(m+2)l]} O(m', l'; \ldots).$$

29. Il nous reste à déterminer le caractère quadratique de la forme

$$[s] = [CC_\nu] + [C_1 C_{\nu+1}] + \ldots + [C_{\nu-1} C_{2\nu-1}]$$

que nous venons d'apprendre à construire. En désignant par $F'_{\alpha\alpha m}$, $F''_{\alpha\alpha m}$ les expressions qui se déduisent de $F_{\alpha\alpha m}$ par le changement de ρ en ρ^p, ρ^{p^2}, ..., l'expression

$$\mathfrak{F}_\alpha = F_{\alpha\alpha m} + F'_{\alpha\alpha m} + \ldots + F^{\nu-1}_{\alpha\alpha m}$$

sera une forme invariante réelle où ne figure qu'une série de variables de chacune des classes conjuguées. [s] étant une somme de formes de ce genre, son caractère sera le produit de leurs caractères.

Cherchons donc le caractère de la forme partielle $\mathfrak{F}_\alpha$.

Soit γ l'ensemble des termes de rang m que contient la forme $F_{\alpha\alpha m}$. On pourrait évidemment transformer $F_{\alpha\alpha m}$ en γ en opérant sur les variables y une substitution de la forme

$$\left|\begin{array}{ll} y^\alpha_m & y^\alpha_m + \lambda_{m,m-1}\, y^\alpha_{m-1} + \ldots + \lambda_{m,0}\, y^\alpha_0 \\ y^\alpha_{m-1} & y^\alpha_{m-1} + \lambda_{m-1,m-2}\, y^\alpha_{m-2} + \ldots + \lambda_{m-1,0}\, y^\alpha_0 \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right|,$$

dont le déterminant est l'unité. Opérant une transformation analogue sur les formes conjuguées, on voit que la forme $\mathfrak{F}_\alpha$ a le même discriminant que la forme

$$\varphi = \gamma + \gamma' + \ldots + \gamma^{\nu-1}$$

obtenue en ajoutant à γ ses diverses conjuguées γ', ..., $\gamma^{\nu-1}$, laquelle est également réelle.

30. Supposons d'abord m impair, $m = 2n - 1$. En posant

$$\gamma_k = e(-1)^k [x^\alpha_{n-1-k} y^\alpha_{n+k} - y^\alpha_{n-1-k} x^\alpha_{n+k}],$$

on aura

$$\gamma = \sum_0^n \gamma_k,$$

et par suite

$$\varphi = \gamma + \gamma' + \ldots + \gamma^{\nu-1} = \sum_0^n [\gamma_k + \gamma'_k + \ldots + \gamma_k^{\nu-1}] = \sum_0^n \varphi_k.$$

Chacune des formes partielles φ_k est réelle et a pour discriminant l'unité. Elle est, en effet, bilinéaire par rapport à x^{α}_{n-1-k} et ses conjuguées d'une part (y^{α}_{n-1-k} étant la $\nu^{\text{ième}}$ de ces conjuguées), à x^{α}_{n+k} et ses conjuguées d'autre part. Or on a

$$\begin{aligned} x^{\alpha}_{n-1-k} &= X_0 + X_1 \rho + \ldots + X_{2\nu-1} \rho^{2\nu-1}, \\ x^{\alpha}_{n+k} &= Y_0 + Y_1 \rho + \ldots + Y_{2\nu-1} \rho^{2\nu-1}, \end{aligned}$$

les X, Y étant des variables réelles. En substituant aux variables complexes qui figurent dans φ_k leurs expressions en fonctions des X et des Y, les imaginaires disparaîtront et φ_k restera bilinéaire. Par un changement de variables opéré sur les Y on pourra la transformer dans la forme équivalente

$$X_0 Y_0 + \ldots + X_{2\nu-1} Y_{2\nu-1}.$$

Or, le discriminant de cette dernière est $(-1)^{2\nu} = +1$.

31. Si m est pair, $m = 2n$, nous poserons

$$\gamma_k = (-1)^k [x^{\alpha}_{n-k} y^{\alpha}_{n+k} + y^{\alpha}_{n-k} x^{\alpha}_{n+k}],$$
$$\delta = x^{\alpha}_n y^{\alpha}_n,$$

et nous aurons

$$\gamma = \delta + \sum_1^n \gamma_k,$$

d'où

$$\varphi = \delta + \delta' + \ldots + \sum_1^n [\gamma_k + \gamma'_k + \ldots].$$

Les formes partielles $\gamma_k + \gamma'_k + \ldots$ sont comme dans le cas précédent de discriminant 1. Mais il reste à déterminer le caractère du discriminant de la forme

$$\delta + \delta' + \ldots.$$

En remplaçant x^{α}_n et ses conjuguées par leurs expressions

$$x^{\alpha}_n = X_0 + X_1 \rho + \ldots + X_{2\nu-1} \rho^{2\nu-1}, \qquad \ldots,$$

nous obtiendrions une forme réelle $\Psi(X_0, X_1, \ldots)$ dont on pourra reconnaître le type en cherchant le nombre des solutions de la congruence

$$\Psi = 0 \qquad (\bmod p).$$

Or, si nous donnons à $X_0, \ldots, X_{2\nu-1}$ des valeurs réelles quelconques, le $k^{\text{ième}}$ conjugué de

$$x_n^\alpha = X_0 + X_1\rho + \ldots + X_{2\nu-1}\rho^{2\nu-1}$$

sera

$$X_0 + X_1\rho^{p^k} + \ldots + X_{2\nu-1}\rho^{(2\nu-1)p^k} \equiv (X_0 + X_1\rho + \ldots)^{p^k} \equiv (x_n^\alpha)^{p^k}.$$

En particulier, son $\nu^{\text{ième}}$ conjugué y_n^α sera $(x_n^\alpha)^{p^\nu}$.

Donc $X_0, \ldots, X_{2\nu-1}$ devront être choisis de telle sorte que l'entier complexe x_n^α satisfasse à la relation

$$(x_n^\alpha)^{p^\nu+1} + (x_n^\alpha)^{(p^\nu+1)p} + \ldots + (x_n^\alpha)^{(p^\nu+1)p^{\nu-1}} \equiv 0.$$

Celle-ci peut se décomposer en deux autres

$$(x_n^\alpha)^{p^\nu+1} \equiv z,$$

$$z + z^p + \ldots + z^{p^{\nu-1}} \equiv 0.$$

En élevant la première à la puissance p^ν et remarquant que

$$(x_n^\alpha)^{p^{2\nu}} \equiv x_n^\alpha,$$

on trouve que z doit satisfaire à la relation

$$z^{p^\nu} \equiv z.$$

Réciproquement, à chaque solution z de cette congruence correspondent $p^\nu + 1$ valeurs de x_n^α, sauf à la solution $z = 0$ à laquelle correspond la valeur unique $x_n^\alpha \equiv 0$.

Reste à trouver les solutions de la seconde congruence. Soit i une racine d'une congruence irréductible de degré ν

$$(5) \qquad i^\nu + \lambda_1 i^{\nu-1} + \ldots \equiv 0.$$

Les racines de la congruence $z^{p^\nu} \equiv z$ auront pour forme générale

$$a + a_1 i + \ldots + a_{\nu-1} i^{\nu-1},$$

les a étant des entiers réels. Les quantités conjuguées z^p, z^{p^2} s'en déduiront en remplaçant dans cette expression la racine i par ses conjuguées. La congruence

$$z + z^p + \ldots + z^{p^{\nu-1}} \equiv 0$$

devient donc

$$(6) \qquad a s_0 + a_1 s_1 + a_2 s_2 + \ldots + a_{\nu-1} s_{\nu-1} \equiv 0,$$

s_k désignant la somme des puissances $k^{\text{ièmes}}$ des racines de la congruence (5). La congruence (6) ne peut être identiquement satisfaite, quelles que soient les valeurs des a, car la relation $\Psi \equiv 0$ serait alors satisfaite pour toutes les valeurs des variables X, ce qui est inadmissible. Donc elle déterminera un des ν nombres a en fonction des autres, qui resteront arbitraires. On aura donc pour z $p^{\nu-1}$ solutions parmi lesquelles la solution $z = 0$.

Le nombre des valeurs correspondantes de x_u^α sera

$$(p^{\nu-1} - 1)(p^\nu + 1) + 1 = p^{2\nu-1} - p^\nu + p^{\nu-1}.$$

Or, si D est le discriminant de la forme ψ, ce même nombre est déterminé (n° **6**) par la formule

$$p^{2\nu-1} + (p^\nu - p^{\nu-1})\left(\frac{-1}{p}\right)^\nu \left(\frac{D}{p}\right), \qquad \text{si } p \text{ est impair};$$

$$2^{2\nu-1} - 2^{\nu-1}(-1)^\nu \left(\frac{2}{D}\right), \qquad \text{si } p = 2.$$

La comparaison de ces formules donne la relation

$$\left(\frac{D}{p}\right) = -\left(\frac{-1}{p}\right)^\nu, \qquad \text{si } p \text{ est impair}$$

$$\left(\frac{2}{D}\right) = (-1)^{\nu+1}, \qquad \text{si } p = 2.$$

32. A chaque série de la classe C qui contient un nombre impair de variables correspond dans l'expression réduite [S] une forme partielle de ce genre. Or le nombre des séries à un nombre impair de variables est évidemment de même parité que le nombre total μ des variables de la classe. Le caractère quadratique de [S] sera donc

$$(-1)^{\mu}\left(\frac{-1}{p}\right)^{\mu\nu}, \qquad \text{si } p \text{ est impair};$$
$$(-1)^{\mu(\nu+1)}, \qquad \text{si } p = 2.$$

III.

