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>

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 $a_1, a_2, \ldots, a_n$ $(n > 4)$. 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 $\left(1 < \alpha < \frac{n}{2}\right)$ 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 $a_1, a_2, \ldots, a_\alpha$, D le sous-groupe correspondant de C; D est formé des substitutions de C qui permutent exclusivement entre elles les lettres $a_1, a_2, \ldots, a_\alpha$. 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 $a_1, a_2, \ldots, a_\alpha$ 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 $a_{\alpha+1}, \ldots, a_n$, c'est-à-dire si $k \geq \alpha+1$, ce que nous supposerons.

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 $a_1, a_2, \ldots, a_\alpha$ 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 $a_1, a_2, \ldots, a_\alpha$ 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 $a_1, a_2, \ldots, a_\alpha$ 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_1 deux fois transitif de degré $p_1 + p_2 + \ldots + p_\mu + 1 = P$, avec

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

$p_1 = n - \alpha$ étant un multiple de p_2, p_2 un multiple de p_3, ..., et F_1 renferme des sous-groupes transitifs de degré $p_1, p_1 + p_2, p_1 + p_2 + p_3, \ldots, p_1 + p_2 + \ldots + p_\mu + 1 = P$, dont chacun est contenu dans le suivant, et $P \leq n$, d'où

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

---

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 $\varpi_1, \varpi_2, \ldots, \varpi_z$ sont les diviseurs premiers de $\alpha!$, Γ_α sera primitif si $k \geq \alpha + 2$, ou si $k = \alpha + 1$ et $n - \alpha = l\varpi_1 \varpi_2 \ldots \varpi_z + m$, l étant un entier quelconque, et m un entier, positif ou négatif, premier à $\varpi_1, \varpi_2, \ldots, \varpi_z$.

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*

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

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*

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

où $d_1, \ldots, d_m$ *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 (mod. 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

$$X = |z,\ a'z| \qquad (\text{mod. } p),$$

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

$$Y = \left|z,\ \frac{1}{z}\right| \quad (\text{mod } p),$$

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^μ ou $YX^\mu = \left| z, \frac{\alpha'^\mu}{z} \right|$ (mod 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

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

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

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

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 $\equiv 0$ (mod 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 F 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 $0, \infty$. Que p soit pair ou impair, ces substitutions sont

celles de la forme

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

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

$$i \equiv a_2 i, \qquad j \equiv a_2 j,$$

ou

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

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

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

ou

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

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 $i_1 \equiv a_2 i^{-1}$ 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 $a\beta-b\alpha$ est résidu quadratique (mod 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 $V''=\left|z,\frac{a_2}{z}\right|$ (mod p), où $-a_2$ est résidu quadratique (mod 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 o, ∞ immobile, groupe dérivé du groupe E′ des puissances de la substitution

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

et de

$$Y' = \left|z, \frac{a_2}{z}\right| \pmod p,$$

où $-a_2$ est résidu quadratique (mod 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 o, ∞ 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 $X^{2\mu}$ et

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

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'_2 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 o, ∞, d'autre part entre les $n-2$ autres indices, et toute substitution de F′ qui permute exclusivement entre eux d'une part o, ∞, d'autre part les $n-2$ autres indices, appartient à D′. Donc U remplace l'un des indices o 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 o 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 o avec $\frac{p^m-1}{2}+2=\frac{p^m+3}{2}$ lettres, et

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

où $\mathfrak{K}'=\frac{p^m-1}{2}\lambda$ est l'ordre du groupe des substitutions de F′ laissant o immobile et contenant E′, et divise $(p^m+1)p^m\frac{p^m-1}{2}=\mathfrak{E}'$; 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 $p^m\leqq 9$, ce que nous supposerons 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

$$\mathfrak{f}'=[(p_1k+1)(q_1k+1)+1](p_1k+1)k,$$

où

$$n=(p_1k+1)(q_1k+1)+1,$$

et où k est l'ordre du groupe K des substitutions de F′ qui laissent o 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 $p_1=2$, $\mathfrak{f}'=\mathfrak{E}'$ contrairement à l'hypothèse $F'<C'$; si $p_1=1$, $p_1k+1=1+\frac{p^m-1}{2}=\frac{p^m+1}{2}$ devrait diviser $n-1=p^m$, ce qui est absurde. Donc $p_1=0$, et

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

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

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

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

Si maintenant -1 est résidu, la substitution $Y'X^{2\mu}$ 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 o, ∞ 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 $p^m \leqq 5$.

