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

ED. MAILLET

Sur les isomorphes holoédriques et transitifs des groupes symétriques ou alternés

Journal de mathématiques pures et appliquées 5^e série, tome 1 (1895), p. 5-34.
<http://www.numdam.org/item?id=JMPA_1895_5_1__5_0>

JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES.

Sur les isomorphes holoédriques et transitifs des groupes symétriques ou alternés;

PAR M. ED. MAILLET,
Ingénieur des Ponts et Chaussées à Toulouse.

INTRODUCTION.

Soit T un sous-groupe d'ordre $\mathfrak{t}$ du groupe symétrique ou alterné S de n éléments $a_1, a_2, \ldots, a_n$ d'ordre s : supposons $s > 2\mathfrak{t}$ et $n > 4$. Considérons un isomorphe S′ holoédrique et régulier (1) de S : au groupe T correspond une répartition des lettres de S′ en systèmes de non-primitivité $\mathfrak{t}$ à $\mathfrak{t}$, et le groupe G des substitutions opérées par S′ entre les systèmes de cette répartition est transitif, de degré $\rho = \frac{s}{\mathfrak{t}}$, et holoédriquement isomorphe à S, le groupe T correspondant

(1) C'est-à-dire transitif et d'ordre égal à son degré (Klein).

au groupe H des substitutions de G qui laissent une même lettre de G immobile (¹).

Réciproquement, tout isomorphe holoédrique de S est de cette forme (²).

Dès lors, T étant donné, G se trouve complètement déterminé : nous dirons que G est l'isomorphe de S issu de S et correspondant à T.

Les groupes transitifs de ce genre ont été étudiés par MM. Kronecker, Jordan et Netto.

M. A. Bochert a montré (³) que, si T ne contient pas de substitution circulaire d'ordre 3, on a

$$\text{Pour le groupe symétrique.....} \quad \rho \geq \left[E\left(\frac{n+1}{2}\right)\right]!$$

$$\text{Pour le groupe alterné.....} \quad \rho \geq \frac{1}{2}\left\{\left[E\left(\frac{n+1}{2}\right)\right]!\right\}$$

$E\left(\frac{n+1}{2}\right)$ étant le plus grand entier contenu dans $\frac{n+1}{2}$.

Ce théorème nous a permis d'établir, au sujet des groupes G définis précédemment, quelques propriétés qui font l'objet de ce Mémoire, et que l'on peut résumer ainsi :

G n'est qu'une fois transitif; il ne peut contenir de groupe de degré $< \rho$ transitif entre les lettres qu'il déplace, ou de substitution circulaire (⁴). *Les exceptions n'ont lieu que pour $n \leq 6$ quand* S *est le groupe symétrique, et pour $n \leq 8$ quand* S *est le groupe alterné.*

(¹) JORDAN, *Traité des substitutions*, p. 58-60; W. DYCK, *Math. Ann.*, t. XXII, p. 90 et suiv.; *voir* aussi notre *Thèse de Doctorat*, p. 12. Nous supposons toujours que G ne se confonde pas avec S.

(²) *Voir* notre *Thèse de Doctorat*, p. 16-17.

(³) *Math. Ann.*, t. XXXIII, p. 584.

(⁴) Cette dernière propriété a été établie par M. Netto dans le cas d'une substitution circulaire d'ordre p^m (p premier) (*J. für Math.*, t. C, p. 436; 1887).

PREMIÈRE PARTIE.

S EST UN GROUPE SYMÉTRIQUE.

I. — Des groupes primitifs G isomorphes au groupe symétrique.

Supposons que le groupe G, défini tout à l'heure, soit primitif; eu égard au théorème de M. A. Bochert que nous avons énoncé, nous distinguerons trois cas : les deux cas où T contient une substitution circulaire d'ordre 2 ou 3 et est ou n'est pas transitif, et le cas où T ne contient pas de substitution circulaire d'ordre 2 ou 3.

a. T *contient une substitution circulaire d'ordre* 2 *ou* 3 *et est transitif.*

Considérons une substitution circulaire d'ordre 2 ou 3 contenue dans T, puis les substitutions circulaires d'ordre 2 ou 3 contenues dans T et ayant quelque lettre commune avec la précédente, puis celles qui ont quelque lettre commune avec les précédentes, et ainsi de suite. Le groupe L dérivé de ces substitutions est transitif entre les l lettres qu'il déplace et dérivé de toutes les substitutions circulaires d'ordre 2 ou 3 contenues dans T et qui déplacent une de ces l lettres. D'après un théorème de M. Hölder (1), L se confond avec le groupe symétrique ou alterné de l éléments : si l'on avait $l = n$, T contiendrait le groupe alterné de n éléments et il faudrait $\rho \leqq 2$, ce que nous avons supposé ne pas avoir lieu; donc $2 \leqq l < n$.

T, étant transitif, contiendra un transformé L′ de L par une substitution de T, lequel sera $\neq$ L et déplacera quelque lettre non déplacée par L. Si L et L′ avaient quelque lettre commune, il y aurait dans L′

(1) *Math. Ann.*, t. XL, p. 55 et suiv. Le théorème de M. Hölder, établi pour un groupe transitif dérivé de substitutions circulaires d'ordre 3, s'établit aussi facilement quand le groupe est dérivé de substitutions circulaires d'ordre 2.

une substitution circulaire d'ordre 2 ou 3 non contenue dans L et déplaçant une lettre de L, puisque L′ est le groupe symétrique ou alterné entre les l lettres qu'il déplace. Mais, d'après le mode de formation de L, il n'y a dans T aucune substitution circulaire d'ordre 2 ou 3 non contenue dans L et qui déplace quelque lettre de L. Donc L′ et L n'ont aucune lettre commune et n'ont d'autre substitution commune que l'unité.

On voit de même que les transformés distincts de L par T n'ont deux à deux aucune substitution commune, à part l'unité, ni aucune lettre commune.

T étant transitif et de degré n, et L de degré l, L a exactement $\frac{n}{l}$ transformés distincts par les substitutions de T : le groupe M dérivé de ces $\frac{n}{l}$ transformés est permutable aux substitutions de T; l divise n.

Dès lors T admet (1) une répartition de ses lettres en systèmes de non-primitivité l à l; par suite, il est contenu dans le groupe K formé de l'ensemble des substitutions de S qui admettent cette répartition. Or, G étant primitif, on sait (2) que H est maximum dans G, par suite T maximum dans S : T ne peut donc être contenu dans K, qui est plus petit que S, que si T = K.

Voyons comment est formé K; S étant le groupe symétrique entre n lettres, K contient en particulier le groupe M_1 dérivé des $\frac{n}{l}$ groupes symétriques de l lettres correspondant aux $\frac{n}{l}$ groupes symétriques ou alternés transformés de L que nous avons trouvés tout à l'heure, et M_1 est d'ordre

$$\mathfrak{M}_1 = (l!)^{\frac{n}{l}},$$

et permutable aux substitutions de K. Toute substitution de K qui laisse immobiles les $\frac{n}{l}$ systèmes de la répartition considérée fait partie

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

(2) W. DYCK, *Math. Ann.*, t. XXII, p. 102. *Voir* aussi notre *Thèse de Doctorat*, p. 18.

de M_1. L'ordre de K est donc

$$\mathfrak{K} = \mathfrak{M}_1 \mathfrak{H},$$

$\mathfrak{H}$ étant l'ordre du groupe Θ des substitutions opérées par K entre les systèmes. Or, S étant le groupe symétrique entre n éléments, K devra contenir une substitution permutant ces systèmes d'une manière quelconque choisie *a priori* et, par suite, Θ sera un groupe symétrique entre les $\frac{n}{l}$ systèmes. Donc

$$\mathfrak{H} = \left(\frac{n}{l}\right)!$$

et

$$\mathfrak{G} = \mathfrak{K} = \left(\frac{n}{l}\right)! (l!)^{\frac{n}{l}}.$$

Ceci posé, la condition nécessaire et suffisante pour que G soit primitif est que H soit maximum dans G ou K maximum dans S. Nous allons voir que cette condition est remplie.

