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

CAMILLE JORDAN

Sur les groupes linéaires (mod$p$) à invariant quadratique

Journal de mathématiques pures et appliquées 7^e série, tome 2 (1916), p. 253-280.
<http://www.numdam.org/item?id=JMPA_1916_7_2__253_0>

Sur les groupes linéaires (mod p) *à invariant quadratique;*

PAR CAMILLE **JORDAN.**

M. Dickson a consacré plusieurs Chapitres de son bel Ouvrage (*Linear Groups*, Teubner, Leipzig, 1901) à l'étude approfondie des groupes de substitutions linéaires mod p (p étant premier) qui laissent invariante une forme quadratique $F(x_1, \ldots, x_n)$ mod p. Il en a déterminé l'ordre et la structure.

Il restait toutefois une lacune à combler dans le cas où p est impair. L'auteur avait montré que le groupe dérivé des carrés des substitutions du groupe en question contenait au moins la moitié des substitutions de celui-ci; mais il aurait pu les contenir toutes.

En s'appuyant sur des relations d'isomorphisme avec d'autres groupes connus, relations très remarquables dont l'établissement constitue une des parties les plus intéressantes de son Livre, M. Dickson avait établi la négative lorsque le nombre n des variables ne surpasse pas *six*. Mais lorsque $n > 6$, il en était réduit à des présomptions.

C'était une lacune importante. Elle a été heureusement comblée par un travail récent du R. P. de Séguier (*Comptes rendus de l'Académie des Sciences*, 1er septembre 1913). Cette théorie peut donc être considérée aujourd'hui comme achevée. Elle semble toutefois susceptible de quelques simplifications, qui font l'objet des pages suivantes.

Analyse.

I.

1. Soit p un nombre premier impair.

Deux formes quadratiques à n variables, F_n et F'_n (mod p) de

déterminants Δ, Δ' seront dites *équivalentes* s'il existe une substitution linéaire S (mod p) qui transforme F_n en F'_n.

Les congruences

$$F_n \equiv a, \qquad F'_n \equiv a \qquad (\text{mod } p)$$

auront évidemment le même nombre de racines.

D'autre part, si T est une substitution linéaire qui transforme F_n en elle-même, la substitution semblable $S^{-1}TS$ transformera F'_n en elle-même. Les groupes G_n, G'_n respectivement formés par les substitutions qui laissent invariantes F_n, F'_n seront donc semblables. Pour étudier l'ordre et la structure des groupes G_n, on pourra donc considérer au lieu de la forme F_n une autre forme quelconque, choisie arbitrairement parmi celles qui lui sont équivalentes.

2. Le déterminant δ de la substitution S qui transforme F_n en F'_n est lié à Δ, Δ' par la relation connue

$$\Delta' \equiv \Delta\delta^2 \qquad (\text{mod } p).$$

Si $\delta \equiv 1$, on aura donc $\Delta \equiv \Delta'$. On dira dans ce cas que l'équivalence est *absolue*.

On aura d'ailleurs dans tous les cas

$$\left(\frac{\Delta'}{p}\right) = \left(\frac{\Delta}{p}\right), \tag{1}$$

$\left(\frac{\Delta}{p}\right)$ désignant le symbole de Legendre.

Réciproquement, l'existence de cette égalité suffit pour assurer l'équivalence de F_n avec F'_n.

On peut en effet, par des substitutions linéaires de déterminant 1 opérées sur F_n : 1° y faire apparaître un terme en x_1^2 s'il n'y existait pas déjà ; 2° faire disparaître ceux des rectangles où figure x_1. On obtient ainsi une transformée

$$a_1 x_1^2 + F(x_2, \ldots, x_n),$$

puis par des opérations analogues, celle-ci

$$a_1 x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2.$$

Soient d'ailleurs α, β deux entiers liés par la relation

$$a_1\alpha^2 + a_2\beta^2 \equiv 1 \qquad (\text{mod } p).$$

La substitution de déterminant 1

$$\begin{vmatrix} x_1 & \alpha x_1 - a_2\beta x_2 \\ x_2 & \beta x_1 + a_1\alpha x_2 \end{vmatrix}$$

transformera

$$a_1x_1^2 + a_2x_2^2 \quad \text{en} \quad x_1^2 + a_1a_2x_2^2.$$

Par une suite d'opérations analogues, on arrivera finalement à la transformée

$$\sum_1^{n-1} x_k^2 + \Delta x_n^2 \tag{2}$$

absolument équivalente à F_n.

On pourra transformer de même F'_n en

$$\sum_1^{n-1} x_k^2 + \Delta' x_n^2. \tag{2'}$$

Mais de l'égalité (1) supposée satisfaite on déduit l'existence d'un entier δ tel que l'on ait

$$\Delta' \equiv \Delta\delta^2 \pmod p,$$

de sorte que la substitution

$$\begin{vmatrix} x_n & \delta x_n \end{vmatrix}$$

transformera (2) en (2)'.

La réduite (2) à laquelle nous avons ramené la forme F_n pourrait être remplacée dans l'étude suivante par une autre forme équivalente quelconque. Nous trouverons même parfois avantage à changer de réduite dans le cours du calcul.

3. Soit, par exemple, à déterminer le nombre des solutions de la congruence

$$F_n \equiv a \pmod p,$$

nombre que nous désignerons par $\mathfrak{N}(n, \Delta, a)$.

La relation évidente

$$\sum_{a=0}^{a=p-1} \mathfrak{N}(n, \Delta, a) = p^n$$

déterminera $\mathfrak{N}(n, \Delta, o)$ lorsqu'on connaîtra les valeurs de ces expressions lorsque $a \gtrless o \pmod p$.

Pour obtenir ces dernières, le plus commode est d'adopter pour forme réduite la suivante :

$$F_m = x_1 y_1 + \ldots + x_m y_m + \varphi,$$

φ étant égal à $(-1)^m \Delta u^2$ si $n = 2m+1$ et à $z^2 + (-1)^m \Delta u^2$ si $n = 2m+2$.

Les solutions de la congruence $F_m \equiv a$ seront de deux sortes :

1° Celles où $x_1, \ldots, x_m$ ne sont pas nuls à la fois; ils pourront être choisis de $p^m - 1$ manières différentes. Pour chacune d'elles on aura une relation linéaire déterminant une des variables y en fonction des $n - m - 1$ variables restantes qui resteront arbitraires. On obtient ainsi $(p^m - 1) p^{n-m-1}$ solutions.

2° Si les x sont tous nuls, les m variables y resteront arbitraires, mais on devra avoir

$$\varphi \equiv a.$$

Si donc ω est le nombre des solutions de cette congruence, on aura $p^m \omega$ solutions de deuxième espèce qui, ajoutées aux précédentes, donneront le nombre total

$$(p^m - 1) p^{n-m-1} + p^m \omega.$$

Reste à déterminer ω.

