JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

CAMILLE JORDAN

Mémoire sur les groupes résolubles

Journal de mathématiques pures et appliquées 7^e série, tome 3 (1917), p. 263-374.
<http://www.numdam.org/item?id=JMPA_1917_7_3__263_0>

Mémoire sur les groupes résolubles;

PAR CAMILLE JORDAN.

Préliminaires.

L'objet principal de notre Traité des Substitutions était la solution des questions suivantes :

PROBLÈME A. — *Construire les groupes résolubles maxima de substitutions entre* N *lettres.*

PROBLÈME B. — *Construire les groupes résolubles primaires maxima contenus dans le groupe des substitutions linéaires homogènes à n variables* (mod. p).

PROBLÈME C. — *Opérer la même construction en n'employant que des substitutions assujetties à reproduire à un facteur près une forme* Φ (mod. p) (*quadratique si* $p = 2$, *bilinéaire gauche à deux systèmes de variables cogrédientes si* p *est impair*) *et de discriminant* $\gtrless 0$ (mod. p).

Nous avons obtenu la solution simultanée de ces trois problèmes par l'établissement d'une échelle de récurrence qui les ramène les uns aux autres jusqu'au moment où le résultat peut s'écrire immédiatement.

Dans un Mémoire postérieur (*Memorie della Pontificia Accademia Romana dei Nuovi Lincei*, vol. XXVI), nous avons simplifié cette analyse et montré que les mêmes procédés de réduction ne cesseraient pas de s'appliquer si, dans l'énoncé du problème C, on supposait Φ quadratique et p impair, ou Φ bilinéaire et $p = 2$.

Nous avons toutefois fait remarquer à la fin de ce travail que parmi

les nombreux groupes que fournit la méthode il en est quelques-uns qui ne sont pas maxima. La solution ne sera donc pleinement satisfaisante que lorsqu'on aura indiqué le moyen de les exclure. L'espace limité dont nous disposions ne nous permettant pas de dresser le Tableau complet de ces exclusions nécessaires, nous nous sommes borné à renvoyer aux Chapitres VI et VII de notre Traité, où la question se trouve discutée, sous les restrictions imposées à la forme Φ dans l'énoncé primitif du problème C. Les méthodes employées restent en effet applicables au cas où ces restrictions seraient supprimées. Mais elles sont présentées dans l'Ouvrage cité sous une forme assez confuse, et quelques fautes de calcul s'y sont glissées et sont à rectifier. Nous nous proposons donc de reprendre cette discussion dans le présent travail, qui formera la suite naturelle du Mémoire des *Nuovi Lincei*.

Une première Section sera consacrée à la réduction du problème A, sujet qui n'avait pas été traité dans le Mémoire susdit.

Dans une deuxième Section, nous abordons les problèmes B et C. Après avoir rappelé sommairement, comme la clarté l'exigeait, le procédé de construction des groupes cherchés établi dans le Mémoire des *Nuovi Lincei* (1), nous donnons le Tableau des précautions à prendre dans l'application de la méthode pour éliminer les groupes qui ne sont pas maxima, et nous montrons que ces exclusions sont nécessaires.

Il est plus malaisé d'établir qu'elles sont suffisantes. Nous y parviendrons en montrant qu'en désignant par L^0 et $\overline{L^0}$ deux quelconques des groupes conservés, L^0 ne peut être contenu dans $\overline{L^0}$ sans lui être identique.

Nous montrerons d'abord (Section III) que si L^0 est un des groupes que la méthode indique comme pouvant être primaire et indécomposable, il le sera en réalité. Il ne pourra donc être contenu dans $\overline{L^0}$ si celui-ci est décomposable.

La proposition à établir étant supposée vraie pour les groupes qui contiennent moins de variables que ceux que l'on considère, nous verrons (Section IV) qu'elle subsiste pour ceux-ci s'ils sont tous deux décomposables.

Reste le cas, plus difficile, où $\overline{L^0}$ est indécomposable. Il exige, pour

(1) Pour les démonstrations, nous renverrons à ce Mémoire en le désignant par la notation abrégée *N. L.*

être traité, l'étude préliminaire de deux des propriétés de ce groupe.

Nous assignerons tout d'abord (Section V) une limite supérieure au nombre des fonctions linéairement distinctes qu'une de ses substitutions peut laisser inaltérées.

Nous étudierons d'autre part certains de ses sous-groupes abéliens et nous déterminerons une limite supérieure de leur ordre (Section VI).

La combinaison de ces résultats nous permettra d'achever la démonstration du théorème :

1° Si L^p n'est pas indécomposable (Section VII),

2° S'il est indécomposable (Section VIII).

I. — Réduction du problème A.

1. *Groupes primitifs.* — Un groupe résoluble G de substitutions entre N lettres contient par définition un (ou plusieurs) sous-groupes invariants abéliens (¹). Soit F l'un de ces sous-groupes, choisi de telle sorte que son ordre soit minimum; nous l'appellerons la *base* de G.

Si G est primitif, F sera nécessairement transitif. D'ailleurs, chacune de ses substitutions (l'unité exceptée) déplace toutes les lettres. Car soient S une de ces substitutions qui laisse immobile la lettre a; b une autre lettre quelconque; T la substitution de F qui remplace a par b; la substitution $T^{-1}ST = S$ laisssera b immobile. Donc elle se réduit à l'unité.

Soit p un nombre premier dont l'ordre divise celui de F; F contiendra des substitutions d'ordre p, formant un groupe F' évidemment abélien et invariant dans G. Son ordre sera une puissance de p, telle que p^n.

D'ailleurs, F étant minimum par hypothèse se confond avec F'.

Donc l'ordre de F, et le nombre des lettres de G, qui lui est égal, sont égaux à p^n; F sera dérivé de n substitutions génératrices $A_1, \ldots, A_n$ d'ordre p et ses substitutions auront pour forme générale

$$A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_n^{\alpha_n},$$

où $\alpha_1, \ldots, \alpha_n$ varient de zéro à $p-1$.

(¹) Un groupe est dit *abélien* lorsque toutes ses substitutions sont échangeables entre elles. Nous avions donné jadis une autre signification à ce terme; mais l'usage ne l'a pas consacrée.

2. Caractérisons les p^n lettres de G au moyen de n indices $x_1, \ldots, x_n$ variables de 0 à $p-1$ (mod p). La lettre à laquelle on attribuera les indices 00... étant arbitrairement choisie, donnons les indices $\alpha_1, \ldots, \alpha_n$ à celle que la substitution $A_1^{\alpha_1} \ldots A_n^{\alpha_n}$ lui fait succéder.

L'égalité

$$A_1^{x_1} \ldots A_n^{x_n} A_1^{\alpha_1} \ldots A_n^{\alpha_n} = A_1^{x_1+\alpha_1} \ldots A_n^{x_n+\alpha_n}$$

montre que cette même substitution remplacera la lettre $(x_1, \ldots, x_n)$ par la lettre $(x_1+\alpha_1, \ldots, x_n+\alpha_n)$.

Si $p^n = 2$, les substitutions de G se réduisent à celles de sa base. Dans le cas contraire, cherchons la forme des nouvelles substitutions que G peut contenir.

3. Soit S l'une d'elles. Elle transformera

$$A_i \quad \text{en} \quad \prod_{k=1}^{k=n} A_k^{a_{ik}} \qquad (i = 1, \ldots, n)$$

(le déterminant des a n'étant pas nul). Or, la substitution T qui remplace l'indice

$$x_k \quad \text{par} \quad \sum_{i=1}^{i=n} a_{ik} x_i \qquad (k = 1, \ldots, n)$$

produit ce résultat.

On aura donc $S = TU$, U étant une nouvelle substitution échangeable à tous les A_i, et par suite faisant partie de la base.

Le groupe G s'obtiendra donc par l'adjonction à sa base de substitutions convenablement choisies dans le groupe linéaire homogène. Celles-ci forment un groupe L isomorphe à G et par suite résoluble. Il devra être maximum dans son espèce.

D'ailleurs, on peut transformer G par une substitution linéaire quelconque exécutée sur les variables x. Cette opération revenant à changer le choix des substitutions A génératrices de la base, les divers groupes ainsi obtenus ne seront différents que par la notation.

4. Pour que G soit primitif, il est encore nécessaire que L soit primaire. S'il existait, en effet, une fonction linéaire homogène φ_1 des variables x telle que ses transformées par les diverses substitutions de L s'exprimassent au moyen de m fonctions linéairement distinctes seulement, $\varphi_1, \ldots, \varphi_m$, m étant moindre que n, on obtiendrait par un changement de variables un groupe semblable à L dont les substitu-

tions auraient toutes la forme suivante :

$$(1)\qquad \left|\begin{array}{ll} x_k & a_{1k}x_1+\ldots+a_{mk}x_m \\ \cdots & \cdots\cdots\cdots\cdots\cdots \\ x_l & a_{1l}x_1+\ldots+a_{nl}x_n \end{array}\right| \quad (k=1,\ \ldots,\ m;\ l=m+1,\ \ldots,\ n).$$

et si l'on réunit dans un même système toutes les lettres pour lesquelles les m indices $x_1, \ldots, x_m$ ont les mêmes valeurs, il est clair que les substitutions ci-dessus feraient succéder à l'ensemble des lettres d'un système celui des lettres d'un autre système. Le groupe G ne serait donc pas primitif.

Cette condition est d'ailleurs suffisante. Supposons, en effet, que G ne soit pas primitif. Celles des substitutions de sa base qui ne déplacent pas le système s auquel appartient la lettre (oo...) formeront un sous-groupe de la base. Soit p^{n-m} son ordre. Il résultera de la combinaison de $n-m$ substitutions génératrices qu'il est permis de supposer n'être autres que $A_{m+1}, \ldots, A_n$. Les substitutions obtenues par la combinaison de celles-là étant les seules de la base qui ne déplacent pas le système s seront permutées entre elles par celles des substitutions de G qui ne déplacent pas s et en particulier par celles de L [lesquelles laissent immobile la lettre (oo...)]. Donc les substitutions de L seront de la forme (1), de sorte qu'il ne sera pas primaire.

Enfin, pour que G soit maximum, il faut encore que L soit maximum dans son espèce. On est ainsi ramené au problème B.

3. *Groupes non primitifs.* — Soient G un groupe résoluble, entre N lettres, transitif mais non primitif; $s_1, s_2, \ldots, s_m$ les systèmes, de N' lettres chacun, entre lesquelles ses lettres sont supposées se partager.

Celles des substitutions de G qui ne déplacent pas le système s_k sont de la forme $S_k T$, où S_k est opérée entre les lettres de s_k et T entre les autres lettres. Elles constituent un sous-groupe H_k de G, qui sera résoluble. Les substitutions partielles S_k forment un groupe Γ_k isomorphe à H_k; lui aussi sera donc résoluble.

Or, on peut établir entre les lettres des divers systèmes une correspondance telle que parmi les substitutions de G qui font succéder s_k à s_1 il y en ait une U_k où chaque lettre soit remplacée par sa correspondante.

Cela posé, chaque substitution de G est de la forme $VS'_1S'_2\ldots S'_m$; V déplaçant les systèmes en remplaçant chaque lettre par sa correspondante et S'_k étant une substitution opérée entre les lettres de s_k.

Or, on voit aisément que grâce à la correspondance établie :

1° Chacune des substitutions S'_k appartiendra à Γ_k (¹);

2° Les groupes $\Gamma_1, \ldots, \Gamma_m$ sont tous semblables;

3° Les déplacements V des systèmes forment un autre groupe Δ isomorphe à G et par suite résoluble; elles transforment d'ailleurs les groupes Γ les uns dans les autres.

Le groupe $(\Delta, \Gamma_1, \ldots, \Gamma_m)$ sera donc résoluble. Mais il contient G. Donc si G est maximum, il se confondra avec lui; et sa construction reviendra à celle des deux groupes Δ et Γ_1 ayant respectivement m et N′ pour nombre de leurs lettres.

Si le groupe G admettait plusieurs répartitions de ses lettres en systèmes, nous supposerons avoir adopté celle où N′ est maximum. Dans ce cas Δ sera primitif; m sera donc une puissance de nombre premier, telle que p^n.

6. Soit $s'_1, s'_2, \ldots$ un autre groupement des lettres en systèmes. Chacun de ces nouveaux systèmes sera contenu en entier dans l'un des anciens. Supposons, en effet, que l'un d'eux s'_1 contînt à la fois une lettre a de s_1 et une autre lettre b d'un autre système, tel que s_2. Les substitutions de Γ_1, laissant b immobile, ne déplaceraient pas s'_1. Les lettres de Γ_1, qu'elles font succéder à a, appartiendraient donc toutes à s'_1. Il contiendrait donc contre l'hypothèse plus de lettres que s_1.

Soient donc $s_{k1}, \ldots, s_{km'}$ ceux des nouveaux systèmes qui sont contenus dans s_k; N″ le nombre des lettres de chacun d'eux. La construction de Γ_1 reviendra à celle de deux groupes successifs, l'un Δ' de déplacements d'ensemble des m' systèmes $s_{11}, \ldots, s_{1m'}$, l'autre Γ_{11} entre les N″ lettres de s_{11}.

Si l'on a choisi les systèmes s' de telle sorte que N″ soit maximum, Δ' sera primitif et m' une puissance de nombre premier telle que $p'^{n'}$.

On verra de même que s'il existe un autre groupement des lettres en nouveaux systèmes s'', contenant chacun N‴ lettres, chacun d'eux sera contenu dans l'un des systèmes s'; et que Γ_{11} résulte de la combinaison d'un groupe Δ'' de substitutions d'ensemble entre ceux des systèmes s'' qu'il contient (lequel sera primitif si N‴ est maximum)

(¹) En effet soit s_l le système auquel V fait succéder s_k. Le groupe G contient la substitution $U_k^{-1} U_l V S'_1 S'_2 \ldots S'_m$ qui ne déplace pas le système s_k mais effectue sur ses lettres l'opération S'_k.

et d'un groupe Γ_{111} de substitutions opérées sur l'un des systèmes s'' que Γ_{11} contient.

Poursuivant ainsi jusqu'à ce qu'on ait épuisé le nombre des groupements possibles en systèmes, on arrivera à un dernier groupe $\Gamma_{11\ldots}$ qui sera primitif comme les Δ. D'où la règle suivante pour la construction des groupes non primitifs maxima :

Décomposer N *en un produit de facteurs successifs* $m, m', \ldots, m^l$ *dont chacun soit une puissance d'un nombre premier; construire des groupes primitifs* $\Delta, \Delta', \ldots \Delta^l$ *de substitutions entre* m *systèmes* s, *puis entre* m' *systèmes* s', *etc.; enfin, entre les* m^l *lettres du dernier système* $s^{(l)}$; *le groupe cherché sera de la forme*

$$(\Delta, \Delta' \ldots \Delta^l)$$

7. Pour qu'il soit maximum, il faut évidemment que chacun des groupes $\Delta, \Delta', \ldots$ le soit; mais il devra en être de même pour chacun des groupes $(\Delta^k, \ldots, \Delta^l)$. Or, cela n'aurait pas lieu si, dans la suite des nombres $m, m', \ldots$, deux nombres consécutifs étaient égaux à 2.

Supposons, en effet, qu'on ait $m = m' = 2$.

Nous aurons deux systèmes s_1, s_2 que Δ permute entre eux; s_1 contiendra deux systèmes s', soient s_{11}, s_{12}, que Γ_1 permute entre eux; s_2 en contient deux autres s_{21}, s_{22} que Γ_2 permute entre eux. Les substitutions de G opéreront donc entre les quatre systèmes s' huit permutations seulement sur les 24 qu'on peut concevoir, lesquelles forment un groupe résoluble D. Le groupe $G = (\Delta, \Delta', \Gamma_{11})$ ne sera donc pas maximum, étant contenu dans le groupe plus général (D, Γ_{11})

Nous pouvons donc formuler cette règle :

Premier cas d'exclusion. — Dans la construction des groupes non primitifs, on rejettera toutes les décompositions $N = mm' \ldots$ où deux facteurs consécutifs sont égaux à 2.

Nous verrons tout à l'heure que cette précaution suffit pour éliminer les groupes non maxima.

8. *Groupes intransitifs.* — Soit G un groupe résoluble non transitif. Groupons ses lettres en classes, en réunissant celles que les substitutions de G permutent entre elles. Chacune de ces substitutions sera un produit de substitutions partielles $S_1, S_2, \ldots$ opérées respectivement entre les lettres des classes $1, 2, \ldots$ Or, il est évident : 1° que les substi-

tutions partielles S_k forment un groupe résoluble et transitif G_k; 2° que le groupe $(G_1, \ldots, G_k, \ldots)$ l'est également. Il contient, d'ailleurs, G. Donc si G est maximum il sera de cette forme. Ainsi, pour former les groupes cherchés, on aura à décomposer N en une somme de nombres $N = N_1 + N_2 + \ldots$ et à construire des groupes résolubles et transitifs $G_1, G_2, \ldots$

Le cas où quelqu'un des nombres N_i serait égal à 1 n'est pas exclu. Le groupe correspondant G_i se réduirait à la substitution 1.

Pour que G soit maximum, il faut que chacun des groupes partiels G_i le soit. Mais cela n'est pas suffisant.

Deuxième cas d'exclusion. — Le groupe G, ainsi formé, devra être rejeté :

1° Si deux des groupes partiels G_1, G_2 sont semblables;

2° Si $G_2 = (\Delta, \Gamma_1, \Gamma_2, \ldots)$ est un groupe décomposable, les groupes $\Gamma_1, \Gamma_2 \ldots$ étant semblables à G_1, et au nombre de 2 ou 3.

Désignant en effet par D le groupe des substitutions d'ensemble qui peuvent être opérées entre les deux, trois ou quatre systèmes de lettres qui figurent dans les groupes semblables G_1, G_2 ou G_1, Γ_1, Γ_2 ou $G_1, \Gamma_1, \Gamma_2, \Gamma_3$, le groupe intransitif (G_1, G_2) serait contenu dans le groupe transitif plus général dérivé de D et de G_1.

Nous aurons à montrer que cette précaution suffit.

9. Les deux cas d'exclusion signalés plus haut sont les seuls à considérer.

Nous allons démontrer en effet que, si G et $\overline{G}$ sont deux groupes résolubles entre N lettres, fournis par la méthode précédente, G ne peut être contenu dans $\overline{G}$, s'il ne lui est identique.

Cette proposition étant supposée établie pour les groupes de moins de N lettres, sera évidemment vraie pour N lettres, si $\overline{G}$ n'est pas transitif.

S'il est transitif, divers cas seront à distinguer.

10. Premier cas : $\overline{G}$ *n'est pas primitif.* — Soient $\overline{s}_1, \ldots, \overline{s}_m$ les systèmes entre lesquels ses lettres sont réparties. On obtiendra $\overline{G}$ en combinant des groupes semblables $\overline{\Gamma}_1, \ldots, \overline{\Gamma}_m$ opérés dans l'intérieur de chaque système avec un groupe $\overline{\Delta}$ de déplacements d'ensemble.

Supposons, pour fixer les idées, que G, contenu dans $\overline{G}$, soit intran-

sitif. Il résultera de la réunion de groupes transitifs $G_1, G_2, \ldots$, contenant chacun une partie des lettres de $\overline{G}$.

Les lettres de chacun des systèmes $\bar{s}_1, \ldots, \bar{s}_m$ appartiendront toutes à un seul de ces groupes partiels. Supposons, en effet que, parmi les lettres de $\bar{s}_1$, les unes, telles que a, figurent dans G_1 et les autres, telles que b, figurent dans G_2. Les substitutions de G_1 laissant b immobile, ne déplaceront pas le système $\bar{s}_1$. Les diverses lettres qu'elles font succéder à a appartiendraient donc à ce système. Donc $\bar{s}_1$ contiendrait toutes les lettres de G_1; il contiendrait de même celles de G_2.

Le groupe intransitif (G_1, G_2) serait donc contenu dans le groupe transitif $\overline{\Gamma}_1$ qui a moins de N lettres, ce qui est impossible, par hypothèse.

Cela posé, soient $\bar{s}_1, \ldots, \bar{s}_k$ ceux des systèmes $\bar{s}$ qui figurent dans G_1. Les lettres de G_1 admettant ce groupement en systèmes, G_1 sera formé par la réunion de groupes semblables $\Gamma_1, \ldots, \Gamma_k$ de substitutions opérées à l'intérieur de ces systèmes avec un groupe Δ_1 de déplacements d'ensemble. Les groupes $\Gamma_1, \ldots, \Gamma_k$ étant respectivement contenus dans les groupes $\overline{\Gamma}_1, \ldots, \overline{\Gamma}_k$, qui contiennent moins de N lettres, leur seront identiques.

Chacun des autres groupes partiels $G_2, \ldots$ résultera de même de la combinaison d'une partie des groupes $\overline{\Gamma}$ avec un groupe Δ_2 de déplacements d'ensemble opérés entre les systèmes correspondants.

Donc G sera formé par l'ensemble des groupes $\overline{\Gamma}$ joints au groupe $(\Delta_1, \Delta_2, \ldots)$ des déplacements d'ensemble qu'il fait subir aux systèmes $\bar{s}$.

Ce groupe $(\Delta_1, \Delta_2, \ldots)$ devra être contenu dans $\overline{\Delta}$ qui n'opère que sur m objets. Il lui sera donc identique. Cela est impossible si G est intransitif comme nous l'avions supposé. S'il est transitif, on n'aura qu'un seul groupe Δ_1, identique à $\overline{\Delta}$ et G sera identique à $\overline{G}$.

11. Deuxième cas : $\overline{G}$ *est primitif, mais* G *ne l'est pas.* — On aura $N = p^n$, et les substitutions de $\overline{G}$ seront de la forme linéaire

$$S = | x_k \quad \Sigma_i a_{ik} x_i + \alpha_k | \qquad (k = 1, \ldots, n).$$

Cherchons combien une substitution de cette forme peut laisser de lettres immobiles.

On aura à satisfaire aux relations

$$x_k \equiv \Sigma_i a_{ik} x_i + z_k \qquad (\mathrm{mod}\, p).$$

Si elles sont identiques, S se réduit à l'unité. Dans le cas contraire, supposons qu'elles se réduisent à $n - m$ relations distinctes. Elles détermineront $n - m$ variables en fonction des autres qui resteront arbitraires, ce qui donne p^m solutions. Ce nombre ne peut en aucun cas surpasser $\frac{1}{2} p^n = \frac{1}{2} \mathrm{N}$.

Donc, toute substitution de $\overline{\mathrm{G}}$ (sauf l'unité) déplace au moins la moitié des lettres. Il en sera de même pour les substitutions de G, s'il s'y trouve contenu.

Donc G ne peut être transitif, et non primitif, car il s'obtiendrait en combinant deux groupes successifs Δ et Γ_1, ce dernier étant primitif et borné aux lettres d'un seul système. Or, pour que Γ_1 ne contînt pas de substitutions déplaçant moins de $\frac{1}{2}$ N lettres, il faudrait évidemment : 1° qu'il n'y eût que deux systèmes ; 2° que Γ_1 se réduisît à sa base et, par suite, ne contînt que deux lettres. Or, les groupes $\mathrm{G} = (\Delta, \Gamma_1)$, ainsi formés, ont été exclus.

12. Supposons donc G intransitif et formé de la réunion des groupes transitifs G_1, G_2, ... Chacun de ceux-ci devra être primitif et contenir au moins la moitié des lettres s'il en contient plus d'une. S'il en contient juste la moitié, il devra se réduire à sa base. Enfin, deux de ces groupes ne peuvent être semblables, ce cas étant exclu.

La seule hypothèse qui satisfasse à toutes ces conditions est qu'on ait deux groupes partiels G_1, G_3, dont le premier soit primitif et contienne $p^n - 1$ lettres, la dernière figurant seule dans G_2.

G_1 étant primitif, le nombre de ses lettres sera une puissance d'un nombre premier, telle que q^m, et sa base B formera un groupe abélien, d'ordre $q^m = p^n - 1$, dérivé de m substitutions génératrices d'ordre q.

Les substitutions de B laissent d'ailleurs immobile une même lettre de $\overline{\mathrm{G}}$ et l'on peut supposer que ce soit celle qu'on a affectée des indices 0, 0, ... Ces substitutions appartiendront donc au groupe linéaire homogène $\overline{\mathrm{L}}$ qui, combiné à la base $\overline{\mathrm{B}}$ de $\overline{\mathrm{G}}$, constitue ce groupe.

13. Or nous aurons à faire plus loin (Section VI) une étude appro-

fondie des groupes abéliens que peut contenir un groupe $\overline{L}$. Parmi les résultats qu'elle nous donnera, figure (**80**) le suivant, que nous admettrons provisoirement, à titre de postulat.

Pour qu'un groupe abélien contenu dans $\overline{L}$ soit d'ordre $p^n - 1$, il faut qu'il résulte des puissances d'une seule substitution, de la forme

$$S = |x_0, \ldots x_r, \ldots \quad ix_0, \ldots, i^r x_r, \ldots| \qquad (r = 0, \ldots, n-1),$$

i étant une racine primitive de la congruence

$$i^{p^n-1} \equiv 1 \pmod{p}$$

et $x_0, \ldots, x_{n-1}$ des variables conjuguées.

On aura donc nécessairement $m = 1$, et G_1 formé des substitutions linéaires

$$|X \quad aX + b| \qquad (\mathrm{mod}\ q),$$

aura pour ordre

$$q(q-1) = (p^n - 1)(p^n - 2).$$

Ses substitutions sont, d'ailleurs, permutables à B, lequel est formé des puissances de la substitution S. Or, les seules substitutions de $\overline{G}$ qui soient permutables à B s'obtiennent en joignant à S la substitution

$$|x_r \quad x_{r+1}| \qquad |r = 0, 1, \ldots, n-1 \pmod{p}|$$

Elles forment un groupe d'ordre $(p^n - 1)n$, lequel devrait contenir G ; d'où la condition

$$n \geq p^n - 2,$$

laquelle n'est satisfaite que si $p = 2$, $n = 2$, ou $p = 3$, $n = 1$; mais ce sont des cas exclus.

14. Troisième cas. — $\overline{G}$ *est primitif ainsi que* G.

Soient $\overline{B}$ la base de $\overline{G}$; $\overline{L}$ le groupe primaire qu'il faut lui adjoindre pour obtenir $\overline{G}$.

Les substitutions de G seront de la forme ST, S appartenant à $\overline{L}$ et T à $\overline{B}$. Les substitutions partielles S formeront un groupe L contenu dans $\overline{L}$; et, G étant supposé primitif, L sera primaire.

On en conclut que la base B de G est identique à $\overline{B}$.

Supposons, en effet, qu'il en soit autrement ; et soient $S, T_1, S_2 T_2, \ldots$

les substitutions génératrices de B. Celles des substitutions partielles S_1, S_2, ... qui ne se réduisent pas à l'unité sont d'ordre p et forment un groupe abélien A invariant dans L.

Soit S_1 l'une d'elles. Elle permute les unes dans les autres les $p^n - 1$ fonctions $a_1 x_1 + \ldots + a_n x_n$. Leur nombre étant premier à p, quelques-unes d'entre elles seront nécessairement inaltérées. Supposons que parmi ces fonctions inaltérées il y en ait k distinctes $x_1, \ldots, x_k$. Les fonctions $a_1 x_1 + \ldots, a_k x_k$ seront également inaltérées et leur nombre $p^k - 1$ sera premier à p.

Soit S_2 une seconde substitution échangeable à S_1. Elle permutera ces fonctions entre elles et en laissera nécessairement d'inaltérées.

Poursuivant ainsi, on voit qu'il existe des fonctions linéaires $a_1 x_1 + \ldots + a_i x_i$ inaltérées par toutes les substitutions S. Les substitutions de L, étant permutables à A, transformeront ces fonctions les unes dans les autres; L_1 ne serait donc pas primaire.

L'identité des bases $\overline{B}$ et B étant ainsi établie, L sera contenu dans $\overline{L}$; mais la construction le suppose maximum; donc $L = \overline{L}$.

II. — Réduction des problèmes B et C. Exclusions nécessaires.

13. Le problème A se trouve ramené, par ce qui précède, au problème B. Celui-ci présente, d'ailleurs, avec le problème C, une analogie si étroite que nous abrégerons l'exposition en les traitant simultanément.

Le problème C se subdiviserait en deux autres, suivant que la forme invariante $\Phi \bmod p$ est une forme bilinéaire Φ_b ou une forme quadratique Φ_q. Mais nous pourrons presque toujours faire disparaître cette distinction par l'introduction dans les formules d'un entier τ égal à zéro si Φ est quadratique, à 1 si Φ est bilinéaire.

Le discriminant de Φ devant être $\not\equiv 0 \bmod p$, le nombre n des variables sera nécessairement pair : 1° si $\tau = 1$, 2° si $\tau = 0$, mais $p = 2$.

Les formes $\Phi_q \pmod p$ appartiennent à deux types distincts, suivant le caractère quadratique de leur discriminant. Si n est un nombre pair $2m$, celles du premier type sont réductibles à la forme

$$x_1 y_1 + x_2 y_2 + \ldots + x_m y_m$$

et celles du second type à la forme

$$x_1 y_1 + \ldots + x_{m-1} y_{m-1} + x_m^2 - g y_m^2 \qquad (g \text{ racine primitive de } p)$$

si p est impair, ou à la forme

$$x_1y_1 + \ldots + x_m y_m + x_m^2 + y_m^2$$

si $p = 2$.

A ces deux types de formes correspondront deux types différents de groupes invariantifs.

Il n'y a pas lieu de retenir cette distinction si n est impair. Car bien qu'on ait encore deux types de fonctions, ils sont invariables par les mêmes substitutions.

16. Une forme Φ étant donnée, soit L l'un des groupes invariantifs cherchés. Si p est impair, chaque substitution S de L laissera Φ absolument invariable, auquel cas nous dirons qu'elle est *propre*; ou la multipliera par un facteur de la forme g^ρ, g étant une racine primitive de p. Nous dirons que cette substitution est *impropre* et *appartient à l'exposant* ρ.

Le groupe L sera d'exposant 1 s'il contient une substitution S d'exposant 1; il résultera de la combinaison de S avec un sous-groupe L^0 formé de ses substitutions propres.

Dans le cas contraire, désignons par g la substitution qui multiplie toutes les variables par g et la forme Φ par g^2. Étant échangeable à toute substitution linéaire, elle appartiendra nécessairement à L supposé maximum. L sera donc d'exposant 2 et s'obtiendra par la combinaison de g avec L^0.

Si $p = 2$, ou si l'on n'a pas de forme invariante, toutes les substitutions de L devront être considérées comme propres et $L = L^0$.

Voici enfin une dernière proposition sur laquelle nous aurons à nous appuyer (Voir le *Journal de Liouville*, 6e série, t. I, 1905, p. 276 à 284).

Le groupe K, *formé par toutes les substitutions qui laissent invariante une forme quadratique* Φ mod 2, *possède un seul sous-groupe invariant* K', *d'ordre moitié moindre et formé par les substitutions paires de* K (1).

Le cas où Φ ne contient que quatre variables fait exception. Dans ce

(1) Une substitution est dite *paire* ou *impaire* suivant que le nombre des fonctions linéaires distinctes qu'elle multiplie par des facteurs constants (égaux ou non) est pair ou impair.

cas, K a pour facteurs de composition $2.2.3.2.3$ et ne contient aucune substitution d'ordre 8.

17. Ces préliminaires posés, rappelons brièvement le procédé de construction des groupes cherchés, tel qu'il a été établi dans le *Mémoire des Nuovi Lincei*.

Un groupe L de substitutions linéaires à n variables est dit *non indécomposable*, si les variables auxquelles il est rapporté peuvent être choisies de telle sorte qu'elles se répartissent en systèmes $\Sigma_1, \ldots, \Sigma_m$ contenant chacun n' variables et tels :

1° Que toute substitution de L remplace les fonctions linéaires des variables de chaque système par des fonctions linéaires des variables d'un même système;

2° Que la forme invariante Φ (s'il y en a une) soit une somme de fonctions partielles $\Phi_1, \ldots, \Phi_m$ ne contenant chacune que les variables d'un seul système.

Le cas où chaque système serait formé d'une seule variable n'est pas exclu.

Ceux des groupes à construire qui sont de cette sorte sont des deux espèces suivantes (*N. L.*, § III).

18. *Groupes semi-primaires.* — Leur existence suppose celle d'une forme invariante ayant pour expression $\Phi_1 + g\Phi_2$ où Φ_1, Φ_2 sont des fonctions semblables, contenant, l'une, les variables x_1, $x_2, \ldots, x_{n'}$ et l'autre les variables $y_1, y_2, \ldots, y_{n'}$.

Construisons un groupe L_1 primaire, résoluble et maximum parmi ceux qui admettent Φ_1 comme forme invariante et sont d'exposant 2. Soit L_1^0 le sous-groupe formé par ses substitutions propres.

Soient L_2, L_2^0 les groupes semblables aux précédents, mais formés avec les variables y.