Il nous suffira d'établir que le groupe R dérivé de K et d'une substitution de S non contenue dans K se confond avec S.

Vérifions d'abord que R est primitif.

Supposons qu'il n'en soit pas ainsi et que R admette une répartition de ses lettres r à r en systèmes de non-primitivité, avec $n > r > 1$. R étant $>$ K, cette répartition ne saurait se confondre avec la répartition l à l considérée tout à l'heure et admise par K, puisque K est formé de l'ensemble des substitutions de S qui admettent cette répartition. K admettra les deux répartitions : on pourra toujours trouver un système de r lettres et un système de l lettres ayant quelque lettre commune sans se confondre : soit s le nombre des lettres communes à ces deux systèmes; on sait (¹) et l'on voit facilement qu'à cet ensemble de s lettres correspondra une répartition des lettres de K s à s, et $s \leqq l$. Chaque système de s lettres est contenu dans un système de l lettres; mais K contenant le groupe symétrique entre les l lettres de chaque système de l lettres, groupe qui est primitif entre ces l lettres, s devra être égal à l ou à 1.

(¹) JORDAN, *Traité des substitutions*, p. 34.

Si l'on avait $s = l$, il faudrait $r > l$; de plus, un système de l lettres qui a quelque lettre commune avec un système de r lettres y est contenu tout entier, puisque $s = l$: chaque système de r lettres est donc formé d'un même nombre de systèmes de l lettres. Soient α, β, γ, ... les systèmes de l lettres, $\alpha_1, \ldots, \alpha_l$ les lettres de α, $\beta_1, \ldots, \beta_l$ celles de β, $\gamma_1, \ldots, \gamma_l$ celles de γ; K contiendra la substitution

$$(\alpha_1\beta_1\gamma_1)(\alpha_2\beta_2\gamma_2)\ldots(\alpha_l\beta_l\gamma_l),$$

où α et β appartiennent à un même système de r lettres, γ à un autre système de r lettres, puisque l'on a ici

$$r \geq 2l, \qquad n \geq 2r.$$

Cette substitution est de la forme $(\alpha\beta\gamma)$ entre les systèmes de l lettres et montre immédiatement que K et R n'admettent pas la répartition supposée en systèmes de r lettres. On n'a donc pas $s = l$.

Si l'on avait $s = 1$, une substitution quelconque $(ab\ldots)\ldots$, contenue dans un des groupes symétriques de l lettres que K renferme, ne déplace d'autres lettres que celles d'un même système de l lettres. Chacune des lettres a, b, ... déplacée par cette substitution fait partie d'un système différent de r lettres, puisque $s = 1$; or une substitution qui admet une répartition en systèmes de r lettres ne peut remplacer une lettre d'un système de r lettres par une lettre d'un autre système de r lettres que si elle déplace toutes les lettres des deux systèmes. Cela ne pourra donc avoir lieu pour $(ab, \ldots), \ldots$ que si $r = 1$, contrairement à l'hypothèse. On n'a donc pas $s = 1$.

R ne peut dès lors admettre aucune répartition de ses lettres en systèmes de non-primitivité avec $n > r > 1$, c'est-à-dire que R est primitif.

Mais R contient une substitution circulaire d'ordre 2 : on en conclut immédiatement que R contient le groupe symétrique de n éléments (1), et, par suite, qu'il se confond avec S.

Le groupe K, choisi comme nous l'avons indiqué, est donc maxi-

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

mum dans S : en posant $K = T$, le groupe G correspondant est toujours primitif et l'on peut dire :

La condition nécessaire et suffisante pour que à un groupe T *transitif entre n lettres et contenant une substitution circulaire d'ordre* 2 *ou* 3, *corresponde un groupe* G *primitif, holoédriquement isomorphe à* S *et issu de* S, *est que* T *soit formé de l'ensemble des substitutions de* S *admettant une même répartition des n lettres de* S *en systèmes de non-primitivité l à l* ($2 \leq l < n$ *et l divisant n*).

Je dis que, en général, les groupes G obtenus ainsi ne sont qu'une fois transitifs : pour le montrer, indiquons un autre moyen de former ces groupes G.

On peut former avec les n lettres de S C_n^l combinaisons de l lettres; on peut ensuite assembler ces C_n^l combinaisons $\frac{n}{l}$ à $\frac{n}{l}$, de façon que les nouveaux assemblages obtenus, que nous appellerons des *hypersystèmes,* contiennent chacun exactement les n lettres de S. Il faudra et il suffira pour cela que les $\frac{n}{l}$ combinaisons entrant dans un hypersystème n'aient deux à deux aucune lettre commune. Les hypersystèmes se distingueront alors les uns des autres, non par les lettres qu'ils renferment, lettres qui sont les mêmes, mais par les $\frac{n}{l}$ combinaisons de l lettres qu'ils renferment.

Chaque substitution de S remplacera chaque combinaison de l lettres par une autre distincte ou non, et, par suite, chaque hypersystème par un autre hypersystème, distinct ou non. Considérons le groupe G_1 des substitutions opérées par S entre ces hypersystèmes.

S étant symétrique contiendra toujours une substitution remplaçant les n lettres par ces mêmes n lettres disposées dans un ordre arbitraire, et, *a fortiori,* un hypersystème quelconque par un hypersystème quelconque. Donc G_1 est transitif.

Nous avons vu précédemment que le groupe T, contenu dans S, admettait une répartition de ses lettres l à l, et que toute substitution admettant cette répartition était contenue dans T. A chaque système

de cette répartition on peut faire correspondre une combinaison de l lettres, et, par suite, à la répartition elle-même, un hypersystème et un seul. Toutes les substitutions de T laisseront donc cet hypersystème immobile. Réciproquement, toute substitution de S laissant cet hypersystème immobile remplace une combinaison de cet hypersystème par une combinaison de cet hypersystème, et admet la répartition considérée, par suite fait partie de T. Le groupe H_1 de G_1 correspondant à T est donc formé de l'ensemble des substitutions de G_1 qui laissent cet hypersystème immobile.

Dès lors, G et G_1 se confondent, à la notation près (1), puisque G et G_1 sont transitifs, holoédriquement isomorphes, et que H et H_1 correspondent tous deux à T; G_1 est donc primitif; je dis qu'il n'est qu'une fois transitif, c'est-à-dire que G ne sera qu'une fois transitif.

En effet, soit

$$(1) \qquad a_1, a_2, \ldots, a_l; a_{l+1}, \ldots, a_{2l}; \ldots; a_{n-l+1}, \ldots, a_n$$

la répartition en systèmes de l lettres admise par T : le groupe T laisse l'hypersystème (1) immobile. La condition nécessaire et suffisante pour que G_1 soit deux fois transitif est que H_1 soit transitif, c'est-à-dire que T permute transitivement entre eux les hypersystèmes autres que l'hypersystème (1).