33. Soit enfin C une classe dont le multiplicateur ρ soit égal à ± 1 $(\bmod p)$. Elle sera sa propre associée.

Soient encore $s_1, s_2, \ldots$ les séries qui forment la classe C; $x_0, \ldots, x_{m_\alpha}$ les variables en nombre $m_\alpha + 1$ de la série s_α; soient enfin, comme précédemment,

$$m_1 = \ldots = m_l = m, \qquad m_{l+1} = \ldots = m_{l+l'} = m' < m, \qquad \ldots.$$

La forme invariante [C] que nous nous proposons de construire aura pour expression

$$[C] = \sum[\alpha\beta] + \sum[\alpha\alpha],$$

$[\alpha\beta]$ étant une fonction bilinéaire des variables de deux séries différentes s_α, s_β, et $[\alpha\alpha]$ une forme quadratique par rapport aux variables d'une seule série s_α.

Chacune des fonctions $[\alpha\beta]$, $[\alpha\alpha]$ devra être invariante séparément.

On trouvera, comme dans le premier cas, l'expression générale des formes $[\alpha\beta]$

$$[\alpha\beta] = \sum_r a_r^{\alpha\beta} f_{\alpha\beta r},$$

les a étant des constantes réelles, car ρ est ici réel.

34. Passons à la considération des formes quadratiques.

Le rang r de l'une quelconque d'entre elles $[\alpha\alpha]$ *sera un nombre pair et ne pourra surpasser* m_α *si* p *est impair,* $m_\alpha + 1$ *si* $p = 2$.

Supposons, en effet, r impair $= 2n+1$. L'ensemble des termes de rang r dans $[\alpha\alpha]$ sera

$$a_0 x_0^\alpha x_{2n+1}^\alpha + a_1 x_1^\alpha x_{2n}^\alpha + \ldots + a_n x_n^\alpha x_{n+1}^\alpha$$

(en supposant identiquement nuls les coefficients de ceux de ces termes où figureraient des variables d'indice $> m_\alpha$).

La substitution S transforme $[\alpha\alpha]$ en $[\alpha\alpha] + \Delta$, Δ devant être identiquement nul. Or les termes de rang maximum dans Δ proviennent exclusivement des termes de rang r écrits ci-dessus : ils sont les suivants :

$$(a_0 + a_1) x_0^\alpha x_{2n}^\alpha + (a_1 + a_2) x_1^\alpha x_{2n-1}^\alpha + \ldots + a_n x_n^\alpha x_n^\alpha$$

et ne pourraient disparaître qu'en supposant nuls tous les coefficients a.

Soit r pair $= 2n$. Les termes de rang maximum seront dans $[\alpha\alpha]$

$$a_0 x_0^\alpha x_{2n}^\alpha + a_1 x_1^\alpha x_{2n-1}^\alpha + \ldots + a_n x_n^\alpha x_n^\alpha$$

et dans Δ

$$(a_0 + a_1) x_0^\alpha x_{2n-1}^\alpha + (a_1 + a_2) x_1^\alpha x_{2n-2}^\alpha + (a_{n-1} + 2a_n) x_{n-1}^\alpha x_n^\alpha.$$

Pour qu'ils disparaissent, il faut qu'on ait

$$2a_n \equiv -a_{n-1} \equiv a_{n-2} \equiv \ldots \equiv (-1)^n a_0.$$

Donc, si p est impair, aucun des coefficients a ne sera nul, car tous le seraient. D'ailleurs, si $2n$ était $> m_\alpha$, la variable x_{2n}^α ne figurant pas dans s_α, il faudrait poser $a_0 = 0$; donc $r = 2n \leqq m_\alpha$.

Les termes de rang maximum dans $[\alpha\alpha]$ seront, par suite (si p est impair),

$$a_n [x_n^\alpha x_n^\alpha - 2 x_{n-1}^\alpha x_{n+1}^\alpha + \ldots + (-1)^n 2 x_0^\alpha x_{2n}^\alpha].$$

On voit par là que la forme $[\alpha\alpha]$, si elle n'est pas identiquement nulle, contient au moins un terme où x_0^α est multiplié par une autre variable x_{2n}^α de rang pair.

Si $p=2$, les relations précédentes donneront

$$a_0 \equiv a_1 \equiv \ldots \equiv a_{n-1} \equiv 0 \pmod 2,$$

et les termes de rang maximum $2n$ se réduiront à un seul

$$a_n x_n^\alpha x_n^\alpha.$$

Passons, dans ce cas, à la considération des termes de rang $2n-1$ contenus dans $[\alpha\alpha]$, à savoir

$$b_0 x_0^\alpha x_{2n-1}^\alpha + b_1 x_1^\alpha x_{2n-1}^\alpha + \ldots + b_{n-1} x_{n-1}^\alpha x_n^\alpha.$$

Dans Δ les termes de rang $2n-2$ dériveront exclusivement de ces termes et du terme $a_n x_n^\alpha x_n^\alpha$ et seront les suivants :

$$(b_0+b_1)x_0^\alpha x_{2n-2}^\alpha + (b_1+b_2)x_1^\alpha x_{2n-3}^\alpha + \ldots + (b_{n-1}+a_n)x_{n-1}^\alpha x_{n-1}^\alpha.$$

Pour qu'ils s'annulent, il faut poser

$$b_0 \equiv b_1 \equiv \ldots \equiv b_{n-1} \equiv a_n \pmod 2,$$

de sorte que l'ensemble des termes de rang $2n$ ou $2n-1$ dans $[\alpha\alpha]$ sera

$$a_n[x_n^\alpha x_n^\alpha + x_{n-1}^\alpha x_n^\alpha + x_{n-2}^\alpha x_{n+1}^\alpha + \ldots + x_0^\alpha x_{2n-1}^\alpha].$$

D'ailleurs, $r = 2n \overline{\gtrless} m_\alpha + 1$, sans quoi le terme en x_{2n-1}^α ne pourrait exister.

35. Cela posé, il est facile de construire une forme invariante particulière $G_{\alpha n}$, telle que parmi ses termes de rang maximum figure le carré $x_n^\alpha x_n^\alpha$ avec le coefficient 1. Si p est impair, on pourra prendre

$$\begin{aligned} G_{\alpha n} = {} & x_n^\alpha x_n^\alpha - 2x_{n+1}^\alpha x_{n-1}^\alpha + \ldots + (-1)^n 2x_{2n}^\alpha x_0^\alpha \\ & + \sum (-1)^{k+k'}(2k+k')\frac{(k+1)(k+2)\ldots(k+k'-1)}{1.2\ldots k'} x_{n+k} x_{n-k-} \\ & (k'>0,\ k+k' \overline{\gtrless} n), \end{aligned}$$

et, si $p=2$,

$$\begin{aligned} G_{\alpha n} = {} & x_n^\alpha x_n^\alpha + x_{n-1}^\alpha x_n^\alpha + x_{n-2}^\alpha(x_{n+1}^\alpha + x_n^\alpha) + x_{n-3}^\alpha(x_{n+2}^\alpha + 2x_{n+1}^\alpha + x_n^\alpha) + \ldots \\ & + x_{n-1-k}^\alpha\left[x_{n+k}^\alpha + kx_{n+k-1}^\alpha + \frac{k(k-1)}{2}x_{n+k-2}^\alpha + \ldots + x_n^\alpha\right] + \ldots . \end{aligned}$$

Pour vérifier l'invariance de ces formes, il suffit de remarquer que dans l'accroissement Δ que leur fait subir la substitution S, un terme en $x_i^\alpha x_{i'}^\alpha$ peut provenir de trois termes de $G_{\alpha n}$; ceux en $x_{i+1}^\alpha x_{i'}^\alpha$, en $x_i^\alpha x_{i'+1}^\alpha$ ou en $x_{i+1}^\alpha x_{i'+1}^\alpha$, et son coefficient sera la somme de leurs coefficients; or on constate sans peine que cette somme est nulle, quels que soient i et k.

On aura évidemment

$$[\alpha\alpha] = a_n G_{\alpha n} + R,$$

R étant une nouvelle forme invariante de rang moindre qu'on pourra réduire de même. On aura ainsi finalement l'expression générale des fonctions $[\alpha\alpha]$, à savoir

$$[\alpha\alpha] = \sum_n a_n^{\alpha\alpha} G_{\alpha n},$$

la sommation s'étendant à toutes les valeurs de n qui ne surpassent pas $\frac{1}{2}(m_\alpha + 1)$.

On aura donc, pour l'expression générale de la forme $[C]$,

$$[C] = \sum_{\alpha,\beta} \sum_r a_r^{\alpha\beta} f_{\alpha\beta r} + \sum_\alpha \sum_r a_r^{\alpha\alpha} G_{\alpha r},$$

les a étant des entiers réels.

36. Il reste à réduire les fonctions que cette expression représente à leurs formes types, et à déterminer leur nombre.

Nous avons supposé que les séries les plus longues $s_1, \ldots, s_l$ étaient au nombre de l et contenaient chacune $m + 1$ variables.

Nous traiterons d'abord le cas où p est impair.