Le groupe cherché L, qui doit être invariantif par rapport à Φ, sera formé des groupes L_1^0, L_2^0 combinés à la substitution

$$\begin{vmatrix} x_1, x_2, \ldots & y_1, y_2, \ldots \\ y_1, y_2, \ldots & gx_1, gx_2, \ldots \end{vmatrix}$$

laquelle est d'exposant 1. Si Φ est quadratique, elle sera du premier ou du second type suivant que $\left(\frac{-g}{p}\right)^{n'}$ sera égal à 1 ou à -1.

19. *Groupes décomposables.* — Leur construction demande :

1° Celle d'un groupe G transitif et résoluble permutant les divers systèmes $\Sigma_1, \ldots, \Sigma_m$ en remplaçant chaque variable par sa correspondante ;

2° Celle d'un groupe primaire L_1 de substitutions linéaires entre les variables de Σ_1 (assujetties d'ailleurs, s'il y a lieu, à reproduire à un facteur près, une forme Φ_1, auquel cas L_1 résultera de la combinaison d'une substitution impropre S_1 et d'un groupe propre L_1^0).

Soient L_k, S_k, L_k^0, Φ_k ce que deviennent L_1, S_1, L_1^0, Φ_1 lorsqu'on y remplace les variables de Σ_1 par celles de Σ_k. Il est évident que le groupe dérivé de G et de L_1 sera résoluble; qu'il contiendra $L_1^0, \ldots, L_m^0$, ainsi que la substitution $S = S_1 S_2 \ldots S_m$; enfin que le groupe L dérivé de G, S, $L_1^0, \ldots, L_m^0$ admettra la forme invariante

$$\Phi = \Phi_1 + \ldots + \Phi_m,$$

laquelle sera du premier type si elle est quadratique, à moins que m ne soit impair et les formes $\Phi_1, \ldots, \Phi_m$ du second type.

L'exposant de L sera d'ailleurs égal à celui de L_1.

Si, parmi les divers groupements des variables en systèmes dont le groupe cherché pourrait être susceptible, nous avons choisi l'un de ceux où les systèmes contiennent chacun le moindre nombre de variables, L_1 sera indécomposable; quant à G, nous avons déjà indiqué comment le problème de sa construction peut être résolu, ou tout au moins réduit au problème B. S'il n'est pas primitif, elle dépendra de la construction de groupes primitifs successifs $G_1, \ldots, G_i$ de degrés $q_1, \ldots, q_i$, les nombres q étant des puissances de nombres premiers et leur produit étant m.

Pour que le groupe L ainsi obtenu soit maximum, il faut évidemment que G et L_1 le soient. Donc, dans la suite des facteurs q ne doivent pas figurer deux nombres consécutifs égaux à 2; mais cette condition n'est pas suffisante. Il faut encore que chacun des groupes $(G_k, \ldots, G_i, L_1)$, et en particulier le dernier (G_i, L_1), soit maximum dans son espèce. Cette condition donnera lieu, comme on le verra plus loin, à quelques nouvelles exclusions.

20. Le procédé de construction qui vient d'être indiqué met, d'ailleurs, en lumière divers groupements en systèmes des variables

de L. Il est clair, en effet, que le groupe $(G_1, \ldots, G_k)$ représente des déplacements d'ensemble entre $q_1 \ldots q_k$ systèmes contenant chacun $q_{k+1} \ldots q_i n'$ variables, l'un d'eux étant formé des variables qui figurent dans le groupe $(G_{k+1}, \ldots, G_i, L_1)$.

Ces groupements en systèmes sont, en général, les seuls possibles. Nous aurons toutefois à constater un cas d'exception.

21. *Groupes complexes.* — Soient L, L', ... des groupes résolubles primaires contenant respectivement n variables $x_1, x_2, \ldots$; n' variables $y_1, y_2, \ldots$, etc. Leur réunion donnera un groupe résoluble de fonctions linéaires de $n + n' + \ldots$ variables.

Si L, L', ... admettent des formes invariantes $\Phi, \Phi', \ldots$ (toutes quadratiques ou toutes bilinéaires) les substitutions du groupe $L^0 + L'^0 + \ldots$ formé par la réunion de leurs sous-groupes propres n'altéreront pas la forme $\Phi + \Phi' + \ldots$.

Nous dirons qu'un groupe ainsi formé est *complexe*. Il joue un rôle analogue à celui des groupes intransitifs.

Pour qu'il soit maximum, il faut évidemment que chacun des groupes L, L', ... le soit. Mais on aura un cas d'exclusion pareil au deuxième cas (**8**).

Troisième cas d'exclusion. — Un groupe complexe ne sera pas maximum :

1° Si deux des groupes partiels L, L' sont semblables;

2° Ou si L' est un groupe décomposable formé de deux ou trois groupes semblables à L et d'un groupe G de substitutions qui les permutent entre eux.

22. *Groupes indécomposables.* — Soit L un de ces groupes; le groupe L^0, formé par ses substitutions propres, contiendra un sous-groupe invariant F, dit *premier faisceau* de L et formé des puissances d'une substitution génératrice f, dont l'ordre ω sera premier à p (*N. L.*, §§ IV et V).

Divers cas sont à distinguer pour la formation de F :

1° *Il n'y a pas de forme invariante.* — Les variables formeront ν séries conjuguées, de μ variables chacune. Nous représenterons celles de la première série par x_α, l'indice α variant de 0 à $\mu - 1$, et leurs $\nu^{\text{èmes}}$ conjuguées par x_γ.

Toute substitution réelle devant faire subir aux variables conju-

guées des altérations conjuguées, on simplifiera l'écriture en indiquant seulement ce qu'elle fait succéder à chaque variable de la première série.

Soit i une racine primitive de la congruence

$$i^{p^\nu-1} \equiv 1 \pmod{p}$$

La substitution f aura la forme

$$f = | \, x_0 \quad i x_0 \, |,$$

et son ordre ω sera $p^\nu - 1$.

Les substitutions de L ne pourront être choisies que parmi celles de la forme

$$P^\alpha Q,$$

P désignant la substitution

$$P = | \, x_0 \quad x_1 \, |,$$

et Q ne déplaçant plus les séries.

Si $\mu = 1$, L sera dérivé des substitutions génératrices f et P, et aura pour ordre ωn, n désignant le nombre des variables.

2° S'il y a une fonction invariante Φ, on pourra distinguer dans les groupes cherchés trois catégories distinctes :

23. *Première catégorie.* — Les variables se partagent en deux systèmes associés dont chacun contient ν' séries de μ variables; p^ν étant > 4.

Désignons encore par x_r les variables du premier système et par x'_r leurs associées. Si la forme Φ est quadratique, elle appartiendra au premier type; dans tous les cas, les variables d'un même système n'y figureront que linéairement.

Le groupe L sera d'exposant 1, car il contiendra la substitution

$$k = \begin{vmatrix} x_r & x_r \\ x'_r & g x'_r \end{vmatrix} \qquad (g \text{ racine primitive de } p).$$

La substitution f sera

$$f = \begin{vmatrix} x_r & i^{p^r} x_r \\ x'_r & i^{-p^r} x'_r \end{vmatrix} \qquad (i^{p^{\nu'}-1} \equiv 1),$$

et son ordre ω sera $p^{\nu'} - 1$.

Les substitutions de L^0 seront de la forme

$$R^\alpha P^\beta Q,$$

où

$$R = \begin{vmatrix} x_r & x'_r \\ x'_r & (-1)^\tau x_r \end{vmatrix}, \qquad P = \begin{vmatrix} x_r & x_{r+1} \\ x'_r & x'_{r+1} \end{vmatrix}$$

Q ne déplaçant plus les séries.

Cette substitution Q sera d'ailleurs déterminée par la transformation qu'elle fait subir aux variables x_0 de la première série du premier système; car leurs conjuguées subissent des altérations conjuguées; et leurs associées x'_r devront être soumises à la substitution adjointe, de telle sorte que la forme

$$\sum_r x_r x'_r$$

reste inaltérée.

Si $\mu = 1$, L sera dérivé des seules substitutions génératrices h, f, P, R; et L^0, dérivé de f, P, R, aura pour ordre

$$\omega = p^{\nu'} n,$$

n désignant le nombre des variables.

24. *Deuxième catégorie.* — On a encore $2\nu'$ séries, mais elles ne forment qu'un seul système, étant toutes conjuguées (les séries r et $\nu' + r$ sont associées). Si Φ est quadratique, elle sera du second type.

Déterminons i par la congruence

$$i^{p^{\nu'}-1} \equiv 1 \pmod{p},$$

L contiendra la substitution d'exposant 1

$$h = \left| x_0 \quad i^{\frac{p^{\nu'}-1}{p-1}} x \right|;$$

et la substitution

$$f = h^{p-1} = \left| x_0 \quad i^{p^{\nu'}-1} x_0 \right|$$

sera d'ordre $\omega = p^{\nu'} + 1$.

Les substitutions de L^0 seront de la forme

$$P^\beta Q,$$

Q ne déplaçant pas les séries et P désignant la substitution

$$P = \left| x_0 \; i^{\frac{p^{\nu'}-1}{2}} x_1 \right|.$$

(La substitution $|x_0 \; x_1|$ ne serait pas propre si Φ était bilinéaire.)

Si $\mu = 1$, L sera dérivé des substitutions k, f, P, et L^0 aura pour ordre

$$\omega . 2\nu' = 2n.$$

25. *Troisième catégorie.* — Elle n'existe que si p est impair. Il n'y a qu'une série, contenant μ variables x; f les multiplie toutes par le même facteur -1; donc $\omega = 2$.

Si $\mu = 1$, L sera formé des puissances de la substitution

$$|x \; gx|.$$

La forme Φ sera Ax^2 et L sera d'exposant 2.

Si $\mu > 1$, la nature de Φ et l'exposant de L seront déterminés plus loin.

26. La question posée étant résolue pour $\mu = 1$, il reste à achever la construction du groupe L lorsque $\mu > 1$.

Elle ne sera possible que si tous les facteurs premiers de μ divisent ω; et le groupe L répondra à l'une des décompositions de μ en un produit de facteurs

$$\mu = \pi^{\sigma}\pi'^{\sigma'}\ldots,$$

π, π', ... étant des nombres premiers, dont quelques-uns peuvent être égaux (*N. L.*, § VII).

Remplaçons l'indice unique x par un système d'indices ε, ε', ..., variables respectivement de 0 à $\pi^{\sigma}-1$ à $\pi'^{\sigma'}-1$, etc. Les substitutions Q, susceptibles de servir à la construction, seront nécessairement de la forme TT'..., où T est de la forme

$$T = \left| |\varepsilon\varepsilon'\ldots|_0 \quad \sum_{l} \alpha^{l}_{\varepsilon} |l\varepsilon'\ldots|_0 \right|,$$

T' de la forme analogue

$$T' = \left| |\varepsilon\varepsilon'\ldots|_0 \quad \sum_{l} \beta^{l}_{\varepsilon} |l\varepsilon'\ldots|_0 \right|,$$

etc.

(Les substitutions T sont évidemment échangeables aux substitutions T′, ...)

27. Désignons indifféremment par θ une racine de la congruence

$$\theta^{\pi} \equiv 1 \pmod{p}$$

ou la substitution d'ordre π

$$\theta = f^{\frac{\omega}{\pi}} = |[\varepsilon\varepsilon' \ldots]_0 \quad \theta[\varepsilon\varepsilon' \ldots]_0|;$$

L° contiendra un second faisceau h d'ordre $\pi^{2\sigma+1}$ jouissant des propriétés suivantes :

1° Ses substitutions sont de l'espèce T;

2° Il est invariant dans L et ne contient aucun sous-groupe jouissant de cette propriété (sauf celui formé des puissances de θ);

3° Il est dérivé de 2σ substitutions fondamentales $C_1, \ldots, C_{2\sigma}$ satisfaisant aux conditions

$$C_k^{\pi} = \theta^{u_k},$$
$$C_k C_i \equiv C_i C_k \theta^{(C_i C_k)}.$$

L'exposant u_k, que nous appellerons le *caractère* de la substitution C_k, sera toujours nul si π est impair; égal à 0 ou à 1 si $\pi = 2$, d'où $\theta = -1$.

L'exposant $(C_i C_k)$ sera dit l'*exposant d'échange* de C_i avec C_k. On a évidemment

$$(C_i C_k) = -(C_k C_i).$$

Soit

$$S = C_1^{\lambda_1} \ldots C_{2\sigma}^{\lambda_{2\sigma}} \theta^{\lambda}$$

une des substitutions de h. Son caractère (qu'il n'y a lieu de considérer que si $\pi = 2$) sera représenté par la forme quadratique

$$\Psi_\theta \equiv \sum_i u_i x_i^2 + \sum_{i,k} (C_i C_k) x_i x_k \pmod{2} \qquad (i = 1, \ldots, 2\sigma;\ k = 1, \ldots, i-1),$$

et son exposant d'échange avec une autre substitution de h,

$$S' = C_1^{\lambda'_1} \ldots C_{2\sigma}^{\lambda'_{2\sigma}} \theta^{\lambda'}$$

le sera par la forme bilinéaire gauche

$$\Psi_\theta = \Sigma (C_i C_k) X_i x_k \pmod{\pi} \qquad (i = 1, \ldots, 2\sigma;\ k = 1, \ldots, 2\sigma).$$

28. Les substitutions fondamentales C_i peuvent d'ailleurs être choisies de telle sorte qu'elles se partagent en σ couples.

$$\begin{matrix} A_1, & \dots & A_\sigma, \\ B_1, & \dots, & B_\sigma \end{matrix}$$

tels :

1° Que tous leurs exposants d'échange soient nuls, sauf pour deux substitutions d'un même couple, pour lesquels on aura

$$(A_k B_k) = -(B_k A_k) = 1.$$

2° Et, si $p = 2$, que toutes ces substitutions aient pour caractère o, sauf A_1 et B_1 dont le caractère commun u pourra être égal à o ou à 1.

La substitution

$$S = A_1^{x_1} B_1^{y_1} \dots A_\sigma^{x_\sigma} B_\sigma^{y_\sigma} \theta^{\lambda}$$

aura alors pour caractère

$$\Psi_q = u(x_1^2 + y_1^2) + \Sigma x_i y_i \qquad (\mathrm{mod}\, 2),$$

forme qui sera du premier ou du second type, suivant que u sera égal à o ou à 1.

Et son exposant d'échange avec la substitution

$$S' = A_1^{x_1} B_1^{y_1} \dots A_\sigma^{x_\sigma} B_\sigma^{y_\sigma} \theta^{\lambda}$$

sera représenté par la forme bilinéaire

$$\Psi_b = \Sigma(X_i y_i - x_i Y_i) \qquad (i = 1, \dots, \sigma),$$

29. Remplaçons l'indice ε par σ indices $\xi_1, \dots, \xi_\sigma$ variables chacun de o à $\pi - 1$. Les variables indépendantes $[\xi_1, \dots, \xi_\sigma, \varepsilon', \dots]_r$ pourront être choisies, si π est impair, de telle sorte que les substitutions A_k, B_k prennent la forme suivante (les indices non écrits étant inaltérés)

$$A_k = |\,[\dots \xi_k \dots]_0 \quad \theta^{\xi_k} [\dots \xi_k \dots]_0\,|,$$
$$B_k = |\,[\dots \xi_k \dots]_0 \quad [\dots \xi_{k+1} \dots]_0\,|.$$

Si $\pi = 2$, A_2, B_2, .., auront encore la même forme; mais si $u = 1$, A_1 et B_1 auront des expressions un peu différentes

$$A_1 = |\,[\xi_1 \dots]_0 \quad j\theta^{\xi_1} [\xi_1 \dots]_0\,|,$$
$$B_1 = |\,[\xi_1 \dots]_0 \quad (\alpha + \beta j \theta^{\xi_1}) [\xi_1 + 1 \dots]\,|,$$

j étant racine primitive de la congruence $j^4 \equiv 1 \bmod p$ et α, β un système de solutions (choisi à volonté) de la congruence

$$\alpha^2 + \beta^2 \equiv -1 \pmod p.$$

L^0 contiendra également d'autres seconds faisceaux d'ordre $\pi'^{2\sigma'+1}$,... qui pourront être ramenés à des formes normales analogues à la précédente. L'ensemble de ces premiers et seconds faisceaux constituera le *noyau* de L.

Ce noyau une fois construit, la forme invariante Φ sera déterminée à un facteur constant près. Si L est de troisième catégorie, on aura nécessairement

$$\tau - \Sigma u \equiv 0 \pmod 2,$$

car si cette condition n'était pas remplie, Φ serait identiquement nulle.

30. La réduction précédente à une forme normale des substitutions génératrices du noyau de L nous a servi comme moyen de démonstration dans le Mémoire des *Nuovi Lincei*. Mais ici, où nous nous bornons à en résumer les résultats, il n'est pas nécessaire de la supposer exécutée. L'exposition y gagnera en clarté.

Soient $\mathfrak{A}$ le groupe des substitutions homogènes à 2σ variables modπ qui reproduisent, à un facteur près, la forme Ψ_q si $\pi > 2$ ou la forme Ψ_h si π est impair, $\mathfrak{A}^0$ le groupe de ses substitutions propres ;

$$\Theta_k = |x_k \; x_{k+1}| \qquad (k = 1, \ldots, 2\sigma)$$

les substitutions génératrices de sa base $\mathfrak{B}$. A chaque substitution propre $\mathfrak{S}$ du groupe $\mathfrak{A}^0$, laquelle transforme Θ_k en

$$\Theta_k = \Theta_1^{\alpha_{1k}} \ldots \Theta_{2\sigma}^{\alpha_{2\sigma k}} \qquad (k = 1, \ldots, 2\sigma),$$

correspond une substitution de l'espèce T (1), définie aux puissances près de f, qui transforme de la même manière les substitutions

$$C_1, \quad \ldots, \quad C_{2\sigma}$$

génératrices de h (*N. L.*, § X).

(1) Les substitutions dont la combinaison permet de l'obtenir ont été indiquées (*N. L.*, n° 32).

Cette substitution T serait d'ailleurs facile à obtenir par la méthode des coefficients indéterminés. Si L doit admettre une forme invariante Φ, T ne l'altérera pas, à moins que les conditions ci-dessous ne soient satisfaites simultanément :

1° L est de troisième catégorie ;
2° 2 n'est pas résidu de π ;
3° La substitution $\mathfrak{S}$ est impaire.

Si ces conditions sont réunies, T multipliera Φ par g, racine primitive de p.

Les seules substitutions de l'espèce T qui puissent appartenir à L sont celles ainsi déterminées, jointes à celles dérivées de f et de h. Elles forment un groupe Γ isomorphe au groupe primitif $\mathcal{G}^0 = (\mathfrak{X}^0, \mathfrak{W})$, la substitution 1 de $\mathcal{G}^0$ correspondant à l'ensemble des puissances de f.

Nous pourrons dire pour abréger qu'une substitution de Γ est paire ou impaire, suivant que sa corrélative dans $\mathfrak{X}$ est elle-même paire ou impaire.

De là résulte le procédé suivant pour former les substitutions T du groupe cherché.

Construisons un groupe $\mathcal{L}$ résoluble et maximum contenu dans $\mathfrak{X}$. A ses substitutions propres correspondront dans Γ des substitutions qui seront celles que nous cherchons.

Celles des substitutions de L qui sont de chacune des formes T', ... s'obtiendront de même par la considération de groupes auxiliaires $\mathcal{L}'$, ... analogues à $\mathcal{L}$.

31. Nous aurons ainsi obtenu toutes les substitutions de L qui ne permutent pas les séries. Mais s'il y a plusieurs séries, il reste à déterminer celles qui les déplacent. On utilisera à cet effet les substitutions impropres des groupes $\mathcal{L}$, $\mathcal{L}'$, ...

Supposons par exemple que L soit de première catégorie. Si l'on peut déterminer dans $\mathcal{L}$, $\mathcal{L}'$, ... des substitutions $\mathfrak{S}_1$, $\mathfrak{S}'_1$, ... qui multiplient respectivement les fonctions invariantes Ψ, Ψ', ... par

$$(-1)^\alpha p^\beta \pmod{\pi}, \qquad (-1)^\alpha p^\beta \pmod{\pi'}, \qquad \ldots,$$

on aura dans L une substitution de la forme $R^\alpha P^\beta TT' \ldots$ correspondante au système des substitutions $\mathfrak{S}_1$, $\mathfrak{S}'_1$, ...

Pour que cette détermination soit possible, il faut et il suffit

que $(-1)^{\alpha} p^{\beta}$ soit résidu quadratique de tous ceux des nombres de la suite $\pi, \pi', \ldots$ pour lesquels le groupe auxiliaire ξ est d'exposant 2.

Cette condition est évidemment satisfaite si $\alpha = 0$, β pair. Le groupe L contiendra donc dans tous les cas une substitution de la forme P^2Q.

Elle devra l'être également pour $\alpha = 1$, $\beta = 0$, ou pour $\alpha = 1$, $\beta = 1$, car si L ne contenait aucune substitution permutant les deux systèmes, il ne serait pas indécomposable. Donc L devra nécessairement contenir une substitution de l'une des deux formes RQ, RPQ.

Si L est de deuxième catégorie, ou n'admet pas de forme invariante, $\varpi_1, \varpi'_1, \ldots$ devront multiplier $\Psi, \Psi', \ldots$ par

$$p^{\beta} \pmod{\pi}, \qquad p^{\beta} \pmod{\pi'}, \qquad \ldots,$$

ce qui est possible si β est pair, mais aura lieu également pour $\beta = 1$ si p est résidu de tous ceux des nombres $\pi, \pi', \ldots$ pour lesquels le groupe auxiliaire est d'exposant 2. Dans ce cas seulement, L contiendra une substitution de la forme PQ; mais il en contiendra toujours une de la forme P^2Q.

32. Il existe certains cas où l'on peut montrer *a priori* que certaines substitutions de la forme $R^{\alpha}P^{\beta}Q$ (ou de la forme $P^{\beta}Q$) appartiennent à L.

Supposons en effet que, parmi les substitutions de cette sorte, il en existe une U qui soit échangeable à toutes celles des seconds faisceaux $h, h', \ldots$; et soit S une substitution quelconque de L. La substitution $S^{-1}U^{-1}SU$ sera propre, ne déplacera pas les séries et sera échangeable aux substitutions de $h, h', \ldots$ (car S les transforme les unes dans les autres). Donc elle se réduira à une puissance de f. Donc U est permutable au groupe L; elle y sera donc contenue, car autrement elle pourrait lui être adjointe pour former un groupe plus général.

En particulier, si tous les nombres $\pi, \pi', \ldots$ sont égaux à 2, on vérifie immédiatement que les substitutions

$$P' = P(A_1B_1)^{\frac{p-1}{2}\alpha}(A'_1B'_1)^{\frac{p-1}{2}\alpha'}\ldots,$$
$$R' = R(A_1B_1)^{\alpha}(A'_1B'_1)^{\alpha'}\ldots$$

satisfont aux conditions imposées à U. Elles appartiennent donc à L.

33. Remarquons enfin que, si plusieurs des nombres π, π', ... sont égaux, celles de leurs substitutions qui ont pu être utilisées pour la construction de L formeront un groupe complexe invariantif pour la forme $\Psi' + \Psi'' + \ldots$. Il devra être maximum parmi ceux de cette espèce pour que L le soit. Cela pourra donner lieu à l'application du troisième cas d'exclusion (n° **21**).

34. Nous sommes maintenant en mesure de déterminer l'exposant d'un groupe L de troisième catégorie.

Si $\left(\frac{2}{p}\right) = +1$, cet exposant sera 2, L résultant de substitutions propres, jointes à la substitution qui multiplie toutes les variables par g.

Si $\left(\frac{2}{p}\right) = -1$, cet exposant ne sera égal à 2 que si les groupes auxiliaires $\mathfrak{L}$, $\mathfrak{L}'$, ... à 2σ, $2\sigma'$, ... variables (mod 2) qui servent à le former et qui laissent invariables les formes quadratiques Ψ, Ψ', ... (mod 2) ne renferment que des substitutions paires.

Soit $\mathfrak{L}$ l'un de ces groupes. Supposons-le, pour plus de généralité, décomposable. Il sera construit à l'aide d'un groupe Δ de déplacements entre les m systèmes et d'un groupe indécomposable Γ_1 à $2\sigma_1$ variables, $m\sigma_1$ étant égal à σ. Si Γ_1 est de première catégorie (ce qui ne peut avoir lieu que si Ψ est du premier type), ces substitutions sont de la forme $\mathfrak{R}^\alpha \mathfrak{P}^\beta \mathfrak{Q}$, et dans l'une d'elles au moins $\alpha = 1$. Or nous avons montré (*Journal de Liouville*, 7e série, t. II, 1916, p. 275 à 280) que les substitutions Δ, $\mathfrak{P}$, $\mathfrak{Q}$ sont paires et que $\mathfrak{R}$ est paire ou impaire en même temps que σ_1.

Supposons au contraire que Γ_1 soit de deuxième catégorie, ce qui arrivera nécessairement pour l'un au moins des groupes $\mathfrak{L}$ si Φ est bilinéaire; car, dans ce cas, Σu étant impair, l'un au moins de ces nombres sera égal à 1 et la forme Ψ qui lui correspond sera du second type.

Dans ce cas, L sera d'exposant 1. Nous allons le démontrer par un procédé de récurrence, qui établira en même temps que tout groupe indécomposable de deuxième catégorie à 2σ variables (mod 2) contient une substitution impaire.

En effet, les substitutions de Γ_1 sont de la forme $\mathfrak{P}^\beta \mathfrak{Q}$ et les substitutions Δ et $\mathfrak{Q}$ sont encore paires. Mais ici $\mathfrak{P}$ est impaire. L sera donc d'exposant 1 si $\mathfrak{L}$ contient une substitution où β soit égal à 1. Mais

cela arrivera nécessairement. C'est évident si chaque série dans Γ_1 n'a qu'une variable. S'il y en a plusieurs, la construction de Γ_1 dépendra de celles de groupes Λ, Λ', ... à $2s$ variables $(\mathrm{mod}\,\varpi)$, $2s'$ variables $(\mathrm{mod}\,\varpi')$, ..., ϖ, ϖ', ... étant des nombres impairs. Pour que Γ_1 ne contînt pas de substitutions de l'espèce demandée, il faudrait : 1° que l'un au moins des groupes Λ, Λ', ..., par exemple Λ, fût d'exposant 2, et par suite de troisième catégorie; 2° que $\left(\frac{2}{\varpi}\right)$ fût égal à -1. D'ailleurs ϖ étant impair, Λ admet une forme invariante bilinéaire.

Si donc la proposition à démontrer n'était pas vraie pour L, elle ne le serait pas pour Λ, qui a moins de variables.

35. Nous pouvons enfin achever la liste des exclusions nécessaires pour ne conserver que des groupes maxima.

Les groupes suivants, non indécomposables, doivent être rejetés comme contenus dans des groupes indécomposables.

Quatrième cas d'exclusion. — Sont à rejeter tous les groupes non indécomposables qui admettent une forme quadratique invariante Φ ne dépendant que de deux variables.

En effet, si Φ est du premier type, on aura

$$\Phi = xy.$$

Les substitutions invariantives seront de l'une des deux formes

$$|x, y \quad ax, by| \qquad \text{ou} \qquad |x, y \quad ay, bx|.$$

Elles dérivent toutes des suivantes :

$$k = |x, y \quad x, gy|, \qquad f = |x, y \quad gx, g^{-1}y|, \qquad h = |x, y \quad y, x|.$$

C'est un groupe résoluble indécomposable de première catégorie.

Si Φ est du second type et p impair, on aura

$$\Phi = x^2 - gy^2.$$

Soit i une racine primitive de la congruence

$$i^{p^2-1} \equiv 1 \qquad (\mathrm{mod}\,p).$$

On aura $g = i^{p+1}$, et Φ sera le produit des deux facteurs conjugués

$$z_0 = x + i^{\frac{p+1}{2}} y, \qquad z_1 = x - i^{\frac{p+1}{2}} y.$$

Les substitutions invariantives formeront un groupe résoluble indécomposable de deuxième catégorie, dérivé des substitutions

$$k = |z_0, z_1 \quad iz_0, i^p z_1|, \qquad f = k^{p-1}, \qquad P = |z_0, z_1 \quad z_1, z_0|.$$

Si Φ est du second type et $p = 2$, on aura

$$\Phi = x^2 + y^2 + xy.$$

et si l'on pose

$$i^3 \equiv 1 \pmod 2, \qquad z_0 = x + iy, \qquad z_1 = x + i^2 y,$$

on aura encore

$$\Phi = z_0 z_1,$$

et les substitutions invariantives formeront un groupe de deuxième catégorie, dérivé de

$$f = |z_0, z_1 \quad iz_0, i^2 z_1|, \qquad P = |z_0, z_1 \quad z_1, z_0|.$$

Les groupes ci-dessus contenant toutes les substitutions invariantives, tout autre groupe que l'on pourrait obtenir, étant contenu dans ceux-là, ne serait pas maximum.

36. *Cinquième et sixième cas d'exclusion.* — Les groupes décomposables sans forme invariante, où

$$q_i = 2, \qquad p^{n'} = 3 \text{ ou } 5,$$

doivent être rejetés.

En effet, si $p^{n'} = 3$, le groupe en question est contenu dans un groupe indécomposable ayant pour noyau

$$f = |x, y \quad -x, -y|. \qquad \begin{matrix} A = |x, y & x, -y|, \\ B = |x, y & y, x|. \end{matrix}$$

Si $p^{n'} = 5$, il le sera dans le groupe qui a le noyau

$$f = |x, y \quad -x, -y|. \qquad \begin{matrix} A = |x, y & 2x, -2y|, \\ B = |x, y & y, -x|. \end{matrix}$$

37. *Septième cas d'exclusion.* — C'est celui d'un groupe décomposable, où $q_i = 4$, $n' = 1$ et $p = 3$ s'il n'y a pas de forme invariante, ou un nombre impair quelconque, s'il y en a une.

S'il n'y a pas de forme invariante, d'où $p = 3$, le groupe (G_i, Γ_i)

est d'ordre 16-24 et formé des substitutions

$$|x, y, z, u \quad \pm x, \pm y, \pm z, \pm u| \qquad (\mathrm{mod}\,3),$$

jointes aux 24 permutations des lettres x, y, z, u. Mais il n'est pas maximum, car on voit sans peine qu'il est contenu dans le groupe qui a un premier faisceau dérivé de

$$f = |x, y, z, u \quad -x, -y, -z, -u|,$$

et un second faisceau dérivé des quatre substitutions

$$\mathrm{A} = |x, y, z, u \quad x, y, -z, -u|, \qquad \mathrm{A}_1 = |x, y, z, u \quad x, -y, z, -u|,$$
$$\mathrm{B} = (xz)(yu). \qquad \mathrm{B}_1 = (xy)(zu)$$

S'il y a une forme invariante, elle sera quadratique et aura pour expression

$$x^2 + y^2 + z^2 + u^2.$$

Les substitutions propres du groupe donné seront encore de la forme précédente. Il faudra y adjoindre la substitution impropre

$$g = |x, y, z, u \quad gx, gy, gz, gu| \qquad (\mathrm{mod}\,p),$$

où g est une racine primitive de p. Mais le groupe ainsi obtenu est contenu dans le groupe de troisième catégorie dont le noyau est dérivé de f, A, A_1, B, B_1, car celui-ci contient aussi la substitution g.

38. Les groupes suivants, qui, d'après leur mode de construction, pourraient être présumés indécomposables, contiennent un sous-groupe abélien invariant ne résultant pas des puissances d'une seule substitution; ils sont donc contenus dans des groupes décomposables et, par suite, ne sont pas maxima.

Huitième cas d'exclusion. — C'est celui des groupes L de première catégorie où $p^\nu = 3^2$.

On a ici $\omega = 3^2 - 1 = 8$; donc $\pi = \pi' = \ldots = 2$. L contient la substitution $\mathrm{R'P'}$ (**32**), dont la transformée par une substitution quelconque de L sera de la forme $\mathrm{R'P'}f^\rho$.

D'ailleurs, $(\mathrm{R'P'})^2 = (-1)^\tau$ est échangeable à toute substitution linéaire. On devra donc avoir

$$(\mathrm{R'P'}f^\rho)^2 = (\mathrm{R'P'})^2 = (-1)^\tau.$$

Mais R'P' transformant f en f^{-3}, on aura

$$(R'P'f^{\rho})^2 = (R'P')^2 f^{-2\rho}.$$

Donc

$$-2\rho \equiv 0 \pmod 8, \qquad \text{d'où} \qquad \rho \equiv 0 \pmod 4.$$

Donc les substitutions de L seront toutes permutables au sous-groupe dérivé de f^2 et de R'P'. D'ailleurs, ce sous-groupe est abélien; car R'P' transforme f^2 en $f^{-6} = f^2$.

39. *Neuvième cas d'exclusion.* — C'est celui des groupes L de deuxième catégorie, où $p^{\nu} = 2^3$.