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 $(\gamma_1\gamma_2)$ ..., 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 o, ∞ comprend un résidu et un non-résidu : si $0 = a'^{2k+1}$ est le non-résidu faisant partie du même système que 1, la considération de X^2 montre que ces systèmes sont

$$1, 0; \quad a'^2, a'^2 0; \quad a'^4, a'^4 0; \quad \ldots; \quad a'^{2\mu}, a'^{2\mu} 0; \quad \ldots.$$

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

Soit $0 \not\equiv -1$; le raisonnement est encore analogue : U n'est pas d'une des formes $X^{2\mu}$ et $Y'X^{2\mu}$. 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 o par i et ∞ par $0i$, avec i différent de o et de ∞, ou o

(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 o 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 o 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 o et de ∞, auxquels sont substitués des systèmes de même forme étant $\leqq 4$ et $\geqq \frac{p^m - 3}{2}$, on a $\frac{p^m - 3}{2} \leqq 4$, $p^m \leqq 11$, 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 $p^m \leqq 11$, 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

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

où σ est un diviseur arbitrairement choisi de m. Ces groupes ne diffèrent de ceux considérés au théorème II que si $m > \sigma \geqq 1$. 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, 2e 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 $C^2_{p^m}$ (ou de degrés $C^2_{2^m}$ et $C^2_{3^m}$ 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 $p^{m\nu}$ dont les m indices sont formés à l'aide de racines d'une congruence irréductible de degré ν.

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^α_n combinaisons α à α des n lettres de C $\left(1 < \alpha < \frac{n}{2}\right)$. 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

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

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

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

k prenant toutes les valeurs entières satisfaisant à

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

et la classe de $\mathrm{U}^{(\alpha)}$ est $\mathrm{C}_n^{\alpha} - \nu_{r,q}$.

Les formules (1) et (2) résolvent complètement le problème de la détermination de la classe de $\mathrm{U}^{(\alpha)}$; 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

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

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

Le sous-groupe des substitutions de C, qui laissent trois lettres arbitrairement choisies immobiles, est semblable au sous-groupe Ψ de C d'ordre $\frac{m}{\tau}$, 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 $\frac{m}{\sigma}$ est impair, et celui où il est pair.

1° Si $\frac{m}{\sigma}$ 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^2_{n-qr}, où $n - qr$ 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 $\frac{m}{\sigma}$. Alors

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

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

le maximum de cette expression s'obtient en prenant pour η la valeur telle que $\frac{m}{\eta\sigma}$ 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^{2m-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 $\frac{m}{\sigma 2^\lambda}$ 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

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

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

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

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* $\left| z, z^{p^\sigma} \right| \pmod p$, *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, $W^{\eta}\left(\eta \text{ diviseur de } \frac{m}{\sigma}\right)$ appartient à C' : la classe est encore $\frac{(p^m-1)(p^m+1)}{2}$.

Si $\frac{m}{\sigma}$ est pair, $W^{\frac{m}{2\sigma}}=\left|z, z^{p^{\frac{m}{2}}}\right| \pmod p$ est d'ordre 2, régulière, et déplace $p^m-p^{\frac{m}{2}}=p^{\frac{m}{2}}\left(p^{\frac{m}{2}}-1\right)$ 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 $\frac{m}{\sigma}$ est $\equiv 0 \pmod 4$ 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 u lettres sont celles qui ont le moins de cycles possibles.*

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

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 $q \geq \frac{u}{3}$.