1° Si $n = 2m+1$, la congruence

$$(-1)^m \Delta u^2 = a$$

aura deux solutions si $\left(\frac{(-1)^m \Delta a}{p}\right) = +1$. Elle n'en a aucune dans le cas contraire. Cela revient à dire qu'elle en a toujours

$$1 + \left[\frac{(-1)^m \Delta a}{p}\right].$$

2° Si $n = 2m+2$, on aura

$$\varphi = z^2 + (-1)^m \Delta u^2.$$

Soit j une racine de la congruence

$$j^2 \equiv (-1)^{m+1}\Delta$$

et posons

$$X = z + ju, \qquad Y = z - ju,$$

d'où $\varphi = XY$.

La congruence $\varphi = a$ deviendra donc

$$XY = a.$$

Si $(-1)^{m+1}\Delta$ est résidu quadratique de p, j, X, Y seront réels et l'on aura évidemment $p-1$ solutions.

Dans le cas contraire, j sera imaginaire, X un entier complexe ayant pour conjugué $Y \equiv X^p$. La congruence deviendra

$$X^{p+1} \equiv a.$$

Or $X^{p+1} - a$ est un diviseur de

$$X^{p^2-1} - a^{p-1} \equiv X^{p^2-1} - 1.$$

Mais on sait que la congruence

$$X^{p^2-1} \equiv 1$$

a $p^2 - 1$ racines. La congruence

$$X^{p+1} \equiv a$$

en aura donc $p+1$.

On aura ainsi dans tous les cas

$$\omega = p - \left(\frac{(-1)^{m+1}\Delta}{p}\right).$$

Substituant pour n et ω leurs valeurs dans l'expression trouvée pour $\mathfrak{N}(n, \Delta, a)$, il viendra après réduction

$$(3)\qquad \begin{cases} \mathfrak{N}(2m+1, \Delta, a) = \left[p^m + \left(\dfrac{(-1)^m \Delta a}{p}\right)\right] p^m, \\ \mathfrak{N}(2m+2, \Delta, a) = \left[p^{m+1} - \left(\dfrac{(-1)^{m+1}\Delta}{p}\right)\right] p^m. \end{cases}$$

4. Cherchons l'ordre $O(n, \Delta)$ du groupe G_n dont les substitutions laissent F_n invariante.

Donnons à F_n son expression réduite

$$\Delta x_1^2 + \Sigma_2^n x_k^2.$$

Soit

$$S = | \; x_k a_k x_1 + b_k x_2 + \dots \; | \qquad (k = 1, 2, \dots, n)$$

une substitution de G_n. Ses coefficients devront satisfaire entre autres conditions à celle-ci :

$$\Delta a_1^2 + \Sigma_2^n a_k^2 = \Delta,$$

laquelle admet, comme on vient de le voir, $\mathfrak{N}(n, \Delta, \Delta)$ solutions. A chacune d'elles correspondent des substitutions de G_n dont nous déterminerons le nombre.

Nous pouvons déterminer une substitution T de déterminant 1 où les coefficients de la première colonne soient $a_1, \dots, a_n$. Elle transformera F_n en une forme équivalente F_n' où le coefficient de x_1^2 soit Δ. Une autre substitution de déterminant 1 fera disparaître les rectangles en x_1 et donnera une nouvelle transformée

$$F_n'' = \Delta x_1^2 + P(x_2, \dots, x_n),$$

P ayant le déterminant 1 et pouvant être transformée en $\Sigma_2'' x_k^2$ par une nouvelle substitution V. La substitution $TUV = S$ transformera donc F_n en elle-même.

Ayant ainsi obtenu pour chacun des $\mathfrak{N}(n, \Delta, \Delta)$ systèmes de valeurs admissibles pour les coefficients a une première substitution de G_n, cherchons s'il en existe d'autres. Soit S' une autre substitution quelconque où les coefficients a soient les mêmes que dans S. Elle appartiendra à G_n en même temps que $S'S^{-1}$. Or cette dernière substitution est évidemment de la forme

$$\begin{vmatrix} x_1 & x_1 + b_1 x_2 + \dots \\ \dots & \dots\dots\dots\dots \\ x_k & b_k x_2 + \dots \\ \dots & \dots\dots\dots \end{vmatrix},$$

et pour qu'elle n'altère pas F_n, il faut et il suffit : 1° que les coefficients $b_1, \dots$ de la première ligne soient nuls; 2° que la substitution qui n'est plus opérée que sur les variables $x_2, \dots, x_n$ n'altère pas la

forme à $n-1$ variables

$$F_{n-1} = x_2^2 + \ldots + x_n^2.$$

Nous obtenons ainsi la formule de récurrence

$$O(n, \Delta) = \mathfrak{N}(n, \Delta, \Delta)\, O(n-1, 1),$$

d'où l'on déduit

$$O(n, \Delta) = \mathfrak{N}(n, \Delta, \Delta)\, \mathfrak{N}(n-1, 1, 1)\, \mathfrak{N}(n-2, 1, 1) \ldots \mathfrak{N}(1, 1, 1).$$

Substituons dans cette expression les valeurs précédemment trouvées pour les $\mathfrak{N}$.

Si $n = 2m+1$, nous aurons

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

$$\mathfrak{N}(2m, 1, 1) = \left[p^m - \left(\frac{-1}{p}\right)^m\right] p^{m-1}.$$

Le produit de ces deux facteurs sera

$$(p^{2m}-1)\, p^{2m-1}.$$

Celui des deux suivants s'obtiendra en changeant m en $m-1$, et ainsi de suite. Enfin le dernier facteur $\mathfrak{N}(1, 1, 1)$ est égal à 2.

Faisant le produit et remarquant que

$$(2m-1) + (2m-3) + \ldots = m^2,$$

il viendra

$$O(2m+1, \Delta) = 2p^{m^2} \Pi_1^m (p^{2k}-1). \tag{4}$$

Si $n = 2m+2$, on aura

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

et, par suite,

$$\begin{aligned} O(2m+2, \Delta) &= \mathfrak{N}(n, \Delta, \Delta)\, O(2m+1, 1) \\ &= 2p^{m^2+m}\left[p^{m+1} - \left(\frac{(-1)^{m+1}\Delta}{p}\right)\right] \Pi_1^m (p^{2k}-1) \end{aligned} \tag{5}$$

3. Pour déterminer la structure de G_n et les substitutions fondamentales dont il est dérivé, la forme réduite qu'il paraît le plus avan-

tageux d'adopter est la suivante :

$$xy + \Sigma_3^n A_k z_k^2,$$

où les A_k peuvent être choisis arbitrairement sous réserve de satisfaire à la condition

$$\left(\frac{-\Pi_3^n A_k}{p}\right) = \left(\frac{\Delta}{p}\right).$$

G_n sera dérivé des substitutions fondamentales suivantes :

$$\begin{aligned}
M_k &= | \; x, y, z_k \quad x, y - A_k x - 2A_k z_k, z_k + x \; |, \\
N_k &= | \; x, y, z_k \quad x - A_k y - 2A_k z_k, y, z_k + y \; |, \\
P &= | \; x, y \quad gx, g^{-1}y \; | \qquad (g \text{ racine primitive de } p), \\
Q &= | \; x, y \quad y, x \; |.
\end{aligned}$$