Il se subdivise en deux autres suivant que m est pair ou impair.

37. Premier cas : *p impair, $m = 2n$.* — Considérons les termes de $[\alpha\alpha]$ qui contiennent les carrés et les rectangles des variables $x'_n, \ldots, x^l_n$. Ils constituent une forme quadratique φ que nous réduirons tout d'abord par une substitution de la forme

$$| \, x', x'', \ldots, \quad a_1 x' + b_1 x'' + \ldots, a_2 x' + b_2 x'' + \ldots, \ldots \, |.$$

On la ramène à une forme équivalente

$$x'_n x'_n + x''_n x''_n + \ldots + 2^l \mathrm{D} x^l_n x^l_n$$

qui présente deux types distincts suivant que $\left(\frac{\mathrm{D}}{p}\right)$ est égal à 1 ou à -1. Le nombre $\mathfrak{M}_l^p(\mathrm{D})$ des formes distinctes φ réductibles à chacun de ces types a été indiqué au n° **7**.

Nous avons laissé de côté le cas où le discriminant D de φ serait nul; mais cette hypothèse est à rejeter; car φ pourrait alors être transformé en une autre forme où l'une des variables, x^l_n par exemple, aurait disparu.

Mais il résulte de l'expression des fonctions f, G que, si x^l_{2n} figurait dans la forme $[\alpha\alpha]$, x^l_n devrait y figurer aussi au moins dans les termes de rang $2n$. Donc $[\alpha\alpha]$ ne contiendra pas x^l_{2n}, et son discriminant sera nul.

38. A cet instant de la réduction, les seuls termes du rang maximum qui contiennent les variables $x'_0, \ldots, x'_{2n}$ sont les suivants :

$$a^{11}_{2n}(x'_n x'_n - 2x'_{n+1} x'_{n-1} + \ldots + 2x'_{2n} x'_0),$$

a''_{2n} étant égal à 1 si $l > 1$, à $2^l\mathrm{D}$ si $l = 1$.

Mais $[\alpha\alpha]$ peut encore contenir des termes où x'_0 soit multiplié par quelqu'une des $\mu - l - 2n$ variables de rang $< 2n$ et qui n'appartiennent pas à la série s_1. Ces termes peuvent être détruits aisément quels que soient leurs coefficients (dont chacun est susceptible de p valeurs distinctes).

Soit en effet $cx'_0 x^\alpha_r$ l'un de ces termes. En opérant la substitution

$$|x'_{2n}, \ldots, x'_{2n-r} \quad x'_{2n} + \lambda x^\alpha_r, \ldots, x'_{2n-r} + \lambda x^\alpha_0|,$$

le coefficient c sera changé en $2a^{11}_{2n}\lambda + c$, et s'annulera par un choix convenable de l'indéterminée λ. La substitution aura pu introduire d'autres termes en x'_0, mais leur rang sera $< r$. En répétant la réduction on fera disparaître tous les termes en question, en commençant par ceux dont le rang est le plus élevé.

39. A ce moment, dans l'expression générale de [C] tous ceux des coefficients $a_r^{\alpha\beta}$ où $\alpha = 1$, $\beta \gtrless \alpha$ ont déjà disparu, de sorte que les variables $x'_0, \ldots, x'_m$ ne figureront plus que dans la fonction partielle

$$[11] = \Sigma a_r^{11} G_{1r}.$$

Les carrés des variables $x'_n, x'_{n-1}, \ldots, x'_0$ figurent dans cette expression avec les coefficients

$$a_n^{11}, \quad a_{n-1}^{11}, \quad a_{n-2}^{11}, \quad \ldots, \quad a_0^{11}.$$

Le premier de ces coefficients est déjà égal à l'unité. Les autres sont susceptibles de p^n systèmes de valeurs également acceptables, car on peut les faire disparaître à volonté.

Effectuons en effet la substitution

$$T = |x'_n, \ \ldots, \ x'_{n-2k} \quad x'_n + \lambda x'_{2k}, \ \ldots, \ x'_{2k} + \lambda x'_0|.$$

Le terme en x'^2_k dans la fonction transformée aura pour coefficient $(-1)^{n-k} 2\lambda + a_k^{11}$ et s'annulera par un choix convenable de λ, les termes de rang plus élevé n'étant pas modifiés. On pourra donc annuler progressivement tous les coefficients en question en commençant par ceux dont le rang est le plus élevé.

40. La partie de [C] qui contient les variables $x'_0, \ldots, x'_{2n}$ est ainsi réduite à G_{1n}. On réduira de même celle qui contient les variables $x''_0, \ldots, x''_{2n}$ à G_{2n}, etc.; enfin celle qui contient les variables x^l_0 à $2^l DG_{ln}$; et l'on aura à ce moment

$$[C] = G_{1n} + G_{2n} + \ldots + 2^l DG_{ln} + \Psi,$$

Ψ étant une forme invariante qui ne contient plus les variables des l premières séries et qui restera à réduire.

Le nombre $O(l, 2n : l', m', \ldots)$ des formes distinctes [C] réductibles à la forme ci-dessus sera d'ailleurs égal à celui $O(l', m', \ldots)$ des formes distinctes de l'espèce Ψ, multiplié par $\mathfrak{G}_l^p(D)$ et par le nombre des valeurs dont sont susceptibles les coefficients arbitraires qu'on a pu faire disparaître dans les dernières phases de la réduction, à savoir

$$p^{\mu-l-2n} p^n p^{\mu-(l-1)-2n} p^n \ldots = \ldots = p^{l(\mu-n)-\frac{l(l+1)}{2}}.$$

On a ainsi la formule suivante

$$\mathrm{O}(l, 2n; l', m'; \ldots) = \mathfrak{A}_l^p(\mathrm{D})\, p^{l(\mu-n)-\frac{l(l+1)}{2}}\, \mathrm{O}(l', m'; \ldots).$$

41. Deuxième cas : *p impair, m impair* $= 2n - 1$. — Les formes G, où le rang maximum des termes est pair et $\overline{\gtrless} m$, ne pourront contenir les variables $x'_m, \ldots, x^l_m$. La partie de [C] qui les contient sera la forme bilinéaire

$$\varphi = \sum_{\alpha, \beta} a_m^{\alpha\beta} x_0^\alpha x_m^\beta,$$

dont le déterminant n'est pas nul. Il est d'ailleurs gauche, en vertu des relations

$$a_m^{\alpha\beta} \equiv (-1)^m a_m^{\beta\alpha} \equiv - a_m^{\beta\alpha}.$$

Donc *l sera nécessairement un nombre pair*.

Écrivons donc $2l$ au lieu de l.

L'expression de φ pourra représenter (n° **8**) $\mathfrak{C}_{2l}^p$ formes distinctes, mais toutes réductibles à la forme type unique

$$\sum_1^l (x_0^{2k-1} x_m^{2k} - x_0^{2k} x_m^{2k-1}).$$

42. Après cette première réduction, les termes de rang maximum dans [C] seront les suivants :

$$\sum_1^l [x_0^{2k-1} x_m^{2k} - x_1^{2k-1} x_{m-1}^{2k} + \ldots - x_m^{2k-1} x_0^{2k}].$$

Mais [C] pourra contenir encore : 1° des termes contenant les carrés de celles des variables x_ρ^α où $\alpha \overline{\gtrless} 2l$, $\rho < n$; 2° des termes en $x_0^\alpha x_\rho^\beta$ où $\alpha \overline{\gtrless} 2l$, $\beta > \alpha$ et $\rho < 2n - 1$.

Le nombre total des termes de ce genre est évidemment

$$\begin{aligned} &2l\, 2n + 2l(\mu - 4ln) \\ &\quad + \frac{2l(2l-1)}{2}(2n-1) = l[2\mu - (2n+1)(2l-1)], \end{aligned}$$

et leurs coefficients seront susceptibles chacun de p valeurs distinctes. Mais, quelque hypothèse que l'on fasse sur les valeurs initiales de ces coefficients, il sera aisé de les annuler successivement.

Supposons, en effet, qu'on ait déjà fait disparaître de [C] tous les termes de l'espèce considérée dont le rang est $> r$, et aussi tous ceux de rang r où $\alpha < 2k-1$. Nous pourrons faire disparaître ceux dont le rang est r et où $\alpha = 2k-1$ ou $2k$.

1° En effet, si [C] contient un terme $cx_0^{2k-1}x_r^\beta$, appliquons la substitution

$$T = | x_m^{2k}, \ \ldots, \ x_{m-r}^{2k} \quad x_m^{2k} - cx_r^\beta, \ \ldots, \ x_{m-r}^{2k} - cx_0^\beta |,$$

[C] se trouvera accru de termes tous de rang $< r$, sauf ceux provenant de l'accroissement des termes de rang m, lesquels seront de rang r. Parmi ceux-ci, un seul $-cx_0^{2k-1}x_r^\beta$ (provenant du terme $x_0^{2k-1}x_m^{2k}$) sera de l'espèce considérée, et viendra détruire celui dont nous avons supposé l'existence.