On a ici

$$\omega = 2^3 + 1 = 9, \qquad \pi = \pi' = \ldots = 3.$$

La substitution P^3, dont le cube est l'unité, transforme f, A_1, B_1, ... en f^4, $A_1^4 = A_1$, B_1, ... Elle appartient donc à L et ses transformées par les substitutions de ce groupe seront de la forme $P^3 f^{\rho}$.

D'ailleurs

$$(P^3 f^{\rho})^3 = P^6 f^{(1+4+16)\rho} = f^{21\rho}$$

doit être égal à l'unité, d'où la condition

$$21\rho \equiv 0 \pmod 9, \qquad \text{d'où} \qquad \rho \equiv 0 \pmod 3.$$

Donc L admet le sous-groupe invariant dérivé de f^3 et de P^3. Mais ce sous-groupe est abélien, car P^3 transforme f^3 en $f^{12} = f^3$.

40. *Dixième cas d'exclusion.* — C'est celui des groupes L dont un second faisceau h dérive d'un seul couple de substitutions A_1, B_1 ayant le caractère $u = 0$.

Les substitutions de L étant permutables à h, le seront au sous-groupe dérivé de celles de ses substitutions qui sont d'ordre 4, lesquelles sont toutes des puissances de $A_1 B_1$. Donc L admet le sous-groupe invariant abélien dérivé de f, $A_1 B_1$. Ce sous-groupe n'est pas formé des puissances d'une seule substitution, à moins qu'on n'ait $\omega = 2$, d'où $f = -1 = (A_1 B_1)^2$.

Mais dans ce cas L devra encore être rejeté, puisqu'il admet un sous-groupe invariant abélien plus général que F.

41. Les sous-groupes suivants, quoique indécomposables, sont contenus dans d'autres groupes plus généraux.

Onzième cas d'exclusion. — C'est celui des groupes L sans forme invariante où $p^\nu = 3^2$.

On a ici

$$\omega = 3^2 - 1 = 8, \qquad \pi = \pi' = \ldots = 2.$$

L contient la substitution P', dont les transformées seront de la forme $P' f^\rho$. D'ailleurs, $P'^2 = (-1)^{\Sigma u}$ étant échangeable à toute substitution linéaire, on devra avoir

$$P'^2 = (P' f^\rho)^2 = P'^2 f^{4\rho}, \qquad \text{d'où} \qquad 4\rho \equiv 0 \pmod 8.$$

Donc ρ est pair.

Cela posé, si $\Sigma u \equiv 1 \pmod 2$, on aura

$$P'^2 = (f^2)^2 = f^4, \qquad P' f^2 = \ldots = f^2 P' f^4.$$

Donc L sera contenu dans le groupe qui a pour premier faisceau f^4 et pour seconds faisceaux, outre ceux de L, un dernier faisceau, dérivé des génératrices f^2 et P'.

Si Σu était pair, on remplacerait P', dans le raisonnement précédent, par la substitution $P' f$, qui jouit des mêmes propriétés, mais dont le carré est f^4.

42. *Douzième cas d'exclusion.* — C'est celui des groupes L de première catégorie, où $p^\nu = 5^2$.

On a ici $\omega = 5^2 - 1 = 24$, et chacun des nombres premiers $\pi, \pi', \ldots$, divisant ω, sera égal à 2 ou à 3.

La substitution R'P' transforme f en f^{-5} et a pour carré $(-1)^{\tau + \Sigma u}$. Elle est échangeable à toutes les substitutions $A_1, B_1, \ldots$ des faisceaux $h, h', \ldots$. Elle appartient donc à L et sera échangeable à toutes ses substitutions aux puissances près de f (**32**).

Soit $R'P' f^\rho$ l'une de ses transformées. On aura nécessairement

$$(R'P')^2 = (R'P' f^\rho)^2 = (R'P')^2 f^{-4\rho},$$

d'où

$$-4\rho \equiv 0 \pmod{24}, \qquad \rho \equiv 0 \pmod 6.$$

L admet donc un sous-groupe invariant dérivé de f^6 et de R'P'.

D'ailleurs R'P' est échangeable à f^4, car elle la transforme en $f^{-20} = f^4$; elle transforme d'autre part f^6 en $f^{-30} = -f^6$.

Donc, si $\tau + \Sigma u$ est impair, L sera contenu dans un groupe de troisième catégorie ayant pour seconds faisceaux $h, h', \ldots$ et $(f^6, R'P')$.

Si $\tau + \Sigma u$ était pair, R'P' serait d'ordre 2, le faisceau $(f^6, R'P')$ aurait pour caractère zéro, ce qui est inadmissible; mais R'P' pourrait être remplacée dans le raisonnement par $R'P'f^3$, qui est d'ordre 4.

43. *Treizième cas d'exclusion.* — C'est celui des groupes L de première catégorie, où $p^\nu = 5$ et $\tau + \Sigma u \equiv 1 \pmod 2$. On a ici $\omega = 1$, $\pi = \pi' = \ldots = 2$; et L contiendra la substitution R' échangeable à f^2, et dont le carré est $(-1)^{\tau+\Sigma u} = -1$. Les substitutions de L seront toutes permutables au groupe (f, R'); L sera donc contenu dans le groupe de troisième catégorie ayant un premier faisceau formé des puissances de f^2 et les seconds faisceaux $h, h', \ldots (f, R')$.

44. *Quatorzième cas d'exclusion.* — On rejettera également les groupes de deuxième catégorie, où $p^\nu = 3$ et $\tau + \Sigma u \equiv 1$.

La démonstration est identique à celle du numéro précédent, en y remplaçant R' par P'.

45. Deux derniers cas d'exclusion résultent de la considération suivante :

Soit toujours L un groupe résoluble à n variables $(\mathrm{mod}\, p)$ et à forme invariante Φ. Ses substitutions propres forment un groupe L^0 ne contenant, si p est impair, qu'une partie des substitutions de L.

Mais si Φ est bilinéaire, on pourra avoir à se servir de L comme groupe auxiliaire pour construire des groupes résolubles à plus de n variables. Nous avons vu que les substitutions de L^0 sont toujours utilisées dans cette construction; mais les substitutions impropres de L ne le seront que sous certaines conditions qui ne seront pas toujours remplies. Si donc il existe un groupe $\overline{L}$ ne contenant pas L, mais tel que $\overline{L}^0$ contienne L^0, certains groupes formés au moyen de l'auxiliaire $\overline{L}$ contiendraient ceux formés de même avec l'auxiliaire L, lesquels ne seraient pas maxima.

46. *Quinzième cas d'exclusion.* — Un groupe L de seconde catégorie où $p^\nu = 7$, $\tau = 1$ et $\Sigma u \equiv 0 \pmod 2$ ne devra être employé comme groupe auxiliaire que si l'une au moins de celles de ses substitutions qui multiplient Φ par un non résidu de 7 est utilisée dans la construction.

On a en effet

$$\omega = 7 + 1 \quad 8, \qquad \pi = \pi' = \ldots \quad 2.$$

L contient la substitution P′ dont le carré est $(-1)^{\tau+\Sigma u} = -1$. Ses transformées par les substitutions de L seront de la forme $P'f^{\rho}$; mais ρ sera nécessairement pair.

En effet, les substitutions permutables aux groupes h, h', ... résultant de la combinaison de P′ avec des substitutions des espèces T, T′, ..., forment respectivement des groupes K, K′, ... Supposons que le groupe K, par exemple, contînt une substitution T_1 qui transforme P′ en $P'f^{\rho_1}$, ρ_1 étant impair. L'ordre de K serait divisible par 8 et K résulterait de la combinaison de T_1 avec un sous-groupe invariant formé par celles de ses substitutions qui sont échangeables à P′. Les trois premiers facteurs de composition seraient donc égaux à 2.

Or cela est impossible, K étant isomorphe à un groupe $\mathfrak{K}$ formé de l'ensemble des substitutions qui laissent invariante une forme quadratique Ψ à 2σ variables (mod 2). Or un semblable groupe n'a en général que deux facteurs de composition, dont un seul est égal à 2; et si $\sigma = 2$, auquel cas il admet une décomposition plus complète, il n'a aucune substitution d'ordre 8 (**16**).

Les substitutions de L^0 seront donc permutables au faisceau dérivé de f^2 et de P′. D'ailleurs,

$$(f^2)^2 = P'^2 = f^4 = -1, \qquad P'f^2 = f^2P'.f^4.$$

L^0 sera donc contenu dans le groupe $\overline{L^0}$ de troisième catégorie construit sur le noyau

$$f^4, \quad h, \quad h', \quad \ldots \quad f^2, P').$$

En adjoignant au groupe L^0 la substitution g qui multiplie toutes les variables par g, racine primitive de 7, on obtiendra un nouveau groupe L′ contenant toutes les substitutions de L qui multiplient Φ par un résidu quadratique; et $\overline{L}$, contenant la substitution g, contiendra encore L′.

47. *Seizième cas d'exclusion.* — Un groupe L de première catégorie où $p^w = 7$, et où les circonstances suivantes sont réunies :

1° Le nombre n des variables de chaque série est une puissance de 2;

2° $\tau = 1; \qquad \Sigma u \equiv 0 \pmod 2$

ne devra être employé comme groupe auxiliaire que si l'une de celles de ses substitutions qui multiplient Φ par un non résidu de 7 est utilisée pour la construction.

Soit, en effet,

$$f,\ h,\ h',\ \ldots$$

son noyau. L^0 sera formé de la combinaison de substitutions T, T', ..., échangeables à f avec f (laquelle est d'ordre 6) et une deuxième substitution R', échangeable à celles de h, h', ... et transformant f en f^{-1}.

Or, considérons un groupe $\overline{L^0}$ de troisième catégorie admettant des seconds faisceaux $\overline{h}$, $\overline{h'}$ ... ayant respectivement autant de génératrices que h, h' et les mêmes caractères et un dernier second faisceau formé d'un seul couple de génératrices A, B ayant pour caractère 1. La forme $\overline{\Phi}$ qu'il laisse invariante sera d'un type $\overline{\tau}$ défini par la relation

$$\overline{\tau} + 1 + \Sigma u \equiv 0 \pmod 2.$$

Donc $\overline{\tau} = 1$ et $\overline{\Phi}$ sera bilinéaire ainsi que Φ. Le groupe $\overline{L^0}$ est formé de substitutions $\overline{T}$, $\overline{T'}$, ... jointes à des substitutions échangeables à toutes celles de $\overline{h}$, $\overline{h'}$; lesquelles résultent de la combinaison de A, B avec deux nouvelles substitutions, l'une U d'ordre 6 transformant circulairement les unes dans les autres les substitutions A, B, AB; l'autre V transformant A, B, U en B, A, U^2.

$\overline{L^0}$ contient un sous-groupe Λ d'indice 4 formé des substitutions U, V, $\overline{T}$, $\overline{T'}$, ... Mais les substitutions U, V et celles de $\overline{h}$, $\overline{h'}$, ... ont entre elles les mêmes relations que f, R' et les substitutions de h, h', ... On pourra donc, par un changement de variables, transformer U, V, $\overline{h}$, $\overline{h'}$, ... en f, R', h, h', ... et si l'on emploie pour la construction de $\overline{L^0}$ les mêmes groupes auxiliaires que pour celles de L^0, les substitutions $\overline{T}$, $\overline{T'}$, ... seront également transformées en T, T', ...; de sorte que L^0 se confondra (à la notation près) avec Λ, et sera contenu dans $\overline{L^0}$.

47 *bis*. Les exclusions précédentes sont suffisantes. Pour le montrer, nous devrons établir :

1° Que si L, $\overline{L}$ sont deux quelconques des groupes conservés, L ne pourra être contenu dans $\overline{L}$ s'il est formé d'une manière différente;

2° Si p étant impair, L, $\overline{L}$ admettent une forme invariante bilinéaire, il faudra, en outre, que L^0 ne soit pas contenu dans $\overline{L^0}$.

La première condition étant toujours satisfaite lorsque la seconde le sera, nous pouvons nous borner le plus souvent à considérer celle-ci, même dans les cas où elle cesserait d'être nécessaire.

Mais cette discussion est longue et difficile. Elle exige l'établissement préalable de diverses propriétés des groupes L^0.

Nous procéderons par récurrence en montrant que les deux propositions précédentes ne pourraient être en défaut, pour les groupes que l'on considère, que si elles l'étaient déjà pour d'autres groupes analogues contenant moins de variables.

L'analyse sera différente suivant que chacun des groupes L^0, $\overline{L^0}$ sera ou non complexe, décomposable ou non. Dans chacun de ces cas nous établirons que $\overline{L^0}$ ne peut contenir L^0 que si certaines inégalités numériques sont remplies. Or elles ne peuvent l'être que dans un petit nombre de cas particuliers dont la discussion relativement facile fera retrouver successivement les cas d'exclusion signalés ci-dessus nécessaires, sans en faire apparaître aucun autre.

III. — Les groupes présumés primaires et indécomposables le sont en réalité.

48. Nous démontrerons dans cette section que les exclusions signalées plus haut comme nécessaires une fois opérées :

1° *Les groupes* L *construits par la méthode des n*^{os} **22** *à* **31** *comme primaires et indécomposables le sont en réalité.*

2° *S'ils sont susceptibles d'être employés comme groupes auxiliaires, le sous-groupe* L^0 *formé par leurs substitutions propres est encore primaire et indécomposable.*

Rappelons la définition des groupes primaires ou indécomposables.

Un groupe est *primaire*, si y_1 étant une fonction linéaire quelconque des variables indépendantes $x_1, \ldots, x_n$; $y_1, y_2, \ldots$ ses transformées par les substitutions du groupe, il existe toujours n fonctions linéaires distinctes parmi leurs combinaisons linéaires $a_1 y_1 + a_2 y_2 + \ldots$

Il est *indécomposable*, s'il n'est pas possible de partager les variables en systèmes

$$(x_1 \ldots x_k), \quad (x'_1, \ldots x'_k), \quad \ldots$$

tels que chaque substitution du groupe remplace les fonctions linéaires

$a_1x_1 + \ldots + a_kx_k$ de l'un de ces systèmes par des fonctions linéaires des variables d'un même système.

Ces définitions supposent que les variables originaires $x_1, \ldots, x_n$ sont réelles. Mais la réduction à la forme normale du noyau de L° nous a conduit à leur substituer de nouvelles variables dans l'expression desquelles figure une quantité i le plus souvent imaginaire. Pour conserver les avantages de ce changement, il conviendra d'exprimer les fonctions linéaires à considérer au moyen de ces nouvelles variables, et d'accepter des valeurs imaginaires pour les coefficients $a_1, a_2, \ldots$

49. 1° L° *est primaire.* — En effet, soit y_1 une fonction réelle quelconque exprimée en fonction des nouvelles variables. Parmi les combinaisons linéaires de y_1 et de ses transformées, cherchons-en une Y qui contienne le moins de variables possible. Elle n'en contiendra qu'une seule.

Supposons en effet qu'on eût

$$Y = Y_r + Y_s + \ldots,$$

$Y_r, Y_s, \ldots$ contenant respectivement les variables des séries $r, s, \ldots$. La substitution f multipliant Y_r, Y_s par des facteurs différents, on pourra, en combinant Y avec sa transformée par f, obtenir une nouvelle fonction Y′ ne contenant plus les variables de la série s.

Donc Y ne peut contenir que les variables $[\xi_1\xi_2\ldots\xi'_1\xi'_2\ldots]_r$ d'une seule série. Si elle en contenait plus d'une, elles différeraient par la valeur de l'un au moins des indices ξ, par exemple ξ_1, et l'on aurait

$$Y = Y_a + Y_b + \ldots,$$

$Y_a, Y_b, \ldots$ contenant respectivement les termes où $\xi = a, b, \ldots$. La substitution A_1 multipliant Y_a, Y_b par des facteurs différents, transformerait Y en une fonction dont la combinaison avec Y donnerait une nouvelle fonction Y′ ne contenant plus les variables de Y_b.

Donc $Y = [\xi_1\xi_2\ldots\xi'_1\xi'_2\ldots]_r$ chacun des indices ξ, r ayant une valeur déterminée. Mais les substitutions $B_1, \ldots$ transformeront Y en fonctions analogues où les ξ prendront toutes les valeurs dont ils sont susceptibles. Enfin chacune de ces fonctions étant de la forme $a_1y_1 + a_2y_2 + \ldots$, où a_1, a_2 sont des imaginaires convenablement choisies, il suffira de remplacer celles-ci par leurs conjuguées pour obtenir les variables conjuguées correspondant aux autres valeurs de r.

Enfin pour les groupes de première catégorie il existe un second

système de variables $[\xi_1 \ldots]'_r$ associées aux précédentes; mais L^o contient une substitution qui permute les deux systèmes. Donc, dans tous les cas, les transformées de y_1 par les substitutions de L^o, combinées entre elles, donneront autant de fonctions distinctes qu'il existe de variables : L^o sera donc primaire.

30. Scolie. — *Le nombre des transformées différentes d'une fonction quelconque* Y *par les substitutions de* L^o *est au moins égal à* $\omega\mu$.

En effet, s'il y a deux systèmes associés, on peut admettre que Y contient les variables du premier système, car s'il n'y figurait que celles du second système on considérerait au lieu de Y sa transformée par la substitution qui échange les deux systèmes.

La fonction Y (ou la partie de cette fonction formée par les variables du premier système) sera une somme de fonctions conjuguées

$$Y_0 + \ldots + Y_\gamma + \ldots$$

dont la première ne contient que les variables $[\xi_1 \xi_2 \ldots]_0$ de la première série. Ses transformées auront une expression analogue.

Si nous supposons que Y_0 contienne deux variables où l'indice ξ_1 par exemple prenne des valeurs différentes, ses π transformées par les puissances de A_1 différeront les unes des autres par le rapport des coefficients correspondants à ces variables.

Si, au contraire, Y_0 ne contient que des variables où ξ_1 ait toujours la même valeur, ses π transformées par les puissances de B_1 seront encore différentes comme ne contenant pas les mêmes variables.

Le même raisonnement pouvant se faire pour chacun des indices ξ, on voit que la transformation de Y_0 par les substitutions des faisceaux h, h', ... donnera au moins μ fonctions différant les unes des autres, soit par les variables qu'elles contiennent, soit par les rapports des coefficients.

Chacune d'elles, transformée par les puissances de f, donnera ω transformées, différant les unes des autres par un facteur constant.

31. 2° L^o *est indécomposable.* — Supposons, en effet, qu'on puisse opérer une répartition des variables en plusieurs systèmes. Parmi les fonctions qui appartiennent à quelqu'un de ces systèmes, soit Y l'une de celles qui contiennent le nombre minimum de variables. Nous allons montrer qu'elle n'en contient qu'une seule.

Supposons tout d'abord qu'elle contînt des variables de m séries, a, b, ... On pourrait écrire

$$Y = Y_a + Y_b + \dots,$$

Y_a, Y_b, ... contenant respectivement les variables des séries a, b, ...

Les transformées de Y par les puissances de f sont au nombre de ω; chacune d'elles appartiendra à un des systèmes supposés. D'ailleurs deux quelconques d'entre elles ne sauraient appartenir au même système, si elles ne sont pas égales à un facteur constant près; car par leur combinaison on pourrait obtenir une nouvelle fonction appartenant encore à ce système, mais où l'une des fonctions partielles aurait disparu. Si donc on désigne par q le nombre des puissances de f qui multiplient Y par un facteur constant, on aura $\frac{\omega}{q}$ transformées appartenant à des systèmes différents et par suite linéairement distinctes. Mais elles s'expriment toutes au moyen des m fonctions Y_a, Y_b, ... On aura donc l'inégalité

$$\frac{\omega}{q} \leqq m \tag{1}$$

dont nous allons établir l'impossibilité.

52. 1° Supposons d'abord qu'il n'y ait pas de forme invariante. On aura $\omega = p^\nu - 1$.

D'autre part, soit δ le plus grand commun diviseur de ν, $b - a$, $c - a$, ... Les nombres a, b, ... appartenant tous à la suite

$$a, \quad a + \delta, \quad a + 2\delta, \quad \dots,$$

on aura

$$m \leqq \frac{\nu}{\delta}.$$

Enfin, une puissance quelconque de f multiplie Y_a, Y_b, ... par k^{p^a}, k^{p^b}, ..., k étant une racine de la congruence

$$k^{p^\nu - 1} \equiv 1 \pmod{p}.$$

Pour qu'elle multiplie Y par un facteur constant, il faudra donc qu'on ait

$$k^{p^a} \equiv k^{p^b} \equiv \dots \pmod{p},$$

d'où

$$k^{p^{b-a}} - 1 \equiv \dots \equiv 1 \pmod{p}.$$

et, par suite,

$$k^{p^\delta-1} \equiv 1 \pmod{p},$$

congruence qui a $p^\delta - 1$ racines. Donc $q = p^\delta - 1$.

L'inégalité (1) devient donc

$$\frac{p^\nu - 1}{p^\delta - 1} \geq \frac{\nu}{\delta} \qquad (\delta \text{ diviseur de } \nu).$$

Elle est évidemment impossible.

33. 2° Si L^0 est de première catégorie, soit d'abord $\nu' > 1$ et

$$Y = Y_a + Y_b + \ldots + Y_{a'} + Y_{b'} + \ldots$$

les séries a, b, ... appartenant au premier système, les séries a', b', ... à son associé.

Soit δ le plus grand commun diviseur de ν', $b - a$, ..., $b' - a'$, ... On aura

$$m = \frac{2\nu'}{\delta}.$$

D'autre part, une puissance de f multipliera Y_a, Y_b, ..., $Y_{a'}$, $Y_{b'}$, ... par k^{p^a}, k^{p^b}, ..., $k^{-p^{a'}}$, $k^{-p^{b'}}$, ... où $k^{p^{\nu'}-1} = 1$. Pour qu'elle multiplie Y par un facteur constant, il faudra donc qu'on ait,

$$k^{p^{\delta'}-1} \equiv 1 \pmod{p},$$

δ' étant le plus grand commun diviseur de δ et de $a + a'$, lequel est au plus égal à δ.

On aura donc l'inégalité

$$\frac{p^{\nu'} - 1}{p^{\delta'} - 1} = \frac{2\nu'}{\delta'},$$

où δ' divise δ, lequel divise ν'.

D'ailleurs $p^{\nu'} > 4$. Cette inégalité n'admettrait donc qu'une seule solution $p^{\nu'} = 3^2$, $\delta = \delta' = 1$. Mais ce cas est exclu (n° **38**).

Reste à considérer le cas où, ν' étant égal à 1, chacun des deux systèmes associés ne contient qu'une série. On aura alors

$$Y = Y_a + Y_{a'}$$

et $m = 2$. D'autre part k devant satisfaire à la relation $k^{p-1} \equiv 1 \pmod{p}$

sera réel. On aura, en outre, $k \equiv k^{-1}$ d'où $k \equiv \pm 1$. Donc $q = 2$ et l'inégalité devient

$$\frac{p-1}{2} \leq 2.$$

Elle serait satisfaite pour $p^{\nu'} = 5$.

Nous réserverons provisoirement l'examen de ce cas d'exception pour ne pas rompre la suite des raisonnements.

54. 3° Si L^0 est de deuxième catégorie, on a $2\nu'$ séries conjuguées et $m \leq \frac{2\nu'}{\delta}$, δ étant le plus grand commun diviseur de $2\nu'$, $b-a$, ...

D'autre part, k devra satisfaire aux deux congruences

$$k^{p^{\delta}-1} \equiv 1, \qquad k^{p^{\nu'}+1} \equiv 1 \pmod{p}.$$

Si δ ne divise pas ν', il sera égal à $2d$, d étant un diviseur de ν' tel que $\frac{\nu'}{d}$ soit impair. On aura, par suite,

$$p^{\delta} - 1 = (p^d - 1)(p^d + 1);$$

$p^d + 1$ divisera $p^{\nu'} + 1$, qui pourra, en outre, avoir (si p est impair) un facteur commun 2 avec $p^d - 1$. On aura donc $q \leq 2(p^d + 1)$ et, par suite,

$$\frac{p^{\nu'}+1}{2(p^d+1)} \leq \frac{2\nu'}{d}.$$

Cette inégalité ne peut avoir lieu $\left(\frac{\nu'}{d} \text{ étant impair}\right)$ que si $p^{\nu'} = 2^3$ et $d = 1$. Mais ce cas est exclu (n° **39**).

Si δ divise ν', on aura

$$k^{p^{\nu'}-1} \equiv 1$$

et comme $p^{\nu'} - 1$ et $p^{\nu'} + 1$ ne peuvent avoir d'autre diviseur commun que 2, on aura

$$\frac{p^{\nu'}+1}{2} \leq \frac{2\nu'}{\delta}.$$

Cette inégalité n'est possible que si $p^{\nu'} = 3$, $\delta = 1$. Nous réserverons encore l'examen de ce cas.

55. Il est donc établi (sauf les deux cas réservés) que l'un des sys-

tèmes dont on a supposé l'existence contient une fonction Y_a où ne figurent que les variables d'une seule série.

Ses transformées par les $\omega\mu^2$ substitutions du noyau de L^0 appartiendront chacune à un système. Or elles s'expriment au moyen de μ fonctions linéairement distinctes. Le nombre des systèmes s_1, s_2, ..., auxquels elles appartiennent ne peut donc dépasser μ.

La substitution f, multipliant chacune des fonctions précédentes par un facteur constant, ne déplacera aucun de ces systèmes.

Les μ^2 substitutions

$$A_1^{\alpha_1} B_1^{\beta_1} \dots A_\sigma^{\alpha_\sigma} B_\sigma^{\beta_\sigma} A_1'^{\alpha_1'} B_1'^{\beta_1'} \dots$$

permuteront transitivement les systèmes s précédents. Donc, l'une d'entre elles U laissera immobile un système donné s_1.

Elle ne déplacera aucun de ces systèmes s_1, s_2, ... Soit, en effet, S une substitution du noyau qui fasse succéder s_k à s_1. La substitution $S^{-1}US$ ne déplacera pas s_k; mais elle est de la forme Uf^ρ et f ne déplace pas s_k; dont U le laisse également immobile.

Celles des substitutions de L^0 qui ne déplacent pas les séries permutent également les systèmes s entre eux. Si T est l'une d'elles, la transformée $T^{-1}UT$ ne les déplacera pas.

Or, si nous supposons pour fixer les idées, que dans la substitution U l'un au moins des exposants $\alpha_1, \beta_1, \dots, \alpha_\sigma, \beta_\sigma$ ne soit pas nul, les transformées $T^{-1}UT$ combinées entre elles reproduisent tout le second faisceau

$$h = \begin{pmatrix} A_1, \dots, A_\sigma \\ B_1, \dots, B_\sigma \end{pmatrix}.$$

Or les transformées de Y_a par les substitutions de ce faisceau dépendent linéairement de π^σ fonctions distinctes, qui toutes feront partie du même système. Le nombre des systèmes s_1, ..., ne pourra donc surpasser $\mu\pi^{-\sigma}$, nombre inférieur à celui $\mu^2\pi^{-2\sigma}$ des substitutions de la forme $A_1'^{\alpha_1'} B_1'^{\beta_1'} \dots$. Par un raisonnement pareil au précédent, on verra qu'il existe un second faisceau h' dont les substitutions laissent immobiles tous les systèmes s_1, ..., et que le nombre de ceux-ci ne pourra pas dépasser $\mu\pi^{-\sigma}\pi'^{-\sigma'}$. Continuant ainsi, on arrive finalement à cette conclusion que toutes les fonctions des variables de la série a appartiennent à un seul système.

Chacune de ces fonctions Y_a, exprimée au moyen des variables

réelles $x_1, \ldots, x_n$, sera de la forme

$$a_1 x_1 + \ldots + a_k x_k$$

où les a sont des quantités complexes. En les remplaçant par leurs conjuguées, on obtiendra les fonctions $Y_1, \ldots$, conjuguées de Y_a qui seront également linéaires en $x_1, \ldots, x_k$ et, par suite, appartiendront au même système.

Donc, sauf pour les groupes de première catégorie, aucune décomposition en plusieurs systèmes n'est possible, puisqu'ils se réduiraient à un seul contenant toutes les variables.

Pour les groupes de première catégorie, on a une décomposition toute trouvée en deux systèmes associés; mais elle ne satisfait pas à la seconde condition, imposée par la définition des groupes indécomposables à forme invariante Φ (**17**). Car ici la forme Φ, bilinéaire par rapport aux variables des deux systèmes, ne peut évidemment pas se décomposer en deux formes partielles $\Phi_1 + \Phi_2$ où ces variables figurent séparées.

56. Passons à l'examen des deux cas réservés.

Groupes de première catégorie où $p' = 5$. — Dans un semblable groupe L, on a deux séries associées, contenant respectivement des variables x et des variables x'; L contient la substitution impropre

$$k = | x, x' \quad x, gx' | \qquad (g = 3).$$

L^0 a pour noyau

$$f = | x, x' \quad gx, g^{-1}x' |, \qquad h = \begin{pmatrix} A_1, & \ldots, & A_\sigma \\ B_1, & \ldots, & B_\sigma \end{pmatrix}, \quad h', \quad \ldots.$$

Les nombres π, π', ... divisant 4, seront égaux à 2; donc

$$\theta = \theta' = \ldots = -1.$$

S'il y avait une décomposition possible en systèmes, leurs fonctions seraient de la forme

$$X + X',$$

X et X' contenant respectivement les variables des deux séries. Si l'une de ces fonctions se réduisait à la forme X, on pourrait achever la démonstration comme dans le cas général.

Or, si la forme invariante Φ est quadratique, L ne pouvant être

employé comme groupe auxiliaire, il suffit de prouver qu'il n'est pas décomposable. On peut donc considérer les transformées de $X + X'$ par les puissances de k. Ces fonctions $X + g^\rho X'$ au nombre de 4 ne dépendent que des deux variables X et X'; donc deux d'entre elles appartiendront au même système, qui contiendra également une fonction des variables d'une seule série, résultant de leur combinaison.

Si Φ est bilinéaire, il faudra démontrer que L^0 est indécomposable. Cela sera établi si nous arrivons à prouver qu'une puissance impaire de f, telle que f^ρ, laisse quelque système immobile; car il contiendra les deux fonctions distinctes $X + X'$ et $g^\rho X + g^{-\rho} X'$ et, par suite, X et X'.

Or, l'hypothèse contraire va nous amener à une contradiction.

57. Tout d'abord, le nombre des systèmes ne peut surpasser celui 2μ des variables. Or, il existe $2\mu^2$ substitutions de la forme

$$f^\rho A^{\alpha_1} B^{\beta_1} \ldots A_1'^{\alpha_1'} B_1'^{\beta_1'} \ldots,$$

où $\rho = 0$ ou 1.

Donc, parmi ces substitutions, il en existera une U qui ne soit pas puissance de f et qui laisse immobile un système donné s_1.

Soit S une autre substitution du noyau qui remplace s_1 par un autre système s_k; $S^{-1}US$ ne déplace pas s_k; mais cette substitution est égale à U ou à $0U$, 0 multipliant toutes les variables par -1 et, par suite, laissant s_k immobile.

On pourra en conclure, comme au n° **55**, que les μ fonctions que les substitutions de h, h', ... font succéder à $X + X'$ appartiennent à un même système. Donc on n'aurait que deux systèmes, que f échangerait entre eux.

58. Cela posé, L^0 contient la substitution

$$R' = R(A_1 B_1)^\alpha (A_1' B_1')^{\alpha'} \ldots$$

dont les transformées par les substitutions de l'espèce T qui laissent Φ invariable et sont permutables à h seront de la forme $R' f^\rho$.

Le groupe K formé par ces substitutions T est isomorphe à un groupe $\mathfrak{X}$ de substitutions linéaires laissant invariante la forme ψ quadratique à 2σ variables mod 2 qui correspond au faisceau h. Il contient un seul sous-groupe invariant K' d'indice 2 formé par celles de ses substitutions dont les corrélatives dans $\mathfrak{X}$ sont paires.

Il contient d'ailleurs la substitution

$$T=\left|\begin{array}{ll}[\xi_1\ldots] & \theta^{\xi_1}[\xi_1\ldots]+[\xi_1+1,\ldots]\\ [\xi_1\ldots]' & g'^{\theta^{\xi_1}}[\xi_1\ldots]'+[\xi_1+1,\ldots]';\end{array}\right| \ (^1)$$

laquelle transforme A_1, B_1, R' en B_1, A_1, $R'f^{1+2u}$.

Celles des substitutions de K qui transforment R' en $R'f^\rho$ (ρ pair) forment évidemment dans K un sous-groupe invariant d'indice 2, qui se confondra nécessairement avec K'. Au contraire, toutes celles de ces substitutions qui correspondent aux substitutions impaires de K transformeront R' en $R'f^\rho$ (ρ impair).