Soit en effet

$$S = \begin{vmatrix} .. & ..... \\ z_k & a_k z_1 + ... \\ .. & ..... \\ x & b z_1 + ... \\ y & c z_1 + ... \end{vmatrix}$$

une quelconque des substitutions de G_n. Ses coefficients devront satisfaire entre autres conditions à la suivante :

$$bc + \Sigma A_k a_k^2 = A_k.$$

Multiplions-la à gauche par la substitution

$$M_k^\lambda = | \; x, y, z_k \quad x, y - \lambda A_k x - \lambda^2 A_k z_k, z_k + \lambda x \; |.$$

Nous obtiendrons une nouvelle substitution $M_k^\lambda S$ où les coefficients de la première colonne sont les mêmes que dans S, sauf a_k et c qui seront remplacés par

$$a_k' = a_k + \lambda b, \qquad c' = c - \lambda A_k b - \lambda^2 A_k a_k.$$

De même la multiplication à gauche par N_k^λ changerait a_k, b en

$$a_k + \lambda c, \qquad b - \lambda A_k c - \lambda^2 A_k a_k.$$

Par des opérations de ce genre et détermination convenable des

constantes λ, on pourra, si b et c ne sont pas nuls à la fois, rendre a_3 égal à 1, annuler les autres coefficients a et enfin b et c.

Si b et c étaient nuls, l'un au moins des coefficients a_k étant différent de zéro, une multiplication préalable par M_k changerait c en $-A_k a_k$ qui n'est plus nul.

On aura donc en appelant Π le produit des facteurs M_k, N_k qui ont été employés

$$\Pi S = S' \qquad \text{d'où} \qquad S = \Pi^{-1} S',$$

S' étant une nouvelle substitution où $a_3 = 1$, les autres coefficients de la première colonne étant nuls.

D'ailleurs S appartenant par hypothèse à G_n, il en est de même de S', qui sera dès lors opérée entre les seules variables $z_4, \ldots, x, y$.

Opérant sur S' comme sur S et ainsi de suite, on finira par mettre S sous la forme $\mathfrak{P} S_1$ où $\mathfrak{P}$ est un produit de substitutions M_k, N_k et S_1 une substitution opérée entre les seules variables x, y, laquelle résultera évidemment de la combinaison des substitutions P et Q.

6. La substitution Q étant d'ordre 2 et de déterminant -1, les substitutions M_k, N_k, P de déterminant 1, considérées seules, donneront naissance à un groupe G'_n d'ordre $\frac{1}{2} O(n, \Delta)$ qui sera un sous-groupe invariant dans G_n.

Le R. P. de Séguier a montré comme il suit l'existence d'un autre sous-groupe invariant G''_n d'indice 2.

Appelons pour abréger *points* de la courbe F_n les systèmes de valeurs entières (mod p) des variables qui satisfont à la relation $F_n \equiv 1$. Chaque substitution S de G_n fait éprouver à ces points une certaine permutation. Suivant que celle-ci appartient ou non au groupe alterné nous dirons que S est *paire* ou *impaire* et nous lui assignerons en conséquence un caractère $+1$ ou -1.

Il est clair que le caractère du produit de deux substitutions S, S' sera le produit de leurs caractères et que si G_n contient des substitutions impaires, celles qui sont paires formeront un sous-groupe invariant d'indice 2.

Or la substitution P est impaire, car elle laisse invariables les points pour lesquels $x = y = 0$ et permute les autres suivant des cycles d'ordre $p - 1$ (nombre pair).

Or à chaque cycle formé des points

$$(x, y, z_3, \ldots)(gx, g^{-1}y, z_3, \ldots)\ldots(g^{p-2}x, g^{-p+2}y, z_3, \ldots),$$

on peut associer, si les z ne sont pas tous nuls, un autre cycle qui s'en déduit en changeant leur signe. Ces cycles sont donc en nombre pair. Reste celui où tous les z sont nuls. Donc le nombre des cycles est impair et la permutation n'appartient pas au groupe alterné.

7. Cherchons de la même manière le caractère de quelques autres substitutions.

Considérons d'abord la substitution

$$| x, y \quad -x, \quad -y |.$$

Elle permute les points de F_n, sauf ceux où $x \equiv y \equiv 0$, suivant des cycles binaires. Ceux formés par les points où les z ne sont pas tous nuls, associés deux à deux, sont en nombre pair. Ceux qui restent se partagent les $p-1$ points définis par la condition $x_1 y_1 \equiv 1$. Leur nombre sera donc $\frac{p-1}{2}$ et le caractère de la substitution sera

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

Passons à la substitution

$$s_k = | z_k \quad -z_k |.$$

Elle permute les points de F_n, sauf ceux où $z_k \equiv 0$, suivant des cycles binaires. Négligeant les couples de cycles associés, il reste à considérer ceux formés par les points définis par $A_k z_k^2 \equiv 1$. Il existe deux semblables points formant un cycle si $\left(\frac{A_k}{p}\right) = 1$; il n'en existe point dans le cas contraire. Le caractère cherché sera donc $-\left(\frac{A_k}{p}\right)$.

Considérons encore la substitution σ_n qui change le signe de toutes les variables. Son caractère sera

$$\left(\frac{-1}{p}\right)\prod\left[-\left(\frac{A_k}{p}\right)\right] = (-1)^{n-2}\left(-\frac{A_3 \ldots A_n}{p}\right) = (-1)^n\left(\frac{\Delta}{p}\right).$$

Enfin les substitutions M_k, N_k d'ordre p permuteront les points

qu'elles déplacent suivant des cycles d'ordre impair p. Elles auront donc pour caractère $+1$.

Nous verrons tout à l'heure que la substitution P^2 dérive de la combinaison des substitutions M_k, N_k. Le groupe Γ_n dérivé des substitutions M_k, N_k aura donc pour ordre $\frac{1}{4}O(n, \Delta)$ et contiendra toutes les substitutions de G_n dont le déterminant et le caractère sont tous deux égaux à $+1$. Ce sera un sous-groupe invariant dans G_n.

On obtiendra le groupe G'_n par l'adjonction à Γ_n de la substitution P; le groupe G''_n par l'adjonction de celle des deux substitutions s_3, Ps_3 dont le caractère est $+1$.

Un troisième groupe invariant G'''_n d'indice 2 sera formé des substitutions de G_n dont le caractère est égal au déterminant.

Enfin le groupe H_n d'ordre 2 formé par les puissances de σ_n sera encore un sous-groupe invariant. Il sera contenu dans Γ_n si l'on a à la fois n pair et $\left(\frac{\Delta}{p}\right) = +1$.

Nous allons montrer que ce sont là en général les seuls sous-groupes invariants de G_n. Il n'y a d'exception que si $p = 3$ et $n = 3$, ou $p = 3$, $n = 4$, $\left(\frac{\Delta}{p}\right) = +1$.

Pour établir cette proposition il nous faut recourir aux expressions remarquables que M. Dickson a données aux substitutions de G_n lorsque $n = 3$ ou 4.