2° Si r est un nombre pair 2ρ, et que [C] contienne un terme

$$cx_\rho^{2k-1}x_\rho^{2k-1},$$

on appliquera la substitution

$$T = | x_m^{2k}, \ \ldots, \ x_{m-r}^{2k} \quad x_m^{2k} - (-1)^\rho cx_r^{2k-1}, \ \ldots, \ x_{m-r}^{2k} - (-1)^\rho cx_0^{2k-1} |.$$

Les termes dont elle accroît [C] seront de rang $< r$, sauf ceux fournis par les termes de rang m, lesquels seront de rang r. Un seul de ces derniers,

$$-cx_\rho^{2k-1}x_\rho^{2k-1}$$

[provenant du terme $(-1)^\rho x_\rho^{2k-1}x_{m-\rho}^{2k}$] sera de l'espèce considérée, et détruira celui dont nous avons supposé l'existence.

3° Pour détruire ensuite successivement les termes de l'espèce considérée dont le rang est égal à r et où $\alpha = 2k$, on emploiera avec le même succès les substitutions

$$|x_m^{2k-1}, \ \ldots, \ x_{m-r}^{2k-1} \quad x_m^{2k-1} - cx_r^\beta, \ \ldots, \ x_{m-r}^{2k-1} - cx_0^\beta|$$

ou, si $r = 2\rho$,

$$|x_m^{2k-1}, \ldots, x_{m-r}^{2k-1} \quad x_m^{2k-1} - (-1)^\rho c x_r^{2k}, \ldots, x_{m-r}^{2k-1} - (-1)^\rho c x_0^{2k}|.$$

43. A ce moment la fonction $[\alpha\alpha]$ (si $\alpha \overline{\underset{<}{}} 2l$) ne contenant plus le carré d'aucune des variables x_r^α sera identiquement nulle.

Les fonctions $[\alpha\beta]$ où $\alpha = 1, \ldots, 2l$ et $\beta > \alpha$ sont également nulles comme ne contenant pas la variable x_0^α, à moins qu'on n'ait à la fois $\alpha = 2k-1$, $\beta = 2k$.

Enfin la fonction $[2k-1, 2k]$ ne contenant x_0^{2k-1} que dans le terme $x_0^{2k-1} x_{2n-1}^{2k}$ se réduira à $f_{2k-1,2k,2n-1}$

On aura donc

$$[\mathrm{C}] = \sum_1^l f_{2k-1,2k,2n-1} + \Psi,$$

Ψ étant une nouvelle fonction invariante qui ne contient plus les variables des $2l$ premières séries.

Le nombre $\mathrm{O}(2n-1, 2l; m', l'; \ldots)$ des fonctions distinctes $[\mathrm{C}]$ sera lié à celui $\mathrm{O}(m', l'; \ldots)$ des fonctions distinctes de l'espèce Ψ par la formule

$$\mathrm{O}(2n-1, 2l, m', n', \ldots) = \varepsilon_{2l}^p\, p^{l[2\mu-(2n+1)(2l-1)]}\mathrm{O}(m', l', \ldots).$$

44. La réduction de la forme $[\mathrm{C}]$ est ainsi ramenée, dans le cas de $m = 2n-1$ comme dans celui de $m = 2n$, à la réduction d'une nouvelle forme Ψ ne contenant plus qu'une partie des variables primitives. En lui appliquant les mêmes procédés de réduction, on ramènera finalement $[\mathrm{C}]$ à une somme de fonctions partielles n'ayant aucune variable commune et dont les unes, de l'espèce f, seront bilinéaires par rapport aux variables de deux séries, contenant chacune un même nombre pair de variables; les autres de l'espèce G contenant les variables d'une seule série en nombre impair.

Si donc on groupe les séries en sous-classes en réunissant ensemble celles de même longueur, *chacune des sous-classes où le nombre des variables est pair devra contenir un nombre pair de séries*. Cette condition est nécessaire pour l'existence de formes invariantes $[\mathrm{C}]$.

Dans l'expression réduite de $[\mathrm{C}]$ figure, d'ailleurs, pour chaque sous-classe à un nombre impair de variables, un coefficient $2^l D$, multipliant la dernière des fonctions partielles G qui correspondent à cette sous-classe; et D peut être pris égal soit à l'unité, soit à un non-résidu quadratique de p choisi à volonté. Il existe donc 2^ρ types de formes [C], ρ désignant le nombre des sous-classes où le nombre des variables est impair.

45. Le caractère de la forme [C] est le produit des caractères des formes partielles qui la composent.

Or les formes bilinéaires f peuvent être ramenées, par un changement de variables, à une somme de rectangles

$$\sum X_k Y_k.$$

Le nombre de variables de chaque série étant pair, elles ont le caractère $+1$.

Quant aux formes G, une transformation linéaire opérée sur les variables $x_{n-1}, \ldots, x_0$ les ramène immédiatement à la forme équivalente

$$x_n x_n + x_{n+1} x_{n-1} + \ldots + x_{2n} x_0$$

dont le discriminant est $(-1)^n 2$. Leur caractère est donc

$$\left(\frac{-1}{p}\right)^n \left(\frac{2}{p}\right).$$

Enfin, le nombre des variables étant impair dans les formes G, le discriminant de $2^l D G_{ln}$ aura pour caractère

$$\left(\frac{-1}{p}\right)^n \left(\frac{2}{p}\right) \left(\frac{2^l D}{p}\right).$$

Par suite la forme partielle

$$G_{1n} + \ldots + G_{l-1,n} + 2^l D G_{ln}$$

aura pour caractère

$$\left(\frac{-1}{p}\right)^{ln} \left(\frac{D}{p}\right),$$

et le caractère de [C] sera

$$\Pi\left(\frac{-1}{p}\right)^{ln}\left(\frac{D}{p}\right)=\left(\frac{-1}{p}\right)^{\sigma}\Pi\left(\frac{D}{p}\right),$$

σ désignant le nombre des séries où le nombre $m+1$ des variables est de la forme $4n+1$.

46. Passons au cas où $p=2$.

Ici encore nous aurons à séparer les deux cas : m pair, ou m impair.

Troisième cas : $p=2$, *m pair* $=2n$. — Parmi les termes de rang maximum, ceux qui contiennent les variables $x'_{2n}, \ldots x^l_{2n}$ sont ceux de la forme bilinéaire

$$\sum a_{2n}^{\alpha\beta} x_0^\alpha x_{2n}^\beta \qquad \begin{pmatrix}\alpha=1,2,\ldots,l \\ \beta=1,2,\ldots,l\end{pmatrix}, \quad \beta \gtrless \alpha$$

dont le déterminant ne sera pas $0 \bmod 2$.

Ce déterminant est congru mod 2 au discriminant de la forme quadratique

$$\varphi=\sum a_{2n}^{\alpha\beta} x_n^\alpha x_n^\beta + \sum a_n^{\alpha\alpha} x_n^\alpha x_n^\alpha,$$

constituée par ceux des termes de rang maximum qui contiennent les variables $x'_n, \ldots, x^l_n$.

Donc ce discriminant D n'est pas $0 \bmod 2$, et *l est nécessairement pair*. Écrivons donc $2l$ à la place de l.

Par une substitution convenable opérée sur les $x', x'', \ldots, x^{2l}$, nous pourrons, suivant le signe du caractère quadratique $\left(\frac{2}{D}\right)$, ramener φ à l'une ou à l'autre des deux formes normales

$$\sum_1^l x_n^{2k-1} x_n^{2k}$$

ou

$$x_n'^2 + x_n''^2 + \sum_1^l x_n^{2k-1} x_n^{2k},$$

et le nombre des formes distinctes φ réductibles à chacun de ces types sera $\mathfrak{N}^2_{2l}(\mathrm{D})$ (n° **7**).

Les termes de rang maximum dans [C] seront dans le premier cas (en remarquant que $+1 \equiv -1 \pmod 2$)

$$\sum_1^l (x_0^{2k-1} x_{2n}^{2k} + x_1^{2k-1} x_{2n-1}^{2k} + \ldots + x_{2n}^{2k-1} x_0^{2k}).$$

Dans le second cas, les deux termes

$$x_n'^2 + x_n''^2$$

devront être ajoutés aux précédents.

47. A ce moment [C] peut encore contenir :

1° Les carrés de celles des variables x_ρ^α où $\alpha \overline{\gtrless} 2l$, $\rho < n$; 2° les produits de celles des variables x_0^α où $\alpha \overline{\gtrless} 2l$ par des variables x_ρ^β où $\beta > \alpha$, $\rho < 2n$.

Les termes de ce genre sont au nombre de

$$2ln + 2l[\mu - 2l(2n+1)] + \frac{2l(2l-1)}{2} 2n = 2l(\mu - 2ln - 2l),$$

et chacun d'eux est susceptible des deux valeurs 0, 1. Mais, quelles que soient leurs valeurs, on pourra les détruire successivement par les mêmes substitutions qu'au n° **42**.

Après leur disparition, suivant que $x_n'^2 + x_n''^2$ figure ou non dans l'expression réduite de φ, [C] sera ramenée à la forme

$$G_{1n} + G_{2n} + \sum_1^l f_{2k-1, 2k, 2n} + \Psi'$$

ou à celle-ci

$$\sum_1^l f_{2k-1, 2k, 2n} + \Psi',$$

Ψ' étant une nouvelle fonction invariante, qui ne contient plus les variables des $2l$ séries les plus longues.