Soient

$$(2) \qquad a'_1, a'_2, \ldots, a'_l; a'_{l+1}, \ldots, a'_{2l}; \ldots; a'_{n-l+1}, \ldots, a'_n;$$

$$(3) \qquad a''_1, a''_2, \ldots, a''_l; a''_{l+1}, \ldots, a''_{2l}; \ldots; a''_{n-l+1}, \ldots, a''_n$$

---

(1) *Voir* notre *Thèse de Doctorat*, p. 15-17, th. V. On conclut, en effet, immédiatement de ce th. V la propriété suivante :

Soient G *et* G_1 *deux groupes transitifs holoédriquement isomorphes, de même degré;* H *et* H_1 *les groupes de* G *et de* G_1 *formés chacun de l'ensemble des substitutions de* G *et de* G_1 *respectivement qui laissent une lettre de* G *et de* G_1 *immobile; si* H_1 *est le groupe de* G_1 *que l'isomorphisme de* G *et de* G_1 *fait correspondre à* H *dans* G, *les groupes* G *et* G_1 *sont identiques à la notation près.*

Voir aussi JORDAN, *Traité des Substitutions*, p. 58-60.

deux hypersystèmes différents de l'hypersystème (1) : T devra renfermer une substitution qui remplace (2) par (3).

T, admettant la répartition (1) en systèmes, remplace tout hypersystème renfermant le système $a_1, a_2, \ldots, a_l$ par un hypersystème renfermant un des systèmes (1). Les hypersystèmes qui ont quelque système ou combinaison commun avec l'hypersystème (1) sont donc permutés exclusivement entre eux par les substitutions de T, et, pour que H_1 soit transitif, il faut que tous les hypersystèmes autres que (1) aient quelque système de l lettres commun avec l'hypersystème (1), ou qu'ils n'en aient aucun.

Or, si $\frac{n}{l} > 2$, on aura toujours un hypersystème différent de (1), et ayant en commun avec (1) un système, par exemple $a_1, a_2, \ldots, a_l$. D'autre part, dans ce cas, on peut assembler les systèmes ou combinaisons de (1) deux à deux ou trois à trois, puis dans chaque assemblage faire passer, par permutation, certaines lettres d'une combinaison à l'autre, de façon que le nouvel hypersystème obtenu n'ait avec (1) aucune combinaison commune. Ainsi, par exemple, l'assemblage

$$(4) \quad a_1, a_2, \ldots, a_l; \quad a_{l+1}, a_{l+2}, \ldots, a_{2l}; \quad a_{2l+1}, a_{2l+2}, \ldots, a_{3l}$$

conduirait à l'assemblage

$$(5) \quad a_{l+1}, a_2, \ldots, a_l; \quad a_{2l+1}, a_{l+2}, \ldots, a_{2l}; \quad a_1, a_{2l+2}, \ldots, a_{3l};$$

et l'hypersystème formé des assemblages analogues à (5) n'aurait avec l'hypersystème (1) aucune combinaison commune. Donc, quand $n > 2l$, il y aura à la fois des hypersystèmes $\neq$ de l'hypersystème (1) et ayant avec lui quelque combinaison de l lettres commune, et des hypersystèmes n'ayant avec l'hypersystème (1) aucune combinaison commune. Dans ce cas, d'après ce qui précède, H_1 ne sera pas transitif.

Soit $n = 2l$.

L'hypersystème (1) devient

$$(6) \qquad a_1, a_2, \ldots, a_l; \quad a_{l+1}\ a_{l+2}, \ldots, a_{2l}.$$

Considérons l'hypersystème

$$(7) \qquad a_1, a_{l+2}, \ldots, a_{2l}; \quad a_{l+1}, a_2, \ldots, a_l,$$

où chaque combinaison a respectivement 1 et $l-1$ éléments communs avec chacune des combinaisons (6). T admettant la répartition en systèmes (6) remplacera l'hypersystème (7) par des hypersystèmes jouissant des mêmes propriétés; par suite, T ne pourra remplacer (7) par un hypersystème dont les combinaisons aient respectivement 2 et $l-2$ éléments communs avec celles de (6), sauf si l'on a

$$2 = l-1, \qquad l-2 = 1$$

ou

$$l = 3$$

(on ne peut d'ailleurs avoir $l < 3$, puisque $n = 2l$ donnerait $n \leq 4$ contrairement à l'hypothèse).

H_1 ne pourra donc être transitif que si l'on a à la fois $n = 2l$, $l = 3$, c'est-à-dire $n = 6$.

Quand $n = 6$ et $l = 3$, on a les hypersystèmes

1.....	$a_1, a_2, a_3;$	a_4, a_5, a_6	6.....	$a_1, a_3, a_5;$	a_2, a_4, a_6
2.....	$a_1, a_2, a_4;$	a_3, a_5, a_6	7.....	$a_1, a_3, a_6;$	a_2, a_4, a_5
3.....	$a_1, a_2, a_5;$	a_3, a_4, a_6	8.....	$a_1, a_4, a_5;$	a_2, a_3, a_6
4.....	$a_1, a_2, a_6;$	a_3, a_4, a_5	9.....	$a_1, a_4, a_6;$	a_2, a_3, a_5
5.....	$a_1, a_3, a_4;$	a_2, a_5, a_6	0.....	$a_1, a_5, a_6;$	a_2, a_3, a_4

que nous numérotons 1, 2, 3, 4, 5, 6, 7, 8, 9, 0 et qui sont en nombre $\frac{6}{2!(3!)} = 10$.

Le groupe T est dérivé des substitutions qui laissent immobile l'hypersystème 1, c'est-à-dire des substitutions

$$(a_1a_2), \quad (a_2a_3), \quad (a_4a_5), \quad (a_5a_6), \quad (a_1a_4)\,(a_2a_5)\,(a_3a_6),$$

auxquelles correspondent dans H_1 les substitutions

$$h_1 = (0,5)(6,9)(7,8); \quad h_2 = (2,5)(3,6)(4,7);$$
$$h_3 = (2,3)(5,6)(0,9); \quad h_4 = (3,4)(6,7)(8,9);$$
$$h_5 = (2,8)(3,7)(5,9).$$

H_1 est dérivé de ces substitutions; il est de degré 9 et transitif, car

les substitutions

$$h_3^2,\ h_3,\ h_3h_4,\ h_2,\ h_2h_3,\ h_2h_3h_4,\ h_2h_3h_4h_1,\ h_2h_3h_1,\ h_2h_4$$

permettent de remplacer respectivement 2 par un quelconque des nombres 2, 3, 4, 5, 6, 7, 8, 9, 0.

S étant dérivé des substitutions (a_1a_2), (a_2a_3), (a_4a_5), (a_5, a_6) et (a_3a_4), G_1 est dérivé des substitutions

$$h_1,\ h_2,\ h_3,\ h_4 \quad \text{et} \quad h_6=(1,2)(6,8)(7,9);$$

il est deux fois transitif et d'ordre $10.9.8$; on voit facilement qu'il n'est pas trois fois transitif. C'est un groupe connu (¹).

Ainsi, sauf le cas de $n=6$, les groupes G_1 et, par suite, les groupes G ne sont qu'une fois transitifs. Ces groupes n'existent pas quand n est premier, et seulement dans ce cas, puisque l est un diviseur arbitrairement choisi de n avec $n > l \geqq 2$.

Le cas des groupes G primitifs correspondant à un groupe T transitif, mais non primitif, se ramène toujours à celui que nous venons d'examiner, car ce groupe T admettant une répartition de ses lettres en systèmes de non-primitivité l à l est toujours contenu dans le groupe K formé de l'ensemble des substitutions de S qui admettent cette répartition. D'après ce qui précède, K contient une substitution circulaire d'ordre 2 ou 3 ; T est maximum dans S, puisque G est primitif et, par suite, se confond avec K.