8. Soit d'abord $n = 3$, d'où

$$F_3 = xy + Az^2.$$

Soient α, β, γ, δ quatre entiers liés par la seule relation

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{p}$$

et considérons les substitutions

	z_3	x	y
z_3	$\alpha\delta + \beta\gamma$	$\alpha\gamma$	$-A^{-1}\beta\delta$
x	$2\alpha\beta$	α^2	$-A^{-1}\beta^2$
y	$-2A\gamma\delta$	$-A\gamma^2$	δ^2

que nous représenterons par le symbole abrégé

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}.$$

On vérifie aisément :

1° Qu'elles n'altèrent pas F_3 ;

2° Qu'elles donnent lieu à la formule de composition

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \begin{vmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{vmatrix} = \begin{vmatrix} \alpha\alpha'+\beta\gamma' & \alpha\beta'+\beta\delta' \\ \gamma\alpha'+\delta\gamma' & \gamma\beta'+\delta\delta' \end{vmatrix}.$$

Il en résulte qu'elles forment un groupe K isomorphe au groupe linéaire

$$| X, Y \quad \alpha X+\beta Y, \gamma X+\delta Y |.$$

Ce dernier groupe K′ est, comme on sait, dérivé des substitutions fondamentales

$$| X, Y \quad X, Y+X |,$$
$$| X, Y \quad X+Y, Y |$$

auxquelles correspondent dans K les substitutions

$$M_3 = | z_3, x, y \quad z_3+x, x, y-\Lambda x-2\Lambda z_3 |,$$
$$N_3 = | z_3, x, y \quad z_3+y, x-\Lambda y-2\Lambda z_3, y |,$$

dont K sera dérivé.

D'ailleurs K′ contenant la substitution

$$| X, Y \quad gX, g^{-1}Y |,$$

K contiendra sa correspondante

$$| z_3, x, y \quad z_3, g^2x, g^{-2}y | = P^2,$$

Celle-ci sera donc dérivée de M_3 et de N_3, ainsi que nous l'avions annoncé.

Le groupe K ne sera donc autre chose que Γ_3.

On sait enfin que le groupe K′ est d'ordre $(p^2-1)p$ et n'a en général d'autre sous-groupe invariant que celui formé des puissances de la substitution

$$\sigma = | X, Y \quad -X, -Y |.$$

Il y a exception si $p = 3$. Dans ce cas le groupe K′, d'ordre 24, con-

tiendra un sous-groupe invariant L′ d'ordre 8, dérivé des deux substitutions

$$| X, Y \quad Y, -X |,$$
$$| X, Y \quad X+Y, X-Y |$$

d'ordre 4 et ayant toutes deux pour carré la substitution σ.

D'ailleurs à la substitution 1 de Γ_3 correspondent dans K′ les deux substitutions

$$| X, Y \quad \varepsilon X, \varepsilon Y | \qquad (\varepsilon = \pm 1).$$

Donc l'ordre de Γ_3 sera $\frac{1}{2}(p^2-1)p$, et il sera simple, à moins qu'on n'ait $p=3$, auquel cas il aura les facteurs de composition 3, 2, 2.

9. Passons au cas où $n=4$. L'expression de F_4 sera

$$xy + z^2 - \Delta u^2.$$

Soit j une racine de la congruence

$$j^2 \equiv \Delta \pmod{p}$$

et prenons pour variables nouvelles

$$x_1 = z + ju, \qquad y_1 = z - ju,$$

F_4 prendra la forme

$$xy + x_1 y_1.$$

Supposons d'abord $\left(\frac{\Delta}{p}\right) = 1$; j, x_1, y_1 seront réels, et Γ_4 contiendra les deux substitutions d'ordre p

$$| x, y_1 \quad x+x_1, y_1 - y |,$$
$$| x_1, y \quad x_1 + x, y - y_1 |,$$

dont la combinaison donnera les $(p^2-1)p$ substitutions de la forme

$$S = \left| \begin{matrix} x, x_1 & ax + bx_1, cx + dx_1 \\ y, y_1 & dy - cy_1, -by + ay_1 \end{matrix} \right|$$

où $ad - bc \equiv 1$.

Elles forment un groupe K évidemment isomorphe au groupe linéaire

$$| x, x_1 \quad ax + bx_1, cx + dx_1 |.$$

Son ordre sera donc $(p^2-1)p$, et il n'aura, si $p>3$, d'autre sous-groupe invariant que celui dérivé de la substitution σ_4 qui multiplie toutes les variables par -1.

Si $p=3$, d'où $(p^2-1)p=24$, il aura un autre sous-groupe invariant L d'ordre 8 et dérivé des substitutions

$$\begin{vmatrix} x, x_1 & x_1, -x \\ y, y_1 & y_1, -y \end{vmatrix}$$

$$\begin{vmatrix} x, x_1 & x+x_1, & x-x_1 \\ y, y_1 & -y-y_1, & -y+y_1 \end{vmatrix}$$

dont le carré est σ_4.

Γ_4 contiendra toutes les substitutions de K ainsi que celles du groupe K_1 transformé de K par la substitution

$$| x_1, y_1 \quad y_1, x_1 |.$$

Ces dernières ont pour expression générale

$$S_1 = \begin{vmatrix} x, x_1 & Ax+By_1 & -By+Ax_1 \\ y, y_1 & Dy-Cx_1 & Cx+Dy_1 \end{vmatrix} \quad \text{où} \quad AD-BC=1.$$

On vérifie sans peine :

1° Que les substitutions S_1 sont échangeables aux substitutions S ;

2° Que les seules substitutions qui soient à la fois de ces deux formes sont les puissances de σ_4.

Les produits SS_1 formeront donc un groupe d'ordre $\frac{1}{2}[(p^2-1)p]^2$. C'est précisément l'ordre de Γ_4, dont nous avons mis ainsi les substitutions sous forme explicite.

Les groupes K, K_1 sont invariants dans Γ_4, ainsi que le groupe des puissances de σ_4. En général il n'y en aura pas d'autre, et les facteurs de composition de Γ_4 seront

$$\frac{(p^2-1)p}{2}, \quad \frac{(p^2-1)p}{2}, \quad 2.$$

Pour $n=3$ les facteurs $\frac{(p^2-1)p}{2}=12$ devront être remplacés par leurs diviseurs premiers 3, 2, 2. Mais dans aucun cas Γ_4 n'aura de sous-groupe invariant qui ne contienne la substitution σ_4.

Soit en effet H un sous-groupe invariant qui contienne une substitution T autre que σ_4. Elle sera de la forme SS_1, l'un au moins des deux facteurs, S par exemple, différant de σ_4. Soit U une substitution de K non échangeable à S; H contiendra la substitution

$$U^{-1}T^{-1}UT = U^{-1}S^{-1}US$$

qui appartient à K sans se réduire à l'unité. Si elle diffère de σ_4, on la combinera avec ses transformées; ce qui reproduira en général le groupe K ou tout au moins (si $p = 3$) son sous-groupe invariant L. Mais celui-ci contient σ_4.

10. Supposons maintenant $\left(\frac{\Delta}{p}\right) = -1$. Les variables x_1, y_1 seront des imaginaires conjuguées. D'ailleurs les substitutions S, S_1 n'altèrent pas F_4 et sont échangeables entre elles, indépendamment de la signification des quantités a, b, c, d, A, B, C, D.