Or, L^0 contiendra nécessairement une de ces substitutions ; car pour éviter de tomber dans un cas exclu (**43**), il faut supposer

$$\tau+\Sigma u\equiv 0 \pmod 2.$$

D'ailleurs, Φ étant bilinéaire, on a $\tau=1$. Donc l'un au moins des nombres u, u', ... sera égal à 1 (nous pouvons supposer que c'est u). Donc la forme ψ sera du second type; et le groupe auxiliaire Λ contenu dans $\mathfrak{H}$ qui sert à la construction de L^0 contiendra une substitution impaire (**34**).

Cela posé, si la substitution R' laisse les systèmes immobiles (ou les échange), sa transformée $R'f^\rho$ les laissera aussi immobiles (ou les échangera). Donc une substitution f^ρ où ρ est impair ne les déplace pas, contrairement à ce qui était supposé.

59. *Groupes de deuxième catégorie où* $p^{\nu'}=3$. — Le groupe L contient toutes les substitutions qu'il aurait en l'absence de forme invariante. Il est donc indécomposable.

Mais si la forme Φ est bilinéaire, il faut encore établir que L^0 est indécomposable. La démonstration est identique à la précédente. Après avoir montré qu'il ne peut y avoir plus de deux systèmes, on remplacera dans le raisonnement la substitution R' par celle-ci :

$$P'=P(A_1B_1)^u(A_1'B_1')^{u'}\ldots$$

et T par la substitution

$$T_1=\left|\begin{array}{ll}[\xi_1\ldots]_s & i\left\{\theta^{\xi_1}[\xi_1\ldots]_0+[\xi_1+1,\ldots]_0\right\}\\ [\xi_1\ldots]_1 & i^3\left\{\theta^{\xi_1}[\xi_1\ldots]_1+[\xi_1+1,\ldots]_1\right\}\end{array}\right|$$

laquelle transforme encore A_1, B_1, P' en B_1, A_1, $P'f^{1+2u}$.

(1) Les indices non inaltérés ne sont pas écrits.

IV. — Cas où ni L^0, ni $\overline{L^0}$ ne sont indécomposables.

60. Il est évident qu'un groupe $\overline{L^0}$ décomposable ne peut contenir un groupe L^0 indécomposable, si celui-ci l'est réellement, ainsi qu'il a été démontré dans la section précédente.

Nous établirons dans celle-ci :

1° Que *si* L^0 *est décomposable et contenu dans* $\overline{L^0}$, *il lui sera identique ;*

2° Que *si* L^0 *est complexe,* $\overline{L^0}$ *ne peut le contenir.*

61. LEMME. — *Le nombre* N *des transformées différentes d'une fonction linéaire quelconque* φ *par les substitutions d'un groupe primaire* L^0 *à n variables* mod p *ne peut être inférieur à* $n+1$. *Il surpassera même ce nombre, sauf pour quelques groupes exceptionnels que nous allons déterminer :*

1° Si L^0 est indécomposable, on aura $N \geqq \omega\mu$ (**50**). Or, s'il n'y a pas de forme invariante, on aura

$$\omega\mu = (p^\nu - 1)\mu, \qquad n+1 = \mu\nu + 1 \qquad (p^\nu > 2);$$

Si L^0 est de première catégorie,

$$\omega\mu = (p^{\nu'} - 1)\mu, \qquad n+1 = 2\mu\nu' + 1 \qquad (p^{\nu'} > 4);$$

S'il est de deuxième catégorie,

$$\omega\mu = (p^{\nu'} + 1)\mu, \qquad n+1 = 2\mu\nu' + 1;$$

S'il est de troisième catégorie,

$$\omega\mu = 2\mu, \qquad n+1 = \mu + 1 \qquad (p \text{ impair}).$$

La comparaison de ces valeurs montre l'exactitude de notre proposition, les groupes exceptionnels étant les suivants :

Groupes sans forme invariante,

$$p^\nu = 3, \qquad \mu = 1, \qquad n = 3;$$

Groupes de première catégorie,

$$p^{\nu'} = 2^3, \qquad \mu = 1, \qquad n = 6;$$

Groupes de deuxième catégorie,

$$p^{\nu'}=2, \quad \mu=1, \quad n=2;$$
$$p^{\nu'}=2^2, \quad \mu=1, \quad n=4;$$

Groupes de troisième catégorie,

$$p \text{ impair}, \quad \mu=1, \quad n=1.$$

2° Si L^0 est décomposable, on aura m systèmes $s_1, \ldots, s_m$ contenant chacun n' variables, avec $n=mn'$. Et L^0 s'obtiendra par la combinaison de m groupes indécomposables $L_1^0, \ldots, L_m^0$, opérant respectivement sur les n' variables des divers systèmes, avec un groupe transitif G de déplacements d'ensemble.

Soit

$$\varphi=\varphi_1+\ldots+\varphi_k,$$

où $\varphi_1, \ldots, \varphi_k$ contiennent respectivement les variables des systèmes $s_1, \ldots, s_k$. Si $k<m$, G contiendra une substitution qui remplace s_1 par s_{k+1}. Elle transforme φ en une fonction

$$\varphi'=\varphi_{k+1}+\ldots$$

contenant les variables de k systèmes, dont quelques-uns pourront être les mêmes qui figurent dans φ. Désignons les autres par

$$\varphi_{k+1}, \quad \varphi_{k+2}, \quad \ldots.$$

Si $m>2k$, on obtiendra de même une transformée

$$\varphi''=\varphi_{2k+1}+\ldots.$$

Continuant ainsi, on obtiendra une suite de transformées $\varphi, \varphi', \ldots$ dans chacune desquelles figure un système que ne contenaient pas les précédentes. Leur nombre est au moins égal à $\frac{m}{k}$. Il sera un entier supérieur à ce nombre, s'il est fractionnaire.

Chacune de ces fonctions $\varphi, \varphi', \ldots$ transformée par les substitutions de $L_1, \ldots, L_m$ donnera au moins $(n'+1)^k$ transformées différentes. On aura donc

$$N \geq \frac{m}{k}(n'+1)^k,$$

nombre évidemment supérieur à $n+1=mn'+1$. Le lemme est donc démontré, et les seuls groupes exceptionnels sont ceux déjà signalés.

62. THÉORÈME. — *Le groupe* L^0 *étant supposé décomposable, ses variables pourront admettre divers groupements en systèmes. Mais ceux indiqués au n° 20 seront les seuls possibles.*

Soit, en effet, $s_1, \ldots, s_m$ celle de ces décompositions où le nombre n' des variables de chaque système est maximum; L^0 résultera de la combinaison de groupes semblables $L_1^0, \ldots, L_m^0$ avec un groupe G de déplacements d'ensemble, lequel sera primitif.

Soit $\overline{s_1}, \overline{s_2}, \ldots$ une autre décomposition en systèmes. Chacune des fonctions φ qui appartiennent à l'un de ces nouveaux systèmes $\overline{s}$ sera de la forme

$$\varphi = X_1 + \ldots + X_m = X_1 + Y,$$

X_k étant une fonction linéaire des variables de s_k.

Supposons que les groupes $L_1^0, \ldots$ ne soient pas exceptionnels (ce qui arrivera nécessairement s'ils sont décomposables). Transformons φ par les substitutions de L_1^0. Chacune de ces transformées

$$X_1 + Y, \quad X_1' + Y, \quad \ldots$$

appartiendra à l'un des nouveaux systèmes $\overline{s}$; elles ne dépendent que des m variables de L_1^0 et de la fonction complémentaire Y; mais leur nombre est supérieur à $m + 1$; elles ne peuvent donc être linéairement distinctes et deux d'entre elles appartiendront à un même système $\overline{s_1}$ qui contiendra également leur différence, laquelle est de la forme X_1.

Les transformées de cette fonction particulière X_1 par les substitutions de L_1^0 appartiendront toutes à l'un des systèmes $\overline{s}$. Soient $\overline{s_1}, \ldots, \overline{s_k}$ ceux de ces systèmes dont quelque fonction dépend ainsi des seules variables de L_1^0. Aucun de ces systèmes ne pourra contenir de fonction dans l'expression de laquelle figurent des variables autres que celles de L_1^0.

Supposons, en effet, que $\overline{s_1}$, qui contient la fonction X_1, contînt une autre fonction $X_2 + Z$ où figurent les variables de L_2^0. Les substitutions de L_2^0 n'altérant pas X_1, ne déplaceront pas le système $\overline{s_1}$. Il contiendra donc les transformées

$$X_2 + Z, \quad X_2' + Z, \quad \ldots$$

et leurs différences $X_2' - X_2, \ldots$ dont la combinaison reproduit toutes les variables du groupe primaire L_2^0. Les substitutions de L_1^0 laissant ces fonctions invariables ne déplaceraient pas le système $\overline{s_1}$ qui contien-

drait les transformées X_1, X'_1, ... de X_1, et, par suite, toutes les variables de L_1^0. Donc, $\overline{s_1}$ contiendrait plus de variables que s_1, contrairement à l'hypothèse.

Chacun des anciens systèmes $s_1, \ldots, s_m$ se confond donc, si $k = 1$, avec un des systèmes nouveaux $\overline{s_1}, \ldots$; si $k > 1$, il est formé de la réunion de k d'entre eux, $\overline{s_1}, \ldots, \overline{s_k}$. Dans ce dernier cas, L_1^0 est décomposable, et on pourra lui appliquer les mêmes raisonnements qu'à L^0.

63. Ces raisonnements ne seraient pas applicables, si les groupes $L_1^0, \ldots, L_m^0$ étaient exceptionnels. Il pourrait, en effet, arriver qu'aucun des systèmes $\overline{s}$ ne contînt de fonction telle que X_1, où ne figurent que les variables de s_1. Soit dans ce cas

$$\Phi = X_1 + X_2 + Y$$

une fonction de l'un des systèmes $\overline{s}$. Si n' est le nombre des variables de chaque système s, les transformées de Φ par les substitutions de L_1^0 et de L_2^0 appartiendront chacune à un système $\overline{s}$. Elles dépendent de $2n'+1$ variables et leur nombre est au moins égal à $(n'+1)^2$. Elles ne peuvent donc être toutes distinctes; donc deux d'entre elles sont nécessairement contenues dans un même système $\overline{s_1}$. Il contiendra leur différence, qui est de la forme $X_1 + X_2$. Les transformées de cette fonction par les substitutions de (L_1^0, L_2^0) appartiendront chacune à un système $\overline{s}$. Leur combinaison reproduit toutes les variables de L_1^0 et de L_2^0.

Soient $\overline{s_1}, \ldots, \overline{s_k}$ les systèmes ainsi obtenus. On voit comme précédemment qu'aucune de leurs fonctions ne peut contenir dans son expression des variables autres que celles de L_1^0, L_2^0. L'ensemble des deux systèmes s_1, s_2 est donc formé par la réunion des k systèmes $\overline{s_1}, \ldots, \overline{s_k}$ dont les fonctions sont de la forme $X_1 + X_2$, aucune d'elles ne se réduisant d'ailleurs à X_1 ni à X_2.

Nous allons montrer que cela est impossible.

64. Soit en effet n' le nombre des variables de L_1^0; le groupe (L_1^0, L_2^0) en contient $2n'$ qui doivent se répartir également entre les systèmes $\overline{s_1}, \ldots, \overline{s_k}$; donc k divise $2n'$. Mais d'autre part les substitutions de L_1^0 donnent de la fonction $X_1 + X_2$ au moins $n'+1$ transformées

différentes, qui ne peuvent appartenir à un même système $\bar{s}$, car il contiendrait leur différence, qui est de la forme X_1. Donc $k \geq n' + 1$. Ces deux résultats ne peuvent se concilier que si $n' = 1$. Or nous n'avons que deux groupes exceptionnels satisfaisant à cette condition, à savoir, s'il n'y a pas de forme invariante, $p^\nu = 3$, $n = 1$, ou si L_1^0 est de troisième catégorie, $\mu = n = 1$, p quelconque. Dans les deux cas, le groupe (L_1^0, L_2^0) est formé des substitutions

$$(x, y, \pm x, \pm y)$$

et l'on a deux systèmes $\overline{s_1}$, $\overline{s_2}$ dont l'un contient la fonction

$$X_1 + X_2 = ax + by$$

et l'autre la fonction

$$ax - by.$$

Il faut ici supposer $m > 2$ pour ne pas tomber dans un cas exclu (**35**) et (**36**). Mais alors les groupes L_3^0, ... seront formés de substitutions des formes

$$|z \pm z|, \quad |u \pm u|, \quad \ldots,$$

Et le groupe G, étant primitif, contiendra une substitution S qui, laissant x immobile, remplace y par une autre variable z. La substitution S transformerait $ax + by$ et $ax - by$ en deux nouvelles fonctions $ax + bz$, $ax - bz$ appartenant à des systèmes $\overline{s_3}$, $\overline{s_4}$ différents des précédents. On aurait ainsi quatre fonctions linéairement distinctes des trois variables x, y, z.

Il est donc établi que les systèmes $\bar{s}$ représentent l'un des groupements en systèmes indiqués au n° **20**. Par suite L^0 résultera de la combinaison d'un groupe primaire $\mathfrak{L}^0$ opéré entre les variables de $\overline{s_1}$ et d'un groupe $\mathfrak{G}$ de déplacements d'ensemble entre les systèmes $\bar{s}$.

65. Cela posé, supposons que L^0 soit contenu dans un autre groupe $\overline{L}^0$ admettant une décomposition des variables en systèmes $\overline{s_1}$, ... et résultant de la combinaison des deux groupes $\overline{G}$ et $\overline{L}_1^0$. L^0 admettant cette même décomposition résultera, comme on vient de le voir, de la combinaison des deux groupes analogues $\mathfrak{G}$ et $\mathfrak{L}^0$ qui devront être respectivement contenus dans $\overline{G}$ et $\overline{L}_1^0$. Mais dans ces derniers groupes le nombre des variables étant moindre que dans $\overline{L}^0$

on doit supposer le théorème démontré. Donc $\mathcal{G}$, $\mathfrak{L}^0$, L^0 sont identiques à $\overline{G}$, $\overline{L_1^0}$, $\overline{L^0}$.

66. Soient maintenant $\overline{L^0}$ un groupe décomposable : $\overline{s_1}$, ..., $\overline{s_m}$ les systèmes minima entre lesquels ses variables puissent être réparties; $\overline{G}$, $\overline{L_1^0}$, ..., $\overline{L_m^0}$ les groupes dont la combinaison produit $\overline{L^0}$.

Supposons que $\overline{L^0}$ contienne un groupe complexe L^0 résultant de la combinaison de groupes primaires partiels L_a^0, L_b^0, ... dépendant chacun d'une partie des variables.

Si le groupe L_a^0 n'est pas exceptionnel, on verra, comme au n° **64**, qu'il a pour variables celles d'un certain nombre des systèmes $\bar{s}$, tels que $\overline{s_1}$, ..., $\overline{s_k}$ et s'obtient en combinant des groupes $\mathfrak{L}_1^0$, ..., $\mathfrak{L}_k^0$ avec un groupe $\mathcal{G}_a$ de déplacement d'ensemble.

Les groupes $\mathfrak{L}_1^0$, ..., $\mathfrak{L}_k^0$ étant contenus dans les groupes L_1^0, ..., L_k^0 de moins de n variables, leur seront identiques.

Si donc aucun des groupes L_a^0, L_b^0, ... n'est exceptionnel, L^0 résultera de la combinaison des groupes L_1^0, ..., L_m^0 avec un groupe $(\mathcal{G}_a, \mathcal{G}_b, \ldots)$ de déplacements d'ensemble des systèmes $\bar{s}$. Ce groupe intransitif devrait être contenu dans le groupe transitif $\overline{G}$, opéré sur m objets seulement; cela est impossible.

67. La présence de groupes exceptionnels dans la suite L_a^0, L_b^0, ... n'infirme pas ce résultat. Supposons en effet que L_a^0 n'étant pas exceptionnel, les groupes suivants L_b^0, L_c^0, ... le soient. Les variables de L_a^0 étant celles des systèmes $\overline{s_1}$, ..., $\overline{s_k}$, celles des systèmes suivants $\bar{s}_{k+1}$, ... seront de la forme

$$\varphi = X_a + X_b + X_c + \ldots.$$

Si l'on peut établir que l'une d'elles se réduit à la forme X_b, on en conclura comme tout à l'heure que L_b^0 a pour variables celles de quelques-uns des systèmes $\bar{s}$.

Or supposons d'abord que φ se réduise à $X_a + X_b$. Si n_b est le nombre des variables de L_b^0, les $n_b + 1$ transformées $\varphi_1, \varphi_1', \ldots$ de φ par les substitutions L_b^0 appartiendraient à des systèmes $\bar{s}_{k+1}$, ... tous différents de $\bar{s}_1$, ..., $\bar{s}_k$. Elles ne peuvent être linéairement distinctes, car en les combinant de manière à éliminer les variables de L_b^0, on arriverait à ce résultat inadmissible que X_a serait à la fois fonction des

variables de $\bar{s}_1, \ldots, \bar{s}_k$, et fonction de celles de $s_{k+1}, \ldots$. Donc deux des fonctions $\varphi_1, \varphi'_1, \ldots$ appartiendront au même système. Il contiendra leur différence qui est de la forme X_b.

Supposons au contraire que φ contienne à la fois X_b et X_c. On verra comme au n° **65** : 1° qu'il existe des fonctions de la forme $X_b + X_c$ appartenant à un système $\bar{s}$; 2° que les $n_b + n_c$ variables des groupes L_b^0, L_c^0 résultent de la combinaison de telles fonctions. Le nombre des systèmes entre lesquels ces fonctions se répartissent doit être un diviseur de $n_b + n_c$. Mais comme on suppose d'autre part qu'aucune de ces fonctions ne se réduit à X_b ou à X_c, ce nombre sera au moins égal à $n_b + 1$ et à $n_c + 1$. Ces relations ne sont compatibles que si $n_b = n_c = 1$. Mais alors les groupes L_b^0, L_c^0 seraient semblables, et ce cas est exclu (**21**).

V. — Maximum du nombre des fonctions linéaires distinctes inaltérées par une substitution d'un groupe L indécomposable.

68. Théorème. — *Un groupe* L *résoluble et indécomposable à n variables ne peut contenir aucune substitution* (*l'unité exceptée*) *qui laisse invariables* N *fonctions linéaires distinctes, si* $N > \frac{3}{4} n$.

Soit en effet S une substitution de L dans laquelle N soit $> \frac{n}{2}$; et soit U une autre substitution de L. Le système des N fonctions que S n'altère pas et celui des N fonctions que la transformée $U^{-1}SU$ n'altère pas ont au moins $2N - n$ fonctions communes que $S^{-1}U^{-1}SU$ n'altérera pas.

Si l'on prend en particulier $U = f$, $S^{-1}f^{-1}Sf$ étant une puissance de f qui laisse des fonctions inaltérées, se réduira à l'unité. Donc S est échangeable à f.

Elle ne peut l'être à toutes les substitutions des seconds faisceaux h, h', car elle se réduirait alors à l'unité. Supposons donc que h, d'ordre $\pi^{2\sigma+1}$, contienne une substitution U non échangeable à S. La substitution $S^{-1}U^{-1}SU$ laisse inaltérées au moins $2N - n$ fonctions. Mais elle appartient à h, dont chaque substitution laisse inaltérées $\frac{n}{\pi}$ fonctions (ou les altère toutes). Donc

$$2N - n \leq \frac{n}{\pi},$$

d'où

$$N \leqq \frac{n}{2}\left(1+\frac{1}{\pi}\right) \leqq \frac{3n}{4},$$

car $\pi \geqq 2$.

69. On peut préciser davantage, si l'ordre ϖ de S est impair. Il est permis de le supposer premier.

LEMME. — *h contient un sous-groupe abélien permutable à* S *et d'ordre* $\pi^{\sigma+1}$.

En effet, il contient la substitution $f^{\frac{\omega}{\pi}} = 0$ qui est échangeable à S. Le groupe h_0 formé par ses puissances va être progressivement élargi par l'adjonction de nouvelles substitutions de h, sans cesser d'être abélien et permutable à S.

Supposons, en effet, que nous ayons déjà obtenu un groupe h_s jouissant de ces propriétés et d'ordre π^{s+1}, s étant $< \sigma$; h contiendra des substitutions échangeables à celles de h_s, sans être contenues dans h_s. Prenons l'une d'elles pour U.

Si $U^{-1}S^{-1}US = U'$ appartient à h_s, S sera permutable au groupe élargi $(h_s, U) = h_{s+1}$.

Dans le cas contraire, U' sera une substitution de h échangeable à celles de h_s et laissant invariables quelques-unes des fonctions que S n'altère pas. Il en sera de même des transformées successives

$$S^{-1}U'S = U'_1, \qquad S^{-1}U'_1S = U'_2, \qquad \ldots.$$

Ces substitutions seront d'ailleurs échangeables entre elles, car $U_1'^{-1}U'^{-1}U'_1U'$, par exemple, est une puissance de 0, mais qui laisse des fonctions invariables. Elle se réduit donc à l'unité.

Le groupe élargi $(h_s, U', U'_1, \ldots)$ est donc abélien. D'ailleurs S lui sera permutable, puisqu'elle l'est à h_s et qu'elle permute circulairement U', U'_1, ...

70. Le groupe abélien h_σ dont l'existence vient d'être établie s'obtient par la combinaison de $\sigma + 1$ substitutions génératrices

$$0, \quad C_1, \quad \ldots, \quad C_\sigma.$$

Ces substitutions C sont d'ordre π si π est impair; si $\pi = 2$ elles auront pour ordre 2 ou 4, suivant leur caractère.

D'ailleurs, si C_i et C_k ont pour caractère 1, on pourra prendre pour

génératrice, au lieu de C_k, celle-ci : $C_i C_k$, qui a pour caractère zéro. On peut donc admettre que $C_2, \ldots, C_\sigma$ aient pour caractère zéro, l'incertitude ne subsistant que pour C_1.

On pourra déterminer dans h des substitutions $D_1, \ldots D_\sigma$ telles que les exposants d'échange $C_i D_k$ soient tous nuls, sauf ceux où $i = k$, qui seront égaux à 1. En outre, si $\pi = 2$, auquel cas on doit tenir compte des caractères, on peut faire en sorte que D_i ait pour caractère zéro, si $i > 1$; car si elle avait le caractère 1, on pourrait lui substituer $C_i D_i$, dont le caractère est zéro.

Quant à D_1, on peut lui supposer le même caractère qu'à C_1 ; car si C_1 avait pour caractère zéro, on remplacerait au besoin D_1 par $C_1 D_1$. Supposons au contraire que le caractère de C_1 soit 1 et que celui de D_1 soit zéro. Les substitutions de h_σ seront de deux sortes; les unes d'ordre 2 dérivées de $C_2, \ldots, C_\sigma, 0$, que nous désignerons d'une manière générique par E; les autres de la forme $C_1 E$, d'ordre 4.

La substitution S étant permutable au groupe des E transformera D_1, qui leur est échangeable, en une substitution qui le soit aussi, mais ne le soit pas à C_1. La transformée aura donc pour expression $D_1 C_1^\rho E$, où $\rho = 0$ ou 1. La transformée de D_1 par S^ϖ aura la forme $D_1 C_1^{\rho\varpi} E$; mais elle doit se réduire à D_1 puisque $S^\varpi = 1$. On aura donc nécessairement $\rho = 0$. Donc S est permutable au groupe $0, D_1, C_2, \ldots C_\sigma$ où la génératrice D_1, qui a pour caractère zéro, a pris la place de C_1.

71. Les substitutions C, D jouissent donc de toutes les propriétés attribuées aux substitutions fondamentales A, B (n° **28**). On pourra donc supposer qu'elles se confondent avec elles et choisir des variables indépendantes $[\xi_1, \ldots, \xi_\sigma \varepsilon']_r$ qui ramènent leur expression à la forme normale (n° **29**). Nous serons alors en mesure de déterminer la forme générale que doit avoir la substitution S.

Soit

$$A_1^{\alpha_{1k}} \ldots A_\sigma^{\alpha_{\sigma k}} \theta^{\alpha_k} \qquad (k = 1, \ldots, \sigma)$$

celle des substitutions de h_σ qu'elle doit transformer en A_k. Posant

$$\eta_k = a_{1k}\xi_1 + \ldots + a_{\sigma k}\xi_k + \alpha_k,$$

on vérifie immédiatement que la substitution S_0 qui remplace chaque variable

$$[\xi_1, \ldots, \xi_\sigma, \varepsilon']_r \quad \text{par la variable} \quad [\eta_1, \ldots, \eta_\sigma, \varepsilon']_r$$

opère la transformation demandée et qu'elle est d'ailleurs permutable au groupe $(\theta, B_1, \ldots, B_\sigma)$.

On aura donc

$$S = S_0 U,$$

U étant échangeable à toutes les substitutions du groupe h_σ.

Si L a un autre second faisceau h', l'indice ε' étant remplacé par σ' indices $\xi'_1, \ldots, \xi'_{\sigma'}$, on verra de même que U est le produit de deux substitutions dont la première S'_0 fera succéder à chaque variable une autre variable, où les indices $\xi'_1, \ldots, \xi'_{\sigma'}$ sont remplacés par $\eta'_1, \ldots, \eta'_{\sigma'}$, fonctions linéaires de $\xi'_1, \ldots, \xi'_\sigma$; la seconde substitution U' étant échangeable à $(\theta', A'_1, \ldots, A'_{\sigma'})$.

72. Supposons, pour abréger, que h' soit le dernier des seconds faisceaux. La substitution U' multipliera chaque variable par un facteur constant.

Les variables seront donc de deux sortes :

1° La première comprendra celles dont les indices satisfont aux relations

$$(1) \qquad \xi_1 \equiv \eta_1, \quad \ldots, \quad \xi_\sigma \equiv \eta_\sigma \pmod{\pi},$$

$$(2) \qquad \xi'_1 \equiv \eta'_1, \quad \ldots, \quad \xi'_{\sigma'} \equiv \eta'_{\sigma'} \pmod{\pi'}.$$

S les reproduira à un facteur près.

Si l'on suppose que les relations (1) se réduisent à q distinctes et les relations (2) à q' distinctes, le nombre m des variables de cette sorte sera évidemment

$$m = \frac{n}{\pi^q \pi'^{q'}}.$$

2° Soit x_1 l'une des $n - m$ variables de la seconde sorte. S la remplacera par $a_1 x_2$, a_1 étant un facteur constant et x_2 une autre variable. Elle remplacera de même $a_1 x_2$ par $a_2 x_3$, etc.; et S étant d'ordre ϖ, la suite $x_1, a_1 x_2, a_2 x_3$ doit se reproduire périodiquement après ϖ termes.

Or, pour que S laisse inaltérée une fonction

$$\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_\varpi x_\varpi,$$

il faut qu'on ait

$$a_1\lambda_1=\lambda_2, \qquad a_2\lambda_2=\lambda_3, \qquad \ldots, \qquad a_{\varpi-1}\lambda_\varpi=\lambda_1,$$

d'où

$$a_1 a_2 \ldots a_{\varpi-1}=1$$

et si cette condition est remplie, on n'aura qu'une fonction invariante, les rapports des λ étant déterminés.

Donc on aura dans l'hypothèse la plus favorable où les m variables de la première sorte seraient toutes inaltérées, la limite supérieure

$$N \leqq \frac{n-m}{\varpi} + m = n\left[\frac{1}{\varpi} + \frac{1}{\pi'\pi'q'} - \frac{1}{\varpi\pi'\pi'q'}\right]$$

et comme $\varpi \geqq 3$, $\pi \geqq 2$, $\pi' \geqq 2$, on aura, si $q+q'>1$,

$$N \leqq \frac{n}{2},$$

l'égalité n'ayant lieu que si $\varpi = 3$.

Soit au contraire $q=1$, $q'=0$. Les relations (2) seront identiques; quant aux relations (1), la substitution linéaire qu'elles opèrent sur les indices pourra, par une transformation linéaire réelle, être mise sous la forme

$$(3) \qquad |\xi_1, \xi_2, \ldots, \xi_\sigma, \quad a\xi_1 + b\xi_2 + \ldots + \alpha, \xi_2, \ldots, \xi_\sigma, \quad (\mathrm{mod}\,\pi);$$

et, pour que S soit d'ordre ϖ, il faudra qu'on ait $a^\varpi = 1 \pmod{\pi}$. Mais on a aussi $a^{\pi-1} \equiv 1 \pmod{\pi}$. Donc si $a>1$, ϖ devra diviser $\pi-1$, et

$$N \leqq n\left[\frac{1}{\varpi} + \frac{1}{\pi} - \frac{1}{\varpi\pi}\right] < \frac{n}{2}.$$

Si $a=1$, la substitution (3) étant d'ordre π, on aura $\varpi = \pi$

$$N \leqq n\left[\frac{2}{\varpi} - \frac{1}{\varpi^2}\right],$$

expression encore moindre que $\frac{n}{2}$, sauf pour $\varpi = 3$ où elle est égale à $\frac{5}{9}n$.

73. Supposons enfin que les relations (1) et (2) soient identiques : S sera échangeable à toutes les substitutions $A_1, \ldots, A_\sigma, A'_1, \ldots, A'_\sigma$. Elle devra donc transformer les substitutions B_i en substitutions de la

forme

$$B'_i = B_i A_1^{q_{i1}} \dots A_\sigma^{q_{i\sigma}} \theta^{\alpha_i} \qquad (i = 1, \dots, \sigma),$$

avec la condition que B'_i et B'_k soient échangeables. D'ailleurs, si elle n'est pas échangeable à tous les B_i, on aura nécessairement $\pi = \varpi$. Autrement S^ϖ transformant B_i en

$$B_i (A_1^{q_{i1}} \dots A_\sigma^{q_{i\sigma}} \theta^{\alpha_i})^\varpi,$$

qui diffère de B_i, ne serait pas égale à l'unité.

Or toutes les transformations de ce genre peuvent s'obtenir (*N. L.*, n° 32), en combinant avec les substitutions

$$A_k = |[\dots \xi_k \dots] \quad \theta^{\xi_k} [\dots \xi_k \dots]|,$$

les suivantes :

$$D_{kl} = |[\xi_1 \dots \varepsilon'] \quad \theta^{-\xi_k \xi_l} [\xi_1 \dots \varepsilon']|,$$

$$E_k = \left|[\xi_1 \dots \varepsilon'] \quad \theta^{-\frac{\xi_k(\xi_k-1)}{2}} [\xi_1 \dots \varepsilon']\right|.$$

On aura donc

$$S = S_0 U,$$

S_0 multipliant toutes les variables de la série principale par θ^φ, où φ est une fonction du second degré en $\xi_1, \xi_2, \dots$ et U les multipliant par des facteurs indépendants de $\xi_1, \xi_2, \dots$.

On voit de même qu'on doit avoir $\pi' = \varpi$ et que U doit être égal à $S'_0 U'$, S'_0 multipliant ces variables par $\theta^{\varphi'}$, où φ' est du second degré en $\xi'_1, \dots, \xi'_{\sigma'}$, et U' les multipliant toutes par un même facteur de la forme θ^d.

Le facteur qui multiplie chaque variable sera donc de la forme

$$\theta^{\varphi+\varphi'+d},$$

et les variables inaltérées seront celles pour lesquelles on a

$$\varphi + \varphi' + d \equiv 0 \pmod{\varpi},$$

Nous avons donc à chercher le nombre des solutions de cette congruence.

74. Par un changement de variables linéaires, nous pourrons la mettre sous la forme

$$\varphi + \psi + h \equiv 0. \pmod{\varpi},$$

φ étant une forme quadratique, ψ une forme linéaire ne contenant chacune qu'une partie des nouvelles variables, et h une constante.

Si ψ n'est pas identiquement nulle, la congruence déterminera une de ces variables, toutes les autres restant arbitraires; on aura donc

$$N = \frac{n}{\varpi} < \frac{n}{2}.$$

Si $\psi = 0$, soient k le nombre des variables de φ, Δ son discriminant. On aura

$$N = \frac{\mathfrak{N}_k}{\varpi^k} n,$$

$\mathfrak{N}_k$ désignant parmi les ϖ^k systèmes de valeurs qu'on peut attribuer aux variables de φ le nombre de ceux qui satisfont à la congruence

$$\varphi + h = 0.$$

Ce nombre $\mathfrak{N}_k$ est donné par les formules connues (*Journal de Liouville*, 7e série, t. II, 1916, p. 257).

Si $k = 2m + 1$,

$$\mathfrak{N}_{2m+1} = \varpi^{2m} - \varpi^m \left[\frac{(-1)^m \Delta h}{\varpi}\right];$$

Si $k = 2m + 2$,

$$\mathfrak{N}_{2m+2} = \varpi^{2m+1} - \varpi^m \left[\frac{(-1)^m \Delta}{\varpi}\right],$$

les expressions entre crochets désignent des symboles de Legendre.

Il résulte de ces formules que N sera $< \frac{n}{2}$ à moins qu'on n'ait

$$\varpi = 3, \qquad k = 1, \qquad \left[\frac{\Delta h}{\varpi}\right] = 1,$$

auquel cas on aura

$$N = \frac{2}{3} n.$$

Nous pouvons donc énoncer le théorème suivant qui précise celui du n° 68.

