

JOURNAL
DE
MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

ED. MAILLET

**Sur une série de groupes primitifs holoédriquement isomorphes
à des groupes plusieurs fois transitifs**

Journal de mathématiques pures et appliquées 5^e série, tome 3 (1897), p. 277-310.

http://www.numdam.org/item?id=JMPA_1897_5_3_277_0



NUMDAM

Article numérisé dans le cadre du programme
Gallica de la Bibliothèque nationale de France
<http://gallica.bnf.fr/>

et catalogué par Mathdoc
dans le cadre du pôle associé BnF/Mathdoc
<http://www.numdam.org/journals/JMPA>

*Sur une série de groupes primitifs holoédriquement isomorphes
à des groupes plusieurs fois transitifs;*

PAR M. ED. MAILLET,

Ingénieur des Ponts et Chaussées.

I.

Soit S un groupe symétrique ou alterné de n éléments $a_1, a_2, \dots, a_n$ ($n > 4$). On sait ⁽¹⁾ que le groupe G_α formé par les substitutions que S opère entre les C_n^α combinaisons α à α des n éléments ($1 < \alpha < \frac{n}{2}$) est primitif.

Soit C un sous-groupe de S , de degré n , k fois transitif; on sait ⁽²⁾, et l'on voit de suite, que C opère entre ces C_n^α combinaisons un groupe Γ_α de substitutions, transitif si $k \geq \alpha$, Γ_α étant un sous-groupe de G_α . On peut se demander si Γ_α est primitif.

Soit Δ_α le sous-groupe des substitutions de Γ_α laissant immobile la combinaison $a_1, a_2, \dots, a_\alpha$, D le sous-groupe correspondant de C ; D est formé des substitutions de C qui permutent exclusivement entre elles les lettres $a_1, a_2, \dots, a_\alpha$. C étant supposé k fois transitif, avec $k \geq \alpha$, D opère entre ces α lettres les substitutions du groupe symétrique;

⁽¹⁾ *Journal de Mathématiques*, p. 16; 1895.

⁽²⁾ Voir *Bull. Soc. math.*, 1896, notre *Note sur les groupes de substitutions*.

de plus les sous-groupes de C et D, formés des substitutions de C et D respectivement laissant immobiles ces α lettres, coïncident et forment un groupe E, $k - \alpha$ fois transitif, par suite transitif si $k \geq \alpha + 1$, et primitif si $k \geq \alpha + 2$. Γ_α n'est qu'une fois transitif, en général, comme G_α qui le contient ⁽¹⁾.

Nous savons ⁽²⁾ que Γ_α sera primitif à la condition nécessaire et suffisante que Δ_α soit maximum dans Γ_α , ou D maximum dans C. Il suffit donc de voir si le groupe dérivé de D et d'une substitution quelconque U de C, non contenue dans C, coïncide avec C.

La substitution U, n'appartenant pas à D, permute une des lettres $a_1, a_2, \dots, a_\alpha$ avec une des $n - \alpha$ autres lettres, et le groupe F, dérivé de D et de U, sera transitif entre les n lettres, si D l'est entre les $n - \alpha$ lettres $a_{\alpha+1}, \dots, a_n$, c'est-à-dire si $k \geq \alpha + 1$, ce que nous supposons.

Si F n'est pas primitif, il admettra une répartition de ses lettres en systèmes de non-primitivité i à i avec $1 < i \leq \frac{n}{2}$, et i divise n . Considérons dans F le sous-groupe L des substitutions de F laissant a_j immobile : L permutera exclusivement entre elles les lettres du système de non-primitivité auquel appartient a_j . Si l'on prend $j \leq \alpha$, L contiendra le sous-groupe des substitutions de D laissant a_j immobile, lequel opère entre les lettres $a_1, a_2, \dots, a_\alpha$ autres que a_j les substitutions du groupe symétrique de $\alpha - 1$ éléments, et, par suite, le groupe E. Donc L permute transitivement ces $\alpha - 1$ lettres (sauf si $\alpha = 2$, mais les raisonnements qui suivent restent applicables) : si une seule d'entre elles appartient au même système de non-primitivité que a_j , elles lui appartiennent toutes, et $i \geq \alpha$. Si une des lettres déplacées par E appartient au même système de non-primitivité que a_j , avec $j \leq \alpha$, toutes les lettres de E, qui est ici transitif, lui appartiennent, et il faudrait $n - \alpha < i \leq \frac{n}{2}$, résultat absurde, en supposant ici $\alpha < \frac{n}{2}$ ⁽³⁾. On en

⁽¹⁾ *Journal de Mathématiques*, p. 23; 1896.

⁽²⁾ W. DYCK, *Math. Ann.*, t. XX et XXII, et notre *Thèse de Doctorat*, p. 18.

⁽³⁾ Il n'y a pas d'intérêt à supposer $\alpha > \frac{n}{2}$, car à toute combinaison des n lettres α à α en correspond une autre formée des $n - \alpha$ autres lettres, et les

conclut, puisque $i \geq 2$, que les lettres $a_1, a_2, \dots, a_\alpha$ forment un système, et que $i = \alpha$.

Les lettres de E formeront alors un certain nombre de systèmes, et il faudra : 1° que $i = \alpha$ divise n ; 2° que E admette une répartition de ses lettres α à α , ce qui est impossible si E est primitif. Il en résulte :

F est primitif : 1° quand $k > \alpha$ et que α ne divise pas n ; 2° quand $k > \alpha$ et que E est primitif ou n'admet pas une répartition de ses lettres α à α ; 3° par suite quand $k \geq \alpha + 2$.

Supposons F primitif : E est de degré $n - \alpha$ et transitif entre $n - \alpha$ lettres.

Si E est primitif entre ces lettres, on sait (1) que F est au moins $\alpha + 1$ fois transitif entre n lettres : le sous-groupe des substitutions de F laissant immobiles $a_1, a_2, \dots, a_\alpha$ est E, en sorte que F et C sont de même ordre, ce qui entraîne $F = C$; dans ce cas D est maximum dans C, et Γ_α est primitif : il en est ainsi en particulier quand E est deux fois transitif entre ses $n - \alpha$ lettres, c'est-à-dire quand $k \geq \alpha + 2$.

Si E n'est pas primitif, et $k = \alpha + 1$, on sait (2) que F renferme un groupe F, deux fois transitif de degré $p_1 + p_2 + \dots + p_\mu + 1 = P$, avec

$$n - \alpha = p_1 > p_2 > \dots > p_\mu > 1,$$

$p_1 = n - \alpha$ étant un multiple de p_2 , p_2 un multiple de p_3 , ..., et F, renferme des sous-groupes transitifs de degré $p_1, p_1 + p_2, p_1 + p_2 + p_3, \dots, p_1 + p_2 + \dots + p_\mu + 1 = P$, dont chacun est contenu dans le suivant, et $P \leq n$, d'où

$$(1) \quad \alpha \geq p_2 + p_3 + \dots + p_\mu + 1, \quad \text{et} \quad p_2 \leq \alpha - 1.$$

deux groupes Γ_α et $\Gamma_{n-\alpha}$ correspondants coïncident à la notation près. Si $\alpha = \frac{n}{2}$, G_α n'est pas primitif, et Γ_α non plus : d'ailleurs C ne pourrait en général être $\frac{n}{2}$ fois transitif sans contenir le groupe alterné.

(1) *Journal de Mathématiques*, p. 383; 1871.

(2) *Journal de Mathématiques*, p. 384-389; 1871, ou p. 20; 1895.

On en conclut d'ailleurs que F est au moins $n - P + 2$ fois transitif.

Si $\mu = 1$, F étant $\alpha + 1$ fois transitif coïncide avec C , et Γ_α est primitif. On n'a d'ailleurs $\mu > 1$ que si $p_2 \geq 2$: Γ_α ne peut donc être imprimitif que si p_2 est égal à un des nombres 2, 3, ..., ou $\alpha - 1$, et, *a fortiori*, que si $n - \alpha$ possède un diviseur > 1 égal à un de ces nombres, c'est-à-dire n'est pas premier à $(\alpha - 1)!$. Donc :

Si F est primitif, il coïncide avec C : 1° quand $k > \alpha + 1$; 2° quand $k = \alpha + 1$, si $n - \alpha$ est premier à $(\alpha - 1)!$.

Rapprochant ce résultat du résultat trouvé précédemment, on conclut :

THÉORÈME I. — *Soit C un groupe k fois transitif entre n lettres, Γ_α l'isomorphe holoédrique de C formé par les substitutions que C opère entre les combinaisons α à α de ses lettres, avec $\alpha < k$. Γ_α sera primitif :*

- 1° *Quand $k > \alpha + 1$;*
- 2° *Quand $k = \alpha + 1$, et que l'on a à la fois $n - \alpha$ premier à $(\alpha - 1)!$ et $\not\equiv 0 \pmod{\alpha}$.*

Par exemple, si $\alpha = 2$, Γ_2 sera primitif si C est quatre fois transitif, ou s'il ne l'est que trois fois, mais que n est impair ; si $\alpha = 3$, Γ_3 sera primitif si C est cinq fois transitif, ou s'il ne l'est que quatre fois, mais que $n - 3$ est impair et premier à 3, c'est-à-dire n de la forme $6h + 2$ ou $6h + 4$; si α est quelconque, et si $\varpi_1, \varpi_2, \dots, \varpi_z$ sont les diviseurs premiers de $\alpha!$, Γ_α sera primitif si $k \geq \alpha + 2$, ou si $k = \alpha + 1$ et $n - \alpha = l\varpi_1 \varpi_2 \dots \varpi_z + m$, l étant un entier quelconque, et m un entier, positif ou négatif, premier à $\varpi_1, \varpi_2, \dots, \varpi_z$.