Considérons donc le produit SS_1 où nous prendrons pour a, b, c, d des entiers complexes $a' + a''j$, ... liés par la seule relation $ad - bc = 1$ et pour A, B, C, D les expressions conjuguées. L'opération ainsi obtenue

$$SS_1 = \begin{vmatrix} x & Aax - Bby + Abx_1 + Bay_1 \\ y & -Ccx + Ddy - Cdx_1 - Dcy_1 \\ x_1 & Acx - Bdy + Adx_1 + Bcy_1 \\ y_1 & Cax - Dby + Cbx_1 + Day_1 \end{vmatrix}$$

représentera une substitution réelle, car les expressions qu'elle fait succéder à x et à y ne changent pas quand on change j en $-j$ et d'autre part celles qui succèdent aux variables conjuguées x_1, y_1 sont également conjuguées.

Ces substitutions SS_1 forment un groupe K évidemment isomorphe au groupe linéaire K' formé des substitutions

$$\begin{vmatrix} X, X_1 & aX + bX_1, cX + dX_1 \\ Y, Y_1 & AY + BY_1, CY + DY_1 \end{vmatrix},$$

où X, X_1 sont des variables complexes et Y, Y_1 leurs conjuguées. Son ordre est $(p^4 - 1)p^2$. Il n'a d'autre sous-groupe invariant que celui formé par les substitutions où $b \equiv B \equiv c \equiv C = 0$ et $a \equiv A \equiv d \equiv D \equiv \pm 1$.

Mais aux deux substitutions de ce sous-groupe correspond dans K la seule substitution 1. Donc K est simple et d'ordre $\frac{1}{2}(p^4-1)p^2$.

Il se confond avec Γ_4; car ces deux groupes ont le même ordre et d'autre part les substitutions de K appartiennent à Γ_4; car leur déterminant $(ad-bc)$ (AD − BC) est égal à + 1. Il en est de même de leurs caractères; car K′ est dérivé de substitutions fondamentales

$$\left|\begin{matrix} X, X_1 & X+lX_1, X_1 \\ Y, Y_1 & Y+LY_1, Y_1 \end{matrix}\right|, \quad \left|\begin{matrix} X, X_1 & X, X_1+mX \\ Y, Y_1 & Y, Y_1+MY \end{matrix}\right|,$$

où l, m sont des entiers complexes, L, M leurs conjugués. Ces substitutions étant d'ordre p impair, il en sera de même de leurs correspondantes génératrices de K. Elles auront donc le caractère + 1.

11. Soit enfin $n>4$. Nous allons démontrer que tout sous-groupe K (autre que H_n), invariant dans G_n, contient Γ_n.

Soient en effet : S une substitution de K qui n'appartienne pas à H_n; T une substitution quelconque de G_n; les substitutions $T^{-1}ST$, $T^{-1}S^{-1}TS$ appartiendront à K et la seconde appartiendra aussi à Γ_n. Nous allons en conclure que si K contient une substitution S qui n'appartienne pas à H_n il contiendra Γ_n.

Supposons F_n mise sous la forme

$$\Sigma A_k x_k^2,$$

G_n contiendra la substitution T_k qui change le signe de la seule variable x_k, et deux cas seront à distinguer :

1° Si S est échangeable à toutes les substitutions T_k, elle sera nécessairement de la forme

$$| x_1, \ldots, x_n \quad a_1x_1, \ldots, a_nx_n |$$

et pour qu'elle n'altère pas F_n, il faut que chacun des a_n soit égal à ± 1. Mais si S n'appartient pas à H_n, ils ne seront pas tous du même signe. Supposons donc pour fixer les idées qu'on ait $a_1 = a_2 = -a_3$.

Celles des substitutions de G_n qui n'altèrent que les variables x_1, x_2, x_3 forment un groupe G_3 d'ordre $2(p^2-1)p$. Celles d'entre elles

qui sont échangeables à S, devant laisser invariantes séparément $A_3x_3^2$ et $A_1x_1^2 + A_2x_2^2$, seront au plus au nombre de $2.2(p \pm 1)$. Donc G_3 contient une substitution U non échangeable à S. Et K contiendra la substitution

$$S_1 = U^{-1}S^{-1}US$$

qui diffère de l'unité, mais est restreinte aux variables x_1, x_2, x_3. Si donc on décompose F_n en une somme de deux formes partielles

$$F_4 = A_1x_1^2 + \ldots + A_4x_4^2, \qquad F_{n-4} = A_5x_5^2 + \ldots,$$

K contiendra une substitution S_1 du groupe G_4 formé par les substitutions de G_n qui sont restreintes aux variables de F_4. Combinée à ses transformées elle reproduira, soit toutes les substitutions de G_4, soit la substitution

$$\sigma_4 = | \; x_1, \ldots, x_4 \quad -x_1, \ldots, -x_4 \; |.$$

12. 2° On arrivera à un résultat analogue si l'une des substitutions T_k, par exemple T_1, n'est pas échangeable à S.

Soit en effet

$$S = \begin{vmatrix} x_1 & \alpha\, x_1 + \beta\, x_2 + \ldots \\ x_2 & a_2x_1 + b_2x_2 + \ldots \\ \ldots & \ldots\ldots\ldots\ldots \\ x_n & a_nx_1 + b_nx_2 + \ldots \end{vmatrix}.$$

Par un changement de variables exécuté sur $x_2, \ldots, x_n$ (il devra être opéré sur F_n en même temps que sur S) on pourra faire disparaître les coefficients $a_3, \ldots, a_n$. Cela fait, K contiendra la substitution

$$S_1 = T_1^{-1}S^{-1}T_1S$$

qui diffère de l'unité, mais laisse évidemment invariables $x_3, \ldots, x_n$. En l'élevant, s'il est nécessaire, à une puissance convenable on obtiendra une nouvelle substitution S_2, d'ordre premier, commune à K et à Γ_n.

Par un nouveau changement de variables opéré sur x_1, x_2 on ramènera S_2 à sa forme canonique. Si son ordre n'est pas égal à p, cette forme canonique sera

$$| \; x_1, x_2 \quad rx_1, r^{-1}x_2 \; |,$$

r pouvant être réel ou complexe (dans ce dernier cas x_1, x_2 seraient des variables complexes et conjuguées). Les variables non écrites z_1, z_2, ... restant inaltérées.

La forme F_n, étant invariante par S_2, devra prendre après le changement de variables la forme

$$A x_1 x_2 + Q,$$

Q étant une fonction quadratique des seuls z.

En la mettant sous la forme

$$A_1 z_1^2 + A_2 z_2^2 + \dots$$

et posant

$$A x_1 x_2 + A_1 z_1^2 + A_2 z_2^2 = F_4,$$

on aura comme dans le cas précédent

$$F_n = F_4 + F_{n-4}.$$

Si S_2 est d'ordre p, elle aura l'une des deux formes canoniques suivantes :

$$(6) \qquad | x_2, x_1, z_1 \quad x_2 + x_1, x_1 + z_1, z_1 |,$$

$$(7) \qquad | x_1, x_2, z_1, z_2 \quad x_1 + z_1, x_2 + z_2, z_1, z_2 |.$$

Dans le premier cas, la forme F_n, pour être invariante, devra avoir pour expression

$$A(x_2 z_1 - x_1^2) + L z_1 + Q,$$

L étant linéaire en z_1, z_2, ... et Q quadratique en z_2, ... On peut d'ailleurs faire disparaître le terme Lz_1 par le changement de x_2 en $x_2 - L$, qui n'altère pas l'expression canonique (6) de S_2.