THÉORÈME. — *Le nombre* N *des fonctions qu'une substitution* S

d'ordre premier ϖ *contenue dans* L *ne peut surpasser*

$$\frac{3}{4}n \quad \text{si} \quad \varpi = 2,$$

$$\frac{n}{2} \quad \text{si} \quad \varpi > 3,$$

$$\frac{2}{3}n \quad \text{si} \quad \varpi = 3.$$

Mais même pour $\varpi = 3$ *il ne peut surpasser* $\frac{n}{2}$ *que si* n *est multiple de* 3.

VI. — Groupes abéliens contenus dans un groupe décomposable.

75. Désignons comme précédemment par L^0 un groupe primaire et résoluble contenu, soit dans le groupe linéaire à n variables mod$p$, soit dans le groupe plus restreint des substitutions linéaires qui laissent absolument invariante une forme Φ.

Par l'adjonction à L^0 de sa base B, nous obtiendrons un groupe résoluble et primitif G^0 de substitutions linéaires non homogènes.

Proposons-nous d'étudier les sous-groupes abéliens contenus dans G^0.

Soit H l'un d'eux. Ses substitutions sont de la forme SU, S appartenant à L^0 et U à B.

76. Supposons d'abord que l'ordre Ω de H soit premier à p.

Les substitutions partielles S', S'', ... de l'espèce S étant homogènes, échangeables entre elles et d'ordre premier à p, pourront être ramenées simultanément à une forme canonique monome. Nous grouperons dans une même série celles des nouvelles variables qui, dans chacune d'elles, ont toujours un même multiplicateur.

Soit s_0 l'une de ces séries contenant l_1 variables x', ..., x^{l_1} et soient a', a'', ... les facteurs par lesquels elles sont toutes multipliées par les diverses substitutions S', S'', ... La détermination de ces facteurs aura exigé la résolution de congruences pouvant entraîner l'introduction d'une imaginaire i racine primitive d'une congruence

$$i^{p^{\gamma_1}-1} \equiv 1 \pmod{p}.$$

Les multiplicateurs $\alpha', \alpha'', \ldots$ seront des puissances de i telles que $i^{\alpha'}, i^{\alpha''}, \ldots$ et si d_1 est le plus grand commun diviseur de $\alpha', \alpha'', \ldots, p^{\nu_1} - 1$, les substitutions S', S'', ... résulteront de la combinaison des puissances de l'une d'entre elles S_1 multipliant les variables de s_0 par i^{d_1}, avec des substitutions S', ... qui ne les altèrent plus.

La substitution S_1U_1 de H dont S_1 est le premier facteur, remplacera $x', \ldots, x^{l_1}$ par

$$i^{d_1}x' + \beta', \quad \ldots, \quad i^{d_1}x^{l_1} + \beta^{l_1},$$

les β étant des entiers complexes formés avec l'imaginaire i. On pourra d'ailleurs faire disparaître ces termes constants en prenant pour variables au lieu de $x', \ldots, x^{l_1}$ celles-ci $x' + \lambda', \ldots, x^{l_1} + \lambda^{l_1}$, les λ étant déterminés par les relations

$$(i^{d_1} - 1)\lambda' \equiv \beta', \quad \ldots, \quad (i^{d_1} - 1)\lambda^{l_1} \equiv \beta^{l_1} \pmod{p}.$$

Quant aux substitutions S''U'', ... de H dont les premiers facteurs n'altèrent pas les variables de s_0, elles les laissent également invariables; car, dans le cas contraire où elles les accroîtraient de termes constants, l'ordre de H serait divisible par p, contrairement à notre hypothèse.

Si d'ailleurs ν_1 est > 1, la série s_0 ne sera pas isolée, mais appartiendra à un système s_1 de ν_1 séries conjuguées $s_0, \ldots, s_r, \ldots, s_{\nu_1 - 1}$; et S_1 multipliera les variables de s_r par i^{p^r}.

S'il y a des séries autres que celles-là, elles pourront de même être assemblées en systèmes analogues à s_1.

Nous pouvons donc formuler le théorème suivant :

THÉORÈME. — *Par un choix convenable des variables indépendantes on pourra ramener toutes les substitutions de* H *à la forme homogène.*

Chacune d'elles sur un produit de puissances de substitutions $S_1, S_2, \ldots$ *n'altérant chacune que les variables d'un seul des systèmes* $s_1, s_2, \ldots$ *entre lesquels lesdites variables peuvent se répartir.*

77. *Remarque.* — L'introduction des imaginaires a été utile pour la démonstration. Mais on peut substituer à l'ensemble formé par chaque variable complexe, jointe à ses conjuguées, celui des variables réelles dont elles dépendent; et la répartition des variables en systèmes subsistera.

78. Les substitutions $S_1, S_2, \ldots$ étant respectivement d'ordre $\frac{p^{\nu_1}-1}{d_1}, \ldots$, l'ordre D de H divisera le produit

$$\prod_k \frac{p^{\nu_k}-1}{d_k}.$$

D'ailleurs, si l_k est le nombre des variables de chaque série de S_k, le nombre n des variables sera au moins égal à $\Sigma l_k \nu_k$. Il serait même plus grand, si quelques variables, n'étant altérées par aucune substitution de H, restaient en dehors des systèmes s.

De la comparaison de ces nombres il résulte évidemment que Ω ne peut en aucun cas surpasser $p^n - 1$; et que pour qu'il atteigne ce nombre il faut qu'on n'ait qu'un seul système s_1, avec

$$\nu_1 = n, \; l' = d' = 1;$$

c'est le résultat invoqué au n° **13**.

79. *Remarque.* — Jusqu'à présent il n'a pas été parlé de forme invariante Φ. S'il y en a une, nous n'avons que peu de chose à ajouter.

Chaque série doit avoir une associée où les multiplicateurs sont réciproques des siens. Les deux associées peuvent d'ailleurs se confondre (groupes de 3e catégorie) ou être conjuguées (2e catégorie) ou enfin appartenir à deux systèmes différents associés l'un à l'autre (1re catégorie).

Dans ce dernier cas, nous réunirons les deux systèmes associés en un seul.

Cela posé, la forme Φ, pour être invariante, ne devra contenir aucun terme où figurent à la fois les variables de deux séries non associées. Elle sera donc une somme de formes partielles $\Phi_1, \Phi_2, \ldots$ ne contenant chacune que les variables d'un seul système. Et cette dernière propriété subsistera si l'on revient des variables complexes à des variables réelles.

Si L^0 est susceptible d'être employé comme groupe auxiliaire pour une construction ultérieure, n sera un nombre pair 2σ et il faudra ou que Φ soit bilinéaire, ou que p soit égal à 2. Dans l'un et l'autre cas, chacune des formes partielles $\Phi_1, \Phi_2, \ldots$ devra contenir un nombre pair de variables (sans quoi le discriminant de Φ serait nul). Leur nombre, ou celui des substitutions $S_1, S_2, \ldots$ génératrices de H, qui lui est égal, ne pourra donc surpasser σ.

80. La détermination des groupes H dont l'ordre est divisible par p est plus difficile. Mais il suffira, pour notre objet, d'obtenir une limite supérieure de leur ordre Ω.

Nous établirons tout d'abord le lemme suivant :

LEMME. — *Étant donné un groupe abélien* I *de substitutions linéaires homogènes à n variables, dont l'ordre Ω soit une puissance de p, on pourra choisir les variables indépendantes de telle sorte qu'elles se partagent en classes telles que chaque substitution de* I *accroisse les variables de chaque classe d'une fonction linéaire de celles des classes suivantes; celles de la dernière classe n'étant pas altérées.*

On peut admettre dans la démonstration que la vérité de cette proposition ait déjà été établie pour les groupes à moins de n variables.

Supposons pour plus de généralité que les variables $x_1, \ldots, x_n$ parcourent chacune le champ des p^ν entiers complexes formés avec une imaginaire d'ordre ν.

Soit S une des substitutions de I. Elle permutera les unes dans les autres les fonctions linéaires (à coefficients complexes) $a_1x_1+\ldots+a_nx_n$. Le nombre $p^{\nu n}-1$ de ces fonctions étant premier à p, il y en aura nécessairement quelques-unes que S n'altère pas. Si parmi ces fonctions inaltérées il y en a m distinctes, $\varphi_1, \ldots, \varphi_m$, on pourra les prendre pour variables indépendantes à la place des dernières variables $x_{n-m+1}, \ldots, x_n$.

Les substitutions de I étant toutes échangeables à S devront permuter ensemble les fonctions inaltérées $b_1\varphi_1+\ldots+b_m\varphi_m$. Chacune d'elles sera donc le produit de trois substitutions partielles, la première S_1 opérée entre les variables $x_1, \ldots, x_{n-m}$; la seconde S_2 les accroissant de fonctions linéaires des φ; la troisième S_3 opérée sur les φ.

Les substitutions S_1 d'une part, S_3 d'autre part, étant opérées entre moins de n variables, on pourra les ramener à la forme requise.

Nous allons maintenant établir le théorème suivant :

81. THÉORÈME. — *L'ordre Ω d'un groupe abélien* H *ne peut surpasser p^n. S'il est égal à p^n,* H *contient des substitutions de* B.

Nous pourrons admettre que le théorème ait déjà été établi pour les groupes à moins de n variables. Il sera encore vrai si H est contenu dans un groupe G^0 qui soit un produit de groupes partiels G_1^0, G_2^0, ... contenant respectivement $n_1, n_2, \ldots$ variables seulement, $n_1+n_2+\ldots$ étant égal à n.

En effet, chaque substitution de H étant un produit de substitutions $S_1, S_2, \ldots$ appartenant respectivement à $G_1^0, G_2^0, \ldots$, Ω ne pourra surpasser $p^{n_1} p^{n_2} \ldots = p^n$.

Ce cas se présentera si I^0 étant décomposable, H ne permute pas transitivement les systèmes $\Sigma_1, \Sigma_2, \ldots$ formés par ses variables.

S'il les permute transitivement, on aura $\Omega = \Omega_1 \Omega_2$, Ω_1 étant l'ordre du groupe abélien formé par les déplacements d'ensemble que H fait éprouver aux systèmes, Ω_2 l'ordre du groupe I formé par celles des substitutions de H qui ne déplacent pas les systèmes, lesquelles seront de la forme

$$V_1 V_2 \ldots V_k \ldots,$$

V_k étant opérée sur les variables de Σ_k.

Or, si l'on a m systèmes, de n' variables chacun, Ω_1 ne pourra surpasser m. D'autre part, les substitutions V_1 sont en nombre au plus égal à $p^{n'}$. Soit enfin une substitution de I où V_1 se réduise à l'unité. Pour qu'elle soit échangeable à celle des substitutions de H qui remplace Σ_1 par Σ_k, il faudra qu'on ait également $V_k = 1$ quel que soit k. Donc $\Omega_2 \leqq p^{n'}$ et $\Omega \leqq m p^{n'}$, quantité inférieure à $p^{m n'} = p^n$.

Si I^0 est indécomposable, mais à forme invariante et de première catégorie, ses variables se répartiront en deux demi-systèmes, et la démonstration se fera de la même manière.

82. Reste à établir le théorème pour les groupes indécomposables qui ne sont pas de première catégorie.

Nous montrerons tout d'abord que le *maximum de* Ω *est une puissance de* p.

Soit, en effet, H un groupe abélien dont l'ordre Ω ne soit ni premier à p ni puissance de p. Il sera le produit de deux groupes partiels H_1, H_2 dont les ordres Ω_1, Ω_2 sont respectivement premiers à p et puissance de p.

Nous avons vu que les variables de H_1 se répartissent en systèmes $s_1, s_2, \ldots$. Les substitutions de H_2, étant échangeables à celles de H_1, devront remplacer les variables de chaque série par des fonctions linéaires de ces mêmes variables et, par suite, celles d'un système par des fonctions de celles de ce système.

Le théorème sera donc démontré en vertu de la remarque du numéro précédent, s'il y a plusieurs systèmes. S'il n'y en a qu'un, H_1 sera formé des puissances d'une seule substitution S_1 multipliant

les variables de la première série par i^d et d'ordre $\frac{p^\nu - 1}{d}$. On aura donc

$$\Omega = \Omega_1 \Omega_2 = \frac{p^\nu - 1}{d} \Omega_2.$$

Mais pour que les substitutions de H_2 soient échangeables à S_1, il faut qu'elles remplacent les variables de cette première série par des fonctions linéaires homogènes de ces variables. Une substitution linéaire opérée sur ces variables n'altérera pas l'expression de S_1 et mettra en évidence les diverses classes de variables dans H_2. Soient $x_1, \ldots, x_m$ les variables de la première classe. Parmi les substitutions de la base, nous en aurons $p^{\nu m}$ qui remplacent

$$x_1, \quad \ldots, \quad x_m \qquad \text{par} \qquad x_1 + \alpha_1, \quad \ldots, \quad x_m + \alpha_m,$$

$\alpha_1, \ldots, \alpha_m$ étant des entiers complexes, et leurs conjuguées par des expressions conjuguées. Toutes ces substitutions U sont évidemment échangeables à celles de H_2 et leur adjonction à celles-ci donnera un groupe H' dont l'ordre $p^{\nu m} \Omega_2$ sera $> \Omega$.

83. Le maximum de Ω ne devra donc être cherché que dans les groupes H dont l'ordre est puissance de p. Les substitutions d'un semblable groupe seront de la forme SU, S étant linéaire homogène et U appartenant à la base de G^0. Son ordre sera $\Omega_1 \Omega_2$, Ω_1 étant l'ordre du groupe I formé par les substitutions partielles S, Ω_2 celui du groupe J formé par celles des substitutions de H qui sont de la forme U. Mais il est évident que le produit des deux groupes I, J est abélien et puisqu'il a le même ordre que H il pourra lui être substitué dans la recherche du maximum.

84. Nous avons d'ailleurs ramené la question au cas où L^0 est indécomposable et non de première catégorie. Soient f la substitution génératrice de son premier faisceau, ν le nombre des séries conjuguées de μ variables chacune.

Si $\nu > 1$, on peut admettre que I ne contienne aucune substitution qui déplace ces séries. On pourrait en effet déterminer un autre groupe H' ne les déplaçant plus et d'ordre supérieur à celui de (I, J).

En effet, désignons par P la substitution qui remplace chaque variable par sa première conjuguée, par Q une substitution qui ne

déplace plus les séries. Si I les déplaçait, il résulterait de la combinaison des puissances d'une substitution $P^{\delta}Q$ (δ divisant ν) avec un groupe I′ formé de substitutions de l'espèce Q. Et l'ordre Ω de (I, J) serait $\frac{\nu}{\delta}\Omega_1$, Ω_1 désignant l'ordre de (I′, J).

Or I′ étant abélien et d'ordre puissance de p, la base de L^0 contiendra $p^{\nu m}$ substitutions échangeables à celles de I′ et remplaçant les variables $x_{10}, \ldots, x_{m0}$ de la première série et de la première classe par $x_{10}+\alpha_1, \ldots, x_{m0}+\alpha_m$ et leurs conjuguées

$$x_{1r}, \ldots, x_{mr} \quad \text{par} \quad x_{1r}+\alpha_1^{p^r}, \ldots, x_{mr}+\alpha_m^{p^r}$$

sans altérer les variables dont le premier indice est $> m$.

Adjoignons-les à (I′, J). Nous obtiendrons un groupe abélien H′ contenu dans L^0 et d'ordre $\frac{p^{\nu m}}{q}\Omega_1$, q désignant le nombre des substitutions adjointes qui appartenaient déjà à J. Ces q substitutions devaient être échangeables à la substitution

$$P^{\delta}Q = \left| x_{kr} \quad \sum_{l} a_{lk}^{p^r} x_{l,r+\delta} \right|$$

$$(k = 1, \ldots, \mu;\ l = 1, \ldots, \mu;\ r = 0, \ldots, \nu-1).$$

Les conditions d'échangeabilité sont

$$\alpha_k \equiv \sum_{1}^{m} a_{lk}\alpha_l^{p^{\delta}} \pmod{p} \qquad (k = 1, \ldots, m),$$

$$0 \equiv \sum_{1}^{m} a_{lk}\alpha_l^{p^{\delta}} \qquad (k = m+1, \ldots, \mu).$$

Ceux des coefficients a_{lk}, où $l \leqq m$ ne pouvant être nuls à la fois, l'une au moins de ces congruences ne sera pas identique; et considérée isolément elle déterminera l'un des α par une congruence de degré p^{δ}, en fonction des $m-1$ autres. Donc $q \leqq p^{\nu(m-1)+\delta}$ et l'ordre de H′ sera $\geqq p^{\nu-\delta}\Omega_1 > \Omega$, car $p^{\nu-\delta} > \frac{\nu}{\delta}$.

85. Il ne reste donc plus à examiner que le cas où L^0 étant indécomposable (et non de première catégorie), les variables forment

ν séries de μ variables chacune, et $H = (I, J)$, I étant abélien d'ordre puissance de p et formé de substitutions qui ne déplacent pas les séries, et J étant l'ensemble des substitutions de la base de G^0 qui sont échangeables à celles de I.

Les substitutions que nous aurons à considérer altérant d'une manière conjuguée les variables conjuguées, il suffira d'indiquer dans l'écriture les altérations qu'elles font subir aux variables de la première série.

Le groupe G^0 peut avoir diverses formes correspondant aux diverses décompositions distinctes de μ en facteurs

$$\mu = \pi^\sigma \pi'^{\sigma'} \dots .$$

Si H est contenu dans plusieurs de ces groupes G^0 nous choisirons pour y appliquer le raisonnement celui où le nombre des facteurs π^σ, $\pi'^{\sigma'}$, ... est le plus grand.

Supposons, pour plus de clarté, qu'il y en ait deux. Les variables (de la première série) étant caractérisées par deux indices ε, η variables de o à $\pi^\sigma - 1$ et de o à $\pi'^{\sigma'} - 1$, L^0 résultera de la combinaison de substitutions des deux formes suivantes :

$$T = \left| [\varepsilon\eta] \quad \sum_l a_{\varepsilon l} [l\eta] \right| \qquad (l = 1, \dots, \pi^\sigma - 1),$$

$$T' = \left| [\varepsilon\eta] \quad \sum_l b_{\eta\eta} [\varepsilon l] \right| \qquad (l = 1, \dots, \pi'^{\sigma'} - 1).$$

Parmi les substitutions de l'espèce T que L^0 contient figurent celles d'un second faisceau h d'ordre $\pi^{2\sigma+1}$ et dérivé de 2σ substitutions génératrices $C_1, \dots, C_{2\sigma}$. Les autres substitutions T que L^0 contient sont permutables à h. Pour les obtenir on construit un groupe auxiliaire résoluble $\mathfrak{L}^0$ de substitutions linéaires homogènes à 2σ variables (mod π). Par l'adjonction des substitutions $\mathfrak{S}_1, \dots, \mathfrak{S}_{2\sigma}$ de sa base on obtient un groupe $\mathfrak{G}^0$ auquel le groupe des substitutions T que l'on cherche sera isomorphe.

Les substitutions de l'espèce T' que contient L^0 s'obtiennent de même par la construction d'un groupe auxiliaire $\mathfrak{L}'^0$ à $2\sigma'$ variables (mod π').

86. Cela posé, soit S une quelconque des substitutions de I. Son ordre sera une puissance de p, telle que p'.

D'ailleurs elle appartient à L^0. Donc elle est de la forme TT' On peut admettre que chacune des deux substitutions partielles T, T′ ait également pour ordre une puissance de p. En effet l'égalité

$$(TT')^{p^l} = 1$$

montre que $T^{p^l} = T'^{-p^l}$ est à la fois de l'espèce T et de l'espèce T′. Mais les seules substitutions communes à ces deux formes sont des puissances de f.

Soit donc

$$T^{p^l} = f^{\alpha}, \qquad T'^{p^l} = f^{-\alpha}.$$

On aura

$$TT' = Tf^{\lambda}.T'f^{-\lambda}.$$

Les deux facteurs de ce nouveau produit seront respectivement des formes T et T′; d'ailleurs ils auront pour ordre des puissances de p si l'on détermine λ par la congruence

$$p^l\lambda + \alpha \equiv 0 \pmod{\omega},$$

ω étant l'ordre de f, lequel est premier à p.

87. Soient donc

$$T_1T'_1, \quad T_2T'_2, \quad \ldots$$

les substitutions de I, les substitutions partielles ayant toutes pour ordre des puissances de p. Aux substitutions T_1, T_2, ... correspondront dans le groupe auxiliaire $\mathcal{G}^0$ des substitutions formant un groupe abélien dont l'ordre, étant une puissance de p, sera premier à π. Il résultera des puissances d'une seule génératrice $\mathfrak{S}_1$. Car s'il y en avait plusieurs, elles altéreraient des variables différentes. La base $\mathfrak{B} = (\mathfrak{S}_1, \ldots, \mathfrak{S}_{2\sigma})$ serait ainsi décomposée en plusieurs bases partielles $\mathfrak{B}_1$, $\mathfrak{B}_2$, ... et le faisceau h qui lui correspond serait décomposé de même en faisceaux partiels h_1, h_2, ... répondant à une décomposition de μ où le facteur π^{σ} serait remplacé par un produit $\pi^{\sigma_1}\pi^{\sigma_2}$, ... contrairement à nos hypothèses.

On verra de même que les substitutions T'_1, T'_2, ... sont des puissances d'une seule d'entre elles, T'_1.

88. Il est donc établi que les substitutions de I sont toutes de la forme $T_1^{\alpha}T_1'^{\beta}$. Mais pour que H soit d'ordre maximum il faut

que I contienne séparément les substitutions T_1^{α}, $T_1'^{\beta}$. Car ce dédoublement, qui accroîtrait l'ordre de I, ne diminuerait pas l'ordre du groupe J formé des substitutions

$$U = |[\varepsilon\eta] \quad [\varepsilon\eta] + a_{\varepsilon\eta}|$$

échangeables à celles de I.

Pour le montrer, transformons T_1^{α} par une substitution de l'espèce T de manière à la ramener à la forme canonique. Les nouvelles variables formeront diverses suites telles que T_1^{α} accroisse chaque variable de l'une d'elles de la variable précédente (la première restant inaltérée). Soient

$$[k\eta] \qquad (k = 1, \ldots, m)$$

les variables d'une de ces suites choisie parmi les plus longues. A chaque valeur de η correspondra une suite semblable.

Opérant d'une manière analogue sur $T_1'^{\beta}$ nous obtiendrons pour chaque valeur de ε une suite

$$[\varepsilon l] \qquad (l = 1, \ldots, m').$$

Considérons les variables $[kl]$ où $k = 1, \ldots, m$, $l = 1, \ldots, m'$.
T_1^{α} remplacera $[kl]$ par $[kl] + [k-1, l]$.
T'^{β} la remplacera par $[kl] + [k, l-1]$.
Donc $T_1^{\alpha} T_1'^{\beta}$ la remplacera par

$$[kl] + [k-1, l] + [k, l-1] + [k-1, l-1].$$

Pour que U soit échangeable à $T_1^{\alpha} T_1'^{\beta}$, on aura la condition

$$a_{k-1,l} + a_{k,l-1} + a_{k-1,l-1} = 0.$$

On en déduit de proche en proche pour toutes les valeurs de k et de l

$$a_{k-1,l} = 0, \qquad a_{k,l'-1} = 0,$$

ce qui montre que U est échangeable à T_1^{α} et à $T_1'^{\beta}$.

En effet, comme il n'existe aucune variable d'indice nul, on aura pour $l = 1$ et quel que soit k

$$a_{k-1,1} = 0.$$

En vertu de cette première relation, il viendra, si $l = 2$,

$$a_{k-1,2} = 0,$$

et ainsi de suite.

On verra de même que

$$a_{k,l-1} = 0.$$

Or les substitutions T_1^α sont des puissances d'une seule d'entre elles que nous pourrons désigner par T_1. De même les substitutions $T_1'^\beta$ seront des puissances d'une seule d'entre elles, T_1'.

Donc I, supposé maximum, résultera de la combinaison des deux génératrices T_1 et T_1'.

89. Il est maintenant facile de déterminer une limite supérieure de l'ordre de H.

En effet, si T_1 et T_1' ont pour ordres respectifs p^λ, $p^{\lambda'}$, on aura

$$\Omega = p^{\lambda+\lambda'} O,$$

O désignant le nombre des substitutions de la forme

$$|[\varepsilon\eta] \quad [\varepsilon\eta] + a_{\varepsilon\eta}|$$

qui sont échangeables à T_1 et à T_1'. Mais nous venons de voir que si T_1 et T_1' contiennent respectivement des suites de m et de m' termes, tous les nombres $a_{\varepsilon\eta}$ où ε ne surpasse pas m et η ne surpasse pas m' doivent être nuls, à l'exception d'un seul $a_{mm'}$. Donc, dans l'hypothèse la plus favorable, le nombre des $a_{\varepsilon\eta}$ non nuls ne peut surpasser $\mu - mm' + 1$. Chacun d'eux étant susceptible de p^ν valeurs, on aura

$$O \leqq p^{n-(mm'-1)\nu},$$

d'où

$$\Omega \leqq p^n . p^{\lambda+\lambda'+(1-mm')\nu}.$$

D'ailleurs, on vérifie aisément que si T_1 remplace

$$[kl] \quad \text{par} \quad [kl] + [k-1, l],$$

T_1'', T_1''', ... le remplaceront par

$$[kl] + [k-p, l] \qquad (\text{mod } p),$$
$$[kl] + [k-p^2, l] \qquad (\text{mod } p),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Donc pour que T_1 soit d'ordre p^λ, il faut que m soit $> p^{\lambda-1}$.

De même $m' > p^{\lambda'-1}$.

On aura donc

$$\Omega \leqq p^n . p^{\lambda+\lambda'-1[(p^{\lambda'-1}+1)(p^{\lambda-1}+1)-1]\nu},$$

expression qui décroît évidemment à mesure que croissent λ et λ'. En les supposant égaux à l'unité elle devient $p^n . p^{2-3\nu}$ nombre $< p^n$.

Nous avons toutefois supposé que I contenait deux génératrices distinctes T_1 et T'_1. S'il n'y en avait qu'une T_1, on aurait l'inégalité

$$\Omega \leqq p^n . p^{\lambda+(1-m)\nu},$$

où le second facteur se réduirait à l'unité, si $\lambda = 1$, $m = 2$, $\nu = 1$.

90. REMARQUE. — *Si* Ω *est égal à* p^n, H *contiendra nécessairement des substitutions de la base* B.

En effet, nous avons vu que les variables étant choisies de manière à se partager en classes les substitutions de B qui n'altèrent que celles de la première classe sont échangeables à celles de H. Si H ne les contenait pas, leur adjonction donnerait un groupe abélien H' d'ordre $> p^n$, ce qui est impossible.

91. Soient L^0 un groupe primaire et indécomposable (avec ou sans forme invariante); f la substitution d'ordre ω qui engendre son premier faisceau; $\mu = \pi^\sigma \pi'^{\sigma'} \ldots$ le nombre des variables de chaque série; $h, h' \ldots$ ses seconds faisceaux. Le noyau de L^0 forme un groupe d'ordre $\omega\mu^2$ jouissant des propriétés suivantes :

Ses substitutions sont échangeables à f, et échangeables entre elles aux puissances près de f.

THÉORÈME. — *Si quelque autre sous-groupe* H *de* L^0 *jouit des mêmes propriétés, son ordre* Ω *ne pourra surpasser* $\omega\mu^2$. *S'il lui est égal,* H *contiendra des substitutions de chacun des faisceaux* $h, h', \ldots$ *autres que les puissances de* f.

En effet, les substitutions de H sont des formes T, T', ... A chaque substitution T correspond une substitution $\mathfrak{S}$ d'un groupe auxiliaire $\mathfrak{G}^0$ à 2σ variables (mod π). Les substitutions $\mathfrak{S}$ correspondant aux substitutions T contenues dans H constituent un groupe abélien $\mathfrak{H}$, dont l'ordre ne peut surpasser $\pi^{2\sigma}$.

Un raisonnement analogue s'applique aux substitutions $T'_1, \ldots$

contenues dans H. Donc Ω aura pour maximum $\pi^{2\sigma}\pi'^{2\sigma'}\ldots$ O, soit μ^2O, O étant le nombre des substitutions qui ont pour correspondante l'unité dans chacun des groupes auxiliaires. Ce sont les puissances de f, en nombre ω. Le maximum cherché est donc $\omega\mu^2$.

D'ailleurs, pour qu'il soit atteint, il faut que $\mathfrak{K}$ contienne des substitutions de la base de $\mathcal{G}_0$. A chacune d'elles correspond une substitution de h, autre que les puissances de f.

On voit de même que H doit contenir des substitutions de h'.

92. Soit L^0 un groupe primaire et résoluble à $2n$ variables (mod 2) et à forme invariante.

L'ordre Ω *d'un groupe abélien* H *contenu dans* L^0 *et dont toutes les substitutions sont d'ordre* 2 *sera au plus égal à* 2^n.

La démonstration se ramène comme au n° **81** au cas où L^0 est indécomposable.

Soit ν' le nombre des séries conjuguées à l'une d'elles; elles contiendront chacune $\mu = \pi^\sigma\pi'^{\sigma'}\ldots$ variables, et les nombres π, π', ... divisant $\omega = 2^{\nu'} \pm 1$ seront impairs.

Celles des substitutions de H qui ne déplacent pas les séries seront des formes T, T', ...

Aux substitutions T correspondront des substitutions $\mathfrak{S}$ d'un groupe auxiliaire $\mathcal{G}^0$ à 2σ variables (mod π) et à forme invariante Ψ. Le groupe $\mathfrak{K}$ de ces substitutions $\mathfrak{S}$ sera abélien et dérivé de substitutions génératrices dont le nombre ne pourra surpasser σ (**79**). L'ordre de $\mathfrak{K}$ sera donc $\leqq 2^\sigma < \pi^\sigma$.

D'ailleurs, les puissances de f étant d'ordre impair, à chaque substitution $\mathfrak{S}$ ne correspondra qu'une seule substitution T qui soit d'ordre 2.

Le nombre des substitutions de H qui ne déplacent pas les séries sera donc

$$\leqq 2^{\sigma+\sigma'+\ldots} \leqq \mu.$$

(Le signe $=$ correspond au cas où $\mu = 1$.)

On a d'ailleurs $2n = 2\nu'\mu$.

Si L^0 est de deuxième catégorie, les $2\nu'$ séries sont toutes conjuguées et H pourra contenir une dernière génératrice rempla-

çant la série r par la série $r + \nu'$. On aurait alors

$$\Omega \leqq 2\mu \leqq 2^{\mu\nu'} \leqq 2^n.$$

Si L^0 est de première catégorie, on aura deux systèmes associés contenant chacun ν' séries conjuguées. D'ailleurs on doit avoir

$$2^{\nu'} > 4, \qquad \text{d'où} \qquad \nu' \geqq 3.$$

L^0 peut contenir une génératrice échangeant les deux systèmes, et si ν' est un nombre pair $2\nu''$ une autre génératrice remplaçant la série r par la série $r + \nu''$. On aura donc :

Si ν' est pair $\geqq 4$,

$$\Omega \leqq 4\mu < 2^{\nu'\mu} < 2^n;$$

Si ν' est impair $\geqq 3$,

$$\Omega \leqq 2\mu \leqq 2^{\nu'\mu} < 2^n.$$

93. Soient L^0 un groupe indécomposable de troisième catégorie; f la substitution génératrice de son premier faisceau (laquelle multiplie toutes les variables par -1); $\mu = 2^\sigma . 2^{\sigma'} \ldots$ le nombre des variables; h, h', ... les seconds faisceaux.

Nous dirons pour abréger qu'un sous-groupe K de L^0 est *binaire* s'il jouit des deux propriétés suivantes :

1° *Ses substitutions sont échangeables entre elles aux puissances près de f;*

2° *Le carré de chacune d'elles est une puissance de f.*

Le groupe H_k formé par la réunion des k seconds faisceaux $h, \ldots, h^{(k-1)}$ est évidemment binaire, et si l'on pose

$$\sigma + \sigma' + \ldots + \sigma^{(k-1)} = s_k,$$

il aura pour ordre 2^{2s_k+1}.

THÉORÈME. — *Un groupe binaire* K *dont les substitutions sont échangeables à celles des seconds faisceaux h^k, ... non contenus dans H_k et dont l'ordre serait 2^{s_k+r} contient au moins 2^r substitutions de H_k.*

En effet, d'après nos notations habituelles, les substitutions de K seront de la forme

$$TT' \ldots T^{(k-1)}.$$

Elles ont pour correspondantes des substitutions

$$\mathfrak{S}\mathfrak{S}'\ldots\mathfrak{S}^{(k-1)}$$

d'un groupe $\mathfrak{C}$ (complexe si $k>1$) de substitutions linéaires homogènes à 2σ variables (mod 2). Celles-ci sont d'ordre 2 et forment un groupe abélien. Leur nombre ne peut donc surpasser 2^{s_k} (**92**).