Le nombre $O(2n, 2l; m', l'; \ldots)$ des formes distinctes $[C]$ susceptibles d'être ramenées à l'un des deux types précédents sera lié au nombre $O(m', l'; \ldots)$ des formes distinctes de l'espèce Ψ par la formule récurrente

$$O(2n, 2l; m', l'; \ldots) = \mathfrak{A}_{2l}^{2}(D).2^{2l.\mu \cdot 2l(n-2l)} O(m', l'; \ldots).$$

48. Quatrième cas : $p = 2$; *m impair* $= 2n - 1$. — Les termes de $[C]$ où figurent les variables $x'_m, \ldots, x^l_m$ constituent une forme bilinéaire symétrique

$$\varphi = \sum_1^l b^\alpha x_0^\alpha x_m^\alpha + \sum_1^l a_m^{\alpha\beta} x_0^\alpha x_m^\beta \qquad \left(\begin{matrix} \alpha = 1, \ldots, l \\ \beta = 1, \ldots, l \end{matrix} \quad \beta \gtrless \alpha\right)$$

de déterminant $\gtrless 0 \bmod 2$ et que nous allons réduire d'abord.

Supposons que l'un des coefficients diagonaux du déterminant, par exemple b^1, soit $\equiv 1 \bmod 2$. Par la substitution

$$\left| x' \quad x' - \sum a_m^{1\beta} x^\beta \right|$$

on ramènera φ à la forme

$$x'_0 x'_m + \varphi',$$

φ' ne contenant plus les variables x'_0, x'_m. Si l'un de ses coefficients diagonaux n'est pas nul (mod 2) on la réduira de même. On continuera ainsi jusqu'à ce qu'on arrive à une forme φ^i où tous les coefficients diagonaux soient nuls. Le déterminant de φ^i pourra être considéré comme gauche par rapport au module 2. Le nombre $l - i$ des couples de variables x_0^α, x_m^α que contient φ^i sera donc pair, et en réduisant φ^i à sa forme type (nº **8**) on aura facilement

$$\begin{aligned}\varphi = x'_0 x'_m + \ldots + x_0^i x_m^i + (x_0^{i+1} x_m^{i+2} - x_0^{i+2} x_m^{i+1}) + \ldots \\ + (x_0^{l-1} x_m^l - x_0^l x_m^{l-1}).\end{aligned}$$

On peut, d'ailleurs, supposer $i < 3$. Considérons, en effet, la forme

$$x'_0 x'_m + x''_0 x''_m + x'''_0 x'''_m \qquad (\bmod 2).$$

Par le changement de variables suivant

$$|x', x'', x''' \quad x'+x''+x''', x'+x'', x'+x'''|,$$

elle serait transformée dans la suivante

$$x'_0 x'_m + (x''_0 x'''_m - x'''_0 x''_m) \qquad (\text{mod } 2),$$

où l'on n'a plus qu'un coefficient diagonal au lieu de trois.

Le nombre $l-i$ étant pair, et $i<3$, il faudra nécessairement supposer $i=1$ si l est impair; on n'aura donc dans ce cas qu'une réduite unique. Mais, si l est pair, on en aura deux, correspondant aux deux hypothèses $i=0$, $i=2$.

49. On obtiendra le nombre $\mathcal{C}^i_{ml}$ de formes distinctes φ réductibles à chacun de ces types en divisant le nombre total $\mathcal{A}^2_l = 2^{\frac{l(l-1)}{2}}\prod_1^l(2^k-1)$ des substitutions linéaires à l variables par le nombre N des substitutions linéaires qui transforment la forme réduite en elle-même.

1° Soit d'abord $i=0$; l étant pair, remplaçons-le par $2l$. On aura (n° **8**) $N=\omega^2_{2l}$, d'où

$$\mathcal{C}^0_{2n-1,2l} = \frac{\mathcal{A}^2_{2l}}{\omega^2_{2l}} = \Theta^2_{2l}.$$

2° Soit $i=1$; l est impair, remplaçons-le donc par $2l+1$. La forme réduite sera

$$\varphi = x'_0 x'_m + \sum(x^{2k}_0 x^{2k+1}_m - x^{2k+1}_0 x^{2k}_m) \qquad (\text{mod } 2).$$

Pour qu'une substitution

$$\sigma = \left| \begin{array}{ll} x' & a_1x'+b_1x''+c_1x'''+\ldots \\ x'' & a_2x'+b_2x''+c_2x'''+\ldots \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \end{array} \right|$$

n'altère pas cette forme, il faut que l'on ait

$$a_1^2+2a_2a_3+\ldots\equiv 1, \qquad a_2b_3+a_3b_2+a_4b_5+a_5b_4+\ldots\equiv 0,$$
$$b_1^2+2b_2b_3+\ldots\equiv 0, \qquad a_2c_3+a_3c_2+a_4c_5+a_5a_4+\ldots\equiv 0,$$

Des premières équations on déduit

$$a_1 \equiv 1, \qquad b_1 \equiv c_1 \equiv d_1 \equiv \ldots \equiv 0,$$

et le déterminant de la substitution se réduira à

$$\begin{vmatrix} b_2 & c_2 & \ldots \\ b_3 & c_3 & \ldots \\ \ldots & \ldots & \ldots \end{vmatrix}.$$

Il ne doit pas être nul. On déduira donc des équations de droite

$$a_2 = a_3 = \ldots = 0,$$

de sorte que la substitution σ laisse x' invariable et se réduit à la forme

$$\begin{vmatrix} x'' & b_2 x'' + c_2 x''' + \ldots \\ x''' & b_3 x'' + c_3 x''' + \ldots \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \end{vmatrix}.$$

Elle devra laisser invariante la partie de φ indépendante des x'. On aura donc, comme dans le cas précédent, $N = \omega_{2l}^2$, et par suite

$$\mathfrak{C}^1_{2n\ 1,2l+1} = \frac{\mathfrak{A}^2_{2l+1}}{\omega^2_{2l}} = (2^{2l+1} - 1)\, 2^{2l} \varepsilon^2_{2l}.$$

3° Soit enfin $i = 2$; l est pair, remplaçons-le par $2l$. La forme canonique de φ sera

$$x'_0 x'_m + x''_0 x''_m + \sum_1^{l-1} (x_0^{2k+1} x_m^{2k+2} - x_m^{2k+1} x_0^{2k+2}).$$

Par la transformation

$$|\ x' \quad x' + x''\ |$$

nous la changerons dans la suivante, qui se prête mieux au calcul,

$$x'_0 x'_m + x'_0 x''_m + x''_0 x'_m + \sum_1^{l-1} (x_0^{2k+1} x_m^{2k+2} - x_m^{2k+1} x_0^{2k+2}).$$

Cherchons à quelles conditions une substitution

$$\left|\begin{array}{ll} x' & a_1 x' + b_1 x'' + c_1 x''' + \ldots \\ x'' & a_2 x' + b_2 x'' + c_2 x''' + \ldots \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right|$$

n'altère pas cette forme.

On trouvera comme tout à l'heure que l'on doit avoir

$$a_1 = 1, \qquad b_1 = c_1 = \ldots = 0.$$

D'ailleurs la substitution

$$\left|\begin{array}{ll} x'' & x'' + \alpha_2 x' + \sum (\alpha_{2k+1} x^{2k+2} + \alpha_{2k+2} x^{2k+1}) \\ x''' & x''' + \alpha_3 x' \\ x^{\text{IV}} & x^{\text{IV}} + \alpha_4 x' \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right|$$

où les $2l-1$ quantités α sont arbitraires, n'altère pas la forme; les autres substitutions inaltérantes résultent évidemment de celles-ci, en nombre 2^{2l-1}, combinées avec des substitutions de la forme plus simple

$$|\; x'', \; x''', \; \ldots \qquad b_2 x'' + c_2 x''' + \ldots, \; b_3 x'' + c_3 x''' + \ldots, \; \ldots \;|.$$

Celles-ci sont au nombre de ω^2_{2l-2}. On aura donc ici $N = 2^{2l-1}\omega^2_{2l-2}$, et par suite

$$\mathfrak{C}^2_{2n-1,2l} = \frac{A^2_{2l}}{\omega^2_{2l-2}} = (2^{2l}-1)(2^{2l-1}-1)2^{2l-2}\mathfrak{S}^2_{2l-2} = (2^{2l}-1)\mathfrak{S}^2_{2l}.$$

50. La réduction de la forme φ étant actuellement terminée, achevons celle de [C].

Soit en premier lieu $i = 0$. Nous pourrons, par les mêmes procédés qu'au n° **41**, faire disparaître de φ : 1° les carrés des variables x^α_ρ où $\alpha \lesseqgtr 2l$, $\rho < n$; 2° les produits $x^\alpha_0 x^\beta_\rho$ où $\alpha \lesseqgtr 2l$, $\beta > \alpha$, $\rho < 2n-1$. Par là [C] sera réduit à la forme

$$[C] = \sum f_{2k-1,2k,2n-1} + \Psi$$

et l'on aura entre le nombre $O^0(2n-1, 2l; m', n'; \ldots)$ des formes $[C]$ réductibles à ce type et le nombre $O(m', n'; \ldots)$ des formes Ψ la relation

$$O^0(2n-1, 2l; m', n'; \ldots) = \mathfrak{S}^2_{2l}\, 2^{l(2\mu-4n-2l+1)}\, O(m', l'; \ldots).$$