Mettant Q sous la forme $A_2 z_2^2 + \dots$ et posant

$$A(x_2 z_1 - z_1^2) + A_2 z_2^2 = F_4,$$

on aura encore

$$F_n = F_4 + F_{n-4}.$$

Dans le second cas, F_n, pour être invariante par S_2, aura nécessairement pour expression

$$A(x_1 z_2 - x_2 z_1) + L_1 z_1 + L_2 z_2 + Q,$$

L_1, L_2 étant linéaires en z_1, z_2, z_3, ... et Q quadratique en z_3, ... D'ailleurs par le changement de x_1, x_2 en $x_1 - L_2$, $x_2 + L_1$ on pourra faire disparaître les termes $L_1 z_1$, $L_2 z_2$.

On pourra donc dans tous les cas mettre F_n sous la forme

$$F_4 + F_{n-4},$$

K contenant une substitution S du groupe Γ_4 formé par celles des substitutions de Γ_n qui sont opérées entre les seules variables de F_4. Il contiendra par suite les transformées de S par les substitutions de Γ_4. Or l'étude de ce groupe a montré que par la combinaison de ces transformées on peut obtenir, suivant le caractère quadratique du déterminant de F_4, soit toutes les substitutions de Γ_4, soit la substitution σ_4.

13. Mettons F_4 sous la forme

$$xy + A_3 z_3 + A_4 z_4$$

et F_{n-4} sous la forme

$$A_5 z_5^2 + \ldots.$$

Si S contient Γ_4 il contiendra sa substitution fondamentale M_3.

D'autre part, s'il contient σ_4, il contiendra la substitution

$$M_5^{-1} \sigma_4^{-1} M_5 \sigma_4 = M_5^{-2}$$

et par suite la substitution M_5 elle-même; or celle-ci, par un simple changement de notation, peut être remplacée par M_3.

Donc, F_n étant mise sous la forme

$$xy + \Sigma_3^n A_k z_k^2,$$

K contiendra la substitution M_3. Il contiendra aussi N_3 qui est sa transformée par la substitution

$$| x, y \quad y, x |.$$

Les coefficients $A_4, \ldots, A_n$ étant arbitraires sous la seule condition

$$\left(-\frac{A_3 \ldots A_n}{p}\right) = \left(\frac{\Delta}{p}\right),$$

on pourra supposer $A_4, \ldots, A_{n-1}$ choisis égaux à A_3 et si $k < n$,

K contiendra les substitutions M_k, N_k transformées de M_3, N_3 par la substitution

$$| x_3, y_3, x_k, y_k \quad x_k, y_k, x_3, y_3 |.$$

Si donc nous désignons par Γ_{n-1} le groupe formé par les substitutions de déterminant 1 et de caractère 1 qui laissent invariante la fonction

$$F_{n-1} = xy + \Sigma_3^{n-1} A_3 x_k^2,$$

K contiendra Γ_{n-1} puisqu'il contient toutes les substitutions fondamentales dont il est dérivé.

Soient d'ailleurs A'_3, A'_4 deux entiers quelconques assujettis à la seule condition

$$A'_3 A'_4 \equiv A_3^2$$

qui permet de choisir arbitrairement A'_3. On pourra déterminer deux fonctions z'_3, z'_4 linéaires en z_3, z_4 telles que l'on ait

$$A_3 z_3^2 + A_3 z_4^2 = A'_3 z_3'^2 + A'_4 z_4'^2,$$

Γ_{n-1} (et par suite K) contiendra la substitution

$$M'_3 = | z'_3, x, y \quad z'_3 + x, x, y - A'_3 x - 2A'_3 z'_3 |.$$

Celle-ci appartient d'ailleurs, ainsi que M_n et N_n, au groupe Γ_4 formé par les substitutions de caractère et de déterminant 1 qui laissent invariante la fonction

$$F_4 = xy + A'_3 z_3^2 + A_n z_n^2$$

de déterminant $-A'_3 A_n$.

Si nous disposons de A'_3 de telle sorte que l'on ait

$$\left(-\frac{A'_3 A_n}{p}\right) = -1,$$

Γ_4 sera simple; donc K, contenant une de ses substitutions M'_3, les contiendra toutes. Il contiendra en particulier M_n et N_n. Il contiendra donc Γ_n, puisqu'il possède toutes ses substitutions fondamentales.

14. Pour déterminer les facteurs de composition de G_n il reste à reconnaître si les sous-groupes G'_n, G''_n, Γ_n auraient d'autres sous-

groupes invariants que ceux de G_n. Dans le cas de la négative, Γ_n ne contenant pas H_n lorsque $\left(\frac{\Delta}{p}\right) = -1$, serait simple. Il en est effectivement ainsi pour $n = 4$. Nous pourrons admettre que cela ait encore lieu pour toutes les valeurs de n inférieures à celle sur laquelle nous raisonnerons.

Dans ces conditions, nous établirons qu'il y a contradiction à admettre que G'_n admette un sous-groupe invariant qui ne soit pas invariant dans G_n.

Mettons en effet F_n sous la forme

$$F_n = A_1 x_1^2 + \ldots + A_n x_n^2 = A_1 x_n^2 + F_{n-1},$$

$A_2, \ldots, A_n$ pouvant être choisis arbitrairement, on peut admettre que $\left(\frac{A_2 \ldots, A_n}{p}\right)$ soit égal à -1. Le groupe Γ_{n-1} correspondant à F_{n-1} sera donc simple par hypothèse.

Cela posé, soient K le sous-groupe invariant dont nous supposons l'existence ; ω son ordre. La substitution Q permutable à G'_n le transformera en un autre groupe K', également invariant dans G'_n. Réciproquement Q transformera K' en K, puisque Q^2, appartenant à G'_n, transforme K en lui-même.

Les substitutions communes à K et à K' forment un groupe L invariant dans G_n. Il sera donc égal à H_n, s'il contient quelque substitution autre que l'unité. Son ordre d sera donc 1 ou 2.

D'ailleurs, S, S' étant deux substitutions prises respectivement dans K et dans K', la substitution $S^{-1}S'^{-1}SS'$ appartiendra à L.

Les substitutions dérivées de la combinaison de K et de K' seront donc de la forme SS' et leur nombre sera $\frac{\omega^2}{d}$.

Elles forment un sous-groupe Λ invariant dans G_n et contenu dans G'_n. Il sera donc identique à Γ_n ou à G'_n, et son ordre sera

$$\frac{1}{4} O(n, \Delta) \quad \text{ou} \quad \frac{1}{2} O(n, \Delta).$$

On aura donc l'égalité

$$\omega^2 = m O(n, \Delta), \tag{8}$$

m ayant l'une des trois valeurs

$$\frac{1}{4}, \quad \frac{1}{2}, \quad 1.$$

15. Or une semblable égalité est impossible. On a en effet

$$\omega = 2\omega' \qquad \text{ou} \qquad \omega = \omega',$$

ω' étant l'ordre du groupe K_1 formé par celles des substitutions de K qui appartiennent à Γ_n. Soit une de celles-ci

$$| \; x_k \quad a_k x_1 + b_k x_2 + \ldots \; | \qquad (k = 1, 2, \ldots, n).$$

Les coefficients a_k satisferont à la relation

$$\Sigma A_k a_k^2 = A_1 \tag{9}$$

qui a $\mathfrak{N}(n, \Delta, A_1)$ solutions.

1° Supposons en premier lieu qu'à chacune d'elles corresponde tout au plus une seule substitution de K_1. On aura

$$\omega \leqq 2\,\mathfrak{N}(n, \Delta, A_1).$$

Mais, d'autre part, le déterminant Δ' de $F_n - A_1 x_1^2$ est $A_1^{-1}\Delta$, qui a le même caractère quadratique que $A_1\Delta$. On aura donc

$$O(n, \Delta) = \mathfrak{N}(n, \Delta, A_1)\, O(n-1, A_1\Delta).$$

On déduirait donc de la relation (8) l'inégalité

$$16\,\mathfrak{N}(n, \Delta, A_1) \geqq O(n-1, A_1\Delta). \tag{10}$$

En se reportant aux expressions (3), (4), (5) des quantités $\mathfrak{N}$ et O, on voit immédiatement que cette inégalité ne saurait avoir lieu, le second membre étant beaucoup plus grand que le premier.

2° Supposons au contraire qu'à une seule solution de la congruence (9) correspondent plusieurs substitutions S, S', ... de K_1. Il contiendra la substitution $S'S^{-1}$ qui appartient à Γ_{n-1}.

Mais Γ_{n-1} est simple et d'ordre

$$\frac{1}{4} O(n-1, A_1\Delta).$$

L'ordre ω de K sera donc au moins égal à ce nombre.

Substituant cette valeur minima et celle de $O(n, \Delta)$ dans l'égalité (8) on arrivera encore à l'inégalité (10) qui est impossible.

16. Raisonnant sur G'_n et Γ_n comme nous venons de le faire sur G_n et G'_n, on verra exactement de même que Γ_n ne peut admettre d'autre sous-groupe invariant que H_n. Il le contiendra effectivement si n est pair et Δ résidu de p, de sorte que G_n aura les sous-groupes invariants successifs

$$G_n, \quad G'_n, \quad \Gamma_n, \quad H_n, \quad 1.$$

Les facteurs de composition seront donc

$$2, \quad 2, \quad \frac{1}{8} O(n, \Delta), \quad 2.$$

Dans tout autre cas, H_n ne faisant plus partie de cette suite, les facteurs de composition seront

$$2, \quad 2, \quad \frac{1}{4} O(n, \Delta).$$

II.

17. Nous avons supposé, dans tout ce qui précède, que p était impair. S'il est égal à 2, le nombre des variables sera nécessairement un nombre pair $2n$.

Ce cas étant complètement discuté dans le Livre de M. Dickson, nous nous bornerons à quelques remarques relatives aux groupes résolubles contenus dans G_{2n}.

Nous avons démontré autrefois, par des considérations indirectes, que G_{2n} contient un sous-groupe invariant G'_{2n} d'indice 2. Mais c'est seulement dans un Mémoire postérieur (*Journal de Liouville*, 1905) que nous avons pu définir ses substitutions par un caractère indépendant du choix des variables indépendantes.

Une substitution S étant donnée, à chaque racine s de la congruence caractéristique correspond au moins une fonction et peut-être plusieurs fonctions distinctes des variables primitives que S multiplie par s. Soit $N(s)$ leur nombre. La somme $\Sigma N(s)$ étendue aux diverses racines

de la congruence caractéristique pourra être paire ou impaire. Nous dirons, suivant le cas, que la substitution S est elle-même paire ou impaire.

Cette définition posée, le résultat est le suivant :

Le groupe G'_{2n} est formé des substitutions paires contenues dans G_{2n}.

18. Une question essentielle dans l'étude des groupes résolubles Γ contenus dans G_{2n} construits par la méthode décrite dans notre *Traité des Substitutions* est de reconnaître pour chacun de ces groupes s'il contient ou non des substitutions qui ne figurent pas dans G'_n.

La solution de cette question, que nous avions obtenue dans cet Ouvrage (n^{os} 671 à 684) par des considérations très compliquées, devient tout à fait simple lorsqu'on s'appuie sur la proposition précédente.

Rappelons en effet quelques-uns des caractères principaux des groupes résolubles en question. Ils sont de plusieurs sortes :

19. 1° *Groupes décomposables.* — Ils correspondent aux diverses décompositions de n en deux facteurs l, m. Les variables s'y répartissent en l systèmes

$$(x_1, \ldots, x_{2m}), \quad (y_1, \ldots, y_{2m}), \quad \ldots.$$

La fonction quadratique invariante F_{2n} est une somme de l fonctions partielles pareilles

$$F(x_1, \ldots, x_{2m}) + F(y_1, \ldots, y_{2m}) + \ldots.$$

Le groupe Γ résulte de la combinaison de substitutions S permutant les systèmes d'un mouvement d'ensemble (de manière à remplacer chaque variable par une autre de même indice) avec des substitutions T opérées sur les seules variables $x_1, \ldots, x_{2m}$: celles-ci formant un groupe Γ_1 résoluble, indécomposable et n'altérant pas la fonction partielle $F(x_1, \ldots, x_{2m})$.

Il est clair que la substitution S est paire ; car s'il est une fonction f_1 des variables $x_1, y_1, \ldots$, qu'elle multiplie par un facteur s, elle reproduira, multipliées par le même facteur, les fonctions $f_2, \ldots, f_{2m}$ for-

mées respectivement avec les variables d'indice 2, ..., $2m$. Le nombre total des fonctions qu'elle multiplie par des facteurs constants sera donc un multiple de $2m$, nombre pair.

20. Reste à savoir si Γ_1 contient ou non des substitutions impaires. La question est ainsi ramenée au cas des groupes indécomposables. Ceux-ci se distinguent en deux catégories :

2° *Groupes indécomposables de première catégorie.* — Les variables s'y partagent en deux systèmes

$$(x_1, x_2, \ldots, x_n), \quad (y_1, y_2, \ldots, y_n).$$

La forme invariante F_{2n} a pour expression

$$x_1 y_1 + x_2 y_2 + \ldots + x_n y_n.$$

Les substitutions de Γ seront de l'une des deux formes $\mathfrak{Q}$ ou $\mathfrak{R}\mathfrak{Q}$; $\mathfrak{R}$ désignant la substitution qui échange les x avec les y, et $\mathfrak{Q}$ le produit d'une substitution partielle

$$S = \left| x_k \quad \sum_i a_{ik} x_i \right|,$$

opérée sur les x, par la substitution *adjointe*

$$S' = \left| y_k \quad \sum_i b_{ik} y_i \right|$$

opérée sur les y. On sait que cette substitution adjointe est la réciproque de la *transposée*

$$| y_k \quad \Sigma a_{ki} y_i |.$$

1° Les substitutions $\mathfrak{Q}$ sont paires. Supposons en effet la substitution S mise sous forme canonique. Les variables s'y partageront en diverses suites ayant chacune une forme telle que la suivante

$$| x_\mu, x_{\mu-1}, \ldots, x_1 \quad s(x_\mu + x_{\mu-1}), s(x_{\mu-1} + x_{\mu-2}), \ldots, s x_1 |.$$

A cette suite répondra dans la transposée la suivante

$$| y_\mu, y_{\mu-1}, \ldots, y_1 \quad s y_\mu, s(y_\mu + y_{\mu-1}), \ldots, s(y_2 + y_1) |.$$

A la fonction x_1, que S multiplie par s, correspondra ainsi une autre fonction y_μ multipliée par s dans la transposée et par s^{-1} dans l'adjointe. Les fonctions des variables x, y que $\mathfrak{Q}$ multiplie par des facteurs constants étant ainsi associées deux à deux seront en nombre pair.

2° Passons à la substitution $\mathfrak{R}$. Dans la substitution partielle

$$| x_k, y_k \quad y_k, x_k |$$

prenons pour variable indépendante $z_k = x_k + y_k$. La substitution considérée n'altère pas z_k et remplace x_k par $z_k - x_k \equiv x_k + z_k \pmod 2$; d'où la forme canonique

$$| x_k, z_k \quad x_k + z_k, z_k |.$$

Les seules fonctions que $\mathfrak{R}$ reproduise à des facteurs constants près sont donc les n fonctions z_k. Donc $\mathfrak{R}$ sera paire ou impaire en même temps que n.

Donc pour que Γ contienne une substitution impaire, il faut que n soit impair. Cette condition est suffisante, car Γ ne peut être indécomposable que s'il contient une substitution de l'espèce $\mathfrak{R}\mathfrak{Q}$.

21. 3° *Groupes indécomposables de deuxième catégorie.* — Ils correspondent aux décompositions de n en un produit de facteurs

$$n = \nu\pi^\sigma\pi'^{\sigma'}\ldots = \nu m,$$

π, π', ... étant des nombres premiers qui divisent $2^\nu + 1$. Par l'introduction d'une racine j d'une congruence irréductible de degré 2ν, les variables indépendantes seront complexes et formeront 2ν séries conjuguées

$$(x_1, \ldots, x_m), (x'_1, \ldots, x'_m)\ldots(x_1^{(2\nu-1)}, \ldots, x_m^{(2\nu-1)})$$

et les substitutions de Γ seront de la forme $\mathfrak{P}^\rho\mathfrak{Q}$, $\mathfrak{P}$ désignant la substitution qui remplace chaque variable x_k^i par sa conjuguée suivante x_k^{i+1} et $\mathfrak{Q}$ un produit de substitutions conjuguées opérées respectivement sur les variables de chacune des séries conjuguées.

1° Les substitutions $\mathfrak{Q}$ sont paires. Car si elles multiplient par un facteur constant s une fonction f des variables de la première série,

elles multiplieront les 2ν fonctions conjuguées f, f', ..., $f^{2\nu-1}$ respectivement par les facteurs s, s', ..., $s^{2\nu-1}$ conjugués de s. Le nombre total des fonctions que $\mathfrak{Q}$ multiplie par des facteurs constants sera donc un multiple de 2ν, nombre pair.

2° Passons à la substitution $\mathfrak{P}$. Elle est le produit de m permutations circulaires

$$(x_1 x'_1 \ldots x_1^{(2\nu-1)}), \quad \ldots, \quad (x_k x'_k \ldots x_k^{(2\nu-1)}), \quad \ldots.$$

Pour qu'une fonction linéaire

$$a x_k + a' x'_k + \ldots$$

des variables d'indice k se reproduise multipliée par s lorsqu'on effectue sur les variables la permutation circulaire indiquée, il faut qu'on ait

$$a \equiv a' s, \quad a' \equiv a'' s, \quad \ldots \quad (\text{mod } 2),$$

d'où

$$s^{2\nu} \equiv 1 \quad (\text{mod } 2).$$

A chaque racine de cette équation correspond ainsi une seule fonction (déterminée à un facteur constant près). Cherchons donc le nombre de ces racines.

Soit $2\nu = 2^\alpha q$, q étant impair. On a

$$s^{2^\alpha q} - 1 \equiv (s^{2^{\alpha-1} q} - 1)^2 \equiv \ldots \equiv (s^q - 1)^{2^\alpha} \quad (\text{mod } 2).$$

D'ailleurs $s^q - 1$ et sa dérivée $q s^{q-1}$ n'ayant pas de racine commune, on aura q racines distinctes.

Le nombre total des fonctions que $\mathfrak{P}$ multiplie par des facteurs constants est donc mq. Or q est impair ; m l'est également, étant un produit de facteurs qui divisent $2^\nu + 1$. Donc $\mathfrak{P}$ est impaire.

Donc Γ contiendra une substitution impaire si parmi ses substitutions, qui sont toutes de la forme $\mathfrak{P}^\rho \mathfrak{Q}$, il en est où ρ soit impair.

22. Or nous avons montré dans notre Traité, par une analyse qu'il est inutile de reproduire ici, que pour former le groupe Γ on est amené à construire :

1° Un groupe H résoluble et général contenu dans le groupe linéaire à 2σ variables (mod π) et dont les substitutions, opérées simultané-

ment sur deux séries de variables cogrédientes

$$(x_1, \ldots, x_{2\sigma}), \quad (X_1, \ldots, X_{2\sigma}),$$

reproduisent à un facteur constant près une forme bilinéaire gauche. Si g est une racine primitive de π, l'exposant de la moindre puissance de g à laquelle le multiplicateur puisse se réduire est 1 ou 2. Cet exposant d se nomme l'exposant du groupe H;

2° Un groupe analogue H′ à $2\sigma'$ variables $(\mathrm{mod}\,\pi')$ et d'exposant d'; g' désignant une racine primitive de π';

Etc.

Pour qu'il existe dans Γ une substitution $\mathfrak{P}^\rho \mathfrak{Q}'$ où ρ ait une valeur donnée, il faut et il suffit qu'on puisse déterminer des entiers e, e', ..., tels que l'on ait à la fois

$$2^\rho \begin{cases} \equiv g^{de} & (\mathrm{mod}\,\pi), \\ \equiv g'^{d'e'} & (\mathrm{mod}\,\pi'), \\ \cdots\cdots\cdots\cdots\cdots & \end{cases}$$

La première congruence pourra toujours être satisfaite si $d = 1$; ou si d étant égal à 2, 2 est résidu quadratique de π. Mais elle sera impossible pour les valeurs impaires de ρ si $d = 2$ et $\left(\frac{2}{\pi}\right) = -1$.

De même pour les autres congruences.

Donc *la condition pour l'existence dans* Γ *d'une substitution impaire est que* 2 *soit résidu quadratique de tous ceux des entiers* π *pour lesquels l'exposant du groupe correspondant est* 2.