Donc parmi les substitutions de K en nombre 2^{s_k+r}, il y en aura au moins 2^r ayant l'unité pour correspondante et par suite appartenant à H_k.

VII. — Un groupe complexe ou décomposable ne peut être contenu dans un groupe indécomposable.

94. Nous rechercherons dans cette Section si un groupe L^0 décomposable ou complexe peut être contenu dans un groupe indécomposable $\overline{L}^0$; et nous verrons que cette hypothèse est inadmissible.

Si L^0 est décomposable, il résultera de la combinaison de groupes indécomposables pareils L_1^0, L_2^0, ..., L_m^0 opérés sur les variables des divers systèmes 1, 2, ..., m avec un groupe transitif G de déplacements d'ensemble. Et si $\overline{L}^0$ contient L^0, il contiendra *a fortiori* le groupe complexe $(L_1^0, L_2^0, \ldots)$.

Nous commencerons par montrer que *la substitution $\overline{f}$ génératrice du premier faisceau de $\overline{L}^0$ est un produit de substitutions φ_1, φ_2, ..., φ_m opérées respectivement sur les variables des systèmes*, 1, 2, ... (et d'une *dernière substitution ψ, opérée sur les variables de $\overline{L}^0$ qui ne figurent pas dans* L^0, *s'il existe de telles variables*).

La démonstration s'appliquera d'ailleurs au cas où m étant égal à 1, le groupe L^0 serait indécomposable, pourvu toutefois qu'il contienne plus d'une variable.

Notre point de départ sera dans la remarque suivante :

Si S, T *sont deux substitutions quelconques de* $\overline{L}^0$, $S^{-1}\overline{f}S$, $T^{-1}\overline{f}T$ *seront des puissances de* $\overline{f}$ *et* $S^{-1}T^{-1}ST$ *lui sera échangeable.*

Soit L_*^0 l'un quelconque des groupes semblables L_1^0, L_2^0, ... Supposons qu'il contienne plusieurs variables se partageant en

séries de μ variables chacune. Si $\mu > 1$, soit

$$\theta_s = \begin{pmatrix} \theta_s, & A_{1s}\dots \\ & B_{1s}\dots \end{pmatrix},$$

l'un des seconds faisceaux de L_s^0, $\overline{f}$ devra être échangeable à la substitution

$$A_{1s}^{-1} B_{1s}^{-1} A_{1s} B_{1s} = \theta_s,$$

laquelle n'altère aucune variable sauf celles du système L_s^0 qu'elle multiplie par des facteurs différents de l'unité.

Pour que $\overline{f}$ soit échangeable à toutes les substitutions $\theta_1, \theta_2, \dots$, il faudra donc qu'elle soit de la forme indiquée

$$\overline{f} = \varphi_1 \varphi_2 \dots \psi.$$

Si $\mu = 1$, L_s^0 sera dérivé d'une substitution f_s génératrice de son premier faisceau, à laquelle il faudra joindre, s'il y a plusieurs séries conjuguées, une substitution P_s qui les permute circulairement, et si L_s^0 est de première catégorie une substitution R_s échangeant les séries associées. Et $\overline{f}$ sera échangeable aux substitutions

$$P_s^{-1} f_s^{-1} P_s f_s = f_s^{1-p}, \qquad R_s^{-1} f_s^{-1} R_s f_s = f_s^{2},$$

dont l'une existe nécessairement si L_s^0 contient plusieurs variables comme nous l'avons supposé. On en déduit, comme dans le cas précédent, que $\overline{f}$ est de la forme $\varphi_1 \varphi_2 \dots \psi$.

Supposons enfin que L_s^0 ne contienne qu'une variable x_s. Il sera formé des puissances de la substitution

$$| x_s \quad g x_s | \qquad (\mathrm{mod}\, p),$$

g désignant une racine primitive de p s'il n'y a pas de forme invariante. S'il y en a une elle sera quadratique; L_s^0 sera de troisième catégorie et l'on aura $g = -1$.

Le groupe G contenant une substitution S qui fait succéder au système s un autre système arbitraire t, $\overline{f}$ sera échangeable à la substitution

$$f_s^{-1} S^{-1} f_s S = f_s^{-1} f_t,$$

laquelle multiplie x_s par g^{-1}, x_t par g, sans altérer les autres variables.

Si donc g n'est pas égal à -1, $\overline{f}$ multipliera x_s et x_t par des facteurs constants et sera encore de la forme requise.

Si $g=-1$, $\overline{f}$ pourrait faire succéder à x_s une fonction linéaire de x_s et de x_t. Mais si L^0 contient un troisième système u différent des précédents, $\overline{f}$ sera échangeable à $f_s^{-1}f_u$ qui multiplie x_s par -1 sans altérer x_t. Donc ici encore $\overline{f}$ multipliera x_s par un facteur constant.

Les seuls cas qui échappent à la démonstration sont donc les suivants :

1° Pas de forme invariante : -1 racine primitive de p; donc $p=3$: en outre, L^0 n'a que deux systèmes. Ce cas est exclu (**36**);

2° L^0 admet une forme invariante : il est décomposable et ne contient que deux variables. Ce cas est également exclu (**35**).

95. Supposons maintenant que L^0 soit complexe et résulte de l'association de groupes primaires L'^0, L''^0, ... supposés chacun maximum dans son espèce.

Il est impossible que parmi ces groupes il y en ait plus d'un ne contenant qu'une variable, car s'il y en avait deux ils seraient semblables et ce cas est exclu (**35**). Si parmi les autres groupes il y en avait un L'^0 décomposable, il contiendrait un groupe complexe $(L_1^0, \ldots, L_m^0)$ qu'on pourrait lui substituer dans le raisonnement. Donc $\overline{L}^0$ contiendrait un groupe complexe

$$L_1^0, \quad \ldots, \quad L_m^0, \quad L_{m+1}^0, \quad \ldots$$

formé de l'association de groupes indécomposables, et $\overline{f}$ serait de la forme

$$\overline{f}=\varphi_1\ldots\varphi_m\varphi_{m+1}\ldots\psi,$$

ψ ne pouvant contenir que la variable d'un dernier groupe qui aurait échappé aux raisonnements précédents.

La question de reconnaître si L^0 peut contenir L^0 est donc ramenée au cas où L^0 est complexe et formé de groupes indécomposables L_1^0, L_2^0, ... et il est démontré que $\overline{f}$ doit être de la forme

$$\overline{f}=\varphi_1\varphi_2\ldots.$$

Toutefois, si plusieurs des groupes L_1^0, L_2^0, ... sont semblables

on devra se rappeler que le groupe $(L_1^0, L_2^0, \ldots)$ n'est pas celui qui nous était donné à l'origine. Il a été déduit de ce dernier par la suppression de déplacements d'ensemble opérés sur ces groupes semblables. Leur rétablissement donnera un ou plusieurs groupes décomposables qui devront être supposés maxima. L'un de ces groupes maxima devrait être contenu dans $\overline{L}^0$.

96. Soit $\overline{\omega}$ l'ordre de $\overline{f}$. Toutes les puissances de cette substitution (sauf l'unité) ne laissant aucune fonction invariable, les substitutions partielles $\varphi_1, \varphi_2, \ldots$ devront également avoir $\overline{\omega}$ pour ordre.

D'autre part, soit L_k^0 l'un quelconque des groupes qui constituent L^0. Ses subtitutions doivent transformer $\overline{f}$ en une de ses puissances. Mais elles n'altèrent pas les facteurs φ autres que φ_k. Donc elles sont toutes échangeables à φ_k. Mais les seules substitutions entre les variables de L_k^0 qui soient échangeables à toutes celles de L_k^0 sont celles de son premier faisceau F_k, dont nous désignerons l'ordre par ω_k. Donc $\overline{\omega}$ divise ω_k.

Cela posé, soient μ_k le nombre des variables de chaque série dans L_k^0,

$$f_k \quad \begin{matrix} A_1 \ldots A_\sigma, & A'_1 \ldots \\ B_1 \ldots B_\sigma, & B'_1 \ldots, \end{matrix}$$

les substitutions dont son noyau est dérivé. Les substitutions f_k $A_1, \ldots, A_\sigma, A', \ldots$ forment un groupe abélien d'ordre $\omega_k \mu_k$. En associant les groupes analogues pour les diverses valeurs de k, on voit que L^0 contient un groupe abélien d'ordre

$$\prod_k \omega_k \mu_k.$$

Mais si $\overline{\mu}$ est le nombre des variables de chaque série dans $\overline{L}^0$, l'ordre d'un semblable groupe contenu dans $\overline{L}^0$ ne peut surpasser $\overline{\omega}\,\overline{\mu}^2$ (**91**).

On aurait donc l'inégalité

$$\prod_k \omega_k \mu_k \leqq \overline{\omega}\,\overline{\mu}^2.$$

Avant de la discuter il conviendra de mettre en évidence les

nombres n_k, $\overline{n}$ de variables contenues dans les groupes L_k^0, $\overline{L}^0$. S'ils contiennent respectivement ν_k et $\overline{\nu}$ séries, on aura évidemment

$$\mu_k = \frac{n_k}{\nu_k}, \qquad \overline{\mu} = \frac{\overline{n}}{\overline{\nu}}.$$

De sorte que l'inégalité deviendra

$$\overline{\nu} \prod_k \frac{\omega_k}{\nu_k} n_k \leq \frac{\overline{\omega}}{\overline{\nu}} \overline{n}^2.$$

97. Or il est aisé de voir que $\frac{\omega_k}{\nu_k}$ ne peut être inférieur à $\frac{\omega}{\overline{\nu}}$, qui lui-même sera plus grand que l'unité.

En effet, s'il n'y a pas de forme invariante, on aura

$$\frac{\overline{\omega}}{\overline{\nu}} = \frac{p^{\overline{\nu}} - 1}{\overline{\nu}};$$

mais $p^{\overline{\nu}} > 2$. Le minimum de cette expression sera donc $\frac{3}{2}$; il correspond à $p^{\overline{\nu}} = 4$. Si p est impair son minimum sera 2.

D'autre part, $\omega_k = p^{\nu_k} - 1$, étant divisible par $\overline{\omega} = p^{\overline{\nu}} - 1$, ν_k sera un multiple de $\overline{\nu}$, tel que $m\overline{\nu}$; donc

$$\frac{\omega_k}{\nu_k} : \frac{\overline{\omega}}{\overline{\nu}} = \frac{p^{m\overline{\nu}} - 1}{m(p^{\overline{\nu}} - 1)},$$

expression croissante avec m et égale à 1 pour $m = 1$.

S'il y a une forme invariante on aura, suivant la catégorie à laquelle appartient $\overline{L}^0$, $\overline{\nu}'$ désignant un entier :

Première catégorie :

$$\overline{\nu} = 2\overline{\nu}'; \qquad \overline{\omega} = p^{\overline{\nu}'} - 1 \qquad (p^{\overline{\nu}'} > 4).$$

Deuxième catégorie :

$$\overline{\nu} = 2\overline{\nu}'; \qquad \overline{\omega} = p^{\overline{\nu}'} + 1.$$

Troisième catégorie :

$$\overline{\nu} = 1; \qquad \overline{\omega} = 2 \qquad (p \text{ impair}).$$

Le minimum de $\frac{\overline{\omega}}{\overline{\nu}}$ sera $\frac{7}{6}$; pour $\overline{\nu}'=3$, $\overline{\omega}=2^3-1$. Mais si p est impair le minimum sera 2.

On aura des expressions analogues pour $\frac{\omega_k}{\nu_k}$ en remplaçant $\overline{\nu}'$ par ν_k'.

Si $\overline{\omega}=p^{\overline{\nu}'}-1$,

$$\nu_k'=m\overline{\nu}', \qquad \omega_k=p^{m\overline{\nu}}-1;$$

si $\overline{\omega}=p^{\overline{\nu}'}+1$,

$$\nu_k'=2m\overline{\nu}', \qquad \omega_k=p^{2m\overline{\nu}'}-1,$$

ou

$$\nu_k'=(2m-1)\overline{\nu}', \qquad \omega_k=p^{(2m-1)\overline{\nu}'}+1.$$

On voit par ces formules que $\frac{\omega_k}{\nu_k}$ croît avec m et que déjà pour $m=1$, il est égal ou même supérieur à $\frac{\overline{\omega}}{\overline{\nu}}$.

Enfin si $\overline{\omega}=2$, les trois formes de ω_k sont admissibles, mais p étant impair, aucune d'elles ne donnera une valeur moindre que 2 à $\frac{\omega_k}{\nu_k}$.

98. On a d'ailleurs

$$\Sigma n_k = n,$$

et les substitutions de L_k^n laissent inaltérées au moins $\overline{n}-n_k$ fonctions des variables. Mais ce nombre ne peut être supérieur à $\frac{3}{4}n$ (**68**). Donc chacun des nombres n_k est au moins égal à $\frac{n}{4}$.

En outre, si $n_k<\frac{n}{2}$, l'ordre Ω_k de L_k^n ne pourra être divisible par aucun facteur premier impair q autre que 3. Il ne le sera même pas par 3 à moins qu'on n'ait à la fois

$$n_k \geqq \frac{\overline{n}}{3}, \qquad \overline{n}\equiv 0 \pmod 3.$$

En effet si ces conditions n'étaient pas remplies $\overline{L}^n$ contiendrait une substitution d'ordre q (ou d'ordre 3) laissant invariantes

$\bar{n} - n_k$ fonctions, nombre supérieur à $\frac{\bar{n}}{2}$, ce qui a été démontré impossible (**74**).

99. Or si Ω_k se réduit d'après ce qui précède à une puissance de 2, p sera impair, μ_k égal à l'unité, et n_k à une puissance de 2. Car si p était égal à 2, l'ordre ω_k du premier faisceau de L_k^0 serait $p^{\nu_k} - 1$ ou $p^{\nu_k} \pm 1$, nombre impair. D'autre part, si μ_k avait un diviseur impair π, L_k^0 contiendrait un second faisceau d'ordre $\pi^{2\sigma+1}$ impair. Si l'on avait $\mu_k = 2^\sigma . 2^{\sigma'} \ldots$, la construction de L_k^0 dépendrait de celle d'un groupe isomorphe à 2σ variables (mod 2), dont le premier faisceau serait d'ordre impair.

Enfin μ_k étant égal à l'unité, on aura

$$\Omega_k = \omega_k n_k.$$

Donc n_k, de même que Ω_k, n'aura aucun diviseur impair.

100. Nous sommes maintenant en mesure de discuter l'inégalité fondamentale

$$\bar{\nu} \prod \frac{\omega_k}{\nu_k} n_k \leq \frac{\bar{\omega}}{\bar{\nu}} \bar{n}^2.$$

Les relations

$$\Sigma n_k = \bar{n}, \qquad n_k \leq \frac{n}{4}$$

montrent que le produit Π ne peut contenir plus de quatre facteurs.

Supposons d'abord qu'il y en ait quatre. On aura

$$n_1 = n_2 = n_3 = n_4 = \frac{1}{4}\bar{n},$$

d'où

$$\bar{n}^2 = 16 n_3 n_4.$$

D'autre part (p étant impair et $\mu_1 = \ldots = \mu_4 = 1$)

$$\frac{\omega_3}{\nu_3}\frac{\omega_4}{\nu_4} \leq \left(\frac{\bar{\omega}}{\bar{\nu}}\right)^2 \leq 4.$$

Enfin

$$n_1 = \nu_1 \mu_1 = \nu_1, \qquad n_2 = \nu_2 \mu_2 = \nu_2.$$

On aura donc *a fortiori*

$$\bar{\nu}\omega_1\omega_2 \leqq 4.$$

D'ailleurs ω_1, ω_2 sont > 1 et puissances de 2. La seule solution sera donc

$$\bar{\nu} = 1, \qquad \omega_1 = \omega_2 = 2.$$

Or s'il n'y a pas de forme invariante, on a

$$\omega_k = p^{\nu_k} - 1.$$

La relation

$$\omega_1 = p^{\nu_1} - 1 = 2$$

donne

$$\nu_1 = 1, \qquad p = 3.$$

S'il y a une forme invariante, les relations montrent que $L_1^0, \ldots$ sont de troisième catégorie; donc

$$\nu_1 = \nu_2 = \ldots = 1.$$

Donc les groupes $L_1^0, \ldots, L_4^0$ ne contiennent chacun qu'une variable, et s'il n'y a pas de forme invariante, le module p est égal à 3. Ce cas a été signalé et exclu (**57**).

101. Passons au cas de trois facteurs.

Soit $n_1 \leqq n_2 \leqq n_3$: n_1 sera compris dans l'intervalle de $\frac{\bar{n}}{4}$ à $\frac{\bar{n}}{3}$; n_2 et n_3 dans celui de n_1 à $\bar{n} - 2n_1$; et leur produit sera au moins égal à $n_1(\bar{n} - 2n_1)$, expression qui varie de $\frac{n^2}{8}$ à $\frac{n^2}{9}$ lorsque n_1 varie de $\frac{n}{4}$ à $\frac{n}{3}$.

Reprenons l'inégalité fondamentale

$$\bar{\nu}\frac{\omega_1}{\nu_1} n_1 \frac{\omega_2}{\nu_2} n_2 \frac{\omega_3}{\nu_3} n_3 \leqq \frac{\bar{\omega}}{\bar{\nu}} \bar{n}^2.$$

On a, comme on vient de le voir, $\bar{n}^2 \leqq 9 n_2 n_3$. D'autre part

$$\frac{\omega_2}{\nu_2}\frac{\omega_3}{\nu_3} \geqq \left(\frac{\bar{\omega}}{\bar{\nu}}\right)^2, \qquad n_1 = \nu_1\mu_1.$$

Il en résulte donc

$$\omega_1\mu_1\bar{\omega} \leqq 9.$$

D'ailleurs ω_1 est divisible par $\overline{\omega}$. Les seules solutions seraient donc

$$\overline{\omega}_1 = \omega_1 = 3, \qquad \mu_1 = 1,$$
$$\overline{\omega} = 2, \qquad \omega_1 = 4, \qquad \mu_1 = 1;$$
$$\overline{\omega} = \omega_1 = 2, \qquad \mu = 1, \text{ ou } 2.$$

102. La première solution est à rejeter.

En effet, s'il n'y a pas de forme invariante, on aura

$$\omega_1 = p^{\nu_1} - 1 = 3, \qquad \text{d'où} \qquad p^{\nu_1} = 2^2, \quad p = 2, \quad \nu_1 = 2 \quad \text{et} \quad \mu_1 = 1.$$

Donc L_1^0 n'a que deux variables (mod 2) et dérive des deux substitutions

$$f_1 = |x_0, x_1 \quad ix_0, i^2x_1|, \qquad P_1 = |x_0, x_1 \quad x_1, x_0| \qquad [i^3 \equiv 1 \pmod 2].$$

S'il y a une forme invariante, L_1^0 ne pourra être ni de première catégorie, car on aurait $\omega_1 = p^{\nu_1} - 1 > 3$ (p^{ν_1} étant > 4), ni de troisième, car on aurait $\omega_1 = 2$.

S'il est de deuxième catégorie, on aura $\nu_1 = 2\nu_1'$, et

$$\omega_1 = p^{\nu_1'} + 1 = 3, \qquad \text{d'où} \qquad p = 2, \qquad \nu_1' = 1.$$

On aura donc encore deux variables x_0, x_1, et L_1^0 aura la même expression que tout à l'heure.

Or $\overline{f}$ devrait être de la forme $\varphi_1\varphi_2\varphi_3$, φ_1 étant une puissance de f_1 échangeable à toutes les substitutions de L_1^0. Mais aucune de ces puissances, sauf l'unité, n'est échangeable à P_1. On aurait donc $\varphi_1 = 1$, et $\overline{f}$ laisserait inaltérées les variables de L_1^0, ce qui est impossible.

103. Soit donc $\overline{\omega} = 2$. S'il n'y a pas de forme invariante la relation $\overline{\omega} = p^{\overline{\nu}} - 1 = 2$ montre qu'on aura $p = 3$, $\overline{\nu} = 1$. Les variables de $\overline{L}^0$ ne forment donc qu'une série; et $\overline{\nu} = 1$.

D'ailleurs $\overline{\mu}$ ne contenant que des facteurs qui divisent $\overline{\omega}$ sera une puissance de 2.

Le nombre des variables de $\overline{L}^0$ n'étant pas divisible par 3, on aura $\mu_1 = 1$ (**99**).

La relation $\omega_1 = 2$ ou 4 deviendra

$$3^{\nu_1} - 1 = 2 \text{ ou } 4.$$

Elle ne peut être satisfaite que si $\nu_1 = 1$, $\omega_1 = 2$.

Donc L_1^0 ne contient qu'une variable x et il est formé des substitutions

$$|x \quad \pm x| \qquad (\text{mod } 3).$$

Donc $\overline{L}^0$ contiendra quatre variables, dont une seule y appartiendra à L_2^0 ; et les mêmes raisonnements qui ont été faits pour L_1^0 montrent que L_2^0 sera formé des substitutions

$$|y \quad \pm y| \qquad (\text{mod } 3).$$

Les groupes L_1^0, L_2^0 sont donc semblables et l'on devra rétablir la substitution qui permute x et y. Mais le groupe décomposable ainsi obtenu est exclu (**36**). Cette hypothèse est donc à rejeter.

S'il y a une forme invariante, la condition $\overline{\omega} = 2$ montre que $\overline{L}^0$ doit être de troisième catégorie. Le nombre $\overline{n}$ de ses variables sera une puissance de 2. Donc $\mu_1 = 1$. Si $\omega_1 = 2$, L_1^0 sera également de troisième catégorie et $n_1 = 1$. Donc $\overline{n} = 4$, $n_2 = 1$, L_1^0, L_2^0 seront formés des substitutions

$$|x \quad \pm x|, \qquad |y \quad \pm y| \qquad (\text{mod } p,\ p \text{ impair}).$$

Après le rétablissement de la substitution

$$|x, y \quad y, x|,$$

on obtiendrait comme dans le cas précédent un groupe décomposable rentrant dans un cas exclu (**35**).

104. Il faut donc supposer $\omega_1 = 4$. On en déduit si L_1^0 est de première catégorie

$$p^{\nu'_1} - 1 = 4, \qquad \text{d'où} \qquad \nu'_1 = 1, \quad p = 5,$$

et s'il est de deuxième catégorie

$$p^{\nu'_1} + 1 = 4, \qquad \text{d'où} \qquad \nu'_1 = 1, \quad p = 3.$$

Dans l'un et l'autre cas $\nu_1 = 2\nu'_1 = 2$. Donc $n_1 = 2$.

La forme partielle Φ_1 que L_1^0 laisse invariante sera quadratique, car en la supposant bilinéaire, on tomberait sur un cas exclu (43 et 44).

Donc L_1^0 sera dérivé des substitutions

$$f_1 = |x, y \quad gx, g^{-1}y|, \qquad R_1 = |x, y \quad y, x| \qquad [g^4 \equiv 1 \pmod 5]$$

ou des substitutions

$$f_1 = |x_0, x_1 \quad i^2 x_0, i^6 x_1|, \qquad P_1 = |x_0, x_1 \quad x_1, x_0| \qquad [i^8 \equiv 1 \pmod 3].$$

Dans les deux cas son ordre sera 8.

Le nombre $\bar{n}$ étant $> 2n_1$, mais $\leq 4n_1$, sera égal à 8; n_2 et n_3 étant pairs, on aura $n_2 = 2$, $n_3 = 4$.

Raisonnant sur L_2^0 comme sur L_1^0 on voit qu'on aura $\omega_2 = 4$ et et que L_2^0 est semblable à L_1^0.

Le groupe décomposable Λ^0 résultant de l'adjonction à L_1^0, L_2^0 de la substitution qui les permute aura pour ordre 2^7. En désignant par O l'ordre de L_3^0, celui du groupe (Λ^0, L_3^0) sera $2^7 O$.

Mais ce groupe doit être contenu dans $\overline{L}^0$, dont l'ordre est égal au produit de 2^7 ordre de son noyau par le nombre Ω^0 des substitutions paires du groupe auxiliaire $\mathfrak{L}$ primaire ou complexe à six variables et à forme invariante quadratique Ψ (mod 2) qui sert à achever sa construction.

Donc O devrait diviser Ω^0. Or il est aisé de voir que cela ne peut avoir lieu.

En effet, si $\mu_3 = 1$, O sera égal à $(5^2 \pm 1)4$ ou à $(3^2 \pm 1)4$.

Si $\mu_3 = 2$, il sera égal à $(5 \pm 1)2.24$ ou à $(3 + 1)2.24$.

Si $\mu_3 = 4$, L_1^0 étant de troisième catégorie, son noyau sera d'ordre 2^5, nombre dont O sera un multiple.

Donc O sera dans tous les cas divisible ou par 2^5 ou par $2^3.13$ ou par $2^3.5$.

Soit, d'autre part, Ω l'ordre de $\mathfrak{L}$.

Si $\mathfrak{L}$ est indécomposable, on aura

$$\Omega = (2^3 \pm 1)6 \text{ ou } (2 + 1)3^2.2.24.$$

Si $\mathfrak{L}$ est décomposable, $\Omega = 2.3\,(2.3)^3$.

Si $\mathfrak{L}$ est complexe, $\Omega = (2^2 + 1)4.2.3$, mais $\mathfrak{L}$ contenant des

substitutions impaires on aura

$$\Omega^0 = \frac{1}{2}\Omega.$$

Donc Ω^0 ne sera divisible ni par 2^5 ni par 13, ni par $2^3 . 5, 3^2$.

104. Passons enfin au cas où L^0 est formé de deux groupes partiels L_1^0, L_2^0. L'inégalité fondamentale deviendra

$$\bar{\nu}\frac{\omega_1}{\nu_1} n_1 \frac{\omega_2}{\nu_2} n_2 \leqq \frac{\bar{\omega}}{\bar{\nu}} \bar{n}^2.$$

D'ailleurs n_1 n_2 sont compris dans l'intervalle de $\frac{1}{4}\bar{n}$ à $\frac{3}{4}\bar{n}$; donc

$$\bar{n}^2 \geqq \frac{16}{3} n_1 n_2.$$

L'inégalité devient donc

$$\bar{\nu}\frac{\omega_1}{\nu_1}\frac{\omega_2}{\nu_2} \leqq \frac{16}{3}\frac{\bar{\omega}}{\bar{\nu}}.$$

Chacun des deux nombres $\frac{\omega_1}{\nu_1}$, $\frac{\omega_2}{\nu_2}$ étant au moins égal à $\frac{\bar{\omega}}{\bar{\nu}}$, l'autre facteur devra être au plus égal à $\frac{16}{3}$.

Soit donc

$$\bar{\nu}\frac{\omega_1}{\nu_1} \leqq \frac{16}{3}, \qquad \bar{\nu}\frac{\omega_2}{\nu_2} < \frac{16}{3}.$$

S'il n'y a pas de forme invariante, la première de ces relations donnera (ν_1 étant un multiple de $\bar{\nu}$, tel que $m_1\bar{\nu}$)

$$p^{m_1\bar{\nu}} - 1 \leqq \frac{16}{3} m_1,$$

et limitera p et $\bar{\nu}$.

Si $p = 2$ ($p^{\bar{\nu}}$ étant nécessairement > 2, d'où $\bar{\nu} > 1$), la seule solution sera $m_1 = 1$, $\nu_1 = \bar{\nu} = 2$. De même $\nu_2 = 2$.

Mais cette solution est inacceptable; car il en résulterait

$$\bar{\omega} = \omega_1 = \omega_2 = 3;$$

le nombre des variables de chaque série dans les groupes $\bar{L}^0$,

L_1^0, L_2^0 serait donc une puissance de 3; on aurait donc $n = 2.3^{\bar{\rho}}$, $n_1 = 2.3^{\rho_1}$, $n_2 = 2.3^{\rho_2}$, et la somme de deux puissances de 3 ne pouvant être puissance de 3, l'égalité $n_1 + n_2 = \bar{n}$ serait impossible.

Si $p = 3$, on a la seule solution $m_1 = 1$, $\bar{\nu} = \nu_1 \nu_2 = 1$; car le cas où $p^{\nu_1} = 3^2$ est exclu (41).

$\bar{\omega}$, ω_1, ω_2 étant égaux à 2, $\bar{n}$, n_1, n_2 seront des puissances de 2. Mais la somme de deux puissances de 2 ne peut être puissance de 2 que si elles sont égales. Donc

$$n_1 = n_2 = \frac{1}{2}\bar{n}.$$

Ces solutions où $n_1 = n_2 = \frac{1}{2}n$ seront discutées plus loin.

Si $p = 5$, on a de même une seule solution

$$\bar{\nu} = \nu_1 = \nu_2 = 1, \qquad \text{d'où} \qquad \bar{\omega} = \omega_1 = \omega_2 = 4;$$

$\bar{n}$, n_1, n_2 seront encore des puissances de 2; et $n_1 = n_2 = \frac{1}{2}\bar{n}$.

Si $p > 5$, on n'a plus aucune solution.

105. Passons au cas d'une forme invariante.

Si $\bar{L}^0$ est de première catégorie, on aura

$$\bar{\nu} = 2\bar{\nu}', \quad \bar{\omega} = p^{\bar{\nu}'} - 1 > 3;$$

L_1^0 et L_2^0 seront de première catégorie; car ω_1, ω_2 doivent être divisibles par $\bar{\omega}$. Or si L_1^0 par exemple était de troisième catégorie, on aurait $\omega_1 = 2$; et s'il était de seconde catégorie, ω_1 serait de la forme $p^{\nu_1} + 1$, qui, divisé par $\bar{\omega}$, donnerait un reste $p^{\nu} + 1$, ν étant $< \nu_1$.

On aura donc

$$\omega_1 = p^{\nu_1} - 1, \qquad \nu_1' = m_1 \bar{\nu}',$$

et l'inégalité

$$p^{m_1 \bar{\nu}'} - 1 \leqq \frac{16}{3} m_1.$$

Le groupe L_2^0 donnera une inégalité toute semblable. Ces inégalités sont impossibles si $p > 5$; ou si p étant égal à 5, $\bar{\nu}' > 1$.

Si $p = 5$ on aura la solution

$$m_1 = m_2 = 1, \qquad \bar{\nu}' = \nu_1 = \nu_2, \qquad \bar{\omega} = \omega_1 = \omega_2 = 4.$$

Ici encore $\bar{n}$, n_1, n_2 seront des puissances de 2 et l'on aura $n_1 = n_2 = \frac{1}{2}n$. Nous sommes convenus de réserver l'examen des cas de ce genre.

Si $p = 2$ ou 3 et $\bar{\nu}' > 2$, les inégalités sont impossibles. On aurait une solution pour $m_1 = m_2 = 1$ et $p^{\bar{\nu}'} = 3^2$; mais ce cas est exclu (**38**).

Enfin $p^{\bar{\nu}'}$ étant > 4, la discussion est terminée.

106. Si $\bar{L}^0$ est de deuxième catégorie, on aura

$$\bar{\nu} = 2\bar{\nu}', \qquad \bar{\omega} = p^{\bar{\nu}'} + 1 > 2,$$

et ni L_1^0, ni L_2^0 ne pourront être de troisième catégorie.

Supposons d'abord que L_1^0 soit de première catégorie. On aura

$$\nu_1 = 2\nu_1', \qquad \nu_1' = 2m_1\bar{\nu}', \qquad \omega_1 = p^{2m_1\bar{\nu}'} - 1,$$

et l'inégalité

$$\bar{\nu}\frac{\omega_1}{\nu_1} \leqq \frac{16}{3}$$

deviendra

$$p^{2m_1\bar{\nu}'} - 1 \leqq \frac{16}{3}2m_1.$$

Cette inégalité est impossible si $p^{\bar{\nu}'} > 3$. Si $p^{\bar{\nu}'} = 3$, elle admettrait une solution pour $m_1 = 1$. Mais elle doit être rejetée, car on aurait $p^{\nu_1'} = 3^2$ et ce cas est exclu (**38**).

Si $p^{\bar{\nu}'} = 2$, on aurait les solutions $m_1 = 1$ ou 2. Mais la première doit être rejetée, $p^{\nu_1'}$ devant être > 4.

On aura donc

$$p = 2, \qquad \bar{\nu}' = 2, \qquad \bar{\omega} = 3, \qquad \bar{n} = 2^{\bar{\nu}'}\bar{\mu} = 2.3^{\bar{\rho}}$$

et, d'autre part,

$$\nu_1' = 4, \qquad \omega_1 = 2^4 - 1 = 3.5; \qquad n_1 = 2\nu_1'\mu_1 = 8.3^{\rho_1}.5^{\sigma_1}.$$

Donc $\bar{n}$ est impairement pair, et n_1 multiple de 8. Il en serait de même pour n_2 si L_2^0 était aussi de première catégorie et l'on ne pourrait avoir $n_1 + n_2 = \bar{n}$.