51. Soit $i=2$. Les termes de $[C]$ dont le rang égale ou surpasse $m=2n-1$ seront les suivants

$$\begin{aligned} & x'_n x'_n + x'_{n-1} x'_n + x'_{n-2} x'_{n+1} + \ldots + x'_{2n-1} x'_0 \\ + & x''_n x''_n + x''_{n-1} x''_n + x''_{n-2} x''_{n+1} + \ldots + x''_{2n-1} x''_0 \\ + & \sum_2^l \left(x_0^{2k-1} x_{2n-1}^{2k} + x_1^{2k-1} x_{2n-2}^{2k} + \ldots + x_{2n-1}^{2k-1} x_0^{2k} \right). \end{aligned}$$

Si $[C]$ contient un terme en x''^2_{n-1}, on pourra le faire disparaître par une substitution de la forme

$$| \; x'_{2n-1}, \; \ldots, \; x'_n, \; \ldots \quad x'_{2n-1} + c x''_{2n-2}, \; \ldots, \; x'_n + c x''_{n-1}, \; \ldots \; |.$$

On détruira de même, par les procédés du n° **42**, tous les termes de la forme $x_0^\alpha x_\rho^\beta$, où $\alpha \lesseqgtr 2l$, $\beta > \alpha$ et $\rho < 2n-1$ et aussi les termes quadratiques $x_\rho^\alpha x_\rho^\alpha$, où $\alpha \lesseqgtr 2l$ et $\rho < n$, à l'exception toutefois du terme en x'^2_{n-1}. Car, par suite de la présence dans $[C]$ du terme x'^2_n, la substitution

$$| \; x'_n, \; x'_{n-1}, \; \ldots \quad x'_n + x'_{n-1}, \; x'_{n-1} + x'_{n-2}, \; \ldots \; |$$

n'altère pas le coefficient de ce terme, et les autres substitutions qui pourraient le détruire feraient reparaître quelqu'un des autres termes que nous voulons supprimer.

Suivant qu'à la fin de nos opérations le terme x'^2_{n-1} sera absent ou non de la fonction $[C]$, elle aura la forme réduite

$$[C] = G_{1n} + G_{2n} + \sum_2^l f_{2k-1, 2k, 2n-1} + \Psi$$

ou

$$[C] = (G_{1n} + G_{1,n-1}) + G_{2n} + \sum_{2}^{l} f_{2k-1,2k,2n-1} + \Psi,$$

Ψ ne contenant plus les variables des $2l$ premières séries.

Le nombre $O^2(2n-1, 2l; m', l'; \ldots)$ des formes $[C]$ réductibles à chacun des deux types ci-dessus sera évidemment donné par la formule

$$O^2(2n-1, 2l; m', n'; \ldots) = \mathfrak{C}^2_{2n-1,2l}\, 2^{l(2\mu-4ln-2l+1)-1}\, O(m', n'; \ldots).$$

52. Soit enfin $i = 1$. On pourra toujours, comme au n° **41**, faire disparaître successivement de $[C]$: 1° les termes en $x_0^\alpha x_\rho^\beta$ où $\alpha \overline{\gtrless} 2l+1$, $\beta > \alpha$, $\rho < 2n-1$; 2° et les termes quadratiques $x_\rho^\alpha x_\rho^\alpha$ où $\alpha \overline{\gtrless} 2l+1$, $\rho < n$, à l'exception toutefois du terme en x'^2_{n-1} dont on ne peut disposer. Suivant que ce terme existera ou non à la fin de la réduction, $[C]$ sera ramené à la forme

$$G_{1n} + G_{1,n-1} + \sum_{1}^{l} f_{2k,2k+1,2n-1} + \Psi$$

ou à celle-ci

$$G_{1n} + \sum_{1}^{l} f_{2k,2k+1,2n-1} + \Psi,$$

Ψ ne contenant plus les variables des $2l+1$ premières séries.

Le nombre des termes à coefficients arbitraires que l'on a fait évanouir étant ici égal à

$$\begin{aligned}(2l+1)[\mu - 2n(2l+1)] + (2n-1)\frac{(2l+1)2l}{2} + (2l+1)n - 1 \\ = (2l+1)(\mu - 2ln - n - l) - 1,\end{aligned}$$

on aura pour le nombre $O^1(2n-1, 2l+1; m', l'; \ldots)$ des formes $[C]$ réductibles à chacun de ces types la formule

$$O^1(2n-1, 2l+1; m', l'; \ldots) = \mathfrak{C}^1_{2n-1,2l+1}\, 2^{(2l+1)(\mu-2ln-n-l)-1}\, O(m', n'; \ldots).$$

35. En appliquant à la forme Ψ les mêmes procédés de réduction qui ont servi pour [C], nous arriverons finalement aux résultats suivants :

Le nombre p étant supposé égal à 2 et la classe C sa propre associée, groupons dans une même sous-classe celles de ses séries qui contiennent le même nombre de variables.

1° Il ne peut exister de fonction invariante que si le nombre des variables est pair dans chaque sous-classe.

2° Toute fonction invariante [C] peut être ramenée à une somme de fonctions partielles ne contenant chacune que les variables d'une seule sous-classe.

Soient $(x'_0, \ldots, x'_m)$, $\ldots$, $(x^l_0, \ldots, x^l_m)$ les variables d'une sous-classe, formée de l séries, de $m+1$ variables chacune, et désignons par $f_{\alpha\beta m}$, $G_{\alpha r}$ les expressions suivantes :

$$\begin{aligned} f_{\alpha\beta m} &= x^\alpha_0 x^\beta_m + x^\alpha_1 x^\beta_{m-1} + (x^\alpha_2 + x^\alpha_1)x^\beta_{m-2} + \ldots \\ &\quad + \left[x^\alpha_{k+1} + k x^\alpha_k + \frac{k(k-1)}{2} x^\alpha_{k-1} + \ldots + x^\alpha_1\right] x^\beta_{m-k-1} + \ldots, \\ G_{\alpha r} &= x^\alpha_r x^\alpha_r + x^\alpha_{r-1} x^\alpha_r + x^\alpha_{r-2}(x^\alpha_{r+1} + x^\alpha_r) + \ldots \\ &\quad + x^\alpha_{r-k-1}(x^\alpha_{r+k} + k x^\alpha_{r+k-1} + \ldots + x^\alpha_r) + \ldots. \end{aligned}$$

La forme canonique partielle correspondant à cette sous-classe aura l'une des expressions suivantes :

1° Si $m = 2n$ (d'où l pair),

$$f_{12m} + f_{34m} + \ldots + f_{l-1,l,m}$$

ou

$$(f_{12,m} + G_{1n} + G_{2n}) + f_{34m} + \ldots + f_{l-1,l,m};$$

2° Si $m = 2n - 1$ et l impair,

$$G_{1n} + f_{23m} + f_{45m} + \ldots + f_{l-1,l,m}$$

ou

$$(G_{1n} + G_{1,n-1}) + f_{23m} + \ldots + f_{l-1,l,m};$$

3° Si $m = 2n - 1$ et l pair,

$$f_{12m} + f_{34m} + \ldots + f_{l-1\,l,m}$$

ou

$$G_{1n} + G_{2n} + f_{34m} + \ldots + f_{l-1,l,m}$$

ou enfin

$$G_{1n} + G_{1,n-1} + G_{2n} + f_{34m} + \ldots + f_{l-1,l,m}.$$

Si donc on désigne par k le nombre total des sous-classes, par k' celui des sous-classes où le nombre des séries ainsi que celui des variables de chaque série sont tous les deux pairs, le nombre des types canoniques distincts sera $2^{k-k'}3^{k'}$.

54. Le caractère quadratique de chacun de ces types canoniques est aisé à déterminer. Il est, en effet, le produit des caractères des formes partielles des espèces

$$f_{\alpha\beta m}, \quad f_{\alpha\beta,2n} + G_{\alpha n} + G_{\beta n}, \quad G_{\alpha n}, \quad G_{\alpha n} + G_{\alpha,n-1}$$

qui y figurent.

Or, la forme $f_{\alpha\beta m}$ étant bilinéaire par rapport à deux systèmes de $m+1$ variables est équivalente à une somme de $m+1$ rectangles. Son caractère est donc $+1$.

La forme $G_{\alpha n}$ peut également se transformer par le changement de variables suivant

$$\begin{aligned} x_{n-1}^{\alpha} + x_{n}^{\alpha} &= X_{n}^{\alpha}, \\ x_{n+1}^{\alpha} + x_{n}^{\alpha} &= X_{n-2}^{\alpha}, \\ \ldots\ldots&\ldots\ldots, \\ x_{n+k}^{\alpha} + k x_{n+k-1}^{\alpha} + \ldots &= X_{n-k-1}^{\alpha}, \\ \ldots\ldots&\ldots\ldots, \end{aligned}$$

en une somme de rectangles

$$x_{n}^{\alpha} X_{n}^{\alpha} + x_{n-2}^{\alpha} X_{n-2}^{\alpha} + \ldots + x_{0}^{\alpha} X_{0}^{\alpha},$$

son caractère sera donc $+1$.

La forme $G_{\alpha n} + G_{\alpha,n-1}$ se transforme de même en posant

$$\begin{aligned} x_{n+1}^{\alpha} + x_{n}^{\alpha} + x_{n-1}^{\alpha} &= X_{n-2}^{\alpha}, \\ (x_{n+2}^{\alpha} + 2x_{n+1}^{\alpha} + x_{n}^{\alpha}) + (x_{n}^{\alpha} + x_{n-1}^{\alpha}) &= X_{n-3}^{\alpha} \\ \ldots\ldots\ldots\ldots\ldots\ldots&\ldots, \end{aligned}$$

en la suivante

$$x_n^\alpha x_n^\alpha + x_{n-1}^\alpha x_{n-1}^\alpha + x_{n-1}^\alpha x_n^\alpha + x_{n-2}^\alpha X_{n-2}^\alpha + \ldots + x_0^\alpha X_0^\alpha,$$

formée de deux carrés et d'une somme de rectangles. Son caractère est donc -1.