Nous pouvons donc dire :

Si l'on forme avec les n lettres de S C_n^l *combinaisons l à l, et que l'on assemble ces* C_n^l *combinaisons* $\frac{n}{l}$ *à* $\frac{n}{l}$ *de façon que chaque assemblage ainsi obtenu forme un hypersystème contenant exactement les n lettres de* S; *si de plus on considère comme distincts deux hypersystèmes qui ne sont pas formés avec les mêmes* $\frac{n}{l}$ *combinaisons; les groupes* G_1 *formés par les substitutions que* S *opère entre*

(¹) Cole, *Quarterly Journal*, mai 1894, p. 44.

ces hypersystèmes coïncident, à la notation près, avec les groupes primitifs G *obtenus précédemment.*

G *n'est qu'une fois transitif : la seule exception a lieu pour* $n = 6$ *où* G *est un groupe de degré* 10, *d'ordre* $10.9.8$, *deux fois transitif, et dérivé des substitutions*

$$(0,5)(6,9)(7,8);\ (2,5)(3,6)(4,7);\ (2,3)(5,6)(0,9);$$
$$(3,4)(6,7)(8,9);\ (1,2)(6,8)(7,9),$$

entre les nombres 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

La condition nécessaire et suffisante pour que ces groupes existent est que n ne soit pas premier.

On peut définir aussi les groupes de cette catégorie en disant que ce sont, parmi les groupes G primitifs considérés dans notre Mémoire, ceux qui correspondent au cas où T est transitif sans être primitif.

b. T *n'est pas transitif entre n lettres.*

Il est inutile de spécifier en outre que T contient une substitution circulaire d'ordre 2 ou 3, car T est encore ici maximum dans S, puisque G est primitif, et T contiendra forcément une substitution circulaire d'ordre 3, puisque $n > 4$.

Si T permute exclusivement entre elles α des lettres de S, il devra contenir le groupe symétrique des substitutions entre ces α lettres et le groupe symétrique entre les $n - \alpha$ autres lettres, sans quoi T ne serait pas maximum dans S.

T contiendra donc le groupe K dérivé du groupe symétrique entre les α lettres $a_1, a_2, \ldots, a_\alpha$ et du groupe symétrique entre les $n - \alpha$ autres lettres $a_{\alpha+1}, \ldots, a_n$. Je dis qu'en général K est maximum dans S, et, par suite, que T = K.

En effet, il suffira d'établir qu'en général le groupe R dérivé de K et d'une substitution de S qui n'y est pas contenue se confond avec S.

Or R est transitif, car la substitution adjointe à K pour former R n'est pas contenue dans K, et, par suite, remplace une des lettres $a_1, \ldots, a_\alpha$ par une des lettres $a_{\alpha+1}, \ldots, a_n$, ou inversement.

R est primitif, si $\alpha \neq \frac{n}{2}$: en effet, on peut, puisque un des deux

nombres α, $n-\alpha$ est $<\frac{n}{2}$, supposer que α soit celui des deux qui est $<\frac{n}{2}$, sans quoi, en prenant $n-\alpha=\alpha'$, on raisonnerait sur α' comme nous allons le faire sur α. Supposons que R ne soit pas primitif, quand $\alpha<\frac{n}{2}$: R étant transitif admettra une répartition de ses lettres i à i, avec $2\leqq i\leqq\frac{n}{2}$. Le groupe symétrique entre $n-\alpha$ lettres contenues dans R admet cette répartition; mais il est primitif entre les lettres qu'il permute; donc, si ce groupe symétrique déplace deux lettres d'un même système, toutes ses lettres, en nombre $n-\alpha$, appartiennent à un même système, et il faudrait $i\geqq n-\alpha>\frac{n}{2}$, ce qui n'a pas lieu; si chacune des $n-\alpha$ lettres de ce groupe symétrique appartenait à un système différent, il y aurait au moins $n-\alpha$ systèmes, et l'on aurait $i<2$, ce qui n'a pas lieu. Il faut, par suite, supposer R primitif quand $\alpha\neq\frac{n}{2}$. R contenant des substitutions circulaires d'ordre 3 et 2 se confond avec le groupe symétrique, d'après un théorème de M. Jordan déjà utilisé.

Ainsi, quand $\alpha\neq\frac{n}{2}$, on aura

$$T=K.$$

Quand $\alpha=\frac{n}{2}$, K n'est pas maximum dans S, puisque l'on peut lui adjoindre une des substitutions (1) (n étant pair)

$$\left(a_1\,a_{\frac{n}{2}+1}\right)\cdots\left(a_{\frac{n}{2}}a_n\right)$$

ou

$$\left(a_1\,a_{\frac{n}{2}+1}\,a_2\,a_{\frac{n}{2}+2}\right)\left(a_3\,a_{\frac{n}{2}+3}\right)\cdots\left(a_{\frac{n}{2}}a_n\right),$$

sans que le groupe R dérivé de K et de cette substitution se confonde

(1) Remarquons que, n étant pair, une de ces deux substitutions est toujours contenue dans le groupe alterné de n éléments; cette observation est utile quand on veut étudier par les mêmes procédés les groupes G primitifs issus du groupe alterné, ainsi que nous l'indiquerons plus loin.

avec S, puisque l'ordre de R sera le double de l'ordre de K; T contiendrait ainsi une substitution de S non contenue dans K; mais cette substitution remplacerait une des lettres $a_1, \ldots, a_{\frac{n}{2}}$ par une des lettres $a_{\frac{n}{2}+1}, \ldots, a_{\frac{n}{2}}$ et T devrait être transitif contrairement à l'hypothèse que nous faisons ici.

Nous pouvons donc dire :

La condition nécessaire et suffisante pour que à un groupe T *non transitif et de degré n, corresponde un groupe* G *primitif, holoédriquement isomorphe à* S *et issu de* S, *est que* T *soit dérivé du groupe symétrique entre* α *des n lettres de* S *et du groupe symétrique entre les* $n - \alpha$ *autres, avec* $1 < \alpha \neq \frac{n}{2}$.

On voit de suite que l'hypothèse $\alpha > \frac{n}{2}$ donnera les mêmes groupes G que l'hypothèse $\alpha < \frac{n}{2}$.

Je dis que les groupes G obtenus ainsi sont une seule fois transitifs : pour le montrer, indiquons d'abord un autre moyen de former ces groupes G.

Considérons les C_n^α produits ou combinaisons des lettres $a_1, \ldots, a_n$, α à α, α étant $\neq \frac{n}{2}$. Chaque substitution de S remplacera chacune de ces C_n^α combinaisons par une de ces mêmes C_n^α combinaisons, et, par suite, opérera entre ces C_n^α combinaisons une certaine substitution. Soit G_1 le groupe formé par ces substitutions.

S étant symétrique contient toujours une substitution remplaçant une des C_n^α combinaisons par une autre arbitrairement choisie, et, par suite, G_1 est transitif.

Le groupe K dérivé du groupe symétrique entre $a_1, \ldots, a_\alpha$ et du groupe symétrique entre $a_{\alpha+1}, \ldots, a_n$ est évidemment formé de l'ensemble des substitutions de S qui laissent immobile la combinaison $a_1 a_2 \ldots a_\alpha$ et $K = T$ puisque $\alpha \neq \frac{n}{2}$. Alors le groupe H_1 formé de l'ensemble des substitutions de G_1 qui laissent une lettre de G_1 immobile, et le groupe H formé de l'ensemble des substitutions de G qui

laissent une lettre de G immobile sont les groupes que l'isomorphisme holoédrique des groupes G et G_1 avec S fait correspondre à T; G et G_1 sont transitifs et de même degré : donc G et G_1 sont identiques à la notation près, et nous n'avons plus qu'à montrer que G_1 est une seule fois transitif.