II. — Applications.

PREMIER CAS. — *C est un groupe symétrique ou alterné.*

C est alors au moins $n - 2$ fois transitif, et l'on peut prendre $k = n - 2$; si $\alpha < \frac{n}{2}$, on a, en général, $n - 2 \geq \alpha + 2$, sauf pour de

petites valeurs de n ; on retrouve ainsi les isomorphes holoédriques et primitifs de la deuxième catégorie ⁽¹⁾ des groupes symétriques ou alternés.

DEUXIÈME CAS. — *C est un des groupes cinq fois transitifs de Mathieu ⁽²⁾.*

On a $n = 12$ ou $n = 24$; le théorème I montre de suite que les groupes Γ_2 et Γ_3 correspondants sont primitifs.

C contient ici un groupe C' quatre fois transitif formé des substitutions de C qui laissent une même lettre immobile, de degré 11 ou 23, et pour lequel le groupe Γ'_2 , analogue à Γ_2 , est primitif.

TROISIÈME CAS. — *C est un groupe linéaire fractionnaire.*

Nous allons établir à cet égard le théorème suivant :

THÉORÈME II. — *Soit C un groupe linéaire fractionnaire d'ordre ε trois fois transitif dérivé des substitutions*

$$V = \left| z; \frac{az + \alpha}{bz + \beta} \right| \quad (\text{mod. } p),$$

où p est premier, et où a, α, b, β, z sont des entiers complexes formés avec une racine ξ d'une congruence irréductible de degré m , c'est-à-dire de la forme

$$d_1 \xi^{m-1} + d_2 \xi^{m-2} + \dots + d_m \quad (\text{mod. } p),$$

où $d_1, \dots, d_m$ sont entiers (mod. p). Le groupe Γ_2 des substitutions opérées par C entre les combinaisons 2 à 2 de ses $p^m + 1$ lettres, est un groupe primitif d'ordre ε , de degré $\frac{(p^m + 1)p^m}{2}$ (quand $p^m > 5$), et de classe $\frac{(p^m - 1)(p^m + 1)}{2}$ si p impair, et 2^{2m-1} si $p = 2$.

⁽¹⁾ *Journal de Mathématiques*, p. 5 à 34; 1895.

⁽²⁾ *Journal de Mathématiques*, 1861 et 1873.

Je dis d'abord que Γ_2 est primitif.

On sait que V sera une substitution à la condition nécessaire et suffisante que $a\beta - b\alpha \not\equiv 0 \pmod{p}$. C est trois fois transitif entre $p^m + 1$ lettres représentées par p^m indices incongrus $\pmod{p}$ et par ∞ .

Ici $n - \alpha = p^m - 1$ n'est premier à 2 que si $p = 2$. Le théorème I montre donc que Γ_2 est primitif quand $p = 2$, mais non quand p est impair.

Dans ce dernier cas, supposons Γ_2 non primitif : si l'on prend $a_1 = 0$, $a_2 = \infty$, le groupe E est formé des puissances de la substitution

$$X = |z, a'z| \pmod{p},$$

où a' est une racine primitive de la congruence $x^{p^m-1} - 1 \equiv 0 \pmod{p}$. Le groupe D est dérivé de E et de la substitution

$$Y = \left| z, \frac{1}{z} \right| \pmod{p},$$

car C ne contient pas de substitutions permutant exclusivement entre eux 0 et ∞ autres que celles dérivées de X et de Y . E étant transitif entre $n - 2$ lettres, le groupe F , dérivé de D et d'une substitution quelconque U de C non contenue dans D , est transitif entre n lettres. Si F est primitif quel que soit U , E étant transitif, on a ici, d'après (1), $\mu = 1$; F coïncide avec C et Γ_2 est primitif. Supposons donc F non primitif pour une valeur de U convenablement choisie : F admet une répartition de ses lettres en systèmes de non-primitivité de 2 lettres, d'après ce qu'on a vu, et 0, ∞ forment un système. Quant aux autres systèmes, ils seront formés chacun des lettres d'un cycle de la substitution $|z, -z| \pmod{p}$; car E étant transitif entre les $n - 2$ lettres, autres que 0 et ∞ qu'il ne déplace pas, est transitif entre les $\frac{n-2}{2}$ systèmes qui les contiennent. E , étant formé des puissances de X , opère entre ces $\frac{n-2}{2}$ systèmes une substitution circulaire d'ordre $\frac{n-2}{2}$, et $X^{\frac{n-2}{2}} = |z, -z| \pmod{p}$ laisse tous ces systèmes immobiles. F ne peut donc être imprimitif que s'il existe une substitution U de C , non contenue dans D , et qui admette la répartition 0, ∞ ; $i, -i$,

où i prend toutes les valeurs $\not\equiv 0$ et incongrues entre elles (mod p). Supposons qu'il en soit ainsi.

U n'est pas contenue dans D, c'est-à-dire n'est pas d'une des formes X^u ou $YX^u = \left| z, \frac{a^u}{z} \right| \pmod{p}$.

Soit

$$U = \left| z; \frac{a_1 z + \alpha_1}{b_1 z + \beta_1} \right| \pmod{p} :$$

U ne peut permuter entre eux 0 et ∞ ; il remplace 0 par i , par exemple, et ∞ par $-i$, c'est-à-dire que

$$\alpha_1 \equiv \beta_1 i, \quad a_1 \equiv -b_1 i, \\ U = \left| z, i \frac{-b_1 z + \beta_1}{b_1 z + \beta_1} \right| \pmod{p}.$$

De plus, si U remplace j par h , elle remplace $-j$ par $-h$ (en supposant j et h différents de 0 et ∞), et

$$i \frac{-b_1 j + \beta_1}{b_1 j + \beta_1} \equiv h, \quad i \frac{b_1 j + \beta_1}{-b_1 j + \beta_1} \equiv -h,$$

d'où

$$b_1^2 j^2 + \beta_1^2 \equiv 0 \pmod{p}.$$

Cette congruence ne pouvant être satisfaite que pour deux valeurs de j dont la somme est $\equiv 0 \pmod{p}$, on est conduit à une contradiction si $p^m > 5$, car le nombre des couples $j, -j$, avec $j \not\equiv 0$, auxquels sont substitués par U des couples de même forme, est $\geq \frac{p^m - 3}{2}$. Donc U ne peut être imprimitif si $p^m > 5$, et Γ_2 est alors primitif.

Pour établir complètement le théorème II, il ne reste plus qu'à déterminer la classe de Γ_2 .

Il suffit pour cela d'étudier le nombre de combinaisons de 2 lettres de C laissées immobiles par les substitutions de C, autres que l'unité, et qui laissent immobile une combinaison donnée, par exemple la combinaison 0, ∞ . Que p soit pair ou impair, ces substitutions sont

celles de la forme

$$V' = |z, a_2 z|, \quad \text{ou} \quad V'' = \left| z, \frac{a_2}{z} \right| \pmod{p},$$

avec $a_2 \not\equiv 0$ dans V' et V'' et $a_2 \not\equiv 1$ dans V' .

V' ne peut laisser une combinaison i, j immobile, avec $i \not\equiv j$, que si

$$i \equiv a_2 i, \quad j \equiv a_2 j,$$

ou

$$i \equiv a_2 j, \quad j \equiv a_2 i.$$

Dans le premier cas, i, j coïncide avec $0, \infty$; dans le deuxième, $i \equiv a_2^2 i, j \equiv a_2^2 j$ donne $a_2^2 \equiv 1$. Si p est impair, on a $a_2 \equiv -1 \pmod{p}$, et la substitution $|z, -z|$ laisse les $\frac{p^m+1}{2}$ combinaisons $0, \infty$ et $i, -i$ immobiles. Si $p = 2$, le deuxième cas donnerait $a_2 \equiv 1$, et V' ne laisse immobile que la combinaison $0, \infty$.

V'' ne peut laisser une combinaison i, j immobile, avec $i \not\equiv j$, que si

$$i \equiv \frac{a_2}{i}, \quad j \equiv \frac{a_2}{j},$$

ou

$$i \equiv \frac{a_2}{j}, \quad j \equiv \frac{a_2}{i}.$$

Dans le premier cas, $i^2 \equiv j^2 \equiv a_2$ ne donne une combinaison que si p impair et a_2 résidu quadratique $\pmod{p}$. Dans le deuxième, $ij \equiv a_2$; on a comme solutions toutes les combinaisons $i, a_2 i^{-1}$, avec $i \not\equiv a_2 i^{-1}$; si p est impair, ces combinaisons sont en nombre $\frac{p^m+1}{2}$ quand a_2 est non-résidu quadratique, et en nombre $\frac{p^m-1}{2}$ quand a_2 est résidu, en y comprenant la combinaison $0, \infty$: car $i_1 \equiv a_2 i_1^{-1}$ donne $i \equiv a_2 i_1^{-1}$; si $p = 2$, $ij \equiv a_2$, avec $i \not\equiv j$, a, en dehors de la solution $0, \infty$, $2^m - 2$ solutions, ce qui ne donne, en y comprenant la combinaison $0, \infty$, que 2^{m-1} combinaisons distinctes.