Enfin, dans la forme

$$f_{\alpha\beta,2n} + G_{\alpha n} + G_{\beta n},$$

les multiplicateurs des variables $x_0^\alpha, x_1^\alpha, \ldots, x_{n-1}^\alpha; x_0^\beta, \ldots, x_{n-1}^\beta$ sont des fonctions linéairement distinctes par rapport aux variables x_{2n}^β, $x_{2n-1}^\beta, \ldots, x_{n+1}^\beta; x_{2n}^\alpha, \ldots, x_{n+1}^\alpha$. En les prenant comme variables indépendantes à la place de ces dernières et les désignant par $X_0^\alpha, \ldots, X_{n-1}^\alpha$; $X_0^\beta, \ldots, X_{n-1}^\beta$ la forme deviendra

$$x_n^\alpha x_n^\alpha + x_n^\beta x_n^\beta + x_n^\alpha x_n^\beta + \sum_1^{n-1} [x_k^\alpha X_k^\alpha + x_k^\beta X_k^\beta].$$

Elle a pour caractère -1.

IV.

55. Soit enfin S une substitution linéaire qui laisse invariante une forme quadratique Φ; proposons-nous de déterminer si elle est paire ou impaire dans le groupe G correspondant à cette forme.

1° Si l'ordre q de la substitution S est impair, S sera paire, car elle est le carré de la substitution $S^{\frac{q+1}{2}}$, laquelle appartient à G.

2° Si Φ est de la forme $\sum x_k y_k$ et que S soit le produit de deux substitutions partielles S_x, S'_y opérées respectivement sur les x et sur les y, S sera paire. Car en combinant les substitutions fondamentales paires M_{ik} (n° **10**) on peut obtenir une substitution Σ qui opère sur les x la substitution S_x. La substitution $S\Sigma^{-1}$ laissera ces variables inaltérées; comme elle laisse Φ invariante, elle ne pourra altérer les y; donc elle se réduit à l'unité. Donc $S = \Sigma$, substitution paire.

56. Lemme. — *Si Φ est une somme de fonctions partielles Φ_1, Φ_2, … contenant des variables différentes, et si G_1 est le groupe* *des substitutions qui, opérées entre les variables de Φ_1, la laissent invariable, toute substitution de* G_1 *appartiendra évidemment au groupe* G; *de plus elle aura dans ce groupe la même parité que dans le groupe* G_1.

Ramenons, en effet, par un changement de variables, chacune des deux formes Φ_1 et $\Psi = \Phi - \Phi_1$ à son expression normale. Si l'une au moins des deux est du premier type (réductible à une somme de rectangles), Φ sera elle-même ramenée à la forme normale, et les substitutions fondamentales d'où dérivent toutes celles de G_1 feront encore partie du système des substitutions fondamentales de G, de sorte que la proposition est évidente.

Mais si Φ_1 et Ψ sont toutes deux du second type, soit, par exemple,

$$\Phi_1 = \xi^2 + \eta^2 + \xi\eta \quad + \sum x'_i y'_i,$$

$$\Psi = \xi_1^2 + \eta_1^2 + \xi_1\eta_1 + \sum x''_k y''_k,$$

il faudra, pour ramener Φ à sa forme normale, opérer une nouvelle transformation, par exemple la suivante :

$$\begin{aligned} x_1 &= \xi + \eta_1, & x_2 &= \xi + \eta + \xi_1 + \eta_1, \\ y_1 &= \eta + \eta_1, & y_2 &= \xi + \eta + \xi_1; \end{aligned}$$

Φ sera transformé en

$$x_1 y_1 + x_2 y_2 + \sum x'_i y'_i + \sum x''_k y''_k.$$

Cela posé, G_1 est dérivé (10) des substitutions fondamentales

$$\begin{aligned}
\mathrm{L}_i &= |x'_i, y'_i \quad y'_i, x'_i|,\\
\mathrm{M}_{ik} &= |x'_i, y'_k \quad x'_i + x'_k, y'_k + y'_i|,\\
\mathrm{L}_0 &= |\xi, \eta \quad \eta, \xi|,\\
\mathrm{N} &= |\xi, \eta \quad \eta, \xi + \eta|,\\
\mathrm{P} &= |\xi, \eta, y'_1 \quad \xi + \eta + x'_1, \xi, \xi + x'_1 + y'_1|;
\end{aligned}$$

les substitutions L_0, L_i étant impaires et les substitutions M_{ik}, N, P paires dans le groupe G_1. Elles conserveront ce même caractère dans le groupe G ; car, en les rapportant aux nouvelles variables, L_0 prendra la forme

$$L_0 = |x_1, y_1 \quad y_1, x_1|$$

et sera une substitution fondamentale impaire du groupe G ; L_i, M_{ik} ne changent pas d'expression et sont, la première impaire, la seconde paire dans le groupe G. Enfin les substitutions N, P étant d'ordre impair (on vérifie immédiatement que $N^3 = P^3 = 1$) sont nécessairement paires.

Notre proposition étant établie pour les substitutions fondamentales de G_1, le sera pour toutes celles qui en dérivent.

57. Théorème. — *Pour que la substitution* S *soit paire, il faut et il suffit que les variables y forment un nombre pair de séries.*

Soient $2n$ le nombre des variables entre lesquelles la substitution S est opérée, l le nombre des séries qu'elles forment. Nous pouvons supposer la proposition établie pour les nombres $2n'$, l', si $n' < n$ ou $n' = n$, mais $l' > l$.

Soit

$$S = \begin{vmatrix} x'_0, x'_1, \ldots & ax'_0, a(x'_1 + x'_0), \ldots \\ x''_0, x''_1, \ldots & bx''_0, b(x''_1 + x''_0), \ldots \\ \ldots, \ldots, \ldots & \ldots, \ldots\ldots\ldots, \ldots \end{vmatrix}.$$

Cette substitution est le produit de la substitution

$$S_1 = \begin{vmatrix} x'_0, x'_1, \ldots & ax'_0, ax'_1, \ldots \\ x''_0, x''_1, \ldots & bx''_0, bx''_1, \ldots \\ \ldots, \ldots, \ldots & \ldots, \ldots, \ldots \end{vmatrix},$$

d'ordre impair, par la substitution

$$S_2 = \begin{vmatrix} x'_0, x'_1, \ldots & x'_0, x'_1 + x'_0, \ldots \\ x''_0, x''_1, \ldots & x''_0, x''_1 + x''_0, \ldots \\ \ldots, \ldots, \ldots & \ldots, \ldots\ldots, \ldots \end{vmatrix},$$

dont l'ordre est une puissance de 2. Chacune d'elles sera donc une puissance de S et appartiendra à G; la substitution S' étant paire, S aura la même parité que S''; d'ailleurs, le nombre des séries y est le même. Il suffira donc d'établir le théorème pour S''.

La démonstration est donc ramenée au cas où toutes les séries ont l'unité pour multiplicateur.

58. Toute forme invariante Φ est, d'ailleurs, réductible, ainsi que nous l'avons vu, à une somme de formes partielles $\Phi' + \Phi'' + \ldots$ contenant chacune les variables d'une seule série, ou de deux séries au plus. La substitution S est, de son côté, le produit de substitutions partielles S', S'', ..., opérées respectivement entre les variables de Φ', de Φ'', ..., et dont chacune laisse Φ invariante.

Le théorème étant établi par hypothèse pour S' et Φ', S'' et Φ'', le sera, en vertu du lemme précédent, pour S' et Φ, pour S'' et Φ, ... et, par suite, pour $S = S'S''\ldots$ et Φ.

Il ne reste donc à démontrer le théorème que dans le cas où S contient une série ou deux au plus.

59. Supposons d'abord qu'il y ait deux séries, de $m + 1$ variables chacune, et soit

$$S = \begin{vmatrix} x'_0, x'_1, \ldots & x'_0, x'_1 + x'_0, \ldots \\ x''_0, x''_1, \ldots & x''_0, x''_1 + x''_0, \ldots \end{vmatrix}.$$

Si Φ n'est pas réductible à une somme de deux fonctions partielles $\Phi' + \Phi''$ contenant chacune les variables d'une seule série, elle le sera à l'une des deux expressions suivantes :

$$f_{12m}$$

ou (si m est un nombre pair $2n$)

$$f_{12,2n} + G_{1n} + G_{2n}.$$

1° Dans le premier cas, f_{12m} étant bilinéaire par rapport aux x' et aux x'', une transformation opérée sur ces dernières variables la ramènera à une somme de rectangles

$$x'_0 X''_0 + \ldots + x'_m X''_m,$$

et S étant le produit de deux substitutions partielles effectuées respectivement sur les x' et sur les X'' sera paire. Le théorème est donc vérifié.