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

$$\nu_{2,w} = \sum_k C_w^k C_{n-2w}^{\alpha-2k}, \tag{3}$$

k prenant toutes les valeurs entières satisfaisant à

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

Si nous supposons u tel que $w \leq \frac{n}{4}$, 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 w et $E\left(\frac{\alpha}{2}\right)$, on a

$$\nu_{2,w} = \sum_0^{k_1} C_w^k C_{n-2w}^{\alpha-2k}; \tag{5}$$

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

Théorème 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* $\left(1 < \alpha < \frac{n}{2}\right)$. *La classe* ω *de* Γ_α *est telle que*

$$\omega \geq C_n^\alpha - C_{n-2w}^\alpha - C_w^1 C_{n-2w}^{\alpha-1} - C_w^2 C_{n-2w}^{\alpha-2} - \ldots - C_w^{k_1} C_{n-2w}^{\alpha-2k_1}, \tag{6}$$

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

nombres $\frac{u}{3}$ *et* $\mathrm{E}\left(\frac{n}{4}\right)$, *et* k_1 *le plus petit des deux nombres* w *et* $\mathrm{E}\left(\frac{z}{2}\right)$.

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^2_{n-qr} combinaisons 2 à 2 des lettres qu'elle laisse immobiles. Si $r = 2$, U_2 laisse immobiles non seulement les C^2_{n-2q} combinaisons analogues, mais encore les q combinaisons de 2 lettres formées chacune des lettres d'un cycle de U_2, soit $q + C^2_{n-2q}$ 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 $\theta = \mathrm{E}\left(\frac{u}{2}\right)$ cycles, c'est-à-dire qu'une limite supérieure de $\nu_{r,q}$ est ici $\nu_{2,\theta}$. 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*

$$\omega \geq C^2_n - \theta - C^2_{n-2} = \frac{4\theta(n-\theta-1)}{2}, \tag{7}$$

où

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

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 $u \geq \frac{1}{4} n$, 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° *Cas où* $\frac{n}{2} > \alpha \geq \frac{2n}{9}$.

Si l'on suppose seulement $u > 2$, 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

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

et

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

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° *Cas où* $\frac{2n}{9} \geq \alpha \geq 3$.

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

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

on a

$$\frac{\omega}{C_n^\alpha} \geq 1 - \sum_0^{k_1} i \Delta_i. \tag{9}$$

(¹) *Math. Ann.*, t. 40.

Or

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

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

puisque $a < b$ entraîne $\frac{a-j}{b-j} \leqq \frac{a}{b}$ pour $j \geqq 0$;

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

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

$$(\alpha-i)\dots(\alpha-2i+1) \leqq \quad (\alpha-i)^i \quad \leqq \alpha^i,$$

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

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

Si alors ε et δ sont des quantités satisfaisant à

$$\frac{\varepsilon n}{2} \geqq 2w \geqq \delta n, \qquad (\varepsilon \leqq 1), \tag{11}$$

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

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

et (10) donne

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

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

$$\frac{\omega}{C_n^\alpha} \geqq 1 - (1-\delta)^\alpha \sum_0^{k_1} \frac{1}{i!} \frac{1}{(1-\delta)^{2i}} \left(\frac{\varepsilon\alpha^2}{3(n-\alpha)}\right)^i.$$

En posant

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

et remarquant que

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

on aura

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

Si l'on pose encore

$$\alpha = \mu n \qquad \text{avec} \qquad \mu \leqq \frac{2}{9}, \tag{14}$$

on a

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

et

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

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

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

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

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

dès que $n \geqq 22$; on aura donc $w \leqq \frac{n}{8}$, et l'on peut prendre ici $\varepsilon = \frac{1}{2}$. D'autre part, $\mathrm{E}\left(\frac{n}{4}\right)$ est $\geqq \mathrm{E}\left(\frac{n+11}{12}\right)$ dès que $\frac{n}{4} \geqq \frac{n+11}{12}$, ou $n \geqq 6$, et $w = \mathrm{E}\left(\frac{n+11}{12}\right) \geqq \frac{n}{12}$. Donc ici $w \geqq \frac{n}{12}$, et l'on peut prendre $\delta = \frac{1}{6}$; alors

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

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

$$\zeta \leq e^{-0,11374\alpha}. \tag{17}$$

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

$$\frac{\omega}{C_n^\alpha} \geq \frac{1}{7}, \tag{18}$$

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

$$\frac{\omega}{C_n^\alpha} \geq 1 - e^{-0,11374\alpha}, \tag{19}$$

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

$$\frac{\omega}{C_n^\alpha} > \frac{1}{2}, \tag{20}$$

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

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

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. Bochert (1).