107. Il faut donc admettre que L_2^0 est de deuxième catégorie; d'où

$$\nu_2 = 2\nu_2' = (2m_2 - 1)\bar{\nu}', \qquad \omega_2 = p^{(2m_2-1)\bar{\nu}'} + 1,$$

et l'inégalité

$$\bar{\nu}\frac{\omega_2}{\nu_2} \leqq \frac{16}{3}$$

devient

$$p^{(2m_2-1)\bar{\nu}'} + 1 \leqq \frac{16}{3}(2m_1 - 1).$$

D'ailleurs, $p^{\bar{\nu}'}$ étant égal à 2, cette inégalité n'a lieu que si $m_2 < 3$.

L'hypothèse $m_2 = 2$ doit être rejetée, car on aurait $p^{\nu_2} = 2^3$, cas exclu.

Il faut donc supposer $m_2 = 1$, d'où

$$\nu'_2 = \bar{\nu}' = 1, \qquad \omega_2 = 3, \qquad n_2 = 2\mu_2 = 2.3^{\rho_2},$$

et n_2 sera impairement pair ainsi que n.

Donc n_1, n_2 ne peuvent être égaux et l'un d'eux sera $< \frac{1}{2}\bar{n}$.

Si $n_1 < \frac{1}{2}n$, ω_1 étant divisible par 5, L^0 contiendrait une substitution d'ordre 5 altérant moins de la moitié des variables, ce qui est inadmissible (74).

Si $n_2 < \frac{1}{2}\bar{n}$, on aura nécessairement $\mu_2 = 1$. Car s'il en était autrement, L_2^0 contiendrait dans ses seconds faisceaux des substitutions d'ordre 3 n'altérant que $\frac{2n_2}{3}$ variables, nombre inférieur à $\frac{\bar{n}}{3}$, ce qui est également inadmissible.

Donc n_2 sera égal à 2, $\bar{n}$ à 8 et n_1 à 6; mais il doit être multiple de 8, ce qui est contradictoire.

108. Nous sommes donc réduits à supposer que L_1^0 est de deuxième catégorie ainsi que L_2^0.

Nous aurons donc l'inégalité

$$p^{(2m_2-1)\bar{\nu}'} + 1 \leqq \frac{16}{3}(2m_2 - 1)$$

et pour L_1^0 une inégalité analogue où m_1 remplacera m_2.

Soient d'abord $p = 2$, $\bar{\nu}' = 1$. On n'aura aucune solution pour $m_2 > 2$. Pour $m_2 = 2$ on aurait $p^{\nu'_2} = 2^3$, cas exclu. Il faudrait donc supposer $m_1 = m_2 = 1$, d'où

$$\omega_1 = \omega_2 = \bar{\omega} = 3,$$

$$n_1 = 2.3^{\rho_1}, \qquad n_2 = 2.3^{\rho_2}, \qquad \bar{n} = 2.3^{\bar{\rho}},$$

valeurs qui ne peuvent satisfaire à la relation

$$n_1 + n_2 = \overline{n}.$$

Si $p = 2$, $\overline{\nu}' = 2$, il faudrait supposer $m_1 = m_2 = 1$

$$\omega_1 = \omega_2 = \overline{\omega},$$
$$n_1 = 4.5^{\rho_1}, \qquad n_2 = 4.5^{\rho_2}, \qquad \overline{n} = 4.5^{\overline{\rho}},$$

et l'égalité $n_1 + n_2 = \overline{n}$ serait encore impossible.

L'hypothèse $p = 2$, $\overline{\nu}' = 3$ doit être rejetée, car $\overline{L}^0$ ne serait pas indécomposable (**39**).

Si $p = 2$, $\overline{\nu}' > 3$, l'inégalité n'admet plus de solution.

Supposons enfin p impair. Si $p^{\overline{\nu}'} > 3$, l'inégalité ne sera pas possible même pour $m_2 = 1$. Si $p^{\overline{\nu}'} = 3$, elle le sera seulement pour $m = 1$. On aura dans ce cas

$$\overline{\omega} = \omega_1 = \omega_2 = 4,$$

$\overline{n}$, n_1, n_2 seront des puissances de 2 et l'on aura

$$n_1 = n_2 = \frac{1}{2}\overline{n}.$$

109. Supposons en dernier lieu que $\overline{L}^0$ soit de troisième catégorie.

Le nombre de ses variables sera une puissance de 2. Si donc $n_1 < \frac{1}{2}\overline{n}$, ω_1, ν'_1 seront des puissances de 2 et $\mu_1 = 1$ (**99**). Donc $n_1 = 2\nu'_1\mu_1$ sera aussi une puissance de 2. Mais il est $\geq \frac{1}{4}\overline{n}$ et $< \frac{1}{2}\overline{n}$. Donc il est égal à $\frac{1}{4}\overline{n}$; et $n_2 = \frac{3}{4}n$ sera divisible par 3. Donc L_2^0 ne pourra être de troisième catégorie, et l'on aura $\omega_2 = p^{\nu'_2} \pm 1$. D'ailleurs $n_2 = 2\nu'_2\mu_2$, et μ_2 n'a pour facteurs premiers que ceux de ω_2. Donc $\omega_2\nu'_2$ sera divisible par 3.

L_1^0 ne pourra non plus être de troisième catégorie. Car il ne contiendrait qu'une seule variable (μ_1 étant égal à 1); L_2^0 en contiendrait 3, nombre impair, ce qui est impossible.

On aura donc

$$n_1 = \nu_1 = 2\nu'_1, \qquad \omega_1 = p^{\nu'_1} \pm 1, \qquad \omega_2 = p^{\nu'_2} \pm 1,$$

$\omega_1\nu'_1$ n'ayant aucun diviseur impair, mais $\omega_2\nu'_2$ étant un contraire divisible par 3.

Enfin $\bar{\nu}$ étant égal à 1 et $\bar{\omega}$ à 2, l'inégalité fondamentale deviendra

$$\frac{p^{\nu_1}\pm 1}{2\nu'_1}\,\frac{p^{\nu_2}\pm 1}{2\nu'_2} \leqq \frac{32}{3}.$$

Il est impossible de satisfaire à cet ensemble de conditions si $p > 5$.

Si $p = 5$, on aurait la solution

$$\nu'_1 = \nu'_2 = 1, \qquad \omega_1 = 5 - 1, \qquad \omega_2 = 5 + 1,$$

μ_1 étant égal à 1, L_1^0, L_2^0, $\bar{L}^0$ contiendraient respectivement 2, 6 et 8 variables; donc $\mu_2 = 3$.

L'ordre de L_1 serait 8; quant à L_2^0, il contiendrait un second faisceau $h = \begin{pmatrix} 0 & A \\ & B \end{pmatrix}$ d'ordre 3^3 et son groupe auxiliaire à deux variables (mod 3) contiendrait dans son ordre un nouveau facteur 3; donc L_2^0 admettrait un groupe sylovien Λ_2 d'ordre 3^4, dont les substitutions seraient d'ailleurs échangeables aux huit substitutions de L_1^0.

Quant au groupe $\bar{L}^0$ de troisième catégorie à huit variables, nous avons indiqué plus haut (**104**) les valeurs diverses que peut avoir son ordre. Pour certaines d'elles on aura encore un groupe sylovien $\bar{\Lambda}$ d'ordre 3^4. Mais les seules substitutions de $\bar{L}^0$ échangeables à toutes celles de ce groupe sont les deux substitutions de son premier faisceau. Donc $\bar{L}^0$ ne peut contenir (L_1^0, L_2^0). Cette solution est donc à rejeter.

Si $p = 3$, ω_2 étant premier à 3, ν'_2 sera divisible par 3. Mais l'inégalité fondamentale ne serait pas satisfaite s'il était > 3. Il en serait de même si $\nu'_2 = 3$ et $\nu'_1 > 2$. D'ailleurs si ν'_1 était égal à 2 et $\omega_1 = 3^2 + 1$ il aurait un diviseur impair; et l'hypothèse $\omega_1 = 3^2 - 1$ ferait tomber dans un cas exclu (**38**). Il faut donc supposer

$$\nu'_1 = 1, \qquad \omega_1 = 3 + 1 = 4,$$
$$\nu'_2 = 3 \quad \text{et} \quad \omega_2 = \begin{cases} \text{ou} & 3^3 - 1 = 26, \\ \text{ou} & 3^3 + 1 = 28. \end{cases}$$

La première hypothèse est à rejeter, car $\bar{L}^0$ ne peut être divisible par 13. La seconde également, quoique $\bar{L}^0$ puisse contenir un groupe

sylovien $\overline{\Lambda}$ formé d'une substitution d'ordre 7; car $\overline{L}^0$ ne contient que deux substitutions échangeables à celle-là, tandis que L_2^0 contient aussi une substitution d'ordre 7, mais échangeable à toutes celles de L_1^0.

110. Supposons en dernier lieu que $\overline{L}^0$ étant toujours de troisième catégorie, on ait $n_1 = n_2 = \frac{1}{2}\overline{n}$, d'où $\overline{n}^2 = 4 n_1 n_2$. L'inégalité fondamentale deviendra

$$\frac{\omega_1}{\nu_1}\frac{\omega_1}{\nu_2} \leqq 8.$$

Si L_1^0, L_2^0 sont des deux premières catégories on aura

$$\frac{p^{\nu_1} \pm 1}{2\nu_1'}\frac{p^{\nu_2} \pm 1}{2\nu_2'} \leqq 8,$$

ν_1', ν_2' n'ayant pas de diviseur impair.

On n'a évidemment aucune solution si $p > 5$.

Si $p = 5$, on aura les solutions

$$\nu_1' = \nu_2' = 1 \left\{ \begin{array}{ll} \omega_1 = 5 - 1, & \omega_2 = 5 - 1, \\ \omega_1 = 5 - 1, & \omega_2 = 5 + 1, \end{array} \right.$$

et, si $p = 3$, les solutions

$$\nu_1' = \nu_2' = 1, \qquad \omega_1 = \omega_2 = 3 + 1;$$

$$\begin{array}{llll} \nu_1' = 1, & \nu_2' = 2, & \omega_1 = 3 + 1, & \omega_2 = 3^2 + 1; \\ \nu_1' = 2, & \nu_2' = 2, & \omega_1 = 3^2 + 1, & \omega_2 = 3^2 + 1. \end{array}$$

Si L_2^0 est de troisième catégorie sans que L_1^0 le soit, on aura $\frac{\omega_2}{\nu_2} = 2$ et l'inégalité devient

$$\frac{p^{\nu_1} \pm 1}{2\nu_1'} \leqq 4,$$

ν_1' n'ayant pas de diviseur impair.

Elle est impossible si $p > 7$.

Si $p = 7$, on a la solution

$$\nu_1' = 1, \qquad \omega_1 = 7 + 1, \qquad \omega_2 = 2.$$

Si $p = 5$, les solutions

$$\nu'_1 = 1, \quad \omega_1 = 5 - 1, \quad \omega_2 = 2;$$
$$\nu'_1 = 1, \quad \omega_1 = 5 + 1, \quad \omega_2 = 2.$$

Si $p = 3$, les solutions

$$\nu'_1 = 1, \quad \omega_1 = 3 + 1, \quad \omega_2 = 2,$$
$$\nu'_1 = 2, \quad \omega_1 = 3^2 + 1, \quad \omega_2 = 2.$$

Enfin si L_1^0 est ainsi que L_2^0 de troisième catégorie, on aura une dernière solution

$$\omega_1 = \omega_2 = 2.$$

111. Notre objet était d'établir que le groupe indécomposable $\overline{L}^0$ ne peut contenir le groupe complexe $L = (L_1, L_2, \ldots)$. Ce but serait déjà atteint si nous n'avions réservé pour une discussion ultérieure certains cas particuliers assez nombreux, mais présentant tous les caractères suivants :

1° Le nombre $\overline{\nu}$ des séries dans $\overline{L}^0$ est égal à 1 ou à 2.

2° Le nombre des variables dans chacune d'elles est une puissance de 2, telle que 2^s.

3° Les groupes partiels L_1^0, L_2^0 sont au nombre de 2; ils contiennent chacun la moitié des variables.

4° Le module p est impair; il ne surpasse pas 7 à moins que L_1^0, L_2^0, $\overline{L}_0$ ne soient tous trois de troisième catégorie, auquel cas il n'est pas déterminé.

L'exposant s est également indéterminé. Mais les considérations suivantes vont nous permettre de le limiter.

112. Soient $\overline{f}$ la substitution génératrice du premier faisceau de $\overline{L}^0$; $\overline{h}$, $\overline{h}'$, ... ses seconds faisceaux.

Leur réunion donnera un groupe

$$\overline{H} = (h, h', \ldots),$$

d'ordre 2^{2s+1} dont les substitutions seront échangeables entre elles aux puissances près de la substitution $\overline{0}$ qui multiplie toutes les variables par -1.

Les autres substitutions de $\overline{H}$ seront de deux sortes : les unes, d'ordre 4, multiplient une moitié des variables par j racine de la congruence $j^2 \equiv -1 \pmod p$ et les autres par $-j$; les autres, d'ordre 2, multiplient une moitié des variables par -1 et n'altèrent pas l'autre moitié.

Désignons par $f_1, h_1, h'_1, \ldots, 0_1$ et par $f_2, h_2, h'_2, \ldots, 0_2$ les expressions analogues pour les groupes L_1^0, L_2^0.

Le groupe $\overline{H}$ contenant la substitution $\overline{0} = 0_1 0_2$ contiendra nécessairement les deux substitutions 0_1, 0_2 s'il contient l'une d'elles.

Il contiendra dans tous les cas des substitutions échangeables à 0_1, formant un groupe Λ.

En effet, s'il contient 0_1, toutes les substitutions de $\overline{H}$ lui étant échangeables au signe près, la moitié d'entre elles lui sera échangeable. L'ordre de Λ sera donc 2^{2s}.

S'il ne contient pas 0_1, cette substitution aura pour correspondante, dans le groupe auxiliaire à $2s$ variables (mod 2) qui sert à la construction de $\overline{L}^0$, une substitution $\overline{\sigma}$ d'ordre 2 ayant une forme canonique telle que la suivante :

$$|x_1, y_1, x_2, y_2, \ldots z_1, \ldots \quad x_1 + y_1, y_1, x_2 + y_2, y_2, \ldots, z_1, \ldots|.$$

Le nombre s' des variables x, z est au moins égal à s. Or $\overline{\sigma}$ est échangeable aux $2^{s'}$ substitutions de la base qui accroissent les x et les z de termes constants sans altérer les y.

A chacune d'elles correspondent dans $\overline{H}$ deux substitutions, $\overline{T}$ et $\overline{T}\,\overline{0}$ échangeables à 0_1 au signe près. On a ainsi $2^{s'+1}$ substitutions dont la moitié au moins sera échangeable à 0_1.

L'ordre O du groupe Λ sera donc au moins égal à 2^s.

Mais nous allons, d'autre part, en déterminer une limite supérieure.

115. Les substitutions de L_1^0, étant échangeables à 0_1 et permutables à $\overline{H}$, seront permutables à Λ.

Soit d'ailleurs $\overline{U}$ une des substitutions de Λ. Étant échangeable à 0_1 elle sera le produit de deux substitutions partielles U_1, U_2 opérées respectivement sur les variables de L_1^0 et de L_2^0. Si deux

d'entre elles

$$\overline{U} = U_1 U_2, \qquad \overline{U}' = U_1 U_2'$$

correspondent à la même substitution partielle U_1, Λ contiendra la substitution

$$\overline{U}^{-1}\overline{U}' = U_2^{-1} U_2',$$

laquelle laisse inaltérées les variables de L_1^0; elle multipliera donc les autres variables par -1 ou les laissera inaltérées.

Si donc $\overline{H}$ ne contient pas les substitutions 0_2, 0_1, on aura $U_2' = U_2$ et O sera égal à O′ nombre des substitutions U_1. Dans le cas contraire il sera égal à $2O'$, U_2' pouvant être égal à U_2 ou à $0_2 U_2$.

Cherchons donc la valeur de O′.

114. Soit S_1 une substitution quelconque de L_1^0; Λ contiendra la substitution

$$S_1^{-1}\overline{U}S_1\overline{U}^{-1} = S_1^{-1}U_1 S_1 U_1^{-1},$$

laquelle laisse inaltérées les variables de L_2^0; elle se réduira donc à 0_1 ou à l'unité.

Si donc 0_1 n'appartient pas à $\overline{H}$, la substitution U_1 devra être échangeable à toutes les substitutions de L_1^0; c'est donc une puissance de f_1. D'ailleurs son ordre doit être un diviseur de 4. Donc si ω_1 est divisible par 4, ce sera l'une des puissances de $f_1^{\frac{\omega_1}{4}}$; et si ω_1 est impairement pair, ce sera l'une des puissances de $f_1^{\frac{\omega_1}{2}}$. Dans le premier cas,

$$2^s \leqq O' \leqq 4, \qquad \text{d'où} \qquad s \leqq 2,$$

et dans le second cas

$$2^s = O' \leqq 2, \qquad \text{d'où} \qquad s = 1.$$

Supposons au contraire que 0_1 appartienne à $\overline{H}$; S pourra transformer U_1 en U_1 ou en $U_1 0_1$. Celles des substitutions de L_1^0 qui sont échangeables à U_1 formeront un sous-groupe L invariant dans L_1^0 et d'indice 2. Soit h_1 l'un des seconds faisceaux, $2^{2\sigma+1}$ son ordre. Il aura au moins $2^{2\sigma}$ substitutions communes avec L; mais leurs transformées reproduiront toutes celles de h_1. Donc chacune des substitutions U_1 sera échangeable à celles des h_1, h_1', ... Mais

elles ne le sont pas nécessairement à f_1. Si elles ne le sont pas toutes, la moitié le seront et se réduiront comme tout à l'heure à des puissances de $f^{\frac{\omega_2}{4}}$ ou de $f^{\frac{\omega_1}{2}}$.

On aura donc, si ω_1 est multiple de 4,

$$2^{2s} = 2O' \leq 2.2.4, \qquad \text{d'où} \qquad s \leq 2,$$

et si ω_1 est impairement pair,

$$2^{2s} = 2O' \leq 2.2.2, \qquad \text{d'où} \qquad s = 1.$$

115. L'exposant s étant ainsi étroitement limité, il est aisé de déterminer l'ordre des groupes $\overline{L}^0$, L_1^0, L_2^0.

En effet, si les variables de $\overline{L}^0$ forment plusieurs séries (leur nombre $\bar{\nu}$ étant égal à 2), $\overline{L}^0$ contient une substitution P′ ou R′ qui les échange (**32**). Le nombre des substitutions qui les laissent immobiles s'obtiendra en multipliant l'ordre $\overline{\omega}\overline{\mu}^2$ de son noyau par l'ordre O_s d'un groupe auxiliaire à $2s$ variables (mod 2).

Si $s = 1$, on aura $O_1 = 6$.

Si $s = 2$, le groupe auxiliaire pourra présenter deux formes distinctes. Pour l'une d'elles on aura $O_2 = 5.2 = 10$, pour l'autre $O_2 = 2.6.6 = 72$.

L'ordre $\overline{\Omega}$ de $\overline{L}^0$ sera donc

$$\overline{\Omega} = \bar{\nu}\overline{\omega}\overline{\mu}^2 O_s.$$

Toutefois, si $\overline{L}^0$ est de troisième catégorie, le groupe auxiliaire devant être restreint à ses substitutions paires, le nombre ci-dessus devra être réduit de moitié.

Les ordres Ω_1, Ω_2 de L_1^0, L_2^0 se calculeront de même, si μ_1, μ_2 ne sont pas égaux à 1. Si $\mu_1 = 1$, on aura simplement $\Omega_1 = \nu_1\omega_1$.

Remarquons enfin que si L_1^0 et L_2^0 sont semblables, le groupe à comparer à $\overline{L}^0$ est le groupe décomposable ζ qu'on obtient par l'adjonction à L_1^0, L_2^0 de la substitution qui les permute; il a pour ordre $2\Omega_1\Omega_2$.

116. Nous pouvons maintenant procéder à la discussion de cas réservés.

I. S'il n'y a pas de forme invariante, on aura deux cas (**105**) :

1°

$$p=3, \qquad \nu_1=\nu_2=\bar{\nu}=1, \qquad \omega_1=\omega_2=\bar{\omega}=2.$$

Il faut supposer $s=1$. Le groupe $\mathfrak{L}$ ne contient donc que deux variables. C'est un cas exclu (**36**).

2°

$$p=5, \qquad \nu_1=\nu_2=\bar{\nu}, \qquad \omega_1=\omega_2=\bar{\omega}=4;$$

L_1^0 et L_2^0 semblables.

Si $s=1$, $\mathfrak{L}$ ne contient que deux variables (mod 5); ce cas est également exclu (**36**).

Si $s=2$, l'ordre de $\mathfrak{L}$ sera $2.(4.2^2.6)^2$ nombre supérieur à l'ordre 4.4^2O_2 de $\overline{L}^0$; $\mathfrak{L}$ ne pourra donc être contenu dans L^0.

II. Il y a une forme invariante; $\overline{L}^0$ est de première ou de deuxième catégorie; L_1^0 et L_2^0 sont semblables et l'on aura deux cas à discuter (**106** et **108**) :

3° ou 4°

$$p=3 \text{ ou } 5, \qquad \nu_1=\nu_2=\bar{\nu}=2, \qquad \omega_1=\omega_2=\bar{\omega}=4.$$

Si $s=1$, d'où $\mu_1=\mu_2=1$, $\bar{\mu}=2$, l'ordre de $\mathfrak{L}$ sera 2.8^2, nombre qui ne divise pas $2.4.2^2.6$, ordre de $\overline{L}^0$.

Si $s=2$, l'ordre de $\mathfrak{L}$ sera $2\,(2.4.2^2.6)^2$ et ne divise pas l'ordre de $\overline{L}^0$ égal à $2.4.4^2O_2$.

III. Il y a une forme invariante, et $\overline{L}^0$ est de troisième catégorie (**110**).

Si $s=1$, on n'a que deux variables; L_1^0, L_2^0 n'en contiendront qu'une. Ils seront donc de troisième catégorie et la forme invariante sera nécessairement quadratique. C'est un cas d'exclusion signalé (**35**).

Il faut donc supposer $s=2$. Le nombre des variables sera quatre, dont deux appartiennent à chacun des groupes L_1^0, L_2^0, et parmi toutes les combinaisons possibles on devra rejeter *a priori* toutes celles où l'un des nombres ω_1, ω_2 ne serait pas divisible par 4.

Les seules combinaisons qui restent sont les suivantes :

$p=5$; L_1^0, L_2^0 semblables et de première catégorie;

$p=3$; L_1^0, L_2^0 semblables et de deuxième catégorie.

Dans les deux cas on a

$$\nu_1' = \nu_2' = 1, \qquad \overline{\nu}' = 1, \qquad \omega_1 = \omega_2 = 1, \qquad \overline{\omega} = 2;$$
$$\mu_1 = \mu_2 = 1, \qquad \overline{\mu} = 1.$$

L'ordre de $\mathfrak{L}$ sera $2[2.4]^2 = 2^7$ et celui de $\overline{\mathrm{L}}^0$ sera $2.2^4.\frac{1}{2}\mathrm{O}_2$. Pour qu'il soit divisible par 2^7, il faut adopter parmi les deux valeurs de O_2 celle-ci : 2.6.6. Dans ce cas, $\Omega = 2^7.3^2$ et $\overline{\mathrm{L}}^0$ contiendra un groupe sylovien Λ d'ordre 2^7 qui devrait coïncider avec $\mathfrak{L}$.

Mais ces deux groupes, bien qu'ayant le même ordre, diffèrent par la structure. En effet, $\mathfrak{L}$ contient un seul sous-groupe invariant $\mathfrak{L}'$ d'indice 2 formé de la réunion des groupes L_1^0, L_2^0. Λ a de même un sous-groupe invariant Λ' d'indice 2 formé par le noyau de $\overline{\mathrm{L}}^0$; $\mathfrak{L}'$ et Λ' devraient coïncider, ce qui ne peut être, car les substitutions d'ordre 4 contenues dans Λ' ne laissent inaltérée aucune fonction des variables, tandis que $\mathfrak{L}'$ contient la substitution f_1 d'ordre 4 qui n'altère pas les variables de L_2^0.

Nous pouvons donc affirmer qu'un groupe décomposable ou complexe, construit avec les précautions indiquées dans la Section II, est maximum.

VIII. — Un groupe indécomposable L^0 ne peut être contenu dans un autre groupe indécomposable $\overline{\mathrm{L}}^0$.

117. Il nous reste à chercher à quelles conditions un groupe indécomposable L^0 pourrait être contenu dans un autre groupe indécomposable $\overline{\mathrm{L}}^0$.

Soient, comme précédemment,

$$f, \quad h = \begin{pmatrix} \theta, & \mathrm{A}_1 \dots \mathrm{A}_\sigma \\ & \mathrm{B}_1 \dots \mathrm{B}_\sigma \end{pmatrix}, \quad h', \quad \dots$$

le noyau de L^0,

$$\overline{f}, \quad \overline{h}, \quad \overline{h}', \quad \dots$$

celui de $\overline{\mathrm{L}}^0$.

Nous établirons successivement :

1° Que $\overline{f}$ est échangeable à toutes les substitutions du noyau de L^0, et par suite sera une puissance de f;

2° Que $\overline{f}$ et f coïncident;

3° Que L^0 et $\overline{L}^0$ ont le même noyau;

4° Et enfin qu'ils coïncident.

118. Comme dans la section précédente, nous nous appuierons sur ce que S, T étant deux substitutions quelconques de L^0, $S^{-1}\overline{f}S$, $T^{-1}\overline{f}T$ seront des puissances de $\overline{f}$ et le commutant $S^{-1}T^{-1}ST$ sera échangeable à $\overline{f}$.

Prenons pour S la substitution A_1 et pour T une substitution de L^0 qui ne lui soit pas échangeable aux puissances près de θ; le commutant $A_1^{-1}T^{-1}A_1T$ et ses transformées combinées ensemble reproduisent tout le faisceau h, et $\overline{f}$ sera échangeable à toutes ses substitutions. De même à celles des autres faisceaux h', ...

D'autre part, si dans L^0 le nombre des séries conjuguées est supérieur à 2, L^0 contiendra une substitution de la forme P^2Q dont le commutant avec f est f^{p^2-1}.

Si L^0 est de première catégorie, il contiendra une substitution de la forme RQ ou de la forme RPQ. Leurs commutants avec f seront respectivement f^{p+1} ou f^2.

Nous allons en conclure que $\overline{f}$ multiplie chaque variable de f par un facteur constant et par suite est échangeable à f.

119. *Premier cas.* — S'il n'y a pas de forme invariante, f sera d'ordre $p^\nu - 1$, et f^{p^2-1} multipliera les variables des séries ρ et $r+\rho$ respectivement par

$$i^{(p^2-1)p^2}, \qquad i^{(p^2-1)p^{r+\rho}}, \qquad [i^{p^\nu-1} \equiv 1 \pmod p].$$

Ces facteurs seront différents, à moins qu'on n'ait

$$(1) \qquad (p^2-1)(p^r-1) \equiv 0 \pmod{p^\nu-1}.$$

Si donc r ne peut être choisi de manière à satisfaire à cette relation, $\overline{f}$ devra remplacer chaque variable par une fonction des seules variables de la même série. Étant d'ailleurs échangeable à A_1, ...

qui multiplient ces variables par des facteurs différents, elle multipliera chacune d'elles par un facteur constant.

Or la relation (1) est impossible si $\nu > 2$; car si $r < \nu - 1$, son premier membre est $< p^\nu - 1$, et si $r = \nu - 1$, sa division algébrique par $p^\nu - 1$ donnera un reste $-p^{\nu-1} - p^2 + p + 1$ négatif et moindre en valeur absolue que $p^\nu - 1$.

Nous réserverons le cas où $\nu = 2$ pour une discussion ultérieure.

120. *Deuxième cas.* — Si L^0 est de première catégorie, on obtiendra le même résultat si celle des substitutions f^{p+1}, f^2 à laquelle $\overline{f}$ est échangeable multiplie les variables des diverses séries par des facteurs tous différents.

Cela aura lieu pour la substitution f^{p+1}, à moins qu'on n'ait par la comparaison de deux séries conjuguées, pour une valeur de r positive et moindre que ν',

$$(2) \qquad (p+1)(p^r - 1) \equiv 0 \pmod{p^{\nu'} - 1},$$

ou par la comparaison d'une série avec son associée ou les conjuguées de celles-ci, pour une valeur de r non négative et $< \nu'$,

$$(3) \qquad (p+1)(p^r + 1) \equiv 0 \pmod{p^{\nu'} - 1}.$$

La première condition est impossible, sauf pour $\nu' = 2$, cas que nous réserverons.

La seconde donnera, si $r = \nu' - 1$,

$$p^{\nu'-1} + p + 2 \equiv 0 \pmod{p^{\nu'} - 1}.$$

Or le premier membre est moindre que $p^{\nu'} - 1$: 1° si $\nu' > 3$; 2° si $\nu' = 3$, $p > 2$; 3° si $\nu' = 2$, $p > 3$.

Or pour $\nu' = 3$, $p = 2$ la congruence n'est pas satisfaite; d'autre part, $p^{\nu'} > 4$ et ne doit pas être égal à 3^2, ce cas étant exclu (**38**).

Il faut donc supposer $\nu' = 1$, d'où

$$p + 3 \equiv 0 \pmod{p - 1} \qquad \text{et} \qquad p = 5.$$

Mais le cas où $p^\nu = 5$ est exclu, si $\tau + \Sigma u$ est pair (**45**); et si $\tau + \Sigma u$ est impair, L^0 contiendra deux substitutions R', S telles que leur commutant $S^{-1}R'SR'^{-1}$ soit une puissance impaire de f (**59**).

Ce commutant f^ρ sera échangeable à $\overline{f}$ et, comme il multiplie

les deux séries par des facteurs différents, notre proposition sera démontrée.

Soit maintenant $r < \nu' - 1$. Le premier membre de la congruence (3) est évidemment $< p^{\nu'} - 1$, si $p > 2$ ou si $\nu' > 4$. Pour $p^{\nu'} = 2^3$, il n'est pas divisible par $2^3 - 1$. Mais pour $p^{\nu'} = 2^4$ on aura la solution $r = 2$, $p^{\nu'} = 2^4$.

Nous réserverons encore l'examen de ce cas.

Si $\overline{f}$ est échangeable à f^2, elle le sera *a fortiori* à f^{p+1}, si p est impair. Le seul cas nouveau est donc celui où $p = 2$. Il donne la congruence

$$2(2^r + 1) \equiv 0 \pmod{2^{\nu'} - 1}$$

et $2^{\nu'} - 1$ étant impair

$$2^r + 1 \equiv 0 \pmod{2^{\nu'} - 1},$$

évidemment impossible puisque $\nu' \geqq 3$.

121. *Troisième cas.* — Si L^0 est de deuxième catégorie, les séries conjuguées seront en nombre pair $2\nu'$, et f multipliera les variables de la $(\rho + 1)^{\text{ième}}$ série par $i^{(p^{\nu'}-1)p^\rho}$, où $i^{p^{2\nu'}-1} \equiv 1 \pmod{p}$.

Pour que la substitution f^{p^r-1} à laquelle $\overline{f}$ est échangeable multiplie par le même facteur deux séries différentes ρ et $\rho + r$, il faudra qu'on ait

$$(p^2 - 1)(p^r - 1) \equiv 0 \pmod{p^{\nu'} + 1},$$

pour une valeur de r positive et moindre que $2\nu'$.

Si $r < \nu' - 1$, le premier membre étant $< p^{\nu'}$, cette congruence est impossible.

Si $r = \nu' - 1$, la division algébrique montre que

$$-p - p^{\nu'-1} - p^2 + 1$$

devrait être divisible par $p^{\nu'} + 1$. Or il lui est inférieur en valeur absolue si $\nu' > 3$. De même si $\nu' = 3$ et $p > 2$. D'ailleurs $\nu' = 3$ et $p = 2$ rentrerait dans un cas exclu (**39**).

Si $\nu' = 2$, $p^2 + 1$ devrait diviser $-2p - p^2 + 1$ et par suite $-2p + 2$, ce qui est évidemment impossible.

Supposons enfin $r \geqq \nu'$. En le changeant en $\nu' + r$, nous aurons la

nouvelle congruence

$$(p^2-1)(p^r+1)\equiv 0 \qquad (\mathrm{mod}\, p^{\nu'}+1),$$

où r peut prendre les valeurs $0, 1, \ldots, \nu'-1$.

Cette congruence est impossible si $r<\nu'-2$, car on aura

$$(p^2-1)(p^r+1)<p^{r+2}+p^2<2p^{r+2}<p^{r+3}<p^{\nu'}.$$

Si $r=\nu'-2$, on aura

$$(p^2-1)(p^{\nu'-2}+1)\equiv -p^{\nu'-2}-2+p^2,$$

expression moindre en valeur absolue que $p^{\nu'}+1$. Il faudrait donc qu'elle s'annulât, ce qui n'a lieu que si $\nu'=3$, $p=2$. Mais ce cas est exclu (**39**).