2° Soient, en second lieu,

$$m = 2n$$

et

$$\begin{aligned}
\Phi &= f_{12,2n} + G_{1n} + G_{2n} \\
&= x'_0 x''_{2n} + x'_1 x''_{2n-1} + (x'_2 + x'_1) x''_{2n-2} + \ldots \\
&\quad + x'_n x'_n + \ldots + x'_0 (x'_{2n-1} + C^1_{n-1} x'_{2n-2} + C^2_{n-1} x'_{2n-3} + \ldots + x'_n) \\
&\quad + x''_n x''_n + \ldots \\
&= x'_0 [x''_{2n} + x'_{2n-1} + C^1_{n-1} x'_{2n-2} + \ldots + x'_n] + \Psi,
\end{aligned}$$

Ψ ne contenant plus les variables x'_0, x''_{2n}.

Changeons x''_{2n} en $x''_{2n} + x'_0$; l'expression de S ne sera pas altérée par cette transformation, et Φ deviendra

$$x'_0 [x'_0 + x''_{2n} + x'_{2n-1} + C^1_{n-1} x'_{2n-2} + \ldots + x'_n] + \Psi,$$
$$x'_0 X''_0 + \Psi,$$

en posant, pour abréger,

$$X''_0 = x'_0 + x''_{2n} + x'_{2n-1} + C^1_{n-1} x'_{2n-2} + \ldots + x'_n.$$

La substitution T qui remplace x'_0 par X''_0 sans altérer les autres variables x, n'altère pas Ψ et permute évidemment les deux fonctions x'_0, X''_0. C'est donc une des substitutions qui laissent Φ invariante; elle est, d'ailleurs, impaire; car, si l'on prenait pour variable nouvelle X''_0 au lieu de x''_{2n}, elle serait la substitution fondamentale impaire qui laisse invariante la fonction partielle $x'_0 X''_0$.

Cela posé, pour vérifier le théorème, il nous faut établir que la substitution S (où le nombre des séries est 2) est paire ou, ce qui revient au même, que la substitution ST est impaire.

Or cette dernière substitution remplace

$$\begin{array}{llllll} x'_{2n}, & \ldots, & x'_1 & \text{par} & x'_{2n}+x'_{2n-1}, & \ldots, & x'_1+x'_0; \\ x''_{2n}, & \ldots, & x''_0 & \text{par} & x''_{2n}+x''_{2n-1}, & \ldots, & x''_0, \end{array}$$

et enfin x'_0 par

$$\begin{aligned} & x'_0+(x''_{2n}+x''_{2n-1})+(x'_{2n-1}+x'_{2n-2}) \\ & \quad +C^1_{n-1}(x'_{2n-2}+x'_{2n-3})+\ldots+(x'_n+x'_{n-1}) \\ & = x'_{2n-1}+C^1_n x'_{2n-2}+\ldots+x'_{n-1}+x'_0+x''_{2n}+x''_{2n-1}. \end{aligned}$$

Son déterminant caractéristique Δ est évidemment égal à $(1-\rho)^{2n+2}\delta$, δ désignant celui de la substitution partielle

$$\left|\begin{array}{cc} x'_{2n-1}, \ldots, x'_1 & x'_{2n-1}+x'_{2n-2}, \ldots, x'_1+x'_0 \\ x'_0 & x'_{2n-1}+C^1_n x'_{2n-2}+\ldots+x'_{n-1}+x'_0 \end{array}\right|.$$

Or on a

$$\delta = \left|\begin{array}{cccccccccc} 1-\rho & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1-\rho & 1 & \ldots & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1-\rho & \ldots & 0 & 0 & \ldots & 0 & 0 \\ . & . & . & \ldots & . & . & \ldots & . & . \\ 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 1-\rho & 1 \\ 1 & C^1_n & C^2_n & \ldots & 1 & 0 & \ldots & 0 & 1-\rho \end{array}\right|$$

et, en développant suivant les coefficients de la dernière ligne,

$$\begin{aligned} \delta &= 1+C^1_n(1-\rho)+C^2_n(1-\rho)^2+\ldots+(1-\rho)^n+(1-\rho)^{2n} \\ &= (1+1-\rho)^n+(1-\rho)^{2n} \equiv \rho^n+(1-\rho)^{2n}. \end{aligned}$$

Soit $n=2^\lambda q$, q étant impair, on aura

$$\Delta \equiv [\rho^q+(1-\rho)^{2q}]^{2^\lambda}(1-\rho)^{2n+2}.$$

Les racines distinctes de δ seront au nombre de $2q+1$, car le polynome $\rho^q + (1-\rho)^{2q}$ n'ayant pas de racine commune avec sa dérivée, qui se réduit à $q\rho^{q-1} \pmod 2$, a $2q$ racines distinctes.

A chacune de ces $2q+1$ racines de la congruence caractéristique correspond d'ailleurs une seule série dans l'expression canonique de ST, car les premiers mineurs de Δ n'ont pas de diviseur commun. L'un d'eux est, en effet, égal à $(1-\rho)^{2n+2}$ et un autre est égal à δ. Or δ n'admet pas la racine $\rho = 1$. Donc ST, sous sa forme canonique, aura un nombre impair $2q+1$ de séries et sera impaire.

60. Supposons enfin que les variables de S ne forment qu'une série. Elles seront en nombre pair $2n$, et l'on aura, soit

$$\Phi = G_{1,n},$$

soit

$$\Phi = G_{1,n} + G_{1,n-1}.$$

Supposons d'abord $n > 1$. En changeant x'_{2n-1} en $x'_{2n-1} + x'_0$, on n'altérera pas l'expression de S, et Φ sera accru du terme x'^2_0.

On aura alors

$$\Phi = x'_0(x'_0 + \varphi) + \Psi,$$

Ψ ne contenant plus les variables x'_0, x'_{2n-1}, et φ étant égal, dans le premier cas, à

$$x'_{2n-1} + C^1_{n-1}x'_{2n-2} + \ldots + x'_n$$

et, dans le second, à

$$x'_{2n-1} + C^1_{n-1}x'_{2n-2} + \ldots + x'_n$$
$$+ x'_{2n-3} + C^1_{n-2}x'_{2n-4} + \ldots + x'_{n-1}.$$

La substitution T, qui remplace x'_0 par $x'_0 + \varphi$ sans altérer les autres variables x', remplacera réciproquement $x'_0 + \varphi$ par x'_0; elle laissera donc Φ invariante et sera impaire.

Il nous faut démontrer que S est impaire ou, ce qui revient au même, que ST est paire.

Or, cette substitution remplace

$$x'_{2n-1}, \quad \ldots, \quad x'_1 \qquad \text{par} \qquad x'_{2n-1} + x'_{2n-2}, \quad \ldots, \quad x'_1 + x'_0$$

et, quant à x'_0, elle le remplace dans le premier cas par

$$\begin{aligned}
&x'_0 + (x'_{2n-1} + x'_{2n-2}) + C^1_{n-1}(x'_{2n-2} + x'_{2n-3}) + \ldots \\
&\quad = x'_0 + x'_{2n-1} + C^1_n x'_{2n-2} + \ldots + x'_{n-1}.
\end{aligned}$$

Dans le second cas, on devra ajouter à cette expression les termes

$$(x'_{2n-3} + x'_{2n-4}) + C^1_{n-2}(x'_{2n-4} + x'_{2n-5}) + \ldots = x'_{2n-3} + C^1_{n-1} x'_{2n-4} + \ldots.$$

Formons le déterminant caractéristique de ST. Il sera, dans le premier cas, identique au déterminant δ du numéro précédent. Il aura $2q$ racines distinctes et à chacune d'elles correspond une seule série dans la forme canonique de ST; car les mineurs de δ n'ont pas de diviseur commun, l'un d'eux étant égal à l'unité. Le nombre des séries dans ST est donc pair et cette substitution sera paire.

Dans le second cas, formons de même le déterminant δ caractéristique de ST et développons-le suivant les éléments de la dernière ligne. On trouvera

$$\begin{aligned}
\delta &= \rho^n + (1-\rho)^{2n} + (1-\rho)^2[1 + C^1_{n-1}(1-\rho) + C^2_{n-1}(1-\rho)^2 + \ldots] \\
&= \rho^n + (1-\rho)^{2n} + (1-\rho)^2\rho^{n-1}.
\end{aligned}$$

La congruence $\delta \equiv 0$ a ses $2n$ racines toutes distinctes, car δ n'a aucune racine commune avec sa dérivée, celle-ci se réduisant à

$$\begin{aligned}
&(1-\rho)^2\rho^{n-2} \pmod 2, &&\text{si } n \text{ est pair;}\\
&\rho^{n-1} \pmod 2, &&\text{si } n \text{ est impair.}
\end{aligned}$$

Donc le nombre des séries dans ST est pair, et cette substitution sera paire.

Soit enfin $n = 1$, on aura

$$S = | \; x_0, x_1 \quad x_0, x_1 + x_0 \; |$$

et

$$\Phi = G_1 = x_1^2 + x_0 x_1 = x_1(x_1 + x_0)$$

ou

$$\Phi = G_1 + G_0 = x_1^2 + x_0 x_1 + x_0^2.$$

Dans le premier cas, posons $x_1 + x_0 = y_1$; il viendra

$$\Phi = x_1 y_1, \qquad S = | \, x_1, y_1 \quad y_1, x_1 \, |,$$

S sera une substitution fondamentale impaire.

Dans le second cas, S sera le produit des deux substitutions fondamentales :

$$L = | \, x_0, x_1 \quad x_1, x_0 \, |, \qquad N = | \, x_0, x_1 \quad x_1, x_1 + x_0 \, |$$

dont la première est impaire et la seconde paire. Donc ici encore S est impaire.