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

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

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

$$\frac{\omega}{C_n^{\alpha}} \geq 1 - e^{-0,172594}. \tag{19 bis}$$

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

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

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

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

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

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

Quand $\alpha = 4$ et $n \geqq 23$, 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 $n \geqq 53$, $\mu \leqq \frac{3}{53}$.

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

3° *Cas où* $\alpha = 2$.

La formule (7) nous donnera

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

dès que

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

ou

$$8\theta^2 - 8\theta(n-1) + n(n-1) \leqq 0. \tag{21}$$

Il faut que θ soit $\geqq$ à la plus petite valeur θ' qui annule le premier membre; or, si $u \geqq \frac{n}{3}$, $\frac{u}{2} \geqq \frac{n}{6}$, on a $\theta \geqq \frac{n}{6} - 1$, 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 $\leqq 0$. On est conduit à l'inégalité $n^2 - 51n \geqq 0$, qui a lieu pour $n \geqq 51$.

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

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

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 $\geqq u$; 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* $u > 2$ *et* $\alpha \geqq \frac{2n}{9}$, *on a*

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

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

Pour $u \geqq \frac{n}{4}$ *et* $n \geqq 22$

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

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

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

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

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

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

où a *est une constante positive.*

3° *Si* $\alpha = 2$, *on a :*

Pour $u \geqq \frac{n}{4}$ *et* $n \geqq 18$

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

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

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

V.

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

Reprenons la substitution

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

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_1 que nous considérons et qui est laissée immobile par U_r, $(a_1^1 \dots a_1^r)$ par exemple. Puisque $k < q$, il y a un cycle, $(a_q^1 \dots a_q^r)$ dont les lettres n'appartiennent pas à γ_1.

Or γ_1 est formé des r lettres $a_1^1, \dots, a_1^r$ 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 $a_1^1, \dots, a_1^r$, ni les lettres $a_q^1, \dots, a_q^r$, 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_1 et γ_q on peut faire correspondre quelques-unes des combinaisons ψ obtenues en remplaçant dans γ_1 une quelconque des lettres $a_1^1, \dots, a_1^r$ par une quelconque des lettres $a_q^1, \dots, a_q^r$; on a au moins $r^2 \geqq 4$ combinaisons ψ distinctes, déplacées par U_r : nous en ferons correspondre 2 à γ_1 et 2 autres à γ_q.

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

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. $C_{n-qr}^{\alpha-1}$, distinctes, déplacées par U_r et distinctes des combinaisons ψ. On a d'ailleurs

$$qr\,C_{n-qr}^{\alpha-1} = \frac{\alpha qr}{n-qr-\alpha+1}\,C_{n-qr}^{\alpha}.$$

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 $\alpha - r$ 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 $\Theta_2 = C_{n-qr}^{\alpha}$ combinaisons distinctes γ' correspondront au moins

$$\Theta_2' = \frac{\alpha qr}{n-qr-\alpha+1}\Theta_2$$

combinaisons ψ' distinctes.

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

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

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

$$C_n^{\alpha} \geq \Theta_1 + \Theta_1' + \Theta_2 + \Theta_2' \geq \left(1+\frac{1}{k}\right)(\Theta_1+\Theta_2),$$

ce qui donne

$$\Theta_1 + \Theta_2 \leq \frac{k}{k+1}\,C_n^{\alpha},$$

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 $k \geq \frac{l-1}{\alpha}$: on pourra donc prendre $k = \frac{l-1}{\alpha}$

$$\omega \geq \frac{\alpha}{\alpha + l - 1} C_n^\alpha, \tag{22}$$

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

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),

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

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

$$\omega \geq \frac{\alpha}{\alpha + 2} C_n^\alpha \geq \frac{1}{2} C_n^\alpha. \tag{24}$$

On a d'ailleurs également $\omega \geq \frac{1}{2} C_n^\alpha$ 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),

$$\omega \geq \frac{\alpha}{\alpha + 3} C_n^\alpha, \tag{25}$$

d'où

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

et

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

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

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

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

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* G *un groupe transitif de degré* n *et de classe* $\geq u \geq \frac{n}{l}$, Γ_α *le groupe des substitutions opérées par* G *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*

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

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

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

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

$$\frac{\omega}{C_n^\alpha} \geq \frac{2}{5},$$

et

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

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*

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