Soit enfin $r=\nu'-1$:

$$\begin{aligned}(p^2-1)(p^{\nu'-1}+1)&=p^{\nu'+1}-p^{\nu'-1}+p^2-1\\ &\equiv -p^{\nu'-1}-p-1+p^2 \bmod p^{\nu'}+1.\end{aligned}$$

Cette dernière expression est négative et moindre en valeur absolue que $p^{\nu'}+1$, si $\nu'>2$. Si $\nu'=2$, elle se réduit à

$$p^2-2p-1\equiv -2(p-1),$$

expression qui ne peut être divisible par p^2+1.

Reste la seule hypothèse $\nu'=1$, dont l'examen sera réservé.

122. Les cas réservés dont nous allons entreprendre la discussion offrent ce caractère commun qu'il ne peut exister plus de deux variables x, x' qui soient multipliées par un même facteur dans chacune des substitutions monomes $A_1, \ldots$ et f^{p^2-1} (ou f^{p+1}) auxquelles nous savons déjà que $\overline{f}$ doit être échangeable; donc $\overline{f}$ sera de la forme

$$\overline{f}=|x, x', \ldots \quad lx+mx', m'x+l'x', \ldots|.$$

Il nous faut établir que $m\equiv m'\equiv 0 \pmod p$.

Nous y arriverons en exprimant que la transformée $\varphi=f^{-1}\overline{f}f$, étant une puissance de $\overline{f}$, lui est échangeable.

Soit en effet

$$f = |\, x,\ x',\ \ldots\quad ax,\ a'x',\ \ldots\,|.$$

On aura

$$\varphi = |\, x,\ x',\ \ldots\quad lx + a^{-1}a'mx',\ aa'^{-1}m'x + l'x',\ \ldots\,|.$$

L'identification de $\overline{f}\varphi$ et de $\varphi\overline{f}$ donnera les relations

$$\left.\begin{aligned} l^2 + aa'^{-1}mm' &\equiv l^2 + a^{-1}a'mm' \\ a^{-1}a'lm + ml' &\equiv lm + a^{-1}a'ml' \\ lm' + aa'^{-1}l'm' &\equiv aa'^{-1}lm' + l'm' \\ a^{-1}a'mm' + l'^2 &\equiv aa'^{-1}mm' + l'^2 \end{aligned}\right\} \pmod p,$$

ou en simplifiant

$$\left.\begin{aligned} [(a^{-1}a')^2 - 1]mm' &\equiv 0 \\ (a' - a)\ m(l' - l) &\equiv 0 \\ (a' - a)\, m'(l' - l) &\equiv 0 \end{aligned}\right\} \pmod p.$$

Si $(a^{-1}a')^2$ n'est pas congru à 1, l'un au moins des nombres m, m' sera nul; l'autre aussi, car dans l'hypothèse contraire on aurait $l' \equiv l$ et l'ordre de $\overline{f}$ serait divisible par p, ce qui est impossible.

Reste à discuter la possibilité de l'hypothèse $(a^{-1}a')^2 \equiv 1$.

123. Dans les deux premiers cas réservés, x, x' appartiennent à des séries conjuguées; a et a' sont respectivement égaux à i et à i^p, i étant racine primitive de la congruence

$$i^{p^2-1} \equiv 1 \pmod p.$$

On devrait donc avoir

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

d'où

$$2(p-1) \equiv 0 \pmod{p^2-1},$$

congruence évidemment impossible.

Dans le troisième cas, L^0 est de première catégorie, $p^{\nu'} = 2^1$; x, x', ne sont pas conjugués et $r = 2$. On aura donc

$$a^{2^1-1} \equiv 1 \qquad \text{et} \qquad a' = a^{-2^1},$$

d'où

$$(a^{-1}a')^2 = a^{-10}, \qquad -10 \equiv 0 \pmod{2^4 - 1},$$

ce qui n'a pas lieu.

Dans le quatrième et dernier cas, L^0 est de deuxième catégorie, et $\nu' = 1$. On aura donc

$$a^{p+1} \equiv 1 \pmod{p}, \qquad a' = a^p,$$
$$(a^{-1}a')^2 = a^{2(p-1)},$$

d'où

$$2(p-1) \equiv 0 \pmod{p+1},$$
$$-4 \equiv 0 \pmod{p+1}.$$

Cette congruence admet la seule solution $p = 3$.

D'ailleurs on tombera sur un cas exclu si $\tau + \Sigma u$ est impair (**44**); et s'il est pair, L^0 contiendra deux substitutions P', S telles que le commutant $S^{-1}P'SP'^{-1}$ soit une puissance impaire de f, telle que f^ρ (**59**). f étant d'ordre 4 sera réciproquement une puissance de f^ρ et sera échangeable à $\overline{f}$.

Il est donc prouvé que dans tous les cas $\overline{f}$ est échangeable à toutes les substitutions du noyau de L^0.

124. Corollaire I. — *$\overline{f}$ sera une puissance de f.*

En effet, soit i l'imaginaire que les variables contiennent dans leur expression. Les facteurs par lesquels $\overline{f}$ multiplie ces variables seront nécessairement des puissances de i et les variables conjuguées seront multipliées par des puissances conjuguées. Enfin, dans le cas des groupes de seconde catégorie où $\nu = 2\nu'$, ces multiplicateurs seront des puissances de $i^{p^{\nu'}-1}$, cette condition étant nécessaire pour que $\overline{f}$ n'altère pas la forme invariante.

125. Corollaire II. — *$\overline{\nu}$ divise ν.*

Nous venons en effet de voir que $\overline{\omega}$ divise ω.

Or s'il n'y a pas de forme invariante,

$$\overline{\omega} = p^{\overline{\nu}} - 1.$$

Si L^0 est de première catégorie,

$$\overline{\nu} = 2\overline{\nu}', \qquad \overline{\omega} = p^{\overline{\nu}'} - 1 \qquad (p^{\nu'} > 4);$$

S'il est de deuxième catégorie,

$$\overline{\nu} = 2\overline{\nu}', \qquad \overline{\omega} = p^{\overline{\nu}'} + 1;$$

S'il est de troisième catégorie,

$$\overline{\nu} = 1, \qquad \overline{\omega} = 2.$$

On aura de même, suivant les cas,

$$\omega = p^{\nu} - 1,\ p^{\nu'} - 1,\ p^{\nu'} + 1,\ 2.$$

Mais, pour que ω soit divisible par $\overline{\omega}$, il faut qu'on ait :
Si $\overline{\omega} = p^{\overline{\nu}} - 1$,

$$\omega = p^{m\overline{\nu}} - 1, \qquad \nu = m\overline{\nu};$$

Si $\overline{\omega} = p^{\overline{\nu}'} - 1$,

$$\omega = p^{m\overline{\nu}'} - 1, \qquad \nu' = m\overline{\nu}', \qquad \nu = m\overline{\nu};$$

Si $\overline{\omega} = p^{\overline{\nu}'} + 1$,

$$\omega = p^{2m\overline{\nu}'} - 1, \qquad \nu' = 2m\overline{\nu}', \qquad \nu = 2m\overline{\nu},$$

ou

$$\omega = p^{(2m-1)\overline{\nu}'} + 1, \qquad \nu' = (2m-1)\overline{\nu}', \qquad \nu = (2m-1)\overline{\nu}.$$

Enfin si $\overline{\omega} = 2$, $\overline{\nu} = 1$ et divise ν.

126. THÉORÈME II. — *Les $\omega\mu^2$ substitutions du noyau de L^{ν} sont échangeables entre elles aux puissances près de $\overline{f}$.*

Elles le sont, en effet, aux puissances près des substitutions

$$\theta = f^{\frac{\omega}{\overline{\pi}}}, \qquad \theta' = f^{\frac{\omega}{\overline{\pi}}}, \qquad \ldots,$$

π, π', ... étant les facteurs premiers de μ. Or

$$\mu\nu = \overline{\mu}\overline{\nu},$$

ces deux expressions représentant le nombre n des variables;

$\overline{\nu}$ divisant ν, μ et par suite π divisera $\overline{\mu}$. Donc π divise aussi $\overline{\omega}$. Donc $\overline{f}^{\frac{\overline{\omega}}{\pi}}$ sera une puissance de $\overline{f}$, qui lui-même est puissance de f. Mais elle est d'ordre π comme θ, et celles des puissances de f qui sont d'ordre π sont des puissances les unes des autres. Donc θ est une puissance de $\overline{f}$.

Or l'ordre d'un groupe contenu dans $\overline{\mathrm{L}}^0$ et dont les substitutions sont échangeables aux puissances près de $\overline{f}$ ne peut surpasser $\overline{\omega}\overline{\mu}^2$. Il ne peut même atteindre ce chiffre que s'il contient des substitutions de chacun des faisceaux $\overline{h}$, $\overline{h}'$, ... (**91**).

Nous avons donc l'inégalité

$$\omega\mu^2 \overline{\leq} \overline{\omega}\overline{\mu}^2,$$

qui nous permettra d'établir la proposition suivante.

127. Théorème III. — *Les premiers faisceaux des groupes* L^0 et $\overline{\mathrm{L}}^0$ *sont identiques.*

1° En effet, supposons d'abord qu'il n'y ait pas de forme invariante. On aura

$$\omega = p^{m\overline{\nu}} - 1, \qquad \overline{\omega} = p^{\overline{\nu}} - 1, \qquad \overline{\mu} = m\mu.$$

L'inégalité devient donc

$$p^{m\overline{\nu}} - 1 \overline{\leq} (p^{\overline{\nu}} - 1)\, m^2.$$

Si m était égal à 1, le théorème serait démontré. Si d'ailleurs on remarque que $p^{\nu} > 2$, on n'aura pour solution où m soit > 1 que celle-ci :

$$p^{\overline{\nu}} = 3, \qquad m = 2.$$

Mais le groupe L^0 qu'elle donnerait est exclu (**41**).

2° Si $\overline{\mathrm{L}}^0$ est de première catégorie il en sera de même pour L^0, et l'inégalité sera la même, sauf le changement de $\overline{\nu}$ en $\overline{\nu}'$. D'ailleurs $p^{\overline{\nu}} > 4$. Il n'existe donc aucune solution où m soit > 1.

3° Si $\overline{\mathrm{L}}^0$ est de deuxième catégorie et L^0 de première, on aura

$$\overline{\mu} = 2m\mu, \qquad \overline{\omega} = p^{\overline{\nu}'} + 1, \qquad \omega = p^{2m\overline{\nu}'} - 1,$$

d'où

$$p^{2m\overline{\nu}'} - 1 \overline{\leq} (p^{\overline{\nu}'} + 1)\, 4m^2.$$

D'ailleurs $\overline{\mu}$ étant pair, $p^{\overline{\nu}}+1$, qu'il divise, le sera. Donc p est impair. L'inégalité admet les solutions

$$p^{\overline{\nu}'}=3, \qquad m=1,$$
$$p^{\overline{\nu}'}=5, \qquad m=1.$$

Mais ces deux cas sont exclus (**38** et **42**).

4° Si $\overline{\mathrm{L}}^0$ est de deuxième catégorie, ainsi que L^0, on aura l'inégalité

$$p^{(2m-1)\overline{\nu}'}+1 \equiv (p^{\overline{\nu}'}+1)(2m-1)^2.$$

Pour $m=1$, le théorème serait démontré. On aurait une autre solution pour $p=2$,

$$m=2, \qquad \overline{\nu}'=1, \qquad \text{d'où} \qquad p^{\overline{\nu}'}=2^3.$$

Mais ce cas est exclu (**39**).

5° Si $\overline{\mathrm{L}}^0$ est de troisième catégorie, on aura

$$\overline{\omega}=2, \qquad \overline{\nu}=1,$$

d'où, si L^0 est de première ou de deuxième catégorie, $\nu=2\nu'$

$$p^{\nu'}-1 \equiv 8\nu'^2 \qquad \text{ou} \qquad p^{\nu'}+1 \equiv 8\nu'^2.$$

D'ailleurs p est impair et ν' puissance de 2. Sous le bénéfice de ces observations, on aura les solutions

$$p^{\nu'}=3,\ 3^2,\ 3^4,\ 5,\ 5^2,\ 7,$$

dont nous réserverons la discussion. D'ailleurs la solution $p^{\nu'}=3$ n'existera pas si L^0 est de première catégorie, car $p^{\nu'}$ doit être >4.

6° Enfin, si $\overline{\mathrm{L}}^0$ et L^0 sont de troisième catégorie, le théorème est vérifié.

128. Théorème. — L^0 *sera identique à* $\overline{\mathrm{L}}^0$.

Remarquons tout d'abord que les substitutions de L^0 sont permutables à chacun des seconds faisceaux $\overline{h}$, $\overline{h}'$, ... Mais il pourrait arriver qu'elles fussent permutables à un sous-groupe $\overline{h}_1$ de $\overline{h}$.

LEMME. — *Celles des substitutions de* $\overline{h}_1$, *qui sont échangeables à toutes les autres, sont les puissances de* $\overline{\theta} = \overline{f}^{\frac{\overline{\omega}}{\pi}}$.

Car dans le cas contraire ces substitutions jointes à f donneraient un faisceau abélien permutable aux substitutions de L^0 et dont les substitutions ne seraient pas puissances d'une seule d'entre elles : L^0 ne serait donc pas indécomposable, contrairement à notre supposition.

$\overline{h}_1$ sera donc d'ordre π^{2s_1+1} et sera dérivé de $2s_1$ substitutions génératrices qu'on pourra prendre pour

$$A_1, \ \ldots, \ A_{s_1},$$
$$B_1, \ \ldots. \ B_{s_1}.$$

Les substitutions de $\overline{h}$ échangeables à toutes celles de $\overline{h}_1$ formeront un sous-groupe complémentaire k d'ordre $\pi^{2(\sigma-s_1)+1}$ et dérivé de $2(\sigma - s_1)$ génératrices.

Soient donc $\overline{h}_1$ un sous-groupe minimum parmi ceux de $\overline{h}$ qui sont permutables aux substitutions de L^0 (et ne se réduisent pas aux puissances de $\overline{f}$); $\overline{h}_2$ un groupe minimum parmi les sous-groupes de k qui jouissent de cette propriété, etc. $\overline{h}$ sera un produit de sous-groupes $\overline{h}_1$, $\overline{h}_2$, ... d'ordres $2s_1+1$, $2s_2+1$, ... ayant en commun les puissances de $\overline{\theta}$.

On pourra, s'il y a lieu, décomposer de même chacun des faisceaux $\overline{h}'$, ... en un produit de groupes partiels.

129. Cela posé, L^0 sera contenu dans un groupe L'^0 ayant pour seconds faisceaux $\overline{h}_1$, $\overline{h}_2$, ..., $\overline{h}_1$, ...

Ces seconds faisceaux seront d'ailleurs identiques à h, h', ... Il résulte en effet du théorème du n° **91** que chacun d'eux doit contenir quelque substitution du noyau de L^0 autre que les puissances de f.

Supposons donc que $\overline{h}_1$ renferme une substitution $f^\lambda tt'$, ..., où t appartienne à h, t' à h', ... Il contiendra ses transformées par les substitutions de L^0. Or, parmi celles-ci, il en existe une échangeable à $f, t', \ldots$ et transformant t en une autre substitution t_1

du groupe h qui ne soit pas de la forme $f^{\alpha}t$; donc $\overline{h}_1$ contiendra la substitution $t_1 t^{-1}$ et ses transformées par les substitutions de L^{α}. Or celles-ci, par leur combinaison, reproduisent tout le faisceau h.

Or, par construction, il ne contient aucun sous-groupe permutable aux substitutions de L^{α}. Donc h contient réciproquement toutes les substitutions de $\overline{h}_1$ et se confond avec lui.

130. Cela posé, $\overline{L}^{\alpha}$ se construit à l'aide de groupes auxiliaires primaires dont l'un $\overline{\Lambda}$ correspond au second faisceau $\overline{h} = (h_1, h_2, \ldots)$ et L^{α} à l'aide de groupes primaires analogues. Ceux de ces groupes $\Lambda_1, \Lambda_2, \ldots$ qui correspondent aux faisceaux $h_1, h_2, \ldots$ formeraient par leur réunion un groupe complexe qui devrait être contenu dans Λ. Or cela est impossible, d'après la Section VII.

L'hypothèse de la décomposition de $\overline{h}$ en un produit de plusieurs groupes différents $h_1, h_2, \ldots$ est donc inacceptable, et il faut admettre qu'on ait $\overline{h} = \overline{h}_1 = h$ et que Λ_1, groupe primaire, soit contenu dans $\overline{\Lambda}$. Le nombre des variables dans ces groupes étant moindre que dans L^{α}, on peut admettre comme démontrée l'identité de Λ_1 et de $\overline{\Lambda}$. Dès lors, les groupes $\overline{L}^{\alpha}$ et L^{α} ayant mêmes premier et second faisceaux, et étant construits avec les mêmes groupes auxiliaires, seront identiques.

131. Nous avons réservé (**127**) l'examen de quelques groupes L^{α} de première et deuxième catégorie pour lesquels p^{ν} a l'une des valeurs suivantes

$$3,\quad 3^2,\quad 3^4,\quad 5,\quad 5^2,\quad 7.$$

Notre longue discussion sera terminée, si nous établissons que, sauf les cas d'exclusion signalés, aucun de ces groupes ne peut être contenu dans un groupe $\overline{L}^{\alpha}$, de troisième catégorie.

S'il existait plusieurs groupes de l'espèce $\overline{L}^{\alpha}$ contenant L^{α}, nous choisirions pour la démonstration l'un de ceux où le nombre des seconds faisceaux $\overline{h}, \overline{h}', \ldots$ est le plus grand possible.

Le nombre des variables de L^{α} est une puissance de 2; et le nombre $2^{\nu'}$ des séries qu'elles forment sera, suivant le cas, 2, 4, ou 8. Désignons-le par 2^{β}.

Si L^{α} est de première catégorie et $\nu' > 1$, L^{α} contiendra (**52**)

les substitutions

$$R', \quad P'$$

et les substitutions $R'^{\alpha}P'^{\beta}f^{\gamma}$ formeront un sous-groupe Γ dont nous désignerons d'une manière générale les substitutions par la lettre U.

Les substitutions qui ne déplacent pas les séries sont des formes T, T', ... définies au n° **26**. Elles sont permutables à Γ. Les puissances de f sont communes à ces diverses formes et à la forme U.

Si, L^0 étant encore de première catégorie, $\nu' = 1$, on n'aura pas de substitution P' et les substitutions de Γ seront de la forme

$$U = R'^{\alpha}f^{\gamma}.$$

Si L^0 est de deuxième catégorie, R' manquera et Γ sera formé des substitutions

$$U = P'^{\beta}f^{\gamma}.$$

Dans tous les cas, les substitutions de L^0 auront pour forme générale

$$UTT'....$$

132. Cela posé, soit $\bar{h}$ l'un des seconds faisceaux de $\bar{L}^0$. Les substitutions communes à $\bar{h}$ et à L^0 formeront dans L^0 un sous-groupe invariant.

Si l'une d'elles V n'appartient pas à U, $\bar{h}$ coïncidera avec un second faisceau h de L^0.

Soit en effet

$$V = UTT'...,$$

l'un au moins des facteurs T, T', ..., par exemple T, ne se réduisant pas à une puissance de f. Si T n'appartient pas à h, on pourra déterminer dans h une substitution S qui ne lui soit pas échangeable aux puissances près de f; et le commutant

$$S^{-1}TST^{-1}$$

serait commun à h et à $\bar{h}$. Il en serait de même de ses transformées, dont la combinaison reproduit h.

Donc $\bar{h}$ contient h et résulte de la combinaison de h avec un

autre groupe partiel h_1, formé par celles de ses substitutions qui sont échangeables à toutes celles de h.

D'ailleurs les substitutions de L^0, étant permutables à $\overline{h}$ et à h, le seront évidemment à h_1. Donc L^0 serait contenu dans un groupe L'^0 analogue à $\overline{L}^0$, mais où le second faisceau $\overline{h}$ serait dédoublé, ce qui est contraire à la définition de $\overline{L}^0$.

Désignons donc par K l'ensemble des seconds faisceaux communs à L^0 et à $\overline{L}^0$; par H et $\overline{H}$ celui des seconds faisceaux respectivement spéciaux à L^0 et à $\overline{L}^0$. Soit $2r$ le nombre des génératrices de H; celui des génératrices de $\overline{H}$ sera évidemment $2(r+\rho)$.

Soient enfin Λ, $\overline{\Lambda}$ les groupes formés par celles des substitutions de L^0 et de $\overline{L}^0$ qui sont échangeables à toutes celles de K. Si L^0 était contenu dans $\overline{L}^0$, Λ le serait dans $\overline{\Lambda}$. Il nous faut démontrer que cela est impossible.

133. A cet effet, considérons parmi les substitutions U un groupe Γ_1, formé comme il suit :

Si les U sont de la forme

$$R'^{\alpha} P'^{\beta} f^{\gamma},$$

Γ_1 aura pour génératrices

$$R', \quad P'^{\frac{\nu'}{2}},$$

auxquelles on joindra $f^{\frac{\omega}{4}}$ si ω est divisible par 4, ou $f^{\frac{\omega}{2}}$ si ω est impairement pair.

L'ordre de ce groupe sera 2^{t+1} où $t=3$, si ω est divisible par 4; $t=2$ dans le cas contraire.

Si les U se réduisent à la forme plus simple

$$R'^{\alpha} f^{\gamma},$$

Γ_1 aura pour génératrices

$$R' \text{ et } f^{\frac{\omega}{4}} \left(\text{ou } f^{\frac{\omega}{2}}\right),$$

et son ordre sera 2^{t+1} où $t=2$ (ou 1 si ω n'est pas divisible par 4).

Si les U sont de la forme

$$P'^{\beta} f^{\gamma},$$

Γ_1 aura pour génératrices

$$P^{\nu'} \quad \text{et} \quad f^{\frac{\omega}{4}} \quad \left(\text{ou } f^{\frac{\omega}{2}}\right),$$

et son ordre sera 2^{t+1}, où $t = 2$ (ou 1).

En adjoignant à Γ_1 les $2r$ substitutions génératrices de H, on obtiendra un groupe binaire (1) (Γ_1, H) d'ordre 2^{2r+t+1} contenu dans Λ et *a fortiori* dans $\overline{\Lambda}$. Si cet ordre est supérieur à $2^{r+\rho+1}$, ce groupe aura au moins

$$2^{2r+t+1-(r+\rho)} = 2^{r+t-\rho+1},$$

substitutions communes avec $\overline{\Pi}$ (**93**).

Mais ces substitutions communes, étant de la forme U, devront appartenir à Γ_1. Elles forment d'ailleurs un groupe permutable aux substitutions de L^0 et en particulier à f. Enfin leur ordre divise 4. Donc si U_1 est l'une d'elles, son commutant avec f_1 qui est une puissance de f_1, élevé à la quatrième puissance, donnera l'unité.

Soit donc $2^{t'+1}$ l'ordre du groupe Γ_2 formé par celles des substitutions de Γ_1 qui satisfont à cette condition; on aura

$$2^{r+t-\rho+1} = 2^{t'+1},$$

d'où

$$r \leq \rho - (t - t').$$

154. Il est d'ailleurs aisé de déterminer $t - t'$.

Si les substitutions de Γ_1 sont de la forme

$$R'^{\alpha} P^{\nu'\frac{\beta}{2}} f^{\gamma} \qquad [\text{où } \gamma \equiv 0 \pmod{\omega}],$$

leur commutant avec f sera

$$f^{\frac{\omega}{4}\left[(-1)^{\alpha} p^{\frac{\nu'}{2}\beta} - 1\right]},$$

et les substitutions de Γ_2 devront satisfaire à la condition

$$(1) \qquad \frac{\omega}{4}\left[(-1)^{\alpha} p^{\frac{\nu'}{2}\beta} - 1\right] \equiv 0 \pmod{p^{\nu'} - 1}.$$

Si elles sont de la forme

$$R'^{\alpha} f^{\gamma} \qquad [\text{où } \gamma \equiv 0 \pmod{\omega_1}],$$

(1) *Voir* au n° **93** la définition de ce terme.

la condition sera

$$(2) \qquad \gamma[(-1)^{\alpha}-1] \equiv 0 \pmod{p^{\gamma'}-1}.$$

Enfin si elles sont de la forme

$$P^{\gamma'\beta}f^{\gamma} \qquad [\text{où } \gamma\gamma \equiv 0 \pmod{\omega}].$$

la condition sera

$$(3) \qquad \gamma(p^{\gamma'\beta}-1) \equiv 0 \pmod{\omega}.$$

153. Nous sommes maintenant en mesure d'étudier successivement les divers cas réservés.

1. Soit $\varrho = 3$, $\omega = 3^4 - 1 = 80$. On aura $t = 3$.

La relation (1) se réduit à

$$\gamma[(-1)^{\alpha}3^{2\beta}-1) \equiv 0 \pmod{80},$$

et n'a d'autre solution que $\alpha = \beta = 0$. D'ailleurs γ est susceptible de 4 valeurs. Donc.

$$t' = 1, \qquad t - t' = 2, \qquad r \leq 1.$$

Si $r = 1$, Π contient un seul couple de substitutions A, B. Elles auront pour caractère 1, car autrement on tomberait dans un cas d'exclusion (**40**). Donc Λ contiendra une substitution S d'ordre 3 qui permute circulairement A, B, AB. Elle sera échangeable à la substitution f d'ordre $3^4 - 1 = 80$ que Λ contient également.

Donc Λ contient Sf d'ordre 240.

Or $\overline{\Lambda}$ ne peut contenir aucune substitution de cet ordre.

En effet, son noyau $\overline{\Pi}$ étant dérivé de 4 couples de substitutions

$$\begin{matrix} A_1, & \ldots, & A_4, \\ B_1, & \ldots, & B_4, \end{matrix}$$

aux substitutions de $\overline{\Lambda}$ correspondront les substitutions paires d'un groupe auxiliaire $\mathfrak{G}$ à 8 variables (mod 2) : et les substitutions de $\overline{\Pi}$ ayant toutes pour ordre un diviseur de 4, il faudrait que $\mathfrak{G}$ contînt une substitution dont l'ordre fût divisible par $\frac{240}{4} = 60$. L'ordre de $\mathfrak{G}$ serait donc divisible par 3 et par 5. Cela ne peut avoir lieu que si $\mathfrak{G}$ est complexe et produit de deux groupes

partiels $\mathfrak{L}_1$, $\mathfrak{L}_2$ à 4 variables, le premier indécomposable d'ordre $(2^2+1).4$, le second décomposable et d'ordre $2.[2.3]^2$.

Toute substitution de $\mathfrak{L}$ est le produit de deux autres $\mathfrak{S}_1$ et $\mathfrak{S}_2$ échangeables entre elles et appartenant respectivement à $\mathfrak{L}_1$ et à $\mathfrak{L}_2$. Mais $\mathfrak{L}_1$ ne contient aucune substitution d'ordre >5, il faudrait donc supposer que $\mathfrak{S}_1$ est d'ordre 5 et par suite $\mathfrak{S}_2$ d'ordre divisible par 12. Mais on voit aisément que $\mathfrak{L}_2$ ne contient aucune substitution de cet ordre.

Si $r=0$, Λ contiendra la substitution f d'ordre 80. Mais $\overline{\Lambda}$ ne pourra la contenir; car sa construction demandera l'emploi d'un groupe auxiliaire $\mathfrak{L}$ produit de deux groupes partiels; l'un $\mathfrak{L}_1$ à 4 variables (mod 2) et d'ordre $(2^2+1)4$, l'autre $\mathfrak{L}_2$ à 2 variables et d'ordre 2.3. La substitution de $\mathfrak{L}$ correspondant à f devrait avoir son ordre divisible par $\frac{80}{4}=20$ et serait de la forme $\mathfrak{S}_1\mathfrak{S}_2$; $\mathfrak{S}_1$ serait d'ordre 5, l'ordre de $\mathfrak{S}_2$ devrait être divisible par 4, ce qui est impossible.

136. II. Soit $p=3$, $\omega=3^4+1=82$. Puisque ω n'est pas divisible par 4, on a $t=1$. D'ailleurs l'inégalité (3), qui devient ici

$$4(3^{4\beta}-1)\equiv 0 \pmod{82},$$

n'est satisfaite que pour $\beta=0$ et γ n'est susceptible que de 2 valeurs. Donc $t-t'=1$, $r\leqq 2$.

Λ contient la substitution f^2 d'ordre 41. Elle ne peut être contenue dans $\overline{\Lambda}$ dont l'ordre est $2.2^{2(r+3)}O$, O désignant l'ordre d'un groupe auxiliaire (mod 2) où le nombre $2(r+3)$ des variables est au plus égal à 10. Or aucun de ces groupes n'a son ordre divisible par 41.

137. III et IV. Si $p=2$ et $\omega=5^2-1$ ou 3^2-1, on tombe sur des cas exclus (**42** et **38**).

138. V. Si $p=2$ et $\omega=5^2+1$, on aura $t-t'=1$, d'où $r\leqq 1$, $r+p\leqq 3$; Λ contient une substitution f^2 d'ordre 13; mais l'ordre de $\overline{\Lambda}$ ne peut être divisible par 13.

139. VI. Si $p=2$ et $\omega=3^p+1$, on aura encore $t-t'=1$, $r\leqq 1$, $r+p\leqq 3$.

Si $r = 1$, H contiendra un couple unique A, B, de caractère nécessairement égal à 1; Λ contiendra une substitution d'ordre 3 transformant A, B en B, AB et une autre substitution f^2 d'ordre 5; $\overline{H}$ contient deux couples de génératrices $\overline{A}_1, \overline{B}_1; \overline{A}_2, \overline{B}_2$. Mais de quelque manière que soit choisi le groupe auxiliaire qui sert à construire $\overline{\Lambda}$, son ordre ne peut être divisible à la fois par 3 et par 5.

Si $r = 0$, Λ contiendra encore f^2, mais l'ordre de $\overline{\Lambda}$ ne peut être divisible par 5.

140. Passons aux cas où $\rho = 1$. Désignant respectivement par Σ_H, $\Sigma_{\overline{H}}$, Σ_K la somme des caractères des couples de substitutions qui engendrent respectivement H, $\overline{H}$, K, on aura dans le groupe L^0

$$\Sigma u = \Sigma_H + \Sigma_K.$$

Et pour que $\overline{L}^0$ admette une forme invariante non nulle, il faut qu'on ait

$$\tau + \Sigma_{\overline{H}} + \Sigma_K \equiv 0 \pmod 2 \qquad (29).$$

On en déduit

$$\tau + \Sigma u \equiv \Sigma_H + \Sigma_{\overline{H}} \pmod 2.$$

Or, r ne peut surpasser ρ. S'il est nul, $\Sigma_H = 0$ et $\Sigma_{\overline{H}} = 1$, car $\overline{H}$ ne contient qu'un seul couple, qui doit avoir 1 pour caractère, si l'on veut éviter de tomber sur un cas exclu (**40**).

Si $r = 1$, Σ_H est égal à 1; et Λ a son ordre divisible par 3. Pour qu'il en soit de même pour $\overline{\Lambda}$, il faut que le groupe auxiliaire à 4 variables (mod 2) qui sert à le construire soit décomposable; auquel cas $\Sigma_{\overline{H}} = 2$.

On aura donc nécessairement

$$\tau + \Sigma u \equiv 1 \pmod 2.$$

Cette condition étant supposée remplie, nous rencontrons, si $\omega = 5 - 1$ ou $3 + 1$, des cas d'exclusion signalés aux n^{os} **43** et **44**.

Si $\omega = 7 + 1$ ou $7 - 1$, L ne peut être contenu dans un groupe $\overline{L}$ de troisième catégorie, celui-ci ne pouvant contenir de substitution qui multiplie sa forme invariante Φ par un non résidu de 7 (car 2 est non résidu).

Mais si L doit être employé comme groupe auxiliaire (ce qui suppose $\tau = 1$), L'' sera contenu dans $\overline{L}''$; cas d'exclusion signalés aux n^{os} **46** et **47**.

141. Il ne reste plus pour terminer cette laborieuse discussion qu'à examiner le cas où $\rho = 1$, $\omega = 5 + 1$. On aura ici $t - t' = 1$, d'où $r = 0$. Le groupe Λ contiendra la substitution f^2 d'ordre 3 et une substitution P' qui la transforme en son carré. Le groupe $\overline{\Lambda}$ est dérivé d'un couple $\overline{A}$, $\overline{B}$ et d'une substitution S qui permute circulairement les substitutions A, B, AB. Il ne contient pas la substitution qui échange A et B, laquelle transformerait S en S^2; car cette substitution correspondrait à une substitution impaire du groupe auxiliaire et 2 n'est pas résidu de 5. Donc $\overline{\Lambda}$ ne peut contenir Λ.