Si G_1 était deux fois transitif, H_1 serait transitif, et T devrait permuter transitivement toutes les combinaisons différentes de la combinaison $a_1 a_2 \dots a_\alpha$. Or T permute exclusivement entre elles d'une part les lettres $a_1, a_2, \dots, a_\alpha$, d'autre part les lettres $a_{\alpha+1}, \dots, a_n$: T permute donc exclusivement entre elles les combinaisons renfermant exactement k des lettres $a_1, a_2, \dots, a_\alpha$; H_1 ne sera donc pas transitif si k est susceptible de deux valeurs, ce qui aura toujours lieu, puisque $k \leqq \alpha$, dès que $\alpha > 1$. L'hypothèse $\alpha = 1$ devant être écartée, parce qu'alors G se confondrait avec S; H_1 n'est pas transitif : G_1 et G ne sont donc qu'une fois transitifs.

Si l'on forme (1) *avec les n lettres de* S *les* C_n^α *combinaisons possibles* α *à* α, *les groupes* G_1 *formés par les substitutions que* S *opère entre ces* C_n^α *combinaisons coïncident, à la notation près, avec les groupes primitifs* G *obtenus précédemment* $\left(\alpha \text{ étant} \neq \frac{n}{2}\right)$.

Par suite G *n'est qu'une fois transitif.*

c. T *ne contient pas de substitution circulaire d'ordre* 2 *ou* 3, *ou, ce qui revient au même,* T *est primitif.*

Nous avons vu que le cas où T n'est pas primitif se ramenait à l'un des deux cas précédents; si d'ailleurs T est primitif, il ne contient pas de substitution circulaire d'ordre 2 ou 3, sans quoi, d'après un théorème connu, il contiendrait le groupe alterné de n éléments, et il faudrait $\rho = \frac{8}{6} \leqq 2$, contrairement à l'hypothèse faite au début du Mémoire.

(1) Ces groupes ont déjà été cités par M. JORDAN (*Comptes rendus*, 2e semestre 1872, p. 1755) et par nous (*Thèse de Doctorat*, p. 22). *Voir* aussi FROBENIUS, *J. für Math.*, t. CI, p. 287.

On a, d'après M. A. Bochert,

$$(8)\qquad \begin{cases} \text{Pour } n \text{ pair} \ldots\ldots\ldots\ldots\ldots & \rho \geqq \left(\frac{n}{2}\right)! \\ \text{Pour } n \text{ impair} \ldots\ldots\ldots\ldots\ldots & \rho \geqq \left(\frac{n+1}{2}\right)! \end{cases}$$

Ces relations permettent de montrer assez simplement que G ne peut être trois fois transitif que pour de petites valeurs de n.

Si en effet G était trois fois transitif il faudrait

$$(9)\qquad \text{ordre } G = \mathfrak{G} = n! \qquad \geqq \rho(\rho-1)(\rho-2)$$

et l'on voit facilement que ceci n'est possible, eu égard aux relations (8), que pour de petites valeurs de n.

De la même manière on pourrait voir que G ne peut renfermer un groupe transitif de degré $< \rho - 1$, sauf pour de petites valenrs de n. En effet, M. Jordan a montré le théorème suivant (¹) :

THÉORÈME. — *Soit* G′ *un groupe primitif et de degré* ρ *contenant un groupe* B *dont les substitutions ne déplacent que p lettres, et les permutent transitivement :* G′ *renferme un groupe de degré* $p+q+r+s+\ldots+1 = P \leqq \rho$, *deux fois transitif; on a*

$$p > q > r > s > \ldots > 1,$$

p étant un multiple de q, q un multiple de r, ...; G′ *renferme une suite de groupes transitifs entre les lettres qu'ils déplacent et de degrés* p, $p+q$, $p+q+r$, ..., $p+q+r+\ldots+1$, *chacun d'eux étant contenu dans ceux qui le suivent. Par suite* G′ *est* $(\rho - P + 2)$ *fois transitif.*

(¹) *Journal de Liouville*, p. 384-389; 1871. Nous modifions l'énoncé eu égard à l'objet que nous avons en vue, mais les résultats donnés ci-dessus sont entièrement établis par M. Jordan dans sa démonstration.

Un cas particulier de ce théorème a été établi par M. NETTO (*J. für Math.*, t. CIII, p. 333; 1888).

Si le groupe transitif que nous considérons renfermait un groupe transitif de degré $< p - 1$, il serait alors $p - P + 2$ fois transitif, et, sauf pour de petites valeurs de n, il faut $p - P + 2 \leq 2$, c'est-à-dire $p = P$.

En remarquant qu'ici $q > 0$, puisque $p < p - 1$ et $p = P$, on est conduit à une inégalité de la forme (9) qui donne en tout cas

$$(10) \qquad \mathcal{G} = n! > \frac{p^3}{2}$$

dès que n n'est pas trop petit, inégalité qui est impossible dès que n surpasse une limite finie, eu égard aux relations (8).

Mais, plus généralement, on peut montrer que G n'est qu'une fois transitif si $n > 5$, en s'appuyant sur le lemme suivant :

LEMME I. — *Dans un groupe* G′ *deux fois transitif quelconque, de degré* p *et d'ordre* $\mathcal{G}'$, *une substitution quelconque a toujours au moins* $p - 1$ *transformées distinctes; par suite, le nombre des substitutions du groupe échangeables à une substitution quelconque de ce groupe est* $\leq \frac{\mathcal{G}'}{p-1}$.

Soient G′ un groupe deux fois transitif, de degré p, et d'ordre

$$\mathcal{G}' = p(p-1)k;$$

$$\Sigma' = (ab\ldots)\ldots$$

une substitution de G′. Les substitutions qui laissent la lettre a immobile forment un groupe H′, transitif entre $p - 1$ lettres, et d'ordre

$$\mathcal{G}' = (p-1)k.$$

Soit

$$\Theta' = (bc\ldots)\ldots$$

une substitution de H′. Ce groupe étant transitif entre les $p - 1$ lettres b, c, ..., on peut choisir Θ' de façon que c soit une lettre arbitraire différente de a et b. Or

$$\Sigma'_1 = \Theta'^{-1}\Sigma'\Theta' = (ac\ldots)\ldots.$$

D'après ce qu'on vient de dire, en faisant varier Θ', on peut faire prendre à c, par suite à Σ'_1, $\rho - 2$ valeurs différentes. En tenant compte de Σ', on voit que Σ' a au moins $\rho - 1$ transformées distinctes par les substitutions de G'.

Soient φ le nombre des transformées distinctes de Σ' par les substitutions de G', ψ l'ordre du groupe des substitutions de G' échangeables à Σ'. On a

$$\mathcal{G}' = \varphi\psi, \tag{11}$$

et, puisque $\varphi \geqq \rho - 1$, on obtient

$$\psi \leqq \frac{\mathcal{G}'}{\rho - 1}. \tag{12}$$

C. Q. F. D.

Ceci posé, supposons que le groupe G soit deux fois transitif, et $G' = G$.

Soient Σ la substitution de S correspondante à Σ'; σ l'ordre de Σ, p son degré. On a évidemment pour Σ, et, par suite, pour Σ',

$$\psi \geqq (n-p)!\,\sigma, \tag{13}$$

ce qui donne, d'après (12),

$$\mathcal{G}' = n! \geqq (n-p)!\,\sigma(\rho - 1). \tag{14}$$

S contenant une substitution circulaire d'ordre 2, pour laquelle $\sigma = 2$, $p = 2$, la relation (14) donne

$$(n-2)!\,2(\rho - 1) \leqq n!$$

ou

$$\rho - 1 \leqq \frac{n(n-1)}{2}. \tag{15}$$

Le rapprochement des relations (8) et (15) donne alors

$$\text{(16)} \quad \begin{cases} \text{Pour } n \text{ pair} \ldots\ldots & \dfrac{n(n-1)}{2} \geqq \left(\dfrac{n}{2}\right)! - 1, \\ \text{Pour } n \text{ impair} \ldots & \dfrac{n(n-1)}{2} \geqq \left(\dfrac{n+1}{2}\right)! - 1. \end{cases}$$

n étant >4, on voit facilement que ces inégalités n'ont lieu que pour n égal à 8, 6 ou 5.

