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

CAMILLE JORDAN

# Recherches sur les substitutions

*Journal de mathématiques pures et appliquées 2^e série*, tome 17 (1872), p. 351-367.
<http://www.numdam.org/item?id=JMPA_1872_2_17__351_0>

# RECHERCHES SUR LES SUBSTITUTIONS;

PAR M. CAMILLE JORDAN,
Ingénieur des Mines, à Paris.

On sait qu'il existe un groupe de 6 lettres trois fois transitif et d'ordre $6.5.4$.

M. Émile Mathieu, généralisant ce résultat, a montré que, si $m$ est un nombre quelconque, premier ou puissance d'un nombre premier, il existera au moins un groupe trois fois transitif de degré $m+1$ et d'ordre $(m+1)\,m(m-1)$. Il a signalé également l'existence d'un groupe de 12 lettres, 5 fois transitif et d'ordre $12.11.10.9.8$.

Ces résultats donnent quelque intérêt à la question suivante :

*Déterminer à quelles conditions doivent satisfaire les deux entiers $m$ et $k$ pour qu'il existe des groupes $k+2$ fois transitifs, de degré $m+k$ et d'ordre $(m+k)\,(m+k-1)\ldots m(m-1)$.*

Nous établirons dans ce Mémoire les deux propositions que voici :

1° *Le nombre $m$ doit être premier ou puissance d'un nombre premier;*

2° *Le nombre $k$ ne peut surpasser l'unité.*

Les seuls groupes qui fassent exception à cette dernière règle sont les groupes symétriques ou alternés et les groupes de 11 et 12 lettres de M. Mathieu. Ce dernier groupe n'est donc pas, comme le groupe trois fois transitif de 6 lettres, le premier anneau d'une série. Il reste unique de son espèce.

Nous déduirons encore de cette recherche le théorème suivant :

*Soit $p$ un nombre premier $> 3$. Il existera trois groupes primitifs de la classe $p$ [*] si $p+1$ est une puissance de 2, un seul dans le cas contraire.*

[*] Nous disons qu'un groupe est de la classe $p$ lorsque celle de ses substitutions qui déplace le moins de lettres en déplace $p$.

## § I. — *Théorèmes généraux.*

**1.** THÉORÈME I. — *Un groupe transitif* G *entre m lettres a, b, c, ... contient nécessairement des substitutions qui déplacent toutes les lettres.*

Soient respectivement $H_a, H_b, H_c, \ldots$ les groupes formés par celles des substitutions de G qui ne déplacent pas les lettres $a, b, c, \ldots$. Ces groupes seront transformés les uns dans les autres par les substitutions de G. Soit, en effet, S une de ces substitutions, qui fasse succéder, par exemple, $b$ à $c$. Le groupe transformé de $H_c$ par S sera contenu dans G, et comme ses substitutions ne déplacent pas $b$, il sera contenu dans $H_b$. Donc $H_b$ contiendra au moins autant de substitutions que $H_c$. Mais, réciproquement, le groupe transformé de $H_b$ par $S^{-1}$ sera contenu dans $H_c$. Donc $H_c$ ne peut contenir moins de substitutions que $H_b$. Donc $H_c$ et $H_b$ contiennent le même nombre de substitutions, et $H_b$ sera le transformé de $H_c$ par S.

D'ailleurs G, étant transitif, contient une substitution au moins qui remplace $a$ par l'une quelconque $b$ des autres lettres $b, c, \ldots$. Cette substitution transformera, comme on vient de le voir, $H_a$ en $H_b$. Donc tous les groupes $H_a, H_b, H_c, \ldots$ seront les transformés de l'un quelconque d'entre eux, $H_a$, par les diverses substitutions de G.

Cela posé, désignons par $N_x$ le nombre de celles des substitutions de $H_a$ qui déplacent précisément $x$ lettres. On aura, en désignant par N le nombre total des substitutions de ce groupe,

$$N = N_{m-1} + N_{m-2} + \ldots + N_x + \ldots + N_0.$$

On peut remarquer d'ailleurs que l'on aura $N_0 = 1$, car $H_a$ contient une seule substitution qui ne déplace aucune lettre (à savoir l'unité) et $N_1 = 0$, aucune substitution ne pouvant déplacer qu'une seule lettre.

Chacun des $m$ groupes $H_a, H_b, H_c, \ldots$ transformés de $H_a$ contiendra évidemment N substitutions, parmi lesquelles $N_x$ ne déplaçant que $x$ lettres. Ces groupes contiendraient donc ensemble $mN_x$ substitu-

tions déplaçant $x$ lettres; mais ces substitutions ne sont pas toutes distinctes.