On en conclut que Γ_2 renferme des substitutions qui laissent $\frac{p^m+1}{2}$

combinaisons immobiles, si p impair, et 2^{m-1} , si $p = 2$, et qu'il n'en contient aucune, à part l'unité, en laissant davantage immobiles. La classe de Γ_2 est donc

$$\frac{p^m+1}{2} p^m - \frac{p^m+1}{2} = \frac{(p^m+1)(p^m-1)}{2},$$

si p impair,

$$\frac{2^m+1}{2} 2^m - 2^{m-1} = 2^{2m-1},$$

si $p = 2$.

Le théorème II est ainsi complètement établi.

Remarque. — Tout groupe linéaire fractionnaire C considéré au théorème II contient, quand p est impair, un sous-groupe deux fois transitif d'ordre moitié moindre C' dérivé des substitutions

$$V = \left| z, \frac{az + \alpha}{bz + \beta} \right| \pmod{p}$$

pour lesquelles $\alpha\beta - b\alpha$ est résidu quadratique $\pmod{p}$.

Le groupe Γ'_2 correspondant à C' , formé des substitutions opérées par C' entre les combinaisons deux à deux de ses $p^m + 1$ lettres est un groupe primitif de même degré $\frac{p^m+1}{2} p^m$ que Γ_2 , de même classe et d'ordre moitié moindre (si p^m est > 11).

En effet, Γ'_2 est transitif et contenu dans Γ_2 ; la classe de Γ'_2 est la même que celle de Γ_2 , car la substitution $V'' = \left| z, \frac{\alpha_1}{z} \right| \pmod{p}$, où $-\alpha_1$ est résidu quadratique $\pmod{p}$, laisse exactement $\frac{p^m+1}{2}$ combinaisons des lettres de C' 2 à 2 immobiles, en sorte que la classe de Γ'_2 , qui n'est pas inférieure à celle de Γ_2 , où il est contenu, est

$$\frac{p^m+1}{2} p^m - \frac{p^m+1}{2} = \frac{p^{2m}-1}{2},$$

comme celle de Γ_2 .

Il reste à voir seulement si Γ'_2 est primitif, c'est-à-dire si le groupe D'

des substitutions de C' qui laissent la combinaison $0, \infty$ immobile, groupe dérivé du groupe E' des puissances de la substitution

$$X^2 = |z, a''z| \pmod{p}$$

et de

$$Y' = \left| z, \frac{a_1}{z} \right| \pmod{p},$$

où $-a_2$ est résidu quadratique $\pmod{p}$, est maximum dans C' . Quand $p^m = 4h + 1$, c'est-à-dire m pair ou $p = 4h' + 1$, on peut prendre $a_2 = 1$, car -1 est résidu quadratique; au contraire, quand $p^m = 4l + 3$, a_2 est non-résidu quadratique.

Le groupe E' permute transitivement d'une part les résidus, d'autre part les non-résidus. De plus, si -1 est non-résidu, il en est de même de a_2 , et Y' remplace un résidu par un non-résidu, en sorte que D' opère entre les $n - 2$ indices autres que $0, \infty$ les substitutions d'un groupe régulier. Au contraire, si -1 est résidu, il en est de même de a_2 , et D' permute transitivement, d'une part les résidus, d'autre part les non-résidus. Dans les deux cas, D' est formé des substitutions X^{2^k} et

$$Y'X^{2^k} = \left| z, \frac{a_2 a'^2}{z} \right| \pmod{p}.$$

Dans le deuxième cas, cette dernière substitution laisse immobile les deux indices $z_1, -z_1$, racines de la congruence $z^2 \equiv a_2 a'^2 \pmod{p}$.

Ceci posé, pour établir que z_1 est primitif, il suffit, d'après ce qui précède, de montrer que le groupe F' , dérivé de D' et d'une substitution quelconque U de C' , autre que celles de D' , coïncide avec C' , quel que soit U .

Supposons qu'il en soit autrement, et $F' < C'$. Je dis d'abord que F' est transitif entre les n indices.

En effet, si -1 est non-résidu, D' est transitif, d'une part entre les indices $0, \infty$, d'autre part entre les $n - 2$ autres indices, et toute substitution de F' qui permute exclusivement entre eux d'une part $0, \infty$, d'autre part les $n - 2$ autres indices, appartient à D' . Donc U remplace l'un des indices 0 ou ∞ par un des $n - 2$ autres indices, et F' permute transitivement les n indices.

Si -1 est résidu, supposons F' non transitif. U va permuter ∞ , par exemple, avec un résidu; dès lors F' va permuter 0 et ∞ transitivement avec tous les résidus, puisque E' les permute transitivement, mais non avec les non-résidus, puisque F' est intransitif. F' permute donc transitivement 0 avec $\frac{p^m-1}{2} + 2 = \frac{p^m+3}{2}$ lettres, et

$$\mathfrak{J}' = \frac{p^m+3}{2} \mathfrak{K}' = \frac{p^m+3}{2} \frac{p^m-1}{2} \lambda,$$

où $\mathfrak{K}' = \frac{p^m-1}{2} \lambda$ est l'ordre du groupe des substitutions de F' laissant 0 immobile et contenant E' , et divise $(p^m+1)p^m \frac{p^m-1}{2} = \mathfrak{C}'$; c'est-à-dire que p^m+3 divise $2p^m(p^m+1)$ et $2p^m(p^m+3)$, par suite la différence $4p^m$ et $4(p^m+3) - 4p^m = 12$, d'où $p^m \leq 9$, ce que nous supposons ne pas avoir lieu. Donc F' est transitif pour $p^m > 9$.

D'après un théorème connu ⁽¹⁾, F' étant un groupe transitif de classe $n-2$ et de degré n , est d'ordre

$$\mathfrak{J}' = [(p, k+1)(q, k+1) + 1](p, k+1)k,$$

où

$$n = (p, k+1)(q, k+1) + 1,$$

et où k est l'ordre du groupe K des substitutions de F' qui laissent 0 et ∞ immobiles, en sorte que $k = \mathfrak{C}'$; si l'on a $p_1 \neq 0$, d'après $\mathfrak{C}' = \frac{n-2}{2}$, l'on a $p_1 = 2$ ou $p_1 = 1$; si $p_1 = 2$, $\mathfrak{J}' = \mathfrak{C}'$ contrairement à l'hypothèse $F' < C'$; si $p_1 = 1$, $p_1 k + 1 = 1 + \frac{p^m-1}{2} = \frac{p^m+1}{2}$ devrait diviser $n-1 = p^m$, ce qui est absurde. Donc $p_1 = 0$, et

$$\mathfrak{J}' = (p^m+1) \frac{p^m-1}{2}.$$

F' admet une répartition de ses indices en systèmes de non-primiti-

(1) Voir notre *Thèse de Doctorat*, p. 70.

tivité de deux indices, le sous-groupe des substitutions de F' qui laisse ∞ immobile coïncidant avec E' : 0 et ∞ forment un système (¹).

Si maintenant -1 est résidu, la substitution $Y'X^{2h}$ laisse immobile les deux indices z_1 et $-z_1$, racines de la congruence $z^2 \equiv a_2 a'^2$, et déplace tous les autres indices; par suite, la répartition est formée du système $0, \infty$ et des systèmes $i, -i$, où i prend toutes les valeurs $\not\equiv 0$ et incongrues entre elles (mod p). En raisonnant comme nous l'avons fait pour C et Γ_2 , on voit qu'il faut $p^m \leq 5$.

Si -1 est non-résidu, il y a $\frac{p^m - 1}{2} = 2h + 1$ systèmes : la substitution X^2 contient dans un de ses cycles les résidus, dans l'autre les non-résidus et est d'ordre $2h + 1$; or, si un système comprenait deux résidus, γ_1, γ_2 par exemple, il y aurait une puissance de X^2 remplaçant γ_1 par γ_2 , par suite γ_2 par γ_1 , et de la forme $(\gamma_1, \gamma_2) \dots$, c'est-à-dire d'ordre pair, ce qui est impossible, car les puissances de X^2 sont d'ordre diviseur de $2h + 1$. Donc, chaque système autre que $0, \infty$ comprend un résidu et un non-résidu : si $\theta = a'^{2h+1}$ est le non-résidu faisant partie du même système que 1 , la considération de X^2 montre que ces systèmes sont

$$1, \theta; \quad a'^2, a'^2 \theta; \quad a'^4, a'^4 \theta; \quad \dots; \quad a'^{2h}, a'^{2h} \theta; \quad \dots$$

Si $\theta \equiv -1$, tout système autre que $0, \infty$ est de la forme $i, -i$: on peut encore raisonner comme nous l'avons fait pour C et Γ_2 ; il faut $p^m \leq 5$.

Soit $\theta \not\equiv -1$; le raisonnement est encore analogue : U n'est pas d'une des formes X^{2h} et $Y'X^{2h}$. Soit

$$U = \left| z, \frac{a_1 z + \alpha_1}{b_1 z + \beta_1} \right| \pmod{p},$$

avec

$$a_1 \beta_1 - b_1 \alpha_1 \equiv A^2 \pmod{p}.$$

U remplace 0 par i et ∞ par θi , avec i différent de 0 et de ∞ , ou 0

(¹) Voir, par exemple, notre *Thèse de Doctorat*, p. 18, th. VII et VIII, et *Ann. Fac. des Sc. de Toulouse*: 1895, D. 18, th. VII.

par θi et ∞ par i . Ce deuxième cas se ramène au premier en posant $\theta i \equiv i'$, $\theta' \equiv \theta^{-1}$, $i \equiv \theta^{-1} i' \equiv \theta' i'$, et il nous suffit de considérer le premier cas. On tire de là

$$U = \left| z, i \frac{b_1 \theta z + \beta_1}{b_1 z + \beta_1} \right| \pmod{p}.$$

Si U remplace j par h , elle remplace θj par θh (j et h étant différents de 0 et de ∞); on en conclut que j doit satisfaire à une congruence du second degré (mod p) ayant au plus deux racines, auxquelles correspondent au plus deux systèmes.

De même, si U remplace j' par $\theta j'$, $\theta j'$ par h' (j' et h' différents de 0 et de ∞), on en conclut que j' doit satisfaire à une congruence du second degré (mod p), ayant au plus deux racines, auxquelles correspondent au plus deux systèmes.

Dès lors, le nombre des systèmes j , θj , avec j différent de 0 et de ∞ , auxquels sont substitués des systèmes de même forme étant ≤ 4 et $\geq \frac{p^m - 3}{2}$, on a $\frac{p^m - 3}{2} \leq 4$, $p^m \leq 11$, c'est-à-dire, puisque ici $p^m = 4h + 3$, $m = 1$, $p = 7$ ou 11.

En résumé, F' ne peut être $< C'$ que si $p^m \leq 11$, et l'on en conclut que Γ'_2 est primitif quand $p^m > 11$. C. Q. F. D.

QUATRIÈME CAS. — C contient le groupe linéaire fractionnaire.

On sait, d'après MM. Mathieu ⁽¹⁾ et Jordan ⁽²⁾, que le groupe linéaire fractionnaire considéré au théorème II est contenu dans un groupe de même degré dérivé de lui et de la substitution

$$W = |z, z^{\sigma}| \pmod{p},$$

où σ est un diviseur arbitrairement choisi de m . Ces groupes ne diffèrent de ceux considérés au théorème II que si $m > \sigma \geq 1$. Les groupes Γ_2 correspondants contiennent les groupes Γ_2 dont il est question dans ce

⁽¹⁾ *Journal de Mathématiques*; 1861.

⁽²⁾ *Comptes rendus de l'Académie des Sciences*; 1872, 2^e sem., p. 1755.

théorème et sont de même degré, par suite sont *a fortiori* primitifs.

De même pour les groupes Γ_2 correspondant aux groupes des substitutions paires des groupes C précédents, quand $p^m > 11$.

CINQUIÈME CAS. — *C est un groupe linéaire.*

On voit immédiatement cette propriété :

Les groupes linéaires les plus généraux de degré p^m à m indices réels (mod p) (p étant premier) opèrent entre les combinaisons 2 à 2 (et 3 à 3 si $p = 2$) de leurs lettres des groupes de substitutions transitifs, mais non primitifs, si $p^m > 3$.

Les groupes linéaires en question contiennent en effet un sous-groupe invariant (c'est-à-dire permutable à leurs substitutions) de degré p^m ; les groupes Γ_2 ont la même propriété et, comme ils sont de degré $C_{p^m}^2$ (ou de degrés C_{2m}^2 et C_m^2 respectivement si $p = 2$), ils contiennent un sous-groupe invariant intransitif, si $p^m < \frac{p^m(p^m-1)}{2}$, c'est-à-dire si $p^m < 3$, et, par suite, ne peuvent être primitifs (¹).

On a une propriété analogue pour les groupes linéaires les plus généraux de degré p^{mv} dont les m indices sont formés à l'aide de racines d'une congruence irréductible de degré v .

III.

Soit C un groupe quelconque, transitif ou non, de degré n et de classe u , Γ_α le groupe, transitif ou non, des substitutions opérées par C entre les C_n^α combinaisons α à α des n lettres de C ($1 < \alpha < \frac{n}{2}$). Γ_α est évidemment contenu dans l'isomorphe holoédrique et primitif G_α du groupe symétrique S de n éléments formé par les substitutions que S opère entre ces combinaisons. Nous allons indiquer le moyen de déterminer la classe de Γ_α et donner une limite inférieure de cette classe; puis nous appliquerons les résultats trouvés au cas où C est au moins

(¹) JORDAN, *Traité des Substitutions*, p. 41.

deux fois transitif entre ses n lettres, et même, plus généralement, au cas où C est de classe $\geq \frac{n}{4}$.

Soient

$$U_r = (a_1^1 \dots a_1^{r_1}) \dots (a_q^1 \dots a_q^{r_q})$$

une substitution de S d'ordre premier r à q cycles, $U^{(\alpha)}$ la substitution correspondante dans G_α . La classe de Γ_α sera la plus petite des classes des substitutions $U^{(\alpha)}$ appartenant à Γ_α , quand r et q prennent toutes les valeurs possibles correspondantes aux substitutions U_r de C , avec $rq > 1$. On doit noter d'ailleurs qu'à deux substitutions semblables de S , et *a fortiori* de C , correspondront deux substitutions semblables de G_α , et *a fortiori* de Γ_α , et par suite de même classe, car on passe toujours de l'une à l'autre par un simple changement dans la manière de désigner les n lettres.

U_r ne peut laisser immobile une combinaison ayant exactement r' lettres communes ($0 < r' \leq r$) avec son premier cycle, par exemple, sans qu'on ait $r' = r$; car U_r remplace ces r' lettres par r' lettres appartenant à la fois à la même combinaison et au même cycle que les r' premières, et ceci n'aurait pas lieu si $r' < r$: donc $r' = r$.

Dès lors, toute combinaison laissée immobile par U_r sera formée des lettres de k cycles de U_r , avec $0 \leq k \leq q$, $k \leq E\left(\frac{\alpha}{r}\right)$, et de $\alpha - kr$ lettres non déplacées par U_r , avec $n - qr \geq \alpha - kr$. Réciproquement, toute combinaison ainsi formée est laissée immobile par U_r . Soit k un entier déterminé satisfaisant aux conditions ci-dessus : une combinaison formée des lettres de k cycles de U_r et de $\alpha - kr$ lettres non déplacées par U_r s'obtiendra en prenant une des C_q^k combinaisons des cycles de U_r , k à k , puis en adjoignant aux kr lettres de cette combinaison une quelconque des $C_{n-qr}^{\alpha-kr}$ combinaisons des $n - qr$ lettres non déplacées par U_r , $\alpha - kr$ à $\alpha - kr$. Le nombre des combinaisons des n lettres α à α , laissées immobiles par U_r et correspondant à la valeur de k considérée, est ainsi $C_q^k C_{n-qr}^{\alpha-kr}$.

Le nombre total des combinaisons laissées immobiles par U_r est ainsi

$$(1) \quad \nu_{r,q} = \sum_k C_q^k C_{n-qr}^{\alpha-kr},$$

k prenant toutes les valeurs entières satisfaisant à

$$(2) \quad 0 \leq k \leq q, \quad k \leq E\left(\frac{\alpha}{r}\right), \quad n - qr \geq \alpha - kr,$$

et la classe de $U^{(\alpha)}$ est $C_n^\alpha - v_{r,q}$.

Les formules (1) et (2) résolvent complètement le problème de la détermination de la classe de $U^{(\alpha)}$; par suite, elles permettront toujours pour un groupe donné C , de trouver la classe du groupe Γ_α correspondant.

Avant de déduire de ces formules une limite inférieure de la classe de Γ_α , nous allons en faire application aux groupes Γ_2 en prenant pour C un des groupes trois fois transitifs considérés au quatrième cas du paragraphe précédent ⁽¹⁾, et dérivé des substitutions

$$V = \left| z, \frac{az + \alpha}{bz + \beta} \right| \pmod{p} \quad \text{et} \quad W = |z, z^{p^r}| \pmod{p}.$$

Il nous suffit d'avoir le nombre de combinaisons de deux lettres laissées immobiles par les substitutions d'ordre premier du groupe laissant immobile une combinaison déterminée, par exemple la combinaison $0, \infty$. Ces substitutions sont comprises parmi celles dérivées de W , V' et V'' qui forment un groupe Φ d'ordre $2^{\frac{m}{r}}(p^m - 1)$.

Le sous-groupe des substitutions de C , qui laissent trois lettres arbitrairement choisies immobiles, est semblable au sous-groupe Ψ de C d'ordre $\frac{m}{r}$, formé des puissances de W , puisque C est trois fois transitif. Donc toute substitution d'ordre premier de C laissant au moins trois lettres immobiles est semblable à une puissance de W .

De même le sous-groupe des substitutions de C , laissant deux lettres arbitrairement choisies immobiles, est semblable au sous-groupe Θ

⁽¹⁾ On peut encore faire application de ces formules (1) et (2) par exemple aux groupes primitifs Γ_2 et Γ_3 correspondant au groupe C cinq fois transitif, de degré 12, et au groupe primitif Γ_2 correspondant au groupe quatre fois transitif contenu dans C , et que nous avons mentionnés plus haut. Ces groupes, qui sont de degrés respectifs 66, 220, 55, sont de classes respectives 56, 198, 48.

de C dérivé de W et de V' . Toute substitution d'ordre premier de C qui laisse exactement deux des lettres de C immobiles, est régulière, et par suite semblable à une puissance de V' , car on a toujours une puissance de V' d'ordre égal à un diviseur premier quelconque de $p^m - 1$.

Enfin une substitution Σ d'ordre 2 de C qui ne laisse pas deux lettres de C immobiles au moins (s'il en existe une dans C), est formée de $\frac{p^m+1}{2}$ cycles, si p impair, et de 2^{m-1} cycles, si $p = 2$.

On en conclut immédiatement que les substitutions d'ordre premier de Φ sont semblables à W ou une de ses puissances, à V' ou une de ses puissances, enfin à Σ .

Il ne nous reste plus qu'à trouver le nombre de combinaisons laissées immobiles par W et ses puissances, et par Σ , car nous savons que pour V' ce nombre est $\frac{p^m+1}{2}$, si p impair, et 1, si $p = 2$.

D'après les formules (1) et (2), ou, comme on le voit de suite, Σ laisse immobiles $\frac{p^m+1}{2}$ combinaisons, si p impair, et 2^{m-1} , si $p = 2$; dans le cas où $p = 2$, Σ existe toujours dans C .

Quant à W , on doit distinguer le cas où son ordre $\frac{m}{\tau}$ est impair, et celui où il est pair.

1° Si $\frac{m}{\tau}$ est impair, les puissances de W sont d'ordre impair, et, d'après (1) et (2), le nombre des combinaisons de 2 lettres que W^η laisse immobile est $C_{n-q\tau}^2$, où $n - q\tau$ est le nombre des lettres laissées immobiles par W^η . Toute puissance de W étant d'ailleurs semblable à une puissance de W d'exposant diviseur de $\frac{m}{\sigma}$, il suffit de supposer η diviseur de $\frac{m}{\tau}$. Alors

$$W^\eta = |z, z^{p^{\eta\tau}}| \pmod{p}$$

laisse autant de lettres immobiles que la congruence $z \equiv z^{p^{\eta\tau}} \pmod{p}$ a de solutions distinctes, soit, puisque $\eta\tau$ divise m , $p^{\eta\tau} + 1$ lettres en y comprenant ∞ . Alors W^η laisse immobile $\frac{p^{\eta\tau}+1}{2} p^{\eta\tau}$ combinaisons, et

le maximum de cette expression s'obtient en prenant pour η la valeur telle que $\frac{m}{\eta^2}$ soit égal au plus petit diviseur premier de $\frac{m}{\sigma}$ qui est ici ≥ 3 .

Ce maximum est alors $\leq \frac{p^{\frac{m}{2}} + 1}{2} p^{\frac{m}{2}} \leq \frac{p^m}{2}$, comme on le vérifie sans peine, en sorte que, quand $\frac{m}{\sigma}$ est impair, la classe est encore $\frac{(p^m + 1)(p^m - 1)}{2}$, si p impair, et $2^{2^{m-1}}$, si $p = 2$, comme pour les isomorphes Γ_2 des groupes linéaires fractionnaires.

2° Si $\frac{m}{\sigma}$ est pair, les puissances de W d'ordre impair sont évidemment les puissances de W^{2^λ} , si 2^λ est la plus haute puissance de 2 qui divise $\frac{m}{\sigma}$, et l'on peut leur appliquer ce qui précède, puisque $\frac{m}{2^{2^\lambda}}$ est impair : donc elles ne laisseront pas plus de $\frac{p^m}{2}$ combinaisons immobiles. Comme nous n'avons besoin de considérer, ainsi que nous l'avons dit, que des substitutions d'ordre premier, il ne nous reste plus à envisager que la puissance de W qui est d'ordre 2, c'est-à-dire la substitution

$$|z, z^{p^{\frac{m}{2}}}| \pmod{p}.$$

Elle laisse évidemment $p^{\frac{m}{2}} + 1$ lettres immobiles, et, par suite, d'après (1) et (2),

$$C_{p^{\frac{m}{2}}+1}^{2^{\frac{m}{2}}} + \frac{p^m - p^{\frac{m}{2}}}{2} = p^m$$

combinaisons. La classe sera ici $p^m \frac{p^m - 1}{2}$.

Nous pouvons alors énoncer ce théorème :

THÉORÈME III. — Soit C le groupe trois fois transitif dérivé du groupe linéaire fractionnaire trois fois transitif considéré au théorème II et de la substitution $|z, z^{p^\sigma}| \pmod{p}$, où σ est un diviseur arbitrairement choisi de m , avec $m > \sigma \geq 1$. Le groupe Γ_2 des substitutions opérées par C entre les combinaisons 2 à 2 de ses

$p^m + 1$ lettres est un groupe primitif, de degré $\frac{(p^m + 1)p^m}{2}$ (quand $p^m > 5$) et de classe $\frac{(p^m - 1)(p^m + 1)}{2}$, si p impair et $\frac{m}{\sigma}$ impair, 2^{2m-1} , si $p = 2$ et $\frac{m}{\sigma}$ impair, $\frac{(p^m - 1)p^m}{2}$, si $\frac{m}{\sigma}$ pair.

Remarque. — On a un théorème analogue pour le groupe C' d'ordre moitié de celui de C formé des substitutions paires de C , quand p est impair.

Si $\frac{m}{\sigma}$ est impair, W^η (η diviseur de $\frac{m}{\sigma}$) appartient à C' : la classe est encore $\frac{(p^m - 1)(p^m + 1)}{2}$.

Si $\frac{m}{\sigma}$ est pair, $W^{\frac{m}{2\sigma}} = |z, z^{p^{\frac{m}{2}}}| \pmod{p}$ est d'ordre 2, régulière, et déplace $p^m - p^{\frac{m}{2}} = p^{\frac{m}{2}}(p^{\frac{m}{2}} - 1)$ lettres, c'est-à-dire est paire, sauf quand $p^{\frac{m}{2}} - 1 = 4h + 2$, par suite quand $p = 4l + 3$ avec $\frac{m}{\sigma} = 4l' + 2$. Dans ce dernier cas, une puissance de W d'ordre premier ne peut être une substitution paire que si elle est d'ordre impair, et la classe du groupe Γ'_2 des substitutions opérées par C' entre les combinaisons 2 à 2 de ses lettres est encore $\frac{(p^m - 1)(p^m + 1)}{2}$, comme quand $\frac{m}{\sigma}$ est impair. Quand au contraire $\frac{m}{\sigma} \equiv 0 \pmod{4}$ ou quand $\frac{m}{\sigma}$ est pair avec $p = 4l + 1$, la classe est $\frac{(p^m - 1)p^m}{2}$.

On en conclut :

La classe de Γ'_2 est la même que celle des groupes Γ'_2 considérés dans la remarque du théorème II, sauf quand $\frac{m}{\sigma} \equiv 0 \pmod{4}$, ou $\frac{m}{\sigma}$ pair avec $p = 4l + 1$, cas où la classe est $\frac{(p^m - 1)p^m}{2}$.

IV.

Cherchons maintenant une limite inférieure de la classe de Γ_α , correspondant à un groupe C quelconque de classe $\geq u$, ou, ce qui revient au même, une limite supérieure de $\nu_{r,q}$.

Afin d'éviter une confusion, nous posons pour un instant

$$U_{r,q} = (a_1^1 \dots a_1^r) \dots (a_q^1 \dots a_q^r);$$

considérons

$$U_{r,q+1} = U_{r,q} (a_{q+1}^1 \dots a_{q+1}^r),$$

quand $r(q+1) \leq n$. Une combinaison laissée immobile par $U_{r,q+1}$ contient toutes les lettres $a_{q+1}^1, \dots, a_{q+1}^r$, ou n'en contient aucune, d'après ce qu'on a vu : dans les deux cas, toutes les lettres de cette combinaison, autres que $a_{q+1}^1, \dots, a_{q+1}^r$, sont permutées exclusivement entre elles par $U_{r,q+1}$, par suite par $U_{r,q}$, en sorte que cette combinaison est laissée immobile par $U_{r,q}$. Donc :

LEMME. — *Parmi les substitutions de S ou de C d'ordre premier donné r et de classe $\geq u$, celles qui laissent immobiles le plus de combinaisons α à α des n lettres sont celles qui ont le moins de cycles possibles.*

Le nombre des cycles de ces substitutions sera alors $\geq E\left(\frac{n+r-1}{r}\right)$.

D'autre part, si

$$U_r = (a_1^1 \dots a_1^r) \dots (a_q^1 \dots a_q^r)$$

avec r premier impair, considérons la substitution

$$V = (a_1^1 a_1^2) \dots (a_1^{r-2} a_1^{r-1}) (a_2^1 a_2^2) \dots (a_2^{r-2} a_2^{r-1}) \dots (a_q^1 a_q^2) \dots (a_q^{r-2} a_q^{r-1}),$$

d'ordre 2 à $q \frac{r-1}{2}$ cycles, et déplaçant $q(r-1)$ lettres. V permute exclusivement entre elles les lettres de chacun des cycles de U_r , et laisse immobiles les lettres que U_r ne déplace pas. Une combinaison laissée immobile par U_r comprend les lettres de k cycles de U_r et $\alpha - kr$ lettres non déplacées par U_r : donc elle est laissée immobile par V , en sorte que le nombre des combinaisons laissées immobiles par V est au moins égal au nombre des combinaisons laissées immobiles par U_r . La condition $qr \geq u$, avec $r \geq 3$, donne d'ailleurs

$$q(r-1) = qr \frac{r-1}{r} \geq u \frac{r-1}{r} \geq \frac{2u}{3},$$

et le nombre des cycles de V est $q \frac{r-1}{2} \geq \frac{u}{3}$.

On obtiendra donc une limite supérieure de $\nu_{r,q}$ pour toutes les substitutions de S d'ordre premier quelconque r à q cycles, avec $qr \geq u$, et *a fortiori* pour celles de C , en cherchant une limite supérieure de $\nu_{2,q}$, pour toutes les valeurs de q telles que $q \geq \frac{n}{3}$.

Le lemme précédent montre d'ailleurs qu'une pareille limite sera précisément $\nu_{2,\omega}$, où ω est le plus petit entier $\geq \frac{n}{3}$. D'après (1) et (2)

$$(3) \quad \nu_{2,\omega} = \sum_k C_{\omega}^k C_{n-2\omega}^{\alpha-2k},$$

k prenant toutes les valeurs entières satisfaisant à

$$(4) \quad 0 \leq k \leq \omega, \quad k \leq E\left(\frac{\alpha}{2}\right), \quad n - 2\omega \geq \alpha - 2k.$$

Si nous supposons u tel que $\omega \leq \frac{n}{4}$, la dernière condition est superflue, puisque $\alpha < \frac{n}{2}$ par hypothèse; la valeur $k = 0$ est admissible, et si k_1 est la plus petite des quantités ω et $E\left(\frac{\alpha}{2}\right)$, on a

$$(5) \quad \nu_{2,\omega} = \sum_{k=0}^{k_1} C_{\omega}^k C_{n-2\omega}^{\alpha-2k};$$

on obtient ainsi deux catégories de valeurs de $\nu_{2,\omega}$, suivant que ω sera $\leq E\left(\frac{\alpha}{2}\right)$ ou $> E\left(\frac{\alpha}{2}\right)$. On en conclut :

THÉOREME IV. — Soient C un groupe quelconque de degré n et de classe $\geq u$, Γ_{α} le groupe des substitutions opérées par C entre les combinaisons α à α de ses n lettres ($1 < \alpha < \frac{n}{2}$). La classe ω de Γ_{α} est telle que

$$(6) \quad \omega \geq C_{\alpha}^{\alpha} - C_{n-2\omega}^{\alpha} - C_{\omega}^1 C_{n-2\omega}^{\alpha-1} - C_{\omega}^2 C_{n-2\omega}^{\alpha-2} - \dots - C_{\omega}^{k_1} C_{n-2\omega}^{\alpha-2k_1},$$

où ω est le plus petit des entiers au moins égaux à un des deux

nombres $\frac{u}{3}$ et $E\left(\frac{n}{4}\right)$, et k , le plus petit des deux nombres w et $E\left(\frac{2}{2}\right)$.

On pourrait *a fortiori* prendre pour w une valeur plus petite, car on obtiendrait une limite inférieure moins avantageuse.

La même formule (6) donne une limite inférieure de la classe des substitutions des isomorphes holoédriques et primitifs G_α des groupes symétrique ou alterné de n éléments correspondant aux substitutions de classe $\geq u$ de ces derniers.

Enfin, dans le cas où $\alpha = 2$, on obtient de suite une limite plus avantageuse que la limite (6). En effet, si alors U_r est une substitution d'ordre premier r à q cycles, elle ne peut laisser immobile une combinaison contenant une lettre d'un cycle et non toutes les lettres de ce cycle. Donc, si r est impair, U_r laisse immobiles exactement les C_{n-qr}^2 combinaisons 2 à 2 des lettres qu'elle laisse immobiles. Si $r = 2$, U_2 laisse immobiles non seulement les C_{n-2q}^2 combinaisons analogues, mais encore les q combinaisons de 2 lettres formées chacune des lettres d'un cycle de U_2 , soit $q + C_{n-2q}^2$ combinaisons. Il en résulte, d'après le lemme et les considérations qui précèdent, que toutes les substitutions de classe $\geq u$ ne laissent pas plus de combinaisons de 2 lettres immobiles qu'une substitution d'ordre 2 à $\theta = E\left(\frac{u}{2}\right)$ cycles, c'est-à-dire qu'une limite supérieure de $v_{r,q}$ est ici $v_{2,\theta}$. Donc :

THÉORÈME V. — Soit C un groupe quelconque de degré n et de classe $\geq u$ Γ_2 , le groupe des substitutions opérées par C entre les combinaisons 2 à 2 de ses n lettres; la classe ω de Γ_2 est telle que

$$(7) \quad \omega \geq C_n^2 - \theta - C_{n-2}^2 = \frac{4\theta(n-\theta-1)}{2},$$

où

$$\theta = E\left(\frac{u}{2}\right).$$

Nous allons appliquer ces formules (6) et (7) au cas où C déplace toutes les combinaisons (ce qui a lieu par exemple si C est transitif

entre n lettres), Γ_α étant alors de degré C_n^α , et, en particulier, au cas où l'on a $\alpha \geq \frac{1}{4}n$, de façon à avoir des limites inférieures plus simples. Ces résultats s'appliqueront en particulier aux groupes au moins deux ou trois fois transitifs d'après certains théorèmes de M. Bochert (1).

$$1^\circ \text{ Cas où } \frac{n}{2} > \alpha \geq \frac{2n}{9}.$$

Si l'on suppose seulement $\alpha > 2$, C ne contient aucune substitution circulaire d'ordre 2. On voit de suite, d'après le lemme précédent, que les substitutions de C ne peuvent laisser plus de combinaisons immobiles qu'une substitution circulaire d'ordre 3 ou une substitution d'ordre 2 à 2 cycles. On en conclut à l'aide des formules (1) et (2) que la classe de Γ_α sera au moins égale à la plus petite des quantités

$$C_n^\alpha - C_{n-3}^\alpha - C_{n-2}^{\alpha-2}$$

et

$$C_n^\alpha - C_{n-4}^\alpha - 2C_{n-5}^{\alpha-2} - C_{n-6}^{\alpha-4}.$$

La classe de Γ_α est alors $\geq \frac{1}{2}C_n^\alpha$.

Quand C ne contient aucune substitution circulaire d'ordre 2 et que $\alpha \geq \frac{2}{9}n$, la classe de Γ_α est $\geq \frac{1}{2}C_n^\alpha$.

$$2^\circ \text{ Cas où } \frac{2n}{9} \geq \alpha \geq 3.$$

Nous appliquerons ici la formule (6) et les hypothèses du théorème IV. Soit

$$(8) \quad \Delta_i = \frac{C_w^i C_{n-2w}^{\alpha-2i}}{C_n^\alpha};$$

on a

$$(9) \quad \frac{\omega}{C_n^\alpha} \geq 1 - \sum_0^{k_1} \Delta_i.$$

(1) *Math. Ann.*, t. 40.

Or

$$\Delta_i = \frac{(n-2w) \dots (n-2w-\alpha+2i+1)}{n(n-1) \dots (n-\alpha+2i+1)} \frac{w(w-1) \dots (w-i+1)}{i!} \\ \times \frac{\alpha \dots (\alpha-2i+1)}{(n-\alpha+2i) \dots (n-\alpha+1)}; \\ \frac{(n-2w) \dots (n-2w-\alpha+2i+1)}{n(n-1) \dots (n-\alpha+2i+1)} \leq \left(\frac{n-2w}{n} \right)^{\alpha-2i},$$

puisque $a < b$ entraîne $\frac{a-j}{b-j} \leq \frac{a}{b}$ pour $j \geq 0$;

$$\frac{w(w-1) \dots (w-i+1)}{(n-\alpha+i) \dots (n-\alpha+1)} \leq \left(\frac{w}{n-\alpha+i} \right)^i \leq \left(\frac{w}{n-\alpha} \right)^i; \\ \frac{\alpha(\alpha-1) \dots (\alpha-i+1)}{(n-\alpha+2i) \dots (n-\alpha+i+1)} \leq \left(\frac{\alpha}{n-\alpha+2i} \right)^i \leq \left(\frac{\alpha}{n-\alpha} \right)^i; \\ (\alpha-i) \dots (\alpha-2i+1) \leq (\alpha-i)^i \leq \alpha^i,$$

en tenant compte de ce que $\alpha < \frac{n}{2}$, $w \leq \frac{n}{4}$; on obtient ainsi

$$(10) \quad \Delta_i \leq \left(\frac{n-2w}{n} \right)^{\alpha-2i} \left(\frac{w}{n-\alpha} \right)^i \left(\frac{\alpha}{n-\alpha} \right)^i \frac{\alpha^i}{i!}.$$

Si alors ε et δ sont des quantités satisfaisant à

$$(11) \quad \frac{\varepsilon n}{2} \geq 2w \geq \delta n, \quad (\varepsilon \leq 1),$$

et que nous déterminerons avec plus de précision suivant les cas, on a

$$\frac{n-2w}{n} \leq 1-\delta, \quad \frac{w}{n-\alpha} \leq \frac{\varepsilon}{4} \frac{9}{7} \leq \frac{\varepsilon}{3},$$

et (10) donne

$$\Delta_i \leq \frac{(1-\delta)^{\alpha-2i}}{i!} \left(\frac{\varepsilon \alpha^2}{3(n-\alpha)} \right)^i.$$

Cette formule a lieu même pour $i = 0$, et l'on en conclut, d'après (9)

$$\frac{w}{C_n^{\alpha}} \geq 1 - (1-\delta)^{\alpha} \sum_{i=0}^{k_1} \frac{1}{i!} \frac{1}{(1-\delta)^{2i}} \left(\frac{\varepsilon \alpha^2}{3(n-\alpha)} \right)^i.$$

En posant

$$(12) \quad \alpha\eta = \frac{1}{(1-\delta)^2} \frac{\varepsilon 2^2}{3(n-2)}$$

et remarquant que

$$\sum_0^{k_1} \frac{(\alpha\eta)^i}{i!} \leq e^{\alpha\eta},$$

on aura

$$(13) \quad 1 - \zeta = 1 - (1 - \delta)^\alpha e^{\alpha\eta} \leq \frac{\omega}{C_n^\alpha}.$$

Si l'on pose encore

$$(14) \quad \alpha = \mu n \quad \text{avec} \quad \mu \leq \frac{2}{9},$$

on a

$$(15) \quad \eta = \frac{1}{(1-\delta)^2} \frac{\varepsilon \mu}{3(1-\mu)}$$

et

$$(16) \quad \zeta = [(1 - \delta)e^\eta]^\alpha;$$

il n'y a plus qu'à trouver une limite supérieure de ζ .

a. $u = \frac{n}{4}$. — Supposons $n \geq 22$.

Le plus petit entier ω supérieur ou égal à $\frac{n}{3} = \frac{n}{12}$ est

$$E\left(\frac{n+11}{12}\right) \leq \frac{n+11}{12} \leq \frac{n}{8},$$

dès que $n \geq 22$; on aura donc $\omega \leq \frac{n}{8}$, et l'on peut prendre ici $\varepsilon = \frac{1}{2}$.

D'autre part, $E\left(\frac{n}{4}\right)$ est $\geq E\left(\frac{n+11}{12}\right)$ dès que $\frac{n}{4} \geq \frac{n+11}{12}$, ou $n \geq 6$, et

$\omega = E\left(\frac{n+11}{12}\right) \geq \frac{n}{12}$. Donc ici $\omega \geq \frac{n}{12}$, et l'on peut prendre $\delta = \frac{1}{6}$; alors

$$\eta \leq \frac{36}{25} \frac{1}{6} \frac{\mu}{1-\mu} \leq \frac{6}{25} \frac{2}{7} \leq \frac{12}{175},$$

et l'on vérifie sans peine à l'aide d'une Table de logarithmes népériens que l'on a

$$\log_e \zeta^{-\frac{1}{\alpha}} \geq 0,11374,$$

d'où

$$(17) \quad \zeta \leq e^{-0,11374\alpha}.$$

Cette formule nous donne d'abord $\zeta \leq \frac{3}{4}$, d'où

$$(18) \quad \frac{\omega}{C_n^2} \geq \frac{1}{4},$$

dès que $\alpha \geq 3$; elle montre de plus, puisqu'elle donne

$$(19) \quad \frac{\omega}{C_n^2} \geq 1 - e^{-0,11374\alpha},$$

que l'on peut toujours prendre α assez grand (avec $n \geq \frac{9}{2}\alpha$), pour que $\frac{\omega}{C_n^2}$ soit aussi voisin que l'on veut de l'unité. Enfin l'on a encore, d'après (17),

$$(20) \quad \frac{\omega}{C_n^2} \geq \frac{1}{2},$$

dès que $\alpha \geq 7$.

La formule (16) montre d'ailleurs de suite que, pour une valeur donnée de α , même < 7 , on aurait pu prendre n assez grand pour que μ soit aussi petit qu'on veut, et en particulier pour que $\zeta \leq \frac{1}{2}$, d'où

$$\frac{\omega}{C_n^2} \geq \frac{1}{2},$$

dès que $\alpha \geq 4$.

Ces formules s'appliquent toujours en particulier quand C est deux fois transitif et $n \geq 26$, d'après un théorème de M. Bocher⁽¹⁾.

(1) *Math. Ann.*, t. 40.

b. $u = \frac{n}{3}$. — Supposons $n \geq 23$.

Le plus petit entier supérieur ou égal à $\frac{n}{3} = \frac{n}{9}$ est

$$E\left(\frac{n+8}{9}\right) \leq \frac{n+8}{9} \leq \frac{n}{8},$$

dès que $n \geq 64$: on aura donc $w \leq \frac{n}{8}$, et l'on peut prendre ici $\varepsilon = \frac{1}{2}$.

D'autre part, $E\left(\frac{n}{4}\right)$ est $\geq E\left(\frac{n+8}{9}\right)$ dès que $\frac{n}{4} \geq \frac{n+8}{9}$, ou $n \geq 7$, et $E\left(\frac{n+8}{9}\right) \geq \frac{n}{9}$. Donc ici $w \geq \frac{n}{9}$, et l'on peut prendre $\delta = \frac{2}{9}$; alors

$$\eta \leq \frac{81}{49} \frac{1}{6} \frac{\mu}{1-\mu} = \frac{27}{98} \frac{\mu}{1-\mu} \leq \frac{27}{343};$$

cette limite de η conduirait encore à une formule analogue à (19), mais un peu plus avantageuse et applicable quand $n \geq 64$. On trouve

$$(19 \text{ bis}) \quad \frac{\omega}{C_n^2} \geq 1 - e^{-0,172592}.$$

On peut aussi, en remarquant que $\frac{n+8}{9} \leq \frac{3n}{20}$ dès que $n \geq 23$, prendre $\varepsilon = \frac{3}{5}$ et arriver ainsi à la limite supérieure de η

$$\eta \leq \frac{81}{49} \frac{3}{5} \frac{1}{3} \frac{\mu}{1-\mu} = \frac{81}{245} \frac{\mu}{1-\mu};$$

la formule (16) donne alors

$$\zeta^{-\frac{1}{2}} = (1-\delta)^{-1} e^{-\eta} = \frac{9}{7} e^{-\eta},$$

$$\frac{1}{2} \log \zeta^{-1} = \log \frac{9}{7} - \eta \geq \log \frac{9}{7} - \frac{81}{245} \frac{\mu}{1-\mu},$$

et, pour que $\zeta \leq \frac{1}{2}$, c'est-à-dire $\frac{\omega}{C_n^2} \geq \frac{1}{2}$, il suffira

$$\log \frac{9}{7} - \frac{\log 2}{2} \geq \frac{81}{245} \frac{\mu}{1-\mu}.$$

Cette condition est toujours satisfaite dès que $\mu \leq \frac{2}{9}$, ce qui est le cas ici, pourvu que $\alpha \leq 5$.

Quand $\alpha = 4$ et $n \geq 23$, on remarque que $\mu = \frac{\alpha}{n} \leq \frac{4}{23}$, et l'inégalité a encore lieu.

Enfin, quand $\alpha = 3$, l'inégalité a encore lieu si l'on prend $n \geq 53$, $\mu \leq \frac{3}{53}$.

Nous signalerons l'application de ces résultats quand C est trois fois transitif.

3° Cas où $\alpha = 2$.

La formule (7) nous donnera

$$\frac{\omega}{C_n^2} \geq \frac{1}{2}$$

dès que

$$\frac{4\theta(n-\theta-1)}{n(n-1)} \geq \frac{1}{2}$$

ou

$$(21) \quad 8\theta^2 - 8\theta(n-1) + n(n-1) \leq 0.$$

Il faut que θ soit $\geq$ à la plus petite valeur θ' qui annule le premier membre; or, si $u \geq \frac{n}{3}$, $\frac{u}{2} \geq \frac{n}{6}$, on a $\theta \geq \frac{n}{6} - 1$, et il suffit que le résultat de la substitution de $\frac{n}{6} - 1$ dans le premier membre de (21) à la place de θ donne un résultat ≤ 0 . On est conduit à l'inégalité $n^2 - 51n \geq 0$, qui a lieu pour $n \geq 51$.

On verrait de la même manière que si $u \geq \frac{n}{3}$, on a $\frac{\omega}{C_n^2} \geq \frac{1}{3}$ pour $n \geq 14$, et que si $u \geq \frac{n}{4}$ on a $\frac{\omega}{C_n^2} \geq \frac{1}{3}$ pour $n \geq 31$, et $\frac{\omega}{C_n^2} \geq \frac{1}{4}$ pour $n \geq 18$.

Enfin, si $u \geq \frac{n}{2}$, on a $\frac{\omega}{C_n^2} \geq \frac{1}{2}$ pour $n \geq 3$.

Les principaux résultats obtenus dans les trois cas que nous venons de considérer peuvent être résumés dans le théorème suivant :

THÉORÈME VI. — Soient C un groupe transitif de degré n et de

classe $\geq u$; Γ_α le groupe des substitutions opérées par C entre les combinaisons α à α de ses n lettres ($1 < \alpha < \frac{n}{2}$). Le degré de Γ_α est C_n^α , et sa classe ω satisfait aux inégalités suivantes :

1° Si $u > 2$ et $\alpha \geq \frac{2n}{9}$, on a

$$\omega \geq \frac{1}{2} C_n^\alpha;$$

2° Si $\frac{2}{9}n \geq \alpha \geq 3$, on a :

Pour $u \geq \frac{n}{4}$ et $n \geq 22$

$$\omega \geq \frac{1}{2} C_n^\alpha, \quad \text{si} \quad \alpha \geq 7,$$

$$\omega \geq \frac{1}{4} C_n^\alpha, \quad \text{si} \quad \alpha \geq 3;$$

Pour $u \geq \frac{n}{3}$, si $n \geq 23$ et $\alpha \geq 4$, ou si $n \geq 53$ et $\alpha = 3$,

$$\omega \geq \frac{1}{2} C_n^\alpha.$$

Que u soit $\geq \frac{n}{4}$ ou $\geq \frac{n}{3}$, on a ici

$$\frac{\omega}{C_n^\alpha} \geq 1 - e^{-a\alpha},$$

où a est une constante positive.

3° Si $\alpha = 2$, on a :

Pour $u \geq \frac{n}{4}$ et $n \geq 18$

$$\omega \geq \frac{1}{4} C_n^\alpha;$$

Pour $u \geq \frac{n}{3}$ et $n \geq 51$, ou $u \geq \frac{n}{2}$ et $n \geq 3$,

$$\omega \geq \frac{1}{2} C_n^\alpha.$$

V.

On peut retrouver des résultats analogues, à certains égards plus avantageux que les précédents, ainsi qu'il suit :

Reprenons la substitution

$$U_r = (a'_1 \dots a'_i) \dots (a'_q \dots a'_q)$$

d'ordre premier r , à q cycles, et supposons $qr > \alpha$.

Nous savons qu'une combinaison laissée immobile par U_r comprendra les lettres de k cycles de U_r , et $\alpha - kr$ lettres non déplacées par U_r , avec $k < q$, puisque $qr > \alpha$.

1° Soit $k > 0$. Prenons un des k cycles dont les lettres font partie de la combinaison γ_i que nous considérons et qui est laissée immobile par U_r , $(a'_1 \dots a'_i)$ par exemple. Puisque $k < q$, il y a un cycle, $(a'_q \dots a'_q)$ dont les lettres n'appartiennent pas à γ_i .

Or γ_i est formé des r lettres $a'_1, \dots, a'_i$ et de l'ensemble Z de $\alpha - r$ autres lettres n'appartenant ni au premier, ni au $q^{\text{ième}}$ cycle de U_r . La combinaison γ_q de α lettres formée de Z et des lettres du $q^{\text{ième}}$ cycle de U_r est également laissée immobile par U_r .

Toute combinaison de α lettres laissée immobile par U_r et différente des deux précédentes en diffère soit parce qu'elle ne comprend ni les lettres $a'_1, \dots, a'_i$, ni les lettres $a'_q, \dots, a'_q$, soit parce qu'elle comprend les lettres d'un de ces cycles, mais que l'ensemble Z' des $\alpha - r$ autres lettres comprend quelque lettre non comprise dans Z .

Alors, à chacune des deux combinaisons γ_i et γ_q on peut faire correspondre quelques-unes des combinaisons ψ obtenues en remplaçant dans γ_i une quelconque des lettres $a'_1, \dots, a'_i$ par une quelconque des lettres $a'_q, \dots, a'_q$; on a au moins $r^2 \geq 4$ combinaisons ψ distinctes, déplacées par U_r : nous en ferons correspondre 2 à γ_i et 2 autres à γ_q .

2° Soit $k = 0$: ceci suppose $n - qr \geq \alpha$.

Le même raisonnement n'est plus applicable; mais aux C_{n-qr}^α combinaisons γ' correspondantes, ne comprenant aucune lettre de U_r , nous pouvons faire correspondre toutes les combinaisons ψ' comprenant $\alpha - 1$ des lettres non déplacées par U_r , et une seule des lettres

déplacées par U_r combinaisons qui sont en nombre qr . C_{n-qr}^{x-1} , distinctes, déplacées par U_r et distinctes des combinaisons ψ . On a d'ailleurs

$$qr C_{n-qr}^{x-1} = \frac{xqr}{n-qr-x+1} C_{n-qr}^x.$$

Dès lors, aux Θ_1 combinaisons distinctes analogues à γ_1 et comprenant les lettres d'un au moins des cycles de U_r , on fera correspondre $\Theta'_1 \geq 2\Theta_1$ combinaisons ψ distinctes 2 à 2, soit parce que les deux cycles de U_r , dont elles comprennent des lettres sans les comprendre toutes, ne sont pas les mêmes, soit, quand ils sont les mêmes, parce que les ensembles des $x-r$ autres lettres ne sont pas les mêmes, soit enfin par celles des lettres des deux cycles de U_r dont ils ne comprennent pas toutes les lettres tout en en comprenant quelqu'une.

Aux $\Theta_2 = C_{n-qr}^x$ combinaisons distinctes γ'_1 correspondront au moins

$$\Theta'_2 = \frac{xqr}{n-qr-x+1} \Theta_2$$

combinaisons ψ' distinctes.

Si l'on choisit une quantité $k \geq \frac{1}{2}$ telle que

$$\frac{xqr}{n-qr-x+1} \geq \frac{1}{k},$$

ce qui a lieu, en posant $qr \geq \frac{n}{l}$ ($l > 1$), si $k \geq \frac{l-1}{x}$, on aura

$$\Theta'_2 \geq \frac{1}{k} \Theta_2,$$

et de même

$$\Theta'_1 \geq 2\Theta_1 \geq \frac{1}{k} \Theta_1,$$

par suite

$$C_n^x \geq \Theta_1 + \Theta'_1 + \Theta_2 + \Theta'_2 \geq \left(1 + \frac{1}{k}\right) (\Theta_1 + \Theta_2),$$

ce qui donne

$$\Theta_1 + \Theta_2 \leq \frac{k}{k+1} C_n^x.$$

et la classe ω de Γ_α est telle que

$$\omega \geq C_n^\alpha - \Theta_1 - \Theta_2 \geq \frac{1}{k+1} C_n^\alpha.$$

k est ici un quelconque des nombres satisfaisant à l'inégalité $k \geq \frac{l-1}{2}$: on pourra donc prendre $k = \frac{l-1}{2}$

$$(22) \quad \omega \geq \frac{2}{\alpha + l - 1} C_n^\alpha,$$

en n'oubliant pas que $qr > \alpha$, ce qui a toujours lieu si la classe u du groupe C est $> \alpha$ et $\frac{n}{n} \geq \frac{1}{l}$.

La formule (22) pour de grandes valeurs de α est moins avantageuse que la formule (19) par exemple ; mais il n'en est pas de même pour de petites valeurs de α . Ainsi :

Si $l = 2$, $u \geq \frac{n}{2}$, auquel cas la condition $u > \alpha$ a lieu si $\alpha < \frac{n}{2}$, on a, d'après (22),

$$(23) \quad \omega \geq \frac{2}{\alpha + 1} C_n^\alpha \geq \frac{2}{3} C_n^\alpha.$$

Si $l = 3$, $u \geq \frac{n}{3}$, $\alpha < \frac{n}{3}$, on a, d'après (22),

$$(24) \quad \omega \geq \frac{2}{\alpha + 2} C_n^\alpha \geq \frac{1}{3} C_n^\alpha.$$

On a d'ailleurs également $\omega \geq \frac{1}{3} C_n^\alpha$ quand $\alpha > \frac{n}{3}$ d'après le théorème VI.

Si $l = 4$, $u \geq \frac{n}{4}$, $\alpha < \frac{n}{4}$, on a, d'après (22),

$$(25) \quad \omega \geq \frac{2}{\alpha + 3} C_n^\alpha,$$

d'où

$$\omega \geq \frac{2}{5} C_n^2 \quad \text{si} \quad \alpha = 2,$$

et

$$\omega \geq \frac{1}{2} C_n^2 \quad \text{si} \quad \alpha \geq 3.$$

D'ailleurs, puisque $\frac{n}{4} > \frac{2}{9}n$, d'après le théorème VI, on a $\omega \geq \frac{1}{3} C_n^2$ quand $\alpha \geq \frac{n}{4}$.

Plus généralement on aura, d'après (22), pour $\alpha < u$,

$$\frac{\omega}{C_n^2} \geq \frac{\alpha}{\alpha + l - 1} > \frac{1}{l},$$

si

$$(\alpha - 1)(l - 1) > 0,$$

ce qui a toujours lieu.

Les résultats que nous venons d'obtenir peuvent alors être résumés dans le théorème suivant :

THÉORÈME VII. — Soit C un groupe transitif de degré n et de classe $\geq u \geq \frac{n}{l}$, Γ_α le groupe des substitutions opérées par C entre les combinaisons α à α de ses n lettres $\left(1 < \alpha < \frac{n}{2}\right)$. Le degré de Γ_α est C_n^α , et sa classe ω satisfait aux inégalités suivantes :

1° Si $u \geq \frac{n}{3}$, $l = 2$, on a

$$\frac{\omega}{C_n^2} \geq \frac{2}{3}.$$

2° Si $u \geq \frac{n}{3}$, $l = 3$, on a

$$\frac{\omega}{C_n^2} \geq \frac{1}{2}.$$

3° Si $u \geq \frac{n}{4}$, $l = 4$, on a

$$\frac{\omega}{C_n^2} \geq \frac{2}{5}.$$

et

$$\frac{\omega}{C_n^\alpha} \geq \frac{1}{3}, \quad \text{si} \quad \alpha \geq 3.$$

4° Enfin on a en général pour $\alpha < u$,

$$\frac{\omega}{C_n^\alpha} \geq \frac{\alpha}{\alpha + l - 1} > \frac{1}{l},$$

l pouvant d'ailleurs être pris $= \frac{n}{u}$, par suite

$$\frac{\omega}{C_n^\alpha} > \frac{u}{n}.$$