La discussion de ces trois cas montre que G n'est deux fois transitif que quand $n = 5$ pour $\rho = 6$.

On peut donc dire :

Un groupe G *primitif, holoédriquement isomorphe à* S, *issu de* S *et correspondant à un groupe* T *de degré n primitif, n'est qu'une fois transitif; les seules exceptions ont lieu quand* $n = 5$ *pour* $\rho = 6$.

Des trois cas a, b, c que nous venons de distinguer nous pouvons conclure que, quel que soit T, les groupes primitifs G ne sont qu'une fois transitifs quand $n > 6$.

En observant que les groupes transitifs G ne peuvent être deux fois transitifs que s'ils sont primitifs, nous en concluons le théorème suivant :

Théorème I. — *En général, un groupe* G *transitif, holoédriquement isomorphe à* S, *issu de* S *et correspondant à un groupe* T *de* S, *n'est qu'une fois transitif; les seules exceptions, correspondant à des groupes connus, ont lieu quand* $n \leqq 6$ *pour des valeurs du degré* ρ *de* G *égales à* 10 *et* 6.

Ce qui précède va nous permettre d'établir la propriété suivante :

Les groupes primitifs G *ne peuvent contenir de substitution circulaire si* $n > 6$.

Supposons qu'un groupe primitif G contienne une substitution circulaire U' d'ordre h.

Soit (U') le groupe formé des puissances de U' : si $h < \rho$, G contient un groupe (U') de degré h transitif entre h lettres. D'après un théorème de M. Jordan dont nous avons donné l'énoncé précédemment, G serait deux fois transitif, ce qui n'a pas lieu, d'après le théorème I, quand $n > 6$.

Supposons donc $h = \rho$.

Les substitutions de (U'), à part l'unité, déplacent ρ lettres. Soient dès lors U la substitution de S correspondante à U', (U) le groupe des

puissances de U. La substitution U est d'ordre ρ; elle ne pourrait être circulaire que si son degré était au moins égal à ρ, et il faudrait $\rho \leqq n$, ce qui n'a pas lieu. Il y a donc λ lettres, avec $\lambda \leqq \frac{n}{2}$, que (U) permute exclusivement entre elles.

Nous distinguerons encore trois cas :

a'. T *est transitif et contient une substitution circulaire d'ordre* 2 *ou* 3.

On sait que S permute transitivement les hypersystèmes en opérant entre eux les substitutions de G. Le groupe (U') étant transitif entre les ρ lettres de G, le groupe (U) devra permuter transitivement les hypersystèmes. Ce groupe, permutant exclusivement entre elles λ lettres de S avec $\lambda \leqq \frac{n}{2}$, et une de ses substitutions remplaçant une combinaison de l lettres qui a exactement λ_1 lettres communes avec ces λ lettres par une combinaison qui a également λ_1 lettres communes avec ces λ lettres, cette substitution remplacera un hypersystème dont les combinaisons ont respectivement $\lambda_1, \lambda_2, \ldots$ lettres communes avec ces λ lettres par un hypersystème dont les combinaisons ont respectivement $\lambda_1, \lambda_2, \ldots$ lettres communes avec ces λ lettres, et $\lambda_1 + \lambda_2 + \ldots = \lambda$. Le groupe (U) ne permuterait donc transitivement les hypersystèmes que s'il n'existait qu'un seul système de nombres $\lambda_1, \lambda_2, \ldots$ satisfaisant à l'égalité $\lambda_1 + \lambda_2 + \ldots = \lambda$. Il est bien évident, puisque $\frac{n}{2} \geqq \lambda \geqq 2$ et $l \geqq 2$, que, parmi les nombres $\lambda_1, \lambda_2, \ldots$, on pourra toujours en trouver deux, par exemple λ_1 et $\lambda_2 < l$, qui soient $\neq 0$. Ces nombres étant tous positifs, on aura au moins les deux systèmes $\lambda_1, \lambda_2, \ldots$ et $\lambda_1 - 1, \lambda_2 + 1, \ldots$, où les nombres λ_i avec $i > 2$ ont la même valeur. Donc (U') ne pourrait être transitif entre les ρ lettres, et, par suite, U' n'existe pas.

Nous supposons ici, bien entendu, $n > 6$.

b'. T *n'est pas transitif.*

(U) doit permuter transitivement les C_n^{α} combinaisons des n lettres α à α que S permute transitivement. Toute substitution de (U) remplacera une combinaison renfermant exactement λ_1 des λ lettres pré-

citées par une autre jouissant de la même propriété. Les nombres λ et α étant ≥ 2, on aura toujours au moins deux valeurs de λ_i. On en conclut que (U') ne pourrait être transitif, et, par suite, que U' n'existe pas.

c'. T *ne contient pas de substitution circulaire d'ordre* 2 *ou* 3.

On pourra appliquer les relations (8).

Soit U_i une substitution de S à ν cycles d'ordres respectifs m_1, m_2, ..., m_ν; h_i son ordre. On aura

$$h_i \leq m_1 m_2 \dots m_\nu. \tag{17}$$

Nous allons chercher une limite supérieure de la valeur de h_i, quel que soit U_i, soit une limite supérieure de $m_1 m_2 \dots m_\nu$.

Si l'on avait $m_1 + m_2 + \dots + m_\nu < n$, il y aurait évidemment dans S une substitution à ν cycles d'ordres respectifs $m_1 + 1$, m_2, ..., m_ν pour laquelle ce produit serait plus grand que pour U_i. La substitution U_i, pour laquelle $m_1 m_2 \dots m_\nu$ a la plus grande valeur possible, est donc telle que

$$m_1 + m_2 + \dots + m_\nu = n. \tag{18}$$

Quand on se donne ν, on voit facilement que le produit des quantités m_1, m_2, ..., m_ν, qui satisfont à (18) et sont positives, est toujours au plus égal à la valeur de ce produit où l'on suppose $m_1, m_2, \dots, m_\nu$ entiers ou non, mais égaux, et, par suite, égaux à $\frac{n}{\nu}$. On aura donc pour toute valeur de ν

$$m_1 m_2 \dots m_\nu \leq \left(\frac{n}{\nu}\right)^\nu. \tag{19}$$

Pour avoir une limite supérieure de $m_1 m_2 \dots m_\nu$, quel que soit U_i ou ν, il suffit d'avoir une limite supérieure de $\left(\frac{n}{\nu}\right)^\nu$.

Or, quand dans cette expression on considère ν comme variant d'une manière continue et restant > 0, et qu'on prend la dérivée

$$\left(\frac{n}{\nu}\right)^\nu \left(\log_e \frac{n}{\nu} - 1\right),$$

on voit facilement qu'il y a un maximum pour $n = e\nu$, et, par suite, que

$$\left(\frac{n}{\nu}\right)^{\nu} \leqq e^{\frac{n}{e}}.$$

Cette inégalité, rapprochée de (17) et (19), donne

$$h_1 \leqq e^{\frac{n}{e}},$$

ce qui donne *a fortiori*, pour la substitution U,

$$h = \rho \leqq e^{\frac{n}{e}},$$

et, à cause de (8),

$$(20) \qquad \begin{cases} \text{pour } n \text{ pair } \left(\frac{n}{2}\right)! \leqq e^{\frac{n}{e}}, \\ \text{pour } n \text{ impair } \left(\frac{n+1}{2}\right)! \leqq e^{\frac{n}{e}}. \end{cases}$$

Pour montrer que U ne peut exister, il suffit de montrer que (20) est impossible.