Soit, en effet, T l'une d'elles; elle laissera immobiles $m - x$ lettres, telles que $a, b, \ldots$; donc elle appartiendra aux $m - x$ groupes $H_a$, $H_b, \ldots$. Donc le nombre des substitutions distinctes contenues dans les groupes $H_a$, $H_b$, $H_c, \ldots$ et déplaçant $x$ lettres sera $\frac{m}{m-x} N_x$, et le nombre total des substitutions distinctes contenues dans ces groupes sera

$$X = mN_{m-1} + \frac{m}{2} N_{m-2} + \cdots + \frac{m}{m-x} N_x + \cdots + \frac{m}{m} N_0.$$

Cela posé, le groupe G contient $mN$ substitutions (*Voir* notre *Traité des substitutions*, n° 44). Celles de ces substitutions qui déplacent moins de $m$ lettres appartiendront évidemment à l'un des groupes $H_a$, $H_b$, $H_c, \ldots$ et seront en nombre X. Il restera donc

$$Y = mN - X = m\left(\frac{1}{2} N_{m-2} + \cdots + \frac{m-x-1}{m-x} N_x + \cdots + \frac{m-1}{m} N_0\right),$$

substitutions déplaçant toutes les lettres.

Le nombre $N_0$ étant égal à l'unité, Y ne pourra s'annuler, et l'on obtiendra sa valeur minimum $m - 1$ en supposant

$$N_{m-2} = N_{m-3} = \ldots = N_1 = 0.$$

2. Théorème II. — *Il ne peut exister de groupe* G *deux fois transitif de degré* $m$ *et d'ordre* $m(m-1)$ *que si* $m$ *est une puissance d'un nombre premier, telle que* $p^n$.

*Le groupe cherché* G *sera contenu dans le groupe linéaire.*

Admettons que le groupe G existe, et suivons les conséquences de cette hypothèse. Le groupe $H_a$, formé par celles des substitutions de G qui laissent immobile une lettre donnée $a$, sera simplement transitif par rapport aux $m - 1$ lettres restantes, et aura pour ordre $m - 1$. Mais son ordre est égal à $(m-1)\Omega$, $\Omega$ étant l'ordre du groupe I formé par celles de ses substitutions qui laissent immobile une seconde lettre $b$; donc $\Omega$ se réduit à 1, et I ne contiendra d'autre substitution que l'unité.

Donc toutes les substitutions de $H_a$, sauf l'unité, déplaceront $m-1$ lettres; donc les quantités $N_{m-2}, \ldots, N_1$, définies comme au numéro précédent, seront nulles, et *le nombre* Y *des substitutions de* G *qui déplacent m lettres sera égal à* $m-1$.

3. *Parmi ces* $m-1$ *substitutions* S, S', ..., *il en existe une seule qui remplace une lettre donnée a par une autre lettre donnée b.*

En premier lieu, il en existe une. Soient, en effet, $\alpha$ une lettre quelconque, $\beta$ celle que S lui fait succéder. Le groupe G, étant deux fois transitif, contiendra une substitution T qui remplace $\alpha$ et $\beta$ par $a$ et $b$; il contiendra la transformée $T^{-1}ST$, laquelle remplace $a$ par $b$; d'ailleurs elle déplace évidemment toutes les lettres, et par suite fera partie du système S, S', ....

En second lieu, il n'en existe qu'une. Supposons en effet qu'on eût deux substitutions distinctes S, S' remplaçant $a$ par $b$. Soit $\beta$ l'une quelconque des $m-1$ lettres $b, c, \ldots$. Le groupe G contiendra une substitution U remplaçant $a, b$ par $a, \beta$. Les transformées de S et de S' par U seront deux substitutions distinctes, appartenant à la suite S, S', ... et remplaçant $a$ par $\beta$. Prenant successivement pour $\beta$ chacune des $m-1$ lettres $b, c, \ldots$, on obtiendrait ainsi $2(m-1)$ substitutions distinctes contenues dans la suite S, S', ..., résultat absurde, cette suite ne contenant que $m-1$ substitutions.

4. *Chacun des cycles de chacune des substitutions* S, S', ... *contient le même nombre p de lettres.* Supposons en effet que S contînt un cycle $(\alpha\beta\ldots)$ de $p$ lettres, et que S', par exemple, en contînt un de $q$ lettres $(\gamma\delta\ldots)$. Le groupe G contient une substitution T qui remplace $\alpha, \beta$ par $a, b$, et une substitution V qui remplace $\gamma, \delta$ par $a, b$. Les deux substitutions $T^{-1}ST$, $V^{-1}S'T$ appartiendront à la suite S, S', ... et remplaceront $a$ par $b$. Elles devront donc se confondre, résultat absurde, car $a$ et $b$ font partie d'un cycle de $p$ lettres dans $T^{-1}ST$, et d'un cycle de $q$ lettres dans $V^{-1}S'V$.

5. *Le nombre p est premier.* En effet, soit $p = \lambda\mu$. Chaque cycle de S contenant $p$ lettres, la substitution $S^\mu$ déplacera encore toutes les lettres et en contiendra $\lambda$ dans chacun de ses cycles. Donc $S^\mu$ ferait

partie de la suite S, S', ..., résultat absurde, ses cycles contenant moins de $p$ lettres.

**6.** *Les substitutions* S, S', ... *jointes à la substitution* 1 *forment un groupe* F. Soient, en effet, S et S' deux d'entre elles. Leur produit SS' appartiendra à la suite 1, S, S', .... En effet, SS' appartient à G; si elle déplace toutes les lettres, elle fera donc partie de la suite S, S'.... Supposons, au contraire, qu'elle laisse immobile une lettre $a$; les deux substitutions S et $S'^{-1}$ remplaceront $a$ par une même lettre. D'ailleurs chacune d'elles déplace toutes les lettres : donc elles seront identiques (**3**), et le produit SS' se réduira à l'unité.

**7.** *Les substitutions de* G *sont permutables à* F. Car, d'une part, elles transforment S, S', ... en substitutions contenues dans G et qui déplacent toutes les lettres, et qui, par suite, se confondent à l'ordre près avec S, S', ...; et, d'autre part, elles transforment la substitution 1 en elle-même.

**8.** *Le nombre m est une puissance de p.* En effet, l'ordre du groupe F est égal à $m$; mais, en vertu d'un théorème de Cauchy (*Traité des substitutions*, n° **40**), si cet ordre était divisible par un nombre premier $q$ autre que $p$, F contiendrait une substitution d'ordre $q$, ce qui n'est pas. Donc $m$ se réduit à une puissance de $p$, telle que $p^n$.

**9.** *L'une au moins des substitutions* S, S', ... *est échangeable à toutes les substitutions de* F. En effet, l'une quelconque des substitutions de F transformera S, S', ... en substitutions qui appartiennent à F et déplacent toutes les lettres, et qui, par suite, se confondront à l'ordre près avec celles de la suite S, S', ....

Cela posé, transformons successivement S, S', ... par les diverses substitutions de F. Les déplacements opérés sur les $p^n - 1$ termes de cette suite par ces diverses transformations formeront un groupe Γ isomorphe à F; l'ordre de ce groupe sera donc un diviseur de l'ordre de F (*Traité des substitutions*, n° **67**); ce sera donc une puissance de $p$.

Groupons maintenant les $p^n - 1$ termes de la suite S, S', ... en

classes, en réunissant ensemble celles que les substitutions de Γ permutent les unes dans les autres, et soient $r, r', \ldots$ les nombres de termes contenus dans chaque classe. Chacun des nombres $r, r', \ldots$ sera un diviseur de $m$ (*Traité des substitutions*, n° 44), c'est-à-dire une puissance de $p$. On a d'ailleurs

$$r + r' + \ldots = p^n - 1.$$

Donc $r, r', \ldots$ ne peuvent être tous divisibles par $p$; donc quelques-uns de ces nombres devront se réduire à l'unité. Donc quelques-uns des termes de la suite S, S', ... ne seront déplacés par aucune des substitutions de Γ, ou, ce qui revient au même, ne seront pas altérés lorsqu'on les transforme par les substitutions de F.

**10.** *Toutes les substitutions de* F *sont échangeables entre elles.* Nous venons, en effet, de montrer que F contient des substitutions différentes de l'unité et échangeables à toutes les autres. Ces substitutions formeront évidemment un groupe E.

Cela posé, chacune des substitutions de G, étant permutable à F, transformera E en un groupe de substitutions contenues dans F et échangeables aux substitutions de F; ce groupe transformé ne sera donc autre que E. Or le groupe G est deux fois transitif, et *a fortiori* primitif. Donc le groupe E, permutable à ses substitutions, sera transitif (*Traité des substitutions*, n° 53); donc son ordre sera un multiple du nombre $p^n$ des lettres qu'il déplace. Donc E contient les $p^n$ substitutions de F, et se confond avec lui.

**11.** *On pourra caractériser les lettres par n indices* $x, y, z, \ldots$, *variables de zéro à* $p-1$, *et choisis de telle sorte que les substitutions de* F *prennent la forme*

$$| \; x, \; y, \; z, \ldots, \; x+\alpha, \; y+\beta, \; z+\gamma, \ldots \; |$$

(*Traité des substitutions*, n° 408). Quant au groupe G, on l'obtiendra évidemment en joignant aux substitutions ci-dessus celles des substitutions de G qui laissent immobile l'une des racines, par exemple celle dont les indices sont tous nuls. Ces dernières substitutions formeront

un groupe H, transitif par rapport aux $m-1$ lettres restantes, et d'ordre $m-1$. Elles sont d'ailleurs permutables à F; elles seront donc de la forme linéaire

$$| x, y, \ldots, ax+by+\ldots, a'x+b'y+\ldots, \ldots | .$$

Notre théorème est donc complétement démontré.

**12.** On voit, par ce qui précède, que la recherche du groupe G revient à celle d'un groupe H, simplement transitif, d'ordre et de degré $p^n-1$, et formé de substitutions linéaires sans termes constants. A chaque manière de déterminer le groupe H correspondra un groupe différent pour G; mais on ne devra considérer comme formes distinctes du groupe H que celles qui ne sont pas susceptibles d'être ramenées l'une à l'autre par un changement d'indices indépendants.

Supposons, en effet, que nous ayons trouvé deux groupes H et H' tels, que les substitutions de H, rapportées aux indices $x, y, z, \ldots$, aient la même forme que les substitutions de H', rapportées à de nouveaux indices $x', y', z', \ldots$, fonctions linéaires des précédents. Les substitutions de F, accroissant $x, y, z, \ldots$ de termes constants, accroîtront également $x', y', z', \ldots$ de termes constants. Ce groupe conservera donc la même forme, qu'il soit rapporté aux indices $x, y, z, \ldots$ ou aux indices $x', y', z', \ldots$. Donc le groupe $(H, F) = G$, rapporté aux indices $x, y, z, \ldots$, et le groupe $(H', F) = G'$, rapporté aux indices $x', y', z', \ldots$, auront la même forme. Ces deux groupes ne diffèrent donc que par la notation, et ne sont pas essentiellement distincts.

**13.** Théorème III. — *Pour qu'il existe un groupe* K $k+2$ *fois transitif de degré* $m+k$ *et d'ordre* $(m+k)(m+k-1)\ldots(m-1)$, *il faut :* 1° *que m soit une puissance de nombre premier;* 2° *que k ne surpasse pas l'unité.*

Ce théorème souffre les exceptions suivantes :

1° Si $m<5$, $k$ pourra être quelconque, et K sera symétrique ou alterné;

2° Si $m=9$, on pourra poser $k=2$ ou 3, et l'on obtiendra pour

K le groupe 4 fois transitif de 11 lettres et le groupe 5 fois transitif de 12 lettres signalés par M. Émile Mathieu.

*Démonstration.* — Supposons que le groupe K existe. Le groupe partiel G, formé par celles de ses substitutions qui laissent immobiles $k$ lettres choisies à volonté, sera deux fois transitif par rapport aux $m$ lettres restantes, et aura pour ordre $m(m-1)$. Cela ne sera possible que si $m$ est une puissance de nombre premier (théorème II). Soit donc $m = p^n$.

Cela posé, admettons que $k$ soit $> 1$. Le groupe G, ayant pour ordre $m(m-1)$, qui est un multiple de 2, contiendra une substitution S d'ordre 2 (théorème de Cauchy). D'ailleurs chaque substitution de G déplace $m$ ou $m-1$ lettres. Donc la substitution S déplacera $m-1$ lettres si $p$ est impair, $m$ lettres si $p$ se réduit à 2.

**14.** *Premier cas.* — Supposons d'abord que $p$ soit impair : S laissera immobile une lettre $a$ parmi celles que déplacent les substitutions de G, et permutera les autres, $b, c, d, e, \ldots$, deux à deux. Soit donc

$$S = (bc)(de)\ldots.$$

Soient maintenant $\alpha, \beta, \gamma, \ldots$ les $k$ lettres du groupe K qui ne figurent pas dans les substitutions de G; le groupe K, étant $k+2$ fois transitif, contiendra une substitution T qui remplace les $k+1$ lettres $a, b, c, \gamma, \ldots$ respectivement par $a, \alpha, \beta, \gamma, \ldots$. Soient $d', e', \ldots$ les lettres par lesquelles T remplace $d, e, \ldots$, lesquelles lettres appartiendront à la suite $b, c, d, e, \ldots$; le groupe K contiendra la substitution

$$U = T^{-1}ST = (\alpha\beta)(d'e')\ldots.$$

Cela posé, le groupe transformé de G par U est contenu dans K; d'autre part, il est clair qu'il ne déplace aucune lettre autre que $a, b, c, d, e, \ldots$ (car U permute ces lettres exclusivement ensemble); donc il se confond avec G, et la substitution U, ou, ce qui revient au même, la substitution

$$V = (d'e')\ldots$$

sera permutable à G. Elle le sera donc au groupe F formé par celles des substitutions de G qui déplacent toutes les lettres $a, b, c, d, e, \ldots$.

Mais on peut caractériser ces lettres par $n$ indices, variables de zéro à $p-1$, et choisis de telle sorte que les substitutions de F prennent la forme

$$| x, y, \ldots, \quad x+\alpha, \quad y+\beta, \ldots |,$$

et que la lettre $a$ ait tous ses indices nuls (**11**).

Cela posé, la substitution V, étant permutable à F et ne déplaçant pas $a$, sera de la forme linéaire sans termes constants

$$| x, \; y, \ldots, \quad ax+by+\ldots, \quad a'x+b'y+\ldots, \; \ldots |.$$

Le nombre des lettres de la suite $a, b, c, \ldots$ qu'elle laisse immobiles est une puissance de $p$. En effet, pour que V ne déplace pas la lettre $x, y, \ldots$, il faudra que l'on ait

$$x = ax+by+\ldots, \quad y = a'x+b'y+\ldots, \; \ldots,$$

et si, parmi ces équations, il en est $n-\mu$ distinctes, elles détermineront $n-\mu$ indices en fonction des autres, qui resteront arbitraires, et seront chacun susceptibles de $p$ valeurs. On aura donc $p^{\mu}$ lettres non déplacées.

Mais S, et par suite, sa transformée U déplacent $m-1$ lettres; donc V en déplace $m-3$ et laisse 3 lettres immobiles, résultat incompatible avec le précédent, à moins que l'on n'ait $p=3$.

**15.** Discutons ce dernier cas. Supposons les indices indépendants choisis de manière à ramener S à sa forme canonique. Cette substitution, étant d'ordre 2, multipliera chaque indice par $\pm 1$; mais il est clair qu'une substitution de cette forme laisse immobiles $3^{\mu}$ lettres, $\mu$ étant le nombre des indices qu'elle n'altère pas. Donc S, ne laissant qu'une lettre immobile, sera de la forme

$$S = | x, \; y, \; z, \ldots \quad -x, \quad -y, \quad -z, \ldots | \text{ mod. } 3,$$

et cette forme ne sera altérée par aucun changement d'indices indépendants, car il est clair que S multipliera par $-1$ une fonction linéaire quelconque des indices $x, y, z$.

Profitons de cette indétermination dans le choix des indices pour

ramener V à sa forme canonique. Cette substitution, étant d'ordre 2, multipliera chaque indice par $\pm 1$. D'ailleurs elle ne laisse que 3 lettres immobiles; donc elle altérera tous ces indices, à l'exception d'un seul. On aura donc

$$V = | x, y, z, \ldots, x, -y, -z, \ldots | \text{ mod. } 3,$$

d'où

$$VS = | x, y, z, \ldots, -x, y, z, \ldots | \text{ mod. } 3.$$

Cette dernière substitution laissera $3^{n-1}$ lettres immobiles et en déplacera $m - 3^{n-1}$. La substitution US, déplaçant en outre les deux lettres $\alpha$, $\beta$, en déplacera en tout $m - 3^{n-1} + 2$. Mais elle appartient à K, dont toutes les substitutions déplacent au moins $m - 1$ lettres. On aura donc $n = 1$ ou 2, d'où $m = 3$ ou 9.

Sauf ces deux cas exceptionnels, le groupe K ne peut donc exister.

**16.** *Deuxième cas.* — Soit maintenant $p = 2$ : S déplacera les $m$ lettres $a, b, c, d, \ldots$. Soit

$$S = (ab)(cd)\ldots$$

et soient, comme précédemment, $\alpha, \beta, \gamma, \ldots$ les lettres de K qui ne figurent pas dans les substitutions de G. Le groupe K, étant $k+2$ fois transitif, contiendra une substitution T qui remplace $a, b, \alpha, \beta, \gamma, \ldots$ par $\alpha, \beta, a, b, \gamma, \ldots$. Soient $c', d', \ldots$ les lettres que T fait succéder à $c, d, \ldots$, lesquelles lettres se confondront à l'ordre près avec $c, d, \ldots$. Le groupe K contiendra la substitution

$$U = T^{-1}ST = (\alpha\beta)(c'd')\ldots,$$

laquelle sera permutable à G. La substitution partielle

$$V = (c'd')\ldots$$

le sera également, et l'on pourra, comme tout à l'heure, la mettre sous la forme linéaire

$$| x, y, \ldots, ax + by + \ldots, a'x + b'y + \ldots, \ldots | \text{ mod. } 2.$$

D'ailleurs cette substitution déplace $m-2$ lettres et son ordre est égal à 2.

Remplaçons les indices $x, y, \ldots$ par d'autres indices indépendants, X, Y, X′, Y′,..., Z,..., choisis de telle sorte que V soit ramené à sa forme canonique. Pour que l'ordre de V se réduise à 2, il faut que cette forme canonique soit la suivante (*Traité des substitutions*, n° **159**) :

$$\left|\begin{array}{ll} \mathrm{X},\ \mathrm{Y}, & \mathrm{X},\ \mathrm{Y}+\mathrm{X} \\ \mathrm{X}',\ \mathrm{Y}', & \mathrm{X}',\ \mathrm{Y}'+\mathrm{X}' \\ \ldots\ldots, & \ldots\ldots\ldots \\ \mathrm{Z} & \mathrm{Z} \\ \ldots\ldots & \ldots\ldots\ldots \end{array}\right| .$$

Soit $\rho$ le nombre des indices X, X′,..., lequel est au plus la moitié du nombre total $n$; les $2^{n-\rho}$ lettres pour lesquelles $\mathrm{X}=\mathrm{X}'=\ldots=0$ ne seront pas déplacées par V. Donc V ne déplace que $m-2^{n-\rho}$ lettres; mais en doit déplacer $m-2$; donc $n-\rho=1$ et $n \leqq 2(n-\rho) \leqq 2$, d'où $m \leqq 2^2$.

Donc, ici encore, le groupe K ne peut exister, sauf les cas d'exception signalés dans l'énoncé du théorème.

**17.** L'examen de ces cas d'exception n'offre aucune difficulté. Si $m<5$, K sera symétrique ou alterné, et son degré pourra être quelconque. Si $m=9$, on opérera comme il suit :

En premier lieu, on cherchera à construire le groupe G, déplaçant 9 lettres, par rapport auxquelles il est deux fois transitif. Ce groupe s'obtiendra (théorème II) en joignant au groupe E, formé des substitutions

$$| x, y, \quad x+\alpha, \quad y+\beta | \text{ mod. } 3,$$

un groupe H, dont les substitutions soient de la forme

$$| x, y, \quad ax+by, \quad a'x+b'y | \text{ mod. } 3,$$

et qui soit d'ordre 8 et simplement transitif par rapport aux 8 lettres qu'il déplace.

Nous avons vu (**15**) que la seule substitution d'ordre 2 que H puisse contenir est la suivante :

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

Donc H contiendra au moins une substitution d'ordre 4 ou 8.

1° Si H contient une substitution T d'ordre 8, il sera exclusivement formé de ses puissances; d'ailleurs cette substitution aura pour forme canonique

$$| z, z_1, \quad iz, i^3 z_1 |,$$

$i$ étant une racine primitive de la congruence

$$i^{3^3} \equiv 1 \bmod. 3,$$

et $z$, $z_1$ deux indices imaginaires conjugués de la forme $X + iY$, $X + i^p Y$, X et Y étant des fonctions linéaires des indices $x$ et $y$; et l'on peut admettre, sans restreindre la généralité de la solution, que X et Y se réduisent respectivement à $x$ et $y$ (**12**).

2° Si H ne contient aucune substitution d'ordre 8, il contiendra une substitution T d'ordre 4, que l'on pourra mettre sous la forme canonique

$$T = | z, z_1, \quad i^2 z, i^6 z_1 |.$$

D'ailleurs il ne contient d'autre substitution d'ordre 2 que la substitution $S = T^2$. Donc il devra contenir une autre substitution U d'ordre 4 et différente des puissances de T. Il contiendra alors les 8 substitutions des formes $T^p$ et $T^p U$, lesquelles sont évidemment distinctes. Il contient d'ailleurs $U^{-1}TU$. Cette substitution ne peut être de la forme $T^p U$, car de l'égalité $U^{-1}TU = T^p U$ on déduirait $U = T^{1-p}$, ce qui est inadmissible. Donc $U^{-1}TU$ sera une puissance de T.

Or il est aisé de voir que les substitutions d'ordre 4 qui transforment T en ses puissances dérivent toutes de la combinaison de la substitution

$$V = | z, z_1, \quad iz_1, i^3 z |$$

avec les puissances de T. Donc H sera dérivé des deux substitutions T et V.

On a donc, en résumé, deux manières distinctes de déterminer le groupe H. Soient $H_1$, $H_2$ ces deux groupes, $G_1 = (E, H_1)$, $G_2 = (E, H_2)$ les deux formes correspondantes du groupe G.

Cela fait, on essayera de s'élever progressivement de chacun des groupes $G_1$, $G_2$ à des groupes 3 fois, 4 fois,... transitifs par l'adjonction de substitutions contenant 1, 2,... lettres nouvelles, ainsi que nous l'avons indiqué ailleurs (*Traité des substitutions*, n° 45). Opérant ainsi, on verra sans difficulté :

1° Que le groupe $G_1$ donne naissance à un groupe 3 fois transitif, après lequel on est obligé de s'arrêter;

2° Que le groupe $G_2$ donne naissance successivement à un groupe 3 fois transitif, à un groupe 4 fois transitif, et enfin à un groupe 5 fois transitif.

Ces deux derniers groupes sont les groupes 4 et 5 fois transitifs de 11 et 12 lettres, découverts par M. Mathieu. Notre analyse montre que ces groupes sont tout à fait exceptionnels, du moins au point de vue où nous nous sommes placés; car il pourrait se faire qu'à d'autres égards ils pussent se rattacher à certaines familles de groupes encore inconnues.

## § II. — *Recherche des groupes primitifs appartenant à la classe q, q étant un nombre premier* $> 3$.

**18.** Tout groupe primitif K de la classe $q$ contiendra par définition une substitution S qui ne déplace que $q$ lettres. Si ces $q$ lettres formaient plusieurs cycles, ils ne pourraient pas contenir tous le même nombre de lettres ($q$ étant premier) : donc en élevant S à une puissance convenable, on obtiendrait une nouvelle substitution contenue dans H et laissant immobiles les lettres de l'un de ces cycles; cette nouvelle substitution déplaçant moins de $q$ lettres, G ne serait pas de la classe $q$, comme on le suppose.

Donc S est une substitution circulaire entre $q$ lettres, et si K a pour degré $n$, il sera $n - p + 1$ fois transitif (*Traité des substitutions*, note C). Les groupes $G_{n-q}$, $G_{n-q+1}$, ..., $G_1$ de degrés $n - 1$, $n - 2$, ..., $q$, respectivement formés par celles des substitutions de K qui lais-

sent immobiles $1, 2, \ldots, n-q$ lettres, seront respectivement $n-q$, $n-q-1, \ldots, 1$ fois transitifs par rapport aux lettres qu'ils déplacent. Ils seront évidemment primitifs; car $G_{n-q}, \ldots, G_2$ sont plusieurs fois transitifs; quant à $G_1$, son degré étant premier, ses lettres ne peuvent se partager en systèmes (qui devraient être également nombreux). En outre, il est clair que chacun des groupes $G_1, G_2, \ldots, G_{n-q}$ appartiendra à la classe $q$.

Pour arriver à construire tous ces groupes primitifs cherchés, tels que K, on pourra donc opérer progressivement, en cherchant à construire les groupes $G_1$, puis les groupes deux fois transitifs, tels que $G_2$, etc.

**19.** Le groupe $G_1$ peut se construire dans tous les cas et d'une seule manière. En effet, il doit contenir S et ses puissances; mais il ne contient aucune autre substitution; car supposons qu'il en contînt une A remplaçant la lettre $a$ par une autre lettre $b$. L'une des puissances de S, telle que $S^\alpha$, remplacerait $b$ par $a$, et $G_1$ contiendrait la substitution $S^\alpha A$, qui déplacerait moins de $q$ lettres, sans se réduire à l'unité, ce qui est absurde.

Si nous caractérisons les lettres de $G_1$ par un indice $x$ variable de zéro à $q-1$ mod. $q$, les puissances de S, dont $G_1$ est dérivé, auront la forme suivante :

$$| \, x, \quad x+\alpha \, | \text{ mod. } q.$$

**20.** Cherchons maintenant à construire un groupe deux fois transitif $G_2$. Ce groupe, ayant pour ordre $q(q+1)$, ne pourra exister que si $q+1$ est une puissance de nombre premier (théorème II). Or $q+1$ est pair; donc il devra être une puissance de 2. Soit $q+1=2^n$, le groupe $G_2$ résultera de la combinaison des substitutions

$$| \, x, y, \ldots, \quad x+\alpha, \quad y+\beta, \ldots \, | \text{ mod. } 2$$

avec un groupe $G_1 = H$, d'ordre $q$ et formé de substitutions linéaires (**11**).

Le groupe H, ayant pour ordre un nombre premier $q$, sera formé des puissances d'une seule substitution S, d'ordre $q=2^n-1$. Cette

substitution, ramenée à la forme canonique, sera nécessairement de la forme

$$S = | z, z_1, z_2, \ldots, \quad iz, i^2 z_1, i^4 z_2, \ldots |,$$

$i$ étant une racine primitive de la congruence $i^q \equiv 1 \bmod 2$, $z$ un indice imaginaire de la forme $X + iY + i^2 Z + \ldots$, et $z_1, z_2, \ldots$ ses conjugués obtenus en changeant $i$ en $i^2$, $i^4, \ldots$; X, Y, Z, ... étant d'ailleurs des fonctions linéaires de $x, y, z, \ldots$ qu'on peut, sans nuire à la généralité de la solution, supposer se confondre respectivement avec $x, y, z, \ldots$ (**12**).

Le groupe $G_2$ pourra donc toujours se construire, et d'une seule manière.

**21.** Passons à la détermination du groupe suivant $G_3$. Désignons maintenant par $a_0, a_1, \ldots, a_{q-1}$ les lettres de $G_1$, et soient

$$S = (a_0, a_1, a_2, \ldots)$$

la substitution circulaire dont les puissances forment ce groupe, $u$ la lettre nouvelle que déplace le groupe $G_2$, $v$ la lettre nouvelle que $G_2$ ne déplaçait pas, mais que $G_3$ déplace. Le groupe $G_3$, contenant $G_2$, renfermera une substitution $T_1$ d'ordre 2 déplaçant $q+1$ lettres, et par suite laissant une lettre immobile; soient $\alpha$ cette lettre, $\xi$, $\gamma$ deux autres lettres formant un cycle dans $T_1$. Le groupe $G_3$, étant 3 fois transitif, contiendra une substitution U qui remplace $\alpha, \xi, \gamma$ par $a_0, u, v$; il contiendra la substitution $U^{-1} T_1 U = \Theta$, laquelle contient le cycle $(uv)$ et ne déplace pas $a_0$. On aura donc $\Theta = AB$, A étant la substitution qui permute $u, v$ sans déplacer les autres lettres, et B une substitution d'ordre 2 ne déplaçant que les $q-1$ lettres $a_1, \ldots, a_{q-1}$. Le groupe $G_3$ contiendra la substitution $\Theta^{-1} S \Theta = B^{-1} S B$, laquelle, laissant $u, v$ immobiles, appartient à $G_1$, et par suite se réduit à une puissance de S, telle que $S^\alpha$. D'ailleurs, $B^2$ se réduisant à l'unité, on aura

$$S^{\alpha^2} = B^{-1} S^\alpha B = B^{-2} S B^2 = S,$$

d'où

$$\alpha^2 \equiv 1 \bmod. q, \quad \alpha \equiv \pm 1.$$

Mais $\alpha$ ne peut être égal à 1, car B, étant échangeable à S, devrait se réduire à l'unité, et $\Theta$ au cycle $(u\nu)$, de telle sorte que $G_3$, au lieu d'appartenir à la classe $q$, appartiendrait à la classe 2. Donc B transformera S en $S^{-1}$, et par suite sera de la forme $(a_1 a_{q-1})(a_2 a_{q-2})\ldots$.

La substitution $\Theta$ ne pourra donc être déterminée que d'une seule manière. D'ailleurs cette substitution, jointe à celles de $G_2$, reproduira toutes celles de $G_3$; car ces substitutions, combinées ensemble, permettent d'amener $\nu$ à la place d'une quelconque des $q+2$ lettres du groupe; après quoi les substitutions de $G_2$, qui ne déplacent pas $\nu$, permettront d'assigner aux autres lettres $q(q+1)$ systèmes de places différents. La combinaison de $G_2$ avec $\Theta$ fournit donc au moins $q(q+1)(q+2)$ substitutions distinctes, c'est-à-dire toutes celles de $G_3$.

**22.** Le groupe $G_3$ ne peut donc être construit que d'une seule manière. Encore faudrait-il, pour être assuré de son existence effective, vérifier que de la substitution $\Theta$, jointe à $G_2$, on ne peut déduire aucune substitution déplaçant moins de $q$ lettres. Mais cette vérification peut se faire immédiatement, en remarquant que les substitutions de la forme linéaire fractionnaire

$$\left| z \quad \frac{az+\alpha}{bz+\beta} \right| \text{mod. } 2,$$

où $a, \alpha, b, \beta, z$ sont des entiers complexes formés avec la racine $i$ d'une congruence irréductible de degré $n$, $z$ étant susceptible, en outre, de prendre $\infty$ pour valeur, forment un groupe trois fois transitif satisfaisant à toutes les conditions imposées à $G_3$.

**23.** S'il existait un groupe $G_4$, on verrait, comme tout à l'heure, qu'il pourrait s'obtenir en combinant à $G_3$ une substitution binaire de la forme $\Theta' = A'B'$, $A'$ étant une substitution qui permute $\nu$ avec une lettre nouvelle $w$, et $B'$ une substitution qui transforme S en $S^{-1}$. Mais on aurait alors $B' = B$, et $G_4$, contenant la substitution $\Theta\Theta' = AA'$, qui ne déplace que 3 lettres, $u, \nu, w$, ne serait pas de la classe $q$. Donc l'existence du groupe $G_4$ est impossible dans tous les cas; à plus forte raison celle des groupes $G_5, \ldots$.

**24.** Nous obtenons donc le théorème suivant :

THÉORÈME. — *Si le nombre premier q n'est pas de la forme* $2^n - 1$, *la classe q ne contiendra qu'un seul groupe, formé des puissances de la substitution circulaire*

$$| \; x \quad x+1 \; | \; \text{mod. } q.$$

*Si q est de la forme* $2^n - 1$, *la classe p contiendra deux autres groupes des degrés* $q+1$ *et* $q+2$, *et respectivement formés des substitutions linéaires*

$$| \; z \quad az+\alpha \; | \; \text{mod. } 2$$

*et des substitutions linéaires fractionnaires*

$$\left| \; z \quad \frac{az+\alpha}{bz+\beta} \; \right|,$$

$z$, $a$, $\alpha$, $b$, $\beta$ *étant des entiers complexes formés avec la racine i d'une congruence irréductible de degré n par rapport au module* 2.