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

CAMILLE JORDAN

Sur la résolution algébrique des équations primitives de degré p^2 (p étant premier impair)

Journal de mathématiques pures et appliquées 2^e série, tome 13 (1868), p. 111-135.
<http://www.numdam.org/item?id=JMPA_1868_2_13__111_0>

SUR LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS PRIMITIVES DE DEGRÉ p^2 (p ÉTANT PREMIER IMPAIR);

PAR M. CAMILLE JORDAN,
Ingénieur des Mines.

Nous avons établi dans un précédent Mémoire (t. XII de ce journal, 2e série) que le groupe de toute équation primitive et soluble par radicaux de degré p^2 s'obtient en combinant aux substitutions de la forme $\begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}$ un groupe $\mathfrak{L}$ de substitutions de la forme linéaire $\begin{vmatrix} x & ax+by \\ y & a'x+b'y \end{vmatrix}$.

Nous démontrerons ici que les groupes des équations cherchées se ramènent tous à l'un des trois types suivants :

Premier type. — Il contient $2(p-1)^2p^2$ substitutions dérivées des suivantes :

$$E=\begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix},\quad F=\begin{vmatrix} x & mx \\ y & m'y \end{vmatrix}\quad\text{et}\quad G=\begin{vmatrix} x & y \\ y & x \end{vmatrix},$$

les constantes α et α' prenant, dans les diverses substitutions du groupe, toutes les valeurs de la suite $0, 1, \ldots, p-1$, et m, m' prenant chacune la suite des valeurs $1, \ldots, p-1$.

Deuxième type. — Il contient $2(p^2-1)p^2$ substitutions dérivées des suivantes :

$$E=\begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix},\quad F=\begin{vmatrix} x & \gamma x+\delta\varepsilon y \\ y & \delta x+\gamma y \end{vmatrix}\quad\text{et}\quad G=\begin{vmatrix} x & x \\ y & -y \end{vmatrix},$$

e étant un résidu quadratique de p choisi arbitrairement; α, α',... variant chacun de 0 à $p-1$, ainsi que γ et δ, en excluant seulement le système de valeurs $\gamma = 0$, $\delta = 0$.

Troisième type. — Il contient $24(p-1)p^2$ substitutions, et change de forme suivant que $p \equiv 1$ ou $\equiv 3 \pmod 4$.

1° Si $p \equiv 1 \pmod 4$, il est dérivé des substitutions suivantes :

$$\mathrm{E} = \begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}, \quad \mathrm{M}_1 = \begin{vmatrix} x & jx \\ y & -jy \end{vmatrix}, \quad \mathrm{P} = \begin{vmatrix} x & x-jy \\ y & x+jy \end{vmatrix},$$

$$\mathrm{F} = \begin{vmatrix} x & ax \\ y & ay \end{vmatrix}, \qquad \mathrm{M}_2 = \begin{vmatrix} x & jy \\ y & jx \end{vmatrix}, \quad \mathrm{Q} = \begin{vmatrix} x & x+y \\ y & x-y \end{vmatrix},$$

j étant une racine de la congruence $j^2 \equiv -1 \pmod p$; α, α' variant de 0 à $p-1$, et a de 1 à $p-1$.

2° Si $p \equiv 3 \pmod 4$, il est dérivé des substitutions suivantes :

$$\mathrm{E} = \begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}, \quad \mathrm{M}_1 = \begin{vmatrix} x & y \\ y & -x \end{vmatrix},$$

$$\mathrm{F} = \begin{vmatrix} x & ax \\ y & ay \end{vmatrix}, \qquad \mathrm{M}_2 = \begin{vmatrix} x & sx+ty \\ y & tx-sy \end{vmatrix},$$

$$\mathrm{P} = \begin{vmatrix} x & -(1+st)x+(s-t^2)y \\ y & (t+s^2)x+(st-s-t)y \end{vmatrix},$$

$$\mathrm{Q} = \begin{vmatrix} x & sx+(t+1)y \\ y & (t-1)x-sy \end{vmatrix},$$

s et t étant deux entiers arbitrairement choisis parmi ceux qui satisfont à la congruence $s^2+t^2 \equiv -1 \pmod p$; α, α', a variant comme précédemment.

Réciproquement, les trois types de groupes ci-dessus appartiennent à des équations primitives solubles par radicaux; ils sont en outre généraux et distincts, sauf les cas d'exception suivants :

1° Si $p = 3$, le premier et le deuxième type sont contenus dans le troisième, qui est seul général;

2° Si $p = 5$, le premier type est contenu dans le troisième.

Galois avait annoncé que les équations primitives et solubles par radicaux rentreraient dans un type unique, sauf pour le neuvième et le vingt-cinquième degré, qui présenteraient certains types exceptionnels. On voit par les énoncés qui précèdent qu'il faut prendre presque exactement le contre-pied de cette assertion.

La méthode dont nous ferons usage pour établir ces propositions s'applique, avec quelques modifications, aux équations primitives d'un degré quelconque. Nous réserverons cette généralisation pour un ouvrage spécial. Il nous suffit présentement de mettre en évidence, par un exemple simple, le fait de la pluralité des types généraux d'équations résolubles.

I.

1. Soient $z \equiv mx + ny \pmod{p}$, $u \equiv m'x + n'y \pmod{p}$ deux fonctions linéaires de x et de y telles, que le déterminant $\begin{vmatrix} m & n \\ m' & n' \end{vmatrix}$ ne se réduise pas à o (mod. p). A chaque système de valeurs de x, y correspondra un système de valeurs de z, u, et réciproquement. Cela posé, au lieu de caractériser les diverses racines de l'équation proposée par les valeurs de x, y qui leur correspondent respectivement, on pourra les caractériser par les valeurs de z, u. Voyons ce que deviennent, après ce changement d'indices, les substitutions du groupe de l'équation.

La substitution $\begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}$, accroissant x et y respectivement de α et α', accroîtra z de $m\alpha + n\alpha'$ et u de $m'\alpha + n'\alpha'$; elle prendra donc la forme $\begin{vmatrix} z & z+m\alpha+n\alpha' \\ u & u+m'\alpha+n'\alpha' \end{vmatrix}$. Si l'on fait varier α et α', $m\alpha + n\alpha'$ et $m'\alpha + n'\alpha'$ prendront successivement tous les systèmes de valeurs possibles. Le faisceau formé par les substitutions $\begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}$ conservera donc sa forme après le changement d'indices.

Considérons maintenant une substitution S de la forme

$$\begin{vmatrix} x & ax+by \\ y & a'x+b'y \end{vmatrix}.$$

Elle remplace z par

$$m(ax + by) + n(a'x + b'y)$$

et u par

$$m'(ax + by) + n'(a'x + b'y).$$

D'ailleurs x et y sont des fonctions linéaires de z, u; donc la substitution considérée remplace z et u par des fonctions linéaires de ces quantités; mais ces fonctions linéaires contiennent les indéterminées m, n, m', n', dont on peut profiter pour simplifier la nouvelle expression de S.

Or il existe en général deux fonctions distinctes, que S multiplie chacune par un simple facteur constant. En effet, pour que $z' = mx + ny$ jouisse de cette propriété, il faudra que l'on ait

$$m(ax + by) + n(a'x + b'y) \equiv kz \equiv k(mx + ny),$$

k étant ce facteur constant; d'où les relations

$$(1) \qquad \begin{cases} ma + na' \equiv km, \\ mb + nb' \equiv kn, \end{cases}$$

qui détermineront le rapport $\frac{m}{n}$, pourvu qu'on prenne pour k une racine de la congruence

$$\begin{vmatrix} a - k & a' \\ b & b' - k \end{vmatrix} \equiv 0 \pmod{p}.$$

1° Si cette congruence a deux racines réelles, α et β, il existera deux fonctions, z, u, que S multipliera respectivement par α et β; en les prenant pour indices à la place de z et de u, on aura ramené S à la forme $\begin{vmatrix} z & \alpha z \\ u & \beta u \end{vmatrix}$.

2° Si ces racines sont imaginaires, soit i une racine d'une congruence irréductible du second degré choisie arbitrairement, celle-ci, par exemple.

$$\xi^2 \equiv e \pmod{p},$$

e étant un non-résidu quadratique de p pris à volonté; les deux racines de l'équation en k seront des entiers complexes conjugués, $\alpha+\beta i$ et $(\alpha+\beta i)^p \equiv \alpha+\beta i^p$, formés avec cette imaginaire; les valeurs correspondantes de $\frac{m}{n}$, déterminées par les relations (1), seront elles-mêmes des imaginaires conjuguées; les deux fonctions z et u seront donc respectivement égales à $X+iY$ et à $X+i^pY$, X et Y étant des fonctions linéaires réelles de x, y; et S, rapporté à ces nouveaux indices, sera de la forme $\begin{vmatrix} z & (\alpha+\beta i)z \\ u & (\alpha+\beta i^p)u \end{vmatrix}$,

3° Si les racines de la congruence (1) sont égales, il n'existe qu'une seule fonction z que S multiplie par un facteur constant. Soit u une autre fonction quelconque de x et y, S prendra la forme

$$\begin{vmatrix} z & \alpha z \\ u & \beta z+\gamma u \end{vmatrix}.$$

On a d'ailleurs $\gamma=\alpha$, sans quoi la congruence

$$\begin{vmatrix} \alpha-k & 0 \\ \beta & \gamma-k \end{vmatrix} \equiv 0 \pmod{p}$$

aurait ses racines inégales, et il y aurait contre l'hypothèse deux fonctions de z, u, ou, ce qui revient au même, de x, y, que S multiplierait par un facteur constant.

Nous obtenons donc ce premier résultat :

Toute substitution linéaire S *peut être ramenée par un choix d'indices convenable à l'une des trois formes canoniques suivantes :*

$$\begin{vmatrix} z & \alpha z \\ u & \beta u \end{vmatrix}, \quad \begin{vmatrix} z & (\alpha+\beta i)z \\ u & (\alpha+\beta i^p)u \end{vmatrix}, \quad \begin{vmatrix} z & \alpha z \\ u & \beta z+\alpha u \end{vmatrix}.$$

2. Cela posé, les substitutions $\mathfrak{L}$ formant un groupe résoluble, on pourra y déterminer un faisceau F de substitutions échangeables entre elles, et auquel toutes les substitutions $\mathfrak{L}$ seront permutables (*voir* le Mémoire cité, Chap. I^er^, théor. IV). S'il y a plusieurs manières de déterminer un premier faisceau F satisfaisant aux deux conditions ci-dessus,

on peut admettre qu'il ait été choisi de manière à contenir le plus grand nombre possible de substitutions. Il contiendra, dans ce cas, toutes les substitutions qui multiplient les deux indices x et y par un même facteur constant.

Soit en effet Σ une de ces substitutions : elle est évidemment échangeable à toute substitution linéaire. Soient, d'autre part, Q, R,... les substitutions qui, étant adjointes successivement à F, reproduisent le groupe $\mathfrak{L}$. Le groupe dérivé des substitutions Σ, F, Q, R,... est évidemment résoluble et contient toutes les substitutions de $\mathfrak{L}$; mais, par hypothèse, il ne peut être plus général : donc il se confond avec $\mathfrak{L}$. En outre, le faisceau (Σ, F) a ses substitutions échangeables entre elles; il est permutable à toutes les substitutions de $\mathfrak{L}$; il jouit donc des propriétés qui caractérisent F, et serait plus général, contrairement à l'hypothèse faite, si F ne contenait pas Σ.

Il peut se faire : 1° que F ne contienne d'autres substitutions que celles de la forme Σ; 2° ou qu'il en contienne quelque autre, S. Ce dernier cas peut se subdiviser en trois autres, suivant la forme canonique à laquelle se réduit S.

3. PREMIER CAS. — S *est réductible à la forme* $\begin{vmatrix} z & \alpha z \\ u & \beta u \end{vmatrix}$, α *étant* $\gtrless \beta$.

Soit $T = \begin{vmatrix} z & az + bu \\ u & b'z + a'u \end{vmatrix}$ une autre substitution quelconque de F : elle doit être échangeable à S; d'où les relations

$$a\alpha z + b\beta u \equiv \alpha(az + bu),$$
$$b'\alpha z + a'\beta u \equiv \beta(b'z + a'u),$$

lesquelles doivent être identiques, quels que soient z et u. On aura en particulier $b\beta \equiv \alpha b$, $b'\alpha \equiv \beta b'$, d'où $b \equiv 0$, $b' \equiv 0$. T se réduira donc à la forme $\begin{vmatrix} z & az \\ u & a'u \end{vmatrix}$.

Soit $U = \begin{vmatrix} z & mz + nu \\ u & n'z + m'u \end{vmatrix}$ une substitution quelconque de $\mathfrak{L}$: elle est permutable à F; donc $U^{-1}SU = T$ ou $SU = UT$, T étant une substitution de la forme que nous venons de déterminer : égalité qui

donne les relations

$$m\alpha z + n\beta u \equiv a\,(mz + nu),$$
$$n'\alpha z + m'\beta u \equiv a'(n'z + m'u),$$

d'où

$$(a - \alpha)\, m \equiv (a - \beta)\, n \equiv (a' - \alpha)\, n' \equiv (a' - \beta)\, m' \equiv 0.$$

Si $(a - \alpha) \gtrless 0$, on aura $m \equiv 0$, et le déterminant $mm' - nn'$ ne pouvant s'annuler, on aura $nn' \gtrless 0$; donc $a' - \alpha \equiv 0$ et $a' - \beta \gtrless 0$, d'où $m' \equiv 0$.

Si $a - \alpha \equiv 0$, on aura $a - \beta \gtrless 0$, d'où $n \equiv 0$, et par suite $m' \gtrless 0$, d'où $a' - \beta \equiv 0$, $a' - \alpha \gtrless 0$, et enfin $n' \equiv 0$.

Les substitutions de $\mathfrak{L}$ seront donc toutes de l'une des formes générales

$$\begin{vmatrix} z & mz \\ u & m'u \end{vmatrix}, \qquad \begin{vmatrix} z & nu \\ u & n'z \end{vmatrix}.$$

Réciproquement, l'ensemble des substitutions de ces deux formes constitue un groupe résoluble, car il s'obtient en combinant aux substitutions du faisceau $\begin{vmatrix} z & mz \\ u & m'u \end{vmatrix}$, lesquelles sont échangeables entre elles, la substitution $\begin{vmatrix} z & u \\ u & z \end{vmatrix}$, qui lui est permutable.

On a ainsi un premier type d'équations solubles par radicaux, dont le groupe s'obtient en combinant ensemble les substitutions

$$\begin{vmatrix} z & mz + \alpha \\ u & m'u + \alpha' \end{vmatrix} \quad \text{et} \quad \begin{vmatrix} z & u \\ u & z \end{vmatrix}.$$

L'ordre de ce groupe est évidemmennt égal à $2\,(p-1)^2 p^2$, α et α' pouvant prendre toutes les valeurs $0, 1, \ldots, p-1$, et m, m' les valeurs $1, \ldots, p-1$.

Par l'extraction d'une racine carrée on pourra réduire ce groupe aux seules substitutions $\begin{vmatrix} z & mz + \alpha \\ u & m'u + \alpha' \end{vmatrix}$. Ce groupe réduit n'étant plus primitif, la résolution de l'équation pourra se ramener à la résolution successive de deux équations du degré p.

4. Deuxième cas. — S *est réductible à la forme* $\begin{vmatrix} z & (\alpha+\beta i)z \\ u & (\alpha+\beta i^p)z \end{vmatrix}$.

Les deux quantités conjuguées $\alpha+\beta i$, $\alpha+\beta i^p$ étant supposées imaginaires, et par suite distinctes, on voit, comme au cas précédent, que les substitutions de $\mathfrak{L}$ se réduisent toutes à l'une des deux formes

$$\begin{vmatrix} z & mz \\ u & m'u \end{vmatrix}, \quad \begin{vmatrix} z & nu \\ u & n'z \end{vmatrix}.$$

Mais ici les indices z et u, exprimés en fonction des indices primitifs, contiennent l'imaginaire i. Les facteurs m, m', n, n', au lieu d'être des entiers réels, comme tout à l'heure, pourront contenir l'imaginaire i. Soit donc

$$m=\gamma+\delta i, \quad n=\varepsilon+\zeta i,$$

on aura nécessairement

$$m'\equiv\gamma+\delta i^p\equiv m^p, \quad n'=\varepsilon+\zeta i^p\equiv n^p.$$

Car il est clair qu'une substitution réelle ne peut remplacer z par $(\gamma+\delta i)z$ ou par $(\varepsilon+\zeta i)u$ sans remplacer en même temps l'indice conjugué u par la fonction conjuguée $(\gamma+\delta i^p)u$ ou $(\varepsilon+\zeta i^p)z$. Les substitutions de $\mathfrak{L}$ seront donc de l'une des formes suivantes :

$$\begin{vmatrix} z & mz \\ u & m^p u \end{vmatrix}, \quad \begin{vmatrix} z & nu \\ u & n^p z \end{vmatrix},$$

m et n étant des entiers complexes $\gamma+\delta i$, $\varepsilon+\zeta i$.

Réciproquement, le groupe formé par l'ensemble de ces substitutions est résoluble; car ses substitutions s'obtiennent évidemment en ajoutant à celles de la première forme, qui sont échangeables entre elles, la substitution $\begin{vmatrix} z & u \\ u & z \end{vmatrix}$, qui les permute les unes dans les autres.

Le groupe $\mathfrak{L}$, ainsi obtenu, a son ordre égal à $2(p^2-1)$. En effet, γ et δ peuvent prendre tous les systèmes de valeurs possibles (pourvu qu'ils ne soient pas nuls à la fois) sans annuler le déterminant

$$(\gamma+\delta i)(\gamma+\delta i^p).$$

On peut donc les choisir de $p^2 - 1$ manières différentes; de même pour ε et ζ.

On peut d'ailleurs très-aisément chasser les imaginaires de l'expression de ses substitutions. En effet, la substitution $\left|\begin{matrix} z & (\gamma + \delta i)\, z \\ u & (\gamma + \delta i^p)\, u \end{matrix}\right|$, remplaçant $z = X + iY$ par $(\gamma + \delta i)(X + iY)$, et la fonction conjuguée $u = X + i^p Y$ par la fonction conjuguée $(\gamma + \delta i^p)(X + i^p Y)$, remplacera évidemment X et Y par la partie réelle et par la partie imaginaire de $(\gamma + \delta i)(X + iY)$, soit respectivement par $\gamma X + \delta e Y$ et $\delta X + \gamma Y$. Cette substitution, rapportée aux indices indépendants X, Y, prendra donc la forme $\left|\begin{matrix} X & \gamma X + \delta e Y \\ Y & \delta X + \gamma Y \end{matrix}\right|$. De même la substitution $\left|\begin{matrix} z & u \\ u & z \end{matrix}\right|$, remplaçant $X + iY$ par $X + i^p Y \equiv X - iY$ et réciproquement, prendra la forme $\left|\begin{matrix} X & X \\ Y & -Y \end{matrix}\right|$.

Combinant aux substitutions ci-dessus les suivantes :

$$\left|\begin{matrix} X & X + \alpha \\ Y & Y + \alpha' \end{matrix}\right|,$$

on obtiendra un groupe contenant $2(p^2 - 1)\, p^2$ substitutions et caractérisant un second type d'équations solubles par radicaux.

3. Troisième cas. — S *est réductible à la forme* $\left|\begin{matrix} z & \alpha z \\ u & \beta z + \alpha u \end{matrix}\right|$, ($\beta$ *étant* $\gtrless$ 0).

Soit $T = \left|\begin{matrix} z & az + bu \\ u & b'z + a'u \end{matrix}\right|$ une substitution quelconque de F : elle sera échangeable à S; d'où les relations

$$a\,\alpha z + b\,(\beta z + \alpha u) \equiv \alpha\,(az + bu)$$
$$b'\alpha z + a'(\beta z + \alpha u) \equiv \beta\,(az + bu) + \alpha\,(b'z + a'u),$$

d'où l'on déduit $b = 0$. Les substitutions de F sont donc toutes de la forme suivante :

$$\left|\begin{matrix} z & az \\ u & b'z + a'u \end{matrix}\right|.$$

Soit maintenant $U = \begin{vmatrix} z & mz + nu \\ u & n'z + m'u \end{vmatrix}$ une substitution quelconque de $\mathfrak{L}$, on aura $SU = UT$, T étant une substitution de la forme que nous venons de déterminer, ce qui fournit les relations

$$m\alpha z + n(\beta z + \alpha u) \equiv a(mz + nu),$$
$$n'\alpha z + m'(\beta z + \alpha u) \equiv b'(mz + nu) + a'(n'z + m'u),$$

d'ou

$$m(\alpha - a) + \beta n \equiv 0, \quad n(\alpha - a) \equiv 0, \text{ etc.}, \quad \text{d'où enfin} \quad n \equiv 0.$$

Les substitutions $\mathfrak{L}$ sont donc toutes de la forme

$$\begin{vmatrix} z & mz \\ u & n'z + m'u \end{vmatrix}.$$

Mais ce groupe, combiné avec les substitutions $\begin{vmatrix} z & z + \alpha \\ u & u + \alpha' \end{vmatrix}$, ne donnera pas un groupe primitif; car si l'on réunit dans un même système les diverses racines qui correspondent à une même valeur de z, il est clair que chacune des substitutions considérées remplacera les racines d'un système par celles d'un même système.

On doit donc rejeter l'hypothèse ci-dessus.

6. Quatrième cas. — F *est formé des seules substitutions* Σ.

On sait qu'on peut déterminer dans $\mathfrak{L}$ un second faisceau G tel, 1° que les substitutions $\mathfrak{L}$ lui soient permutables; 2° qu'il contienne F; 3° que ses substitutions soient échangeables entre elles aux F près (*voir* le Mémoire déjà cité, Chap. I^er^, théorème IV).

Si ce faisceau G peut être choisi de plusieurs manières, nous ferons en sorte qu'il contienne le moindre nombre possible de substitutions.

Dans cette hypothèse, soient S_1 une substitution quelconque de G, $S_2, S_3, \ldots$ ses transformées par les diverses substitutions de $\mathfrak{L}$; le faisceau dérivé de $(F, S_1, S_2, \ldots)$ satisfait évidemment aux trois relations qui caractérisent G; il est contenu en outre dans G, et comme il ne peut être moins général, il se confond avec lui.

Parmi les substitutions $S_2, \ldots$, il en existe une au moins non échan-

geable à S_1, car s'il n'en est pas ainsi, soit φ le faisceau formé par celles des substitutions de G qui jouissent ainsi que F et S_1 de la propriété d'être échangeables à toutes les substitutions G, elles sont échangeables entre elles; d'ailleurs les substitutions $\mathcal{L}$ lui sont permutables, car étant permutables à G, elles transforment chaque substitution de φ, telle que φ_1, en une substitution contenue dans G et échangeable aux substitutions transformées de celles de G, lesquelles ne sont autres que les G; la transformée de φ_1 fera donc elle-même partie de φ.

Le faisceau φ jouirait donc des mêmes propriétés que F, quoique plus général, contrairement à nos hypothèses.

Supposons donc que $S_2 = T^{-1} S_1 T$ ne soit pas échangeable à S_1, la substitution $S_1^{-1} T^{-1} S_1 T = M_1$ fera partie de G, mais sans se réduire à la forme F, car elle n'est pas échangeable à S_1, et les F le sont. D'autre part, son déterminant se réduit à l'unité, car soient d et δ les déterminants respectifs de S_1 et de T, le déterminant de M_1 sera égal à $d^{-1}\delta^{-1}d\delta \equiv 1$.

Soient $M_2 = T^{-1} M_1 T$, $M_3 = U^{-1} M_1 U, \ldots$, les transformées de M_1 par les substitutions $\mathcal{L}$, leur déterminant sera égal à 1; en outre, d'après ce que nous venons de démontrer, l'une d'elles au moins, telle que M_2, ne sera pas échangeable à M_1, et par suite ne fera pas partie de F.

Il est donc prouvé que G *contient deux substitutions* M_1 *et* M_2 *de déterminant* 1, *lesquelles ne font pas partie de* F, *et ne sont pas échangeables entre elles.*

7. On peut remplacer x et y par d'autres indices z et u, choisis de manière à ramener M_1 à sa forme canonique. Ce changement d'indices n'altérera pas la forme des substitutions F, car chacune d'elles, multipliant x et y par un même facteur constant, multipliera par le même facteur toute fonction linéaire de ces indices.

M_1 *ne peut se réduire à la forme* $\begin{vmatrix} z & \alpha z \\ u & \beta z + \alpha u \end{vmatrix}$; car s'il en était ainsi, soit $T = \begin{vmatrix} z & az + bu \\ u & b'z + a'u \end{vmatrix}$ une substitution quelconque de G; elle est échangeable, aux F près, à S; on aura donc une relation telle que $ST = TSf$, f désignant la substitution qui multiplie les indices

par un même facteur constant f. Cette égalité donne les relations

$$a\alpha z + b(\beta z + \alpha u) \equiv f\alpha(az + bu)\ldots,$$

d'où

$$\alpha b = f\alpha b, \quad a\alpha + b\beta = f\alpha a,$$

d'où enfin

$$b = 0.$$

les substitutions de G se réduisent donc toutes à la forme

$$\begin{vmatrix} z & az \\ u & b'z + a'u \end{vmatrix},$$

chaque substitution de $\mathfrak{L}$ étant permutable à G, transformera M_1 en une substitution de cette forme; et le groupe $\mathfrak{L}$ combiné aux substitutions $\begin{vmatrix} z & z+\alpha \\ u & u+\alpha' \end{vmatrix}$ ne donnera pas un groupe primitif (*voir* le troisième cas).

8. Soit donc $M_1 = \begin{vmatrix} z & \alpha z \\ u & \beta u \end{vmatrix}$, α et β étant deux entiers différents, réels ou imaginaires conjugués. Le déterminant de M_1 étant égal à l'unité, on aura $\alpha\beta \equiv 1$. La substitution $T = \begin{vmatrix} z & az+bu \\ u & b'z+a'u \end{vmatrix}$ satisfaisant à la relation $M_1 T = TM_1 f'$, on aura les conditions

$$a\alpha z + b\beta u \equiv f\alpha(az + bu),$$
$$b'\alpha z + a'\beta u \equiv f\beta(b'z + a'u),$$

d'où

$$a\alpha \equiv f\alpha a, \quad b\beta \equiv f\alpha b, \quad b'\alpha \equiv fb'\beta, \quad a'\beta \equiv fa'\beta.$$

Si l'on n'a pas à la fois $a = a' = 0$, il viendra $f = 1$, puis $b = b' = 0$. Si au contraire $a = a' = 0$, bb' sera $\gtrless 0$, sans quoi le déterminant de T s'annulerait, et l'on aura

$$\beta \equiv f\alpha, \quad \alpha \equiv f\beta, \quad \text{d'où} \quad f^2 \equiv 1,$$

et comme β diffère de α,

$$f = -1, \quad \beta \equiv -\alpha.$$

Substituant cette valeur dans la relation $\alpha\beta \equiv 1$, il vient

$$\alpha^2 \equiv -1 \pmod{p}.$$

Deux cas seront à distinguer ici suivant que p sera de la forme $4n+1$ ou de la forme $4n+3$.

9. 1° Supposons p de la forme $4n+1$. La congruence

$$a^2 \equiv -1 \pmod{p}$$

aura deux racines réelles $\pm j$, et M_1 prendra la forme réelle

$$M_1 = \begin{vmatrix} z & jz \\ u & -ju \end{vmatrix}.$$

D'après ce qu'on vient de voir, parmi les substitutions de G, les unes lui seront échangeables et seront de la forme $\begin{vmatrix} z & az \\ u & a'u \end{vmatrix}$, les autres la transformeront en $M_1\theta$ (θ étant la substitution qui multiplie tous les indices par -1), et seront de la forme $\begin{vmatrix} z & bu \\ u & b'z \end{vmatrix}$. En particulier M_2 sera de cette dernière forme; on peut d'ailleurs y supposer $b = j$; car soit $b \equiv jm \pmod{p}$; on pourrait prendre mu pour indice indépendant à la place de u, ce qui n'altérerait pas l'expression des F ni celle des M_1.

Soit donc $b = j$. Le déterminant de M_2 étant égal à l'unité, on aura

$$jb' \equiv -1 \equiv j^2, \quad \text{d'où} \quad b' = j,$$

et enfin

$$M_2 = \begin{vmatrix} z & ju \\ u & jz \end{vmatrix}.$$

Les substitutions de G sont toutes de la forme $M_1^{\rho_1} M_2^{\rho_2} f$, f étant une

des substitutions de F, et chacun des exposants ρ_1, ρ_2 étant égaux à zéro ou à 1.

Soit en effet T une quelconque de ces substitutions; nous venons de voir qu'elle transforme M_1 en M_1 ou en $M_1\theta$; elle devra de même transformer M_2 en M_2 ou $M_2\theta$. Supposons pour fixer les idées que T transforme M_1 et M_2 en $M_1\theta$ et $M_2\theta$, posons

$$T = M_1 M_2 T_1,$$

$T_1 = (M_1 M_2)^{-1} T$ sera échangeable à la fois à M_1 et à M_2; étant échangeable à M_1, elle se réduira à la forme $\begin{vmatrix} z & az \\ u & bu \end{vmatrix}$; pour qu'elle soit échangeable à M_2, il faudra en outre qu'on ait $b = a$; donc T_1 multiplie les indices par un même facteur constant, et par suite fait partie de F.

Soit maintenant U l'une quelconque des substitutions $\mathfrak{L}$; les transformées de M_1 et M_2 par cette substitution appartiennent au faisceau G; soient respectivement $M_1^{\rho'_1} M_2^{\rho'_2} f'$ et $M_1^{\rho''_1} M_2^{\rho''_2} f''$ ces transformées, leurs déterminants doivent se réduire à l'unité; mais ils sont respectivement égaux aux déterminants de f' et de f'', donc chacune des deux substitutions f', f'' doit se réduire à θ ou à $\theta^2 = 1$. En outre, ces deux substitutions sont échangeables entre elles à $\theta^{\rho'_1\rho''_2 - \rho''_1\rho'_2}$ près. Mais elles le sont à θ près, car on a

$$M_1^{-1} M_2^{-1} M_1 M_2 = \theta,$$

d'où

$$(U^{-1} M_1 U)^{-1} . (U^{-1} M_2 U)^{-1} . U^{-1} M_1 U . U^{-1} M_2 U$$
$$= U^{-1} M_1^{-1} M_2^{-1} M_1 M_2 U = U^{-1} \theta U = \theta,$$

donc

$$\rho'_1 \rho''_2 - \rho''_1 \rho'_2 \equiv 1 \pmod 2.$$

Cela posé, U résultera de la combinaison de F, M_1, M_2 avec la substitution $P = \begin{vmatrix} z & z - ju \\ u & z + ju \end{vmatrix}$, qui transforme M_1 et M_2 en M_2 et $M_1 M_2$, et la substitution $Q = \begin{vmatrix} z & z + u \\ u & z - u \end{vmatrix}$, qui les transforme en M_2 et M_1.

En effet

P	transforme	M_1	en	M_2,	et	M_2	en M_1M_2,
P^2	»	M_1		M_1M_2,		M_2	$M_2M_1M_2 = M_2$,
Q	»	M_1		M_2,		M_2	M_1,
QP	»	M_1		M_1M_2,		M_2	M_2,
QP^2	»	M_1		M_1,		M_2	M_1M_2.

On voit par ce tableau que $\rho'_1, \rho'_2, \rho''_1, \rho''_2$ étant égaux à zéro ou à 1, et satisfaisant à la relation $\rho'_1\rho''_2 - \rho'_2\rho''_1 \equiv 1 \pmod 2$, de quelque manière que ces indices soient d'ailleurs choisis, l'une des substitutions 1, P, P^2, Q, QP, QP^2 transformera M_1 et M_2 en $M_1^{\rho'_1}M_2^{\rho'_2}$ et $M_1^{\rho''_1}M_2^{\rho''_2}$. (Si par exemple on pose $\rho'_1 = 1$ et $\rho''_2 = 0$, d'où $\rho'_2 = 1$ et $\rho''_2 = 1$, la substitution P^2 produira la transformation voulue : de même pour les autres systèmes de solutions.) Soit $V = Q^\tau P^\tau$ cette substitution; $V^{-1}U$ transformera M_1 et M_2 en M_1f' et M_2f''. Soit $f' = \theta^{\mu_1}$, $f'' = \theta^{\mu_2}$, μ_1 et μ_2 étant égaux à 0 ou à 1; la substitution $\left(M_1^{\mu_1}M_2^{\mu_2}\right)^{-1}V^{-1}U = f$ sera échangeable à M_1 et M_2, et par suite se réduira à la forme F; on aura donc

$$U = VM_1^{\mu_1}M_2^{\mu_2}f.$$

Donc toutes les substitutions du groupe cherché $\mathfrak{L}$ appartiennent comme nous l'avons annoncé au groupe (F, M_1, M_2, P, Q). Mais réciproquement $\mathfrak{L}$ contient toutes les substitutions de ce groupe, car nous allons prouver qu'il est résoluble. En effet, les F sont échangeables entre eux, M_1 leur est échangeable, M_2 est permutable au faisceau (F, M_1), P l'est au faisceau (F, M_1, M_2), enfin Q l'est à (F, M_1, M_2, P), car elle l'est au faisceau partiel (F, M_1, M_2), et d'autre part la substitution $Q^{-1}PQ$, transformant M_1 et M_2 en $M_2M_1 = M_1M_2\theta$ et M_1, est égale à P^2M_1f, $f = (P^2M_1)^{-1}Q^{-1}PQ$ étant échangeable à la fois à M_1 et à M_2, et appartenant par suite au faisceau F; donc $Q^{-1}PQ$ appartient au faisceau (F, M_1, M_2, P).

L'expression générale des substitutions $\mathfrak{L}$ est, comme on l'a vu,

$Q^{\lambda} P^{\nu} M_1^{\mu_1} M_2^{\mu_2} f$, λ, μ_1, μ_2 étant égaux à 0 ou à 1, et ν à 0, 1 ou 2, enfin f étant l'une des $p-1$ substitutions de F. Deux substitutions correspondant à des valeurs différentes de λ, ν, μ_1, μ_2, f sont d'ailleurs évidemment distinctes. L'ordre de $\mathfrak{L}$ est donc égal à $24(p-1)$.

En combinant ce groupe avec les substitutions $\begin{vmatrix} z & z+\alpha \\ u & u+\alpha' \end{vmatrix}$, on obtient le troisième et dernier type de groupes résolubles dont l'ordre sera $24(p-1)p^2$.

10. 2° Supposons maintenant p de la forme $4n+3$. La congruence $\alpha^2 \equiv -1 \pmod{p}$ a deux racines imaginaires, $\alpha = j$ et $\beta \equiv -j \equiv j^p$. M_1 prend la forme canonique $\begin{vmatrix} z & jz \\ u & j^p u \end{vmatrix}$, z et u étant deux indices imaginaires conjugués. On voit, comme dans l'hypothèse précédente, que M_2 est de la forme $\begin{vmatrix} z & bu \\ u & b'z \end{vmatrix}$. D'ailleurs M_2, remplaçant z par bu, remplacera u par la fonction conjuguée $b^p z$; donc $b' \equiv b^p$. En outre, son déterminant étant égal à 1, on aura

$$b^{p+1} \equiv -1 \pmod{p}.$$

Cette dernière congruence a $p+1$ racines, respectivement égales à $\tau^{\frac{p-1}{2}}, \tau^{3\frac{p-1}{2}}, \ldots, \tau^{(2p+1)\frac{p-1}{2}}$, τ étant une racine primitive de la congruence $\tau^{p^2-1} \equiv 1 \pmod{p}$. Soit $r = s + tj$ l'une de ces racines, choisie à volonté : on peut supposer $b = r$; car admettons qu'il n'en soit pas ainsi, et soit

$$b = \tau^{\frac{p-1}{2}(2n+1)}, \quad r = \tau^{\frac{p-1}{2}(2n'+1)},$$

d'où

$$b = r\,\tau^{(p-1)(n-n')}.$$

Prenons pour indices indépendants, à la place de z et de u, les indices $\tau^{n-n'} z = z'$ et $\tau^{(n-n')p} u = u'$, lesquels sont également conjugués.

Ce changement d'indices, qui n'altère pas la forme des substitutions F, M_1, donnera à M_2 la forme voulue $\begin{vmatrix} z' & ru' \\ u' & r^p z' \end{vmatrix}$.

On voit maintenant, comme dans l'hypothèse précédente : 1° que les substitutions de G sont toutes de la forme $M_1^{\rho_1} M_2^{\rho_2} f$; 2° que si l'on peut déterminer deux substitutions P et Q qui transforment respectivement M_1, M_2 en M_2, $M_1 M_2$ et en M_2, M_1, $\mathfrak{L}$ sera formé des substitutions (F, M_1, M_2, P, Q) en nombre $24(p-1)$.

Or les substitutions P et Q existent en effet, et s'obtiennent aisément par la méthode des coefficients indéterminés. Mais auparavant il convient de ramener à la forme réelle les substitutions M_1 et M_2.

Soit $z = X + jY$, $u = X + j^p Y = X - jY$: M_1, remplaçant $X + jY$ par $j(X - jY)$, sera égale à $\begin{vmatrix} X & Y \\ Y & -X \end{vmatrix}$.

Quant à M_2, elle remplace $X + jY$ par $(s + tj)(X - iY)$. Rapportée aux indices X, Y, elle prendra donc la forme $\begin{vmatrix} X & sX + tY \\ Y & tX - sY \end{vmatrix}$, s et t étant deux entiers qui peuvent être choisis arbitrairement, pourvu qu'ils satifassent à la condition $(s + tj)^{p+1} \equiv -1 \pmod{p}$, laquelle peut s'écrire ainsi :

$$(s + tj)(s + tj^p) \equiv s^2 + t^2 \equiv -1 \pmod{p}.$$

On trouvera ensuite

$$P = \begin{vmatrix} X & -(1+st)X + (s - t^2)Y \\ Y & (t+s^2)X + (st - s + t)Y \end{vmatrix} \quad \text{et} \quad Q = \begin{vmatrix} X & sX + (t+1)Y \\ Y & (t-1)X - sY \end{vmatrix}.$$

En combinant le groupe que nous venons de construire avec les substitutions $\begin{vmatrix} X & X + \alpha \\ Y & Y + \alpha' \end{vmatrix}$, on aura le troisième type de groupes résolubles sous la forme indiquée pour le cas où p est de la forme $4n + 3$.

II.

11. Il est démontré par ce qui précède que tout groupe résoluble général et primitif de degré p^2 appartient à l'un des trois types énoncés. Il nous reste à prouver réciproquement : 1° que les groupes résolubles fournis comme nous l'avons indiqué sont primitifs; 2° que, sauf les exceptions signalées plus haut, ils sont généraux et distincts.

Pour établir la première proposition, nous nous appuierons sur le lemme suivant :

LEMME. — *Soit* L *un groupe de substitutions de la forme linéaire* $\begin{vmatrix} x & ax+by \\ y & b'x+a'y \end{vmatrix}$. *Si ses substitutions, jointes aux suivantes* $\mathrm{E} = \begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}$, *ne forment pas un groupe primitif, il existera une fonction des indices que toute substitution de* L *multipliera par un facteur constant.*

Supposons, en effet, que le groupe (L, E) ne soit pas primitif, les racines que ce groupe permute se partagent en systèmes tels, que chacune des substitutions (L, E) remplace les racines de chaque système par celles d'un même système. Soit Σ l'un de ces systèmes, ρ l'une des racines qu'il contient; les substitutions E permutent transitivement les racines : l'une d'elles au moins, S, remplacera donc ρ par une autre racine du même système, et par suite ne déplacera pas ce système.

La substitution S ne déplacera aucun système; car, soit Σ' un autre système quelconque, parmi les substitutions E il en existe une, S', qui remplace ρ par une racine ρ' du système Σ', et qui, par suite, remplace les racines de Σ par celles de Σ'; S remplaçant les racines de Σ les unes par les autres, $S'^{-1}SS'$ remplacera les racines de Σ' les unes par les autres; mais S' et S sont échangeables, donc $S'^{-1}SS' = S$ ne déplace pas le système Σ'.

Soit $\mathrm{S} = \begin{vmatrix} x & x+\alpha_0 \\ y & y+\alpha'_0 \end{vmatrix}$. Ses puissances $\begin{vmatrix} x & x+m\alpha_0 \\ y & y+m\alpha'_0 \end{vmatrix}$ ne dé-

placent évidemment pas les systèmes, et toute autre substitution de E les déplace ; car soit $T = \begin{vmatrix} x & x+\alpha_1 \\ y & y+\alpha'_1 \end{vmatrix}$ une substitution telle, qu'on n'ait pas à la fois $\alpha_1 \equiv m\alpha_0$ et $\alpha'_1 \equiv m\alpha'_0$: le déterminant $\alpha_0\alpha'_1 - \alpha'_0\alpha_1$ sera $\gtrless 0 \pmod p$; on pourra donc, quels que soient α et α', satisfaire à la fois aux deux congruences

$$m\alpha_0 + n\alpha_1 \equiv \alpha, \quad m\alpha'_0 + n\alpha'_1 \equiv \alpha'.$$

Donc les substitutions de la forme $S^m T^n = \begin{vmatrix} x & x+m\alpha_0+n\alpha_1 \\ y & y+m\alpha'_0+n\alpha'_1 \end{vmatrix}$ reproduisent toutes celles du groupe E.

Cela posé, s'il y avait un système que T ne déplaçât pas, T n'en déplacerait aucun d'après ce que nous venons de voir ; les substitutions $S^m T^n$ ou E ne déplaceraient pas ces systèmes, ce qui est absurde, car elles permutent transitivement toutes les racines.

On peut maintenant déterminer deux fonctions des racines

$$X = cx + dy \quad \text{et} \quad Y = d'x + c'y$$

telles, que S accroisse X d'une unité sans altérer Y, et que T accroisse Y d'une unité sans altérer X. En effet il suffira pour cela que c, d, d'une part, et d', c', d'autre part, satisfassent aux congruences suivantes :

$$\left.\begin{matrix} c\alpha_0 + d\alpha'_0 \equiv 1 \\ c\alpha_1 + d\alpha'_1 \equiv 0 \end{matrix}\right\} \pmod p, \qquad \left.\begin{matrix} d'\alpha_0 + c'\alpha'_0 \equiv 0 \\ d'\alpha_1 + c'\alpha'_1 \equiv 1 \end{matrix}\right\} \pmod p,$$

lesquelles comportent toujours un système de solutions, le déterminant $\alpha_0\alpha'_1 - \alpha'_0\alpha_1$ étant $\gtrless 0 \pmod p$.

Prenons X, Y pour indices indépendants à la place de x, y, les substitutions de L prendront la forme $\begin{vmatrix} X & a_1X + b_1Y \\ Y & b'_1X + a'_1Y \end{vmatrix}$. Or une substitution de cette forme transforme $S = \begin{vmatrix} X & X+1 \\ Y & Y \end{vmatrix}$ et $T = \begin{vmatrix} X & X \\ Y & Y+1 \end{vmatrix}$ en $S^{a_1}T^{b'_1}$ et $S^{b_1}T^{a'_1}$; d'autre part, les substitutions L remplaçant les

lettres de chaque système par celles d'un même système, et S ne déplaçant pas les systèmes, il est clair que ses transformées par les L ne les déplaceront pas; elles se réduiront donc à des puissances de S. Le coefficient b'_1 sera donc toujours nul, et chacune des substitutions de L multipliera Y par un facteur constant.

12. Or il est aisé de voir que parmi les trois types de groupes déterminés plus haut, il n'en existe aucun qui jouisse de la propriété signalée au lemme précédent.

Car considérons le premier type, par exemple. Son premier faisceau F est formé des substitutions $\begin{vmatrix} x & ax \\ y & by \end{vmatrix}$, et les seules fonctions des indices qu'elles multiplient par un facteur constant sont évidemment x et ses multiples, ou y et ses multiples; aucune de ces dernières n'est multipliée par un facteur constant dans la substitution $\begin{vmatrix} x & y \\ y & x \end{vmatrix}$.

Considérons maintenant le second type. Son premier faisceau contient une substitution qui ne peut être ramenée à la forme canonique que par l'introduction d'imaginaires; il n'existe donc aucune fonction réelle des indices que cette substitution multiplie par un facteur constant.

Les mêmes raisonnements s'appliquent au troisième type.

Il est donc prouvé que les trois types de groupes que nous avons obtenus sont primitifs; il reste à s'assurer s'ils sont généraux et distincts.

13. Théorème I. — *Tout groupe* H *du premier type est général si* $p > 5$.

En effet, si H n'était pas général, il serait contenu dans un autre groupe plus général, H_1, lequel serait réductible au second ou au troisième type. Il ne peut se réduire au second type, car son ordre serait égal à $2(p^2-1)p^2$; d'ailleurs il devrait être un multiple de celui de H, lequel est égal à $2(p-1)^2p^2$. Donc p^2-1 serait un multiple de $(p-1)^2$ ou $p+1$ un multiple de $p-1$, ce qui n'a pas lieu si $p > 3$.

D'autre part, H_1 ne peut se ramener au troisième type. En effet,

soit l une racine primitive du nombre p : H contient la substitution $\begin{vmatrix} x & lx \\ y & y \end{vmatrix}$, laquelle est d'ordre $p-1$, et laisse immobiles p racines, à savoir celles pour lesquelles $x=0$. Or le groupe H_1 du troisième type, dans lequel H devrait être contenu, ne renferme aucune semblable substitution. En effet, soit $\mathfrak{L}=(F, M_1, M_2, P, Q)$ le groupe de substitutions linéaires qui, combinées aux substitutions $\begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}$, reproduisent H_1 : l'une quelconque de ses substitutions, S, transforme, comme nous l'avons vu, M_1 et M_2 en substitutions de la forme $M_1^{\rho_1} M_2^{\rho'_2} \theta^{\mu'}$, $M_1^{\rho''_1} M_2^{\rho''_2} \theta^{\mu''}$, $\rho'_1, \rho'_2, \mu', \rho''_1, \rho''_2, \mu''$ étant égaux à 0 ou à 1 et satisfaisant à la relation $\rho'_1\rho''_2 - \rho''_1\rho'_2 \equiv 1 \pmod 2$, enfin θ étant la substitution qui multiplie les deux indices par -1. Il est aisé de voir que, de quelque manière que $\rho'_1, \rho'_2, \mu', \rho''_1, \rho''_2, \mu''$ soient choisis, l'une des quatre premières puissances de S sera échangeable à M_1 et à M_2. Car si, par exemple, S transforme M_1 et M_2 en $M_2\theta$ et M_1M_2, S^2 les transformera en $M_1M_2\theta$ et en $M_2\theta M_1M_2 = M_1M_2M_2 = M_1\theta$, et S^3 les transformera en $M_2\theta M_1M_2\theta = M_1$ et en $M_2\theta\theta = M_2$. Donc, r étant un entier au plus égal à 4, S^r sera échangeable à M_1 et à M_2, et par suite se réduira à la forme $\begin{vmatrix} x & ax \\ y & ay \end{vmatrix}$.

Cela posé, soit T la substitution d'ordre $p-1$ et laissant p racines immobiles que H_1 devrait contenir; elle est évidemment le produit d'une substitution linéaire S par une substitution E_1 appartenant à la forme générale E. Soit donc $T = SE_1$: on aura évidemment $T^r = S^r E_2$, E_2 étant encore une substitution de la forme E. Soit donc

$$T^r = \begin{vmatrix} x & ax+\alpha \\ y & ay+\alpha' \end{vmatrix};$$

cette substitution doit laisser d'ailleurs immobiles les p racines que T laissait immobiles; donc a se réduit à 1, et α, α' à zéro, car s'il en était autrement, les congruences $x \equiv ax+\alpha$ et $y \equiv ay+\alpha'$ ne comportant tout au plus qu'un système de solutions, T^r ne laisserait qu'une racine immobile.

Donc T^r se réduit à 1, et T est tout au plus d'ordre 4, nombre inférieur à $p-1$.

14. Théorème II. — *Les groupes du premier type ne sont pas généraux si* $p = 3$ ou 5.

En effet, si $p = 3$, la substitution $\begin{vmatrix} x & x+y \\ y & x-y \end{vmatrix}$ est permutable au groupe proposé H, et peut lui être adjointe de manière à former un groupe plus général.

Si $p = 5$, H est dérivé des substitutions

$$E = \begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}, \quad A = \begin{vmatrix} x & 2x \\ y & 2y \end{vmatrix}, \quad B = \begin{vmatrix} x & 2y \\ y & y \end{vmatrix} \quad \text{et} \quad C = \begin{vmatrix} x & y \\ y & x \end{vmatrix},$$

et l'on vérifie aisément que les substitutions

$$E,\ A,\ D = \begin{vmatrix} x & x \\ y & -y \end{vmatrix}, \quad C,\ G = \begin{vmatrix} x & x+y \\ y & 2y-2x \end{vmatrix}, \quad B,$$

forment l'échelle d'un nouveau groupe résoluble, qui sera évidemment plus général que H.

15. Théorème III. — *Tout groupe* H *du deuxième type est général si* $p > 3$.

En effet, s'il n'était pas général, il serait contenu dans un autre groupe plus général H_1, lequel serait réductible au premier ou au troisième type. Il ne peut se réduire au premier type, car son ordre $2(p-1)^2p^2$ devrait être un multiple de celui de H, $2(p^2-1)p^2$, ce qui est absurde. D'autre part, il ne peut se réduire au troisième type, car nous venons de voir que T étant une substitution quelconque d'un groupe du troisième type, et r un entier au plus égal à 4, T^r se réduit à la forme $\begin{vmatrix} x & ax+\alpha \\ y & ay+\alpha' \end{vmatrix}$, substitution dont la puissance $p-1$ se réduit évidemment à la forme $\begin{vmatrix} x & x+\beta \\ y & y+\beta' \end{vmatrix}$, et dont la puissance $(p-1)p$ se réduit à l'unité. Si donc H était contenu dans un groupe

du troisième type, chacune de ces substitutions élevée à la puissance $r(p-1)p$ se réduirait à l'unité (r désignant un des quatre nombres 1, 2, 3, 4).

Or, soit $\mathfrak{L}$ le groupe des substitutions linéaires qui concourent avec les E à la formation de H : ce groupe, étant rapporté aux indices imaginaires z et u, contient la substitution $\begin{vmatrix} z & mz \\ u & m^p u \end{vmatrix}$, où m est une racine primitive de la congruence $m^{p^2-1} \equiv 1 \pmod{p}$. L'ordre de cette substitution est égal à p^2-1, celles de ses puissances qui se réduisent à l'unité sont donc celles dont le degré est un multiple de p^2-1 ; donc p^2-1 devrait diviser $r(p-1)p$, et comme il est premier à p, il diviserait $r(p-1)$; donc $p+1$ diviserait r, ce qui est absurde si $p > 3$.

16. Théorème IV. — *Le groupe du deuxième type n'est pas général si* $p = 3$.

En effet, ses substitutions dérivent des suivantes :

$$\mathrm{E} = \begin{vmatrix} z & z+\beta \\ u & u+\beta^p \end{vmatrix}, \quad f = \begin{vmatrix} z & mz \\ u & m^p u \end{vmatrix}, \quad \text{et} \quad \mathrm{G} = \begin{vmatrix} z & u \\ u & z \end{vmatrix},$$

m étant une racine primitive de la congruence

$$m^{8-1} \equiv 1 \pmod{p}.$$

Or on vérifie aisément que les substitutions

$$\mathrm{E}, \quad f^2, \quad \mathrm{G}f, \quad \mathrm{U} = \begin{vmatrix} z & mz+u \\ u & z+m^p u \end{vmatrix}, \quad f$$

forment l'échelle d'un groupe résoluble plus général que le proposé.

17. Théorème V. — *Tout groupe* H *du troisième type est général.*

En effet, s'il était contenu dans un autre groupe H_1 réductible au premier ou au second type, les propriétés générales des substitutions de H_1 s'appliqueraient en particulier à celles de H. Or nous allons voir qu'il n'en est pas ainsi.

Supposons H_1 appartenant au premier type. Ses substitutions sont toutes de l'une des formes

$$\begin{vmatrix} x & ax+\alpha \\ y & by+\alpha' \end{vmatrix} \quad \text{ou} \quad \begin{vmatrix} x & ay+\alpha \\ y & bx+\alpha' \end{vmatrix},$$

et il est clair que le carré de l'une quelconque d'entre elles appartiendra à la première de ces deux formes.

Soient donc S et T deux substitutions quelconques de H_1,

$$S^2 = \begin{vmatrix} x & ax+\alpha \\ y & by+\alpha' \end{vmatrix} \quad \text{et} \quad T^2 = \begin{vmatrix} x & a_1x+\alpha_1 \\ y & b_1y+\alpha'_1 \end{vmatrix}$$

leurs carrés : il est clair que la substitution $S^{-2}T^{-2}S^2T^2$ se réduit à la forme $\begin{vmatrix} x & x+\beta \\ y & y+\beta' \end{vmatrix}$, et que son ordre sera égal à p, si l'on n'a pas $\beta = \beta' = 0$, et qu'il se réduit à 1 dans le cas contraire.

Si H_1 appartient au second type, ses substitutions jouiront de la même propriété, car en rapportant ce groupe aux indices imaginaires conjugués z et u, les substitutions $\begin{vmatrix} x & x+\alpha \\ y & y+\alpha' \end{vmatrix}$ prendront la forme $\begin{vmatrix} z & z+\gamma \\ u & u+\gamma^p \end{vmatrix}$, γ et γ^p étant des constantes imaginaires conjuguées, et les substitutions de H_1 seront de l'une des deux formes

$$\begin{vmatrix} z & mz+\gamma \\ u & m^pu+\gamma^p \end{vmatrix} \quad \text{ou} \quad \begin{vmatrix} z & nu+\gamma \\ u & n^pz+\gamma^p \end{vmatrix}.$$

Leurs carrés S^2, T^2,... seront tous de la première forme, et les substitutions telles que $S^{-2}T^{-2}S^2T^2$ seront de la forme $\begin{vmatrix} z & z+\gamma \\ u & u+\gamma^p \end{vmatrix}$; leur ordre sera donc égal à p ou à 1.

Or H contient les deux substitutions P et PM_1, qui étant prises pour

S et T, ne jouissent pas de la propriété ci-dessus assignée. On a en effet

$$\begin{aligned} P^{-2}(PM_1)^{-2}P^2(PM_1)^2 &= P^{-2}.M_1^{-1}P_1^{-1}M_1^{-1}P^{-1}.P^2.PM_1PM_1 \\ &= P^{-2}M_1^{-1}P^2.P^{-3}M_1^{-1}P^3.P^{-1}M_1P.M_1 \\ &= (M_1M_2)^{-1}(M_2M_1M_2)^{-1}M_2M_1 \\ &= M_2^{-1}M_1^{-1}M_2^{-1}M_1^{-1}M_2^{-1}M_2M_1 = M_1^{-1}\theta, \end{aligned}$$

substitution dont l'ordre est égal à 4.