Or, on voit facilement que ces inégalités n'ont lieu que pour $n \leqq 6$.

En résumé, dans les trois cas a', b', c' que nous venons de traiter, U′ ne peut exister si $n > 6$. Donc les groupes primitifs G ne peuvent contenir de substitution circulaire si $n > 6$.

II. — Des groupes transitifs G non primitifs isomorphes au groupe symétrique.

D'après ce que nous avons vu précédemment, quand un groupe G est primitif et que $n > 6$, il ne peut contenir un sous-groupe de degré $< \rho$ transitif entre les lettres qu'il permute; car, d'après un théorème de M. Jordan énoncé plus haut, G serait deux fois transitif, ce qui est contraire au théorème I quand $n > 6$.

On peut se demander si la même propriété existe quand G est transitif sans être primitif.

Supposons que G soit transitif sans être primitif, et contienne un groupe K de degré $< \rho$ transitif entre les lettres qu'il permute.

Considérons une répartition maxima des lettres de G en systèmes de non-primitivité, c'est-à-dire une répartition telle qu'il n'y en ait aucune autre dont chaque système puisse être formé par la réunion de plusieurs systèmes de la première. On sait (1), et l'on voit facilement, que les substitutions opérées par G entre les systèmes de la répartition maxima forment un groupe primitif, que nous désignerons par G'.

Soit H le groupe des substitutions de G qui permutent exclusivement entre elles les lettres d'un des systèmes de cette répartition. Le groupe K étant de degré $< \rho$ laissera immobile quelque lettre de G, et, par suite, permutera exclusivement entre elles les lettres d'un système; il fera donc partie de H ou d'un de ses transformés par les substitutions de G : supposons que ce soit de H, par exemple.

Si l'une des lettres déplacées par K appartient au même système qu'une lettre laissée immobile par K, le groupe K permute exclusivement entre elles les lettres de ce système en en déplaçant quelques-unes. Comme il est transitif entre les lettres qu'il déplace, il ne déplace que des lettres de ce système. Aux substitutions de K correspond dans le groupe G' la substitution 1 et l'ordre $\mathcal{G}'$ de G' est $<$ l'ordre $\mathcal{G}$ de G : G étant le groupe symétrique, il faut $\mathcal{G}' = 2$, puisque $n > 4$. Il n'y a que deux systèmes, et K déplace les lettres d'un seul système.

Si aucune des lettres déplacées par K n'appartient au même système qu'une lettre qu'il laisse immobile, ou bien H contiendra un groupe L permutable aux substitutions de G, ou il n'en contiendra pas. Dans le premier cas, ce groupe L permutera exclusivement entre elles les lettres de chaque système de la répartition maxima considérée, comme on le voit facilement, et aura pour correspondant dans G' l'unité, en sorte que $\mathcal{G}' < \mathcal{G}$, d'où $\mathcal{G}' = 2$: il y aura encore deux systèmes, K ne déplaçant que les lettres d'un seul système. Dans le second cas, $\mathcal{G}' = \mathcal{G}$: le groupe K' correspondant à K dans G' est d'ordre $\mathfrak{K}' =$ ordre de K $= \mathfrak{K}$, transitif, et de degré évidemment plus petit que le degré ρ' de G'.

(1) *Voir* notre *Thèse de Doctorat*, p. 19.

1° $\mathcal{G}' = 2$. — Le groupe H d'ordre $\mathcal{G}$ est holoédriquement isomorphe au groupe alterné de n éléments et laisse immobile un des systèmes, par suite, les deux. Les substitutions que H opère entre les lettres de chaque système forment un groupe isomorphe à H, par suite, d'ordre $\mathcal{G}$ ou 1, puisque H est simple (1). Pour le système dont K déplace les lettres, ce sera évidemment $\mathcal{G}$, puisque $\mathfrak{K} > 1$; pour l'autre, au contraire, ce sera évidemment 1, puisque $\frac{\mathcal{G}}{\mathfrak{K}} < \mathcal{G}$. Dès lors, le groupe H ne déplacerait que les lettres d'un seul système, et, par suite, ne serait pas permutable aux substitutions de G, qui est transitif entre les systèmes. On n'a donc pas $\mathcal{G}' = 2$.

2° $\mathcal{G}' = \mathcal{G}$. — Le groupe G′ serait primitif, holoédriquement isomorphe au groupe symétrique G, et contiendrait un groupe K′ de degré plus petit que ρ' et transitif entre les lettres qu'il permute. Nous avons vu que, quand $n > 6$, cela ne peut avoir lieu, à moins que G′ ne se confonde avec le groupe symétrique de n éléments. Supposons qu'il en soit ainsi : le groupe H′ de G′ correspondant à H est le groupe symétrique de $n - 1$ éléments.

Or, G étant transitif, H permute transitivement les lettres du système qu'il laisse immobile, lettres que K ne déplace pas. H opère entre les lettres de ce système les substitutions d'un groupe H_1 d'ordre $\mathcal{G}_1$ isomorphe à H et d'ordre $\leq \frac{\mathcal{G}}{\mathfrak{K}} < \mathcal{G}$. Le groupe H′ étant symétrique entre $n - 1$ éléments, et H contenant un groupe d'ordre $\frac{\mathcal{G}}{\mathcal{G}_1}$ permutable à ses substitutions, on aura, quand $n > 5$, $\mathcal{G} = \frac{\mathcal{G}}{2}\mathcal{G}_1$, c'est-à-dire $\mathcal{G}_1 = 2$. Chaque système comprendra dès lors deux lettres, et, comme il y a n systèmes, puisque G′ est de degré n, on aura $\rho = 2n$.

Mais H contient un groupe M formé de toutes les substitutions de H qui ne déplacent pas les lettres du système que H laisse immobile et M est d'ordre $\mathfrak{M} = \frac{\mathcal{G}}{2}$. M contient K, et son correspondant M′ dans G′ se confond avec le groupe alterné de $n - 1$ éléments, puisque $n > 5$. G′ renfermant le groupe alterné de n éléments, qui contient M′,

(1) JORDAN, *Traité des substitutions*, p. 56 et 66.

G renferme un groupe H_2 d'ordre $\frac{G}{2}$, contenant M et K, isomorphe au groupe alterné de n éléments, et permutable aux substitutions de G.

Si H_2 est transitif entre $2n$ lettres, il contient un groupe d'ordre $\frac{G}{2}\frac{1}{2n}$ formé de l'ensemble de ses substitutions qui laissent une même lettre immobile, et l'on peut toujours choisir cette lettre de façon que ce groupe soit contenu dans M. Le groupe M' contiendrait donc un groupe d'ordre $\frac{G}{2}\frac{1}{2n} = \frac{6}{4}$ moitié moindre que l'ordre de M', ce qui est absurde puisque M' est le groupe alterné de $n-1$ éléments et que $n > 5$.

Si H_2 n'est pas transitif, G admet une répartition de ses lettres en deux systèmes de non-primitivité, H_2 permutant exclusivement entre elles les lettres de chaque système (¹). En raisonnant sur H_2 et sur cette répartition comme nous l'avons fait sur H et sur la répartition correspondante, on retombe sur le cas où $G' = 2$, cas que nous avons écarté.

Nous pouvons par suite conclure :

THÉORÈME II. — *Un groupe* G, *transitif, holoédriquement isomorphe à* S, *issu de* S *et correspondant à un groupe* T *de* S, *ne peut contenir un groupe* K *transitif entre les lettres qu'il déplace, et de degré plus petit que celui de* G, *quand* $n > 6$.

De même, nous avons vu que, quand G est primitif, il ne peut contenir de substitution circulaire si $n > 6$. On peut encore se demander si la même propriété existe quand G est transitif sans être primitif.

Nous allons d'abord établir le lemme suivant.

LEMME II. — *Un groupe transitif ne peut renfermer de substitution circulaire d'ordre h que s'il est primitif ou composé avec un sous-groupe d'ordre non premier à h.*

Soit Γ un groupe transitif, non primitif, renfermant une substitution circulaire U d'ordre h. Considérons une répartition maxima en systèmes de non-primitivité admise par Γ, et soient Γ' le groupe des

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

substitutions opérées par Γ entre les systèmes, U′ la substitution d'ordre h' de Γ′ correspondant à U : Γ′ est primitif (¹).

Si l'on a $h' < h$, l'isomorphisme des deux groupes ne peut être holoédrique : au sous-groupe de Γ formé des puissances de $U^{\frac{h}{h'}}$ correspond dans Γ′ la substitution 1 ; Γ est composé (²) avec un sous-groupe qui contient $U^{\frac{h}{h'}}$ et dont l'ordre est divisible par $\frac{h}{h'}$, c'est-à-dire non premier à h.

Supposons maintenant $h = h'$: U′ est la substitution que U opère entre les systèmes de la répartition considérée. Le groupe des puissances de U étant transitif entre les lettres de Γ que U déplace, et *a fortiori* entre les systèmes que U déplace, le groupe des puissances de U′ sera transitif entre les lettres de Γ′ que U′ déplace, et U′ sera aussi une substitution circulaire ; mais le nombre des systèmes que U déplace étant évidemment plus petit que le nombre des lettres de Γ qu'elle déplace, le degré de U′, par suite son ordre, devrait être plus petit que celui de U, contrairement à l'hypothèse $h' = h$. Cette hypothèse doit donc être écartée. C. Q. F. D.

Ceci posé, considérons un groupe G, holoédriquement isomorphe à S, transitif, sans être primitif, et supposons qu'il contienne une substitution circulaire U d'ordre h.

D'après le théorème II, on ne peut avoir $h < \rho$, ρ étant le degré de G, quand $n > 6$.

Soit alors $h = \rho$: on a $h > n$.

Considérons une répartition maxima en systèmes de non-primitivité admise par G, et soit G′ le groupe des substitutions opérées par G entre les systèmes ; d'après le lemme II, G′ est d'ordre plus petit que celui de G, sans quoi G serait primitif et renfermerait une substitution circulaire, ce que nous avons vu être impossible quand $n > 6$. On en conclut facilement que G′ est d'ordre 2, quand $n > 6$, c'est-à-dire que la répartition admet deux systèmes. Le groupe H, formé par l'ensemble des substitutions de G qui laissent immobile un des systèmes,

(¹) *Voir* notre *Thèse de Doctorat*, p. 19.

(²) JORDAN, *Traité des substitutions*, p. 56.

les laissera tous deux immobiles, et sera d'ordre $\frac{G}{2}$. Il ne contiendra pas U qui permute entre eux les deux systèmes, mais il contiendra U^2, d'ordre $\frac{\rho}{2}$, et le groupe des puissances de U^2 permute transitivement les lettres de chaque système, U^2 opérant entre elles une substitution circulaire. Soit H_1 le groupe des substitutions opérées par H entre les lettres d'un de ces systèmes : il est de degré $\frac{\rho}{2}$ et transitif, isomorphe à H, et, puisque H est simple et permutable aux substitutions de G, holoédriquement isomorphe à H et au groupe alterné de n éléments. D'après le théorème VI établi plus loin, H_1 devant ici contenir une substitution circulaire d'ordre $\frac{\rho}{2}$ se confondra avec le groupe alterné de n éléments quand $n > 8$, et l'on aura

$$\rho = 2n$$

quand $n > 8$. Il en sera évidemment de même pour le groupe H_2 des substitutions opérées par H entre les lettres de l'autre système.

Quand n est égal à 8 ou à 7, les diverses valeurs possibles de ρ s'écartent facilement en remarquant que $h = \rho$ et que $\rho \leq 15$ pour $n = 8$ et $\rho \leq 12$ pour $n = 7$.

Il ne nous reste donc à examiner que le cas où $\rho = 2n$, H_1 étant un groupe alterné de n éléments.

Le sous-groupe de S qui correspond à H est le groupe alterné de n éléments et celui qui correspond au groupe K des substitutions de G et H laissant une même lettre de G immobile est un groupe alterné de $n - 1$ éléments.

Si V est la substitution de S correspondant à U, V est d'ordre $\rho = 2n$: U étant une substitution circulaire d'ordre ρ, les substitutions de G échangeables à U sont les puissances de U, et de même les substitutions de S échangeables à V sont les puissances de V. Donc V n'est pas circulaire, puisque S ne contient pas de substitution circulaire d'ordre $> n$ et que le nombre de substitutions de S échangeables à V est $2n$: V contient plusieurs cycles.

Si V contenait deux cycles de même ordre, $(a_1, a_2, \ldots, a_\lambda)$, $(b_1, b_2, \ldots, b_\lambda)$, ..., S contiendrait la substitution $(a_1, a_2, \ldots, a_\lambda)$

échangeable à V et qui n'est pas une puissance de V. Ceci est impossible d'après ce qui précède, et les ordres $m_1, m_2, \ldots, m_k$ des cycles de V, avec $k \geq 2$, sont différents.

D'autre part, ni U, ni ses puissances, à part l'unité, ne sont contenues soit dans K, soit dans un de ses transformés par les substitutions de G, puisque U est une substitution circulaire d'ordre ρ. Par suite, ni V, ni ses puissances, à part l'unité, ne peuvent être contenus dans les groupes correspondants de S, c'est-à-dire dans un groupe alterné de $n-1$ éléments.

Or, si m_1, par exemple, est impair, la substitution de S formée par le cycle de V qui est d'ordre m_1 sera échangeable à V, devra, par suite, être une puissance de V et sera contenue dans un groupe alterné de $n-1$ éléments de S, puisque m_1 est impair et $< n$. Ceci est impossible d'après ce qui précède.

Si m_1 et m_2 sont pairs, on a $m_1 \neq m_2$, et, par exemple, $m_1 < m_2$: V^{m_1} est différent de l'unité, déplace au plus $n - m_1$ lettres, est contenue dans un groupe alterné de $n-1$ éléments, puisque m_1 est pair. Ceci est encore impossible d'après ce qui précède.

On voit donc que, en tout cas, V ne peut exister; il en est de même de U et l'on en conclut :

THÉORÈME III. — *Un groupe* G, *transitif, holoédriquement isomorphe à* S, *issu de* S, *et correspondant à un groupe* T *de* S, *ne peut contenir de substitution circulaire quand* $n > 6$.

SECONDE PARTIE.

S EST UN GROUPE ALTERNÉ.

Les raisonnements étant de tous points semblables à ceux qui précèdent, il nous suffira à peu près d'énoncer les résultats.

Les groupes primitifs G se subdivisent encore en trois catégories :

Première catégorie. — T est transitif sans être primitif (ici T contient une substitution circulaire d'ordre 3, mais non une d'ordre 2).

Deuxième catégorie. — T est intransitif.

Troisième catégorie. — T est primitif.

Pour les deux premières catégories G sera formé de l'ensemble des substitutions du groupe analogue correspondant au cas du groupe symétrique et qui correspondent dans le groupe symétrique à des substitutions paires (¹).

On peut dire :

THÉORÈME IV. — *En général,* G *n'est qu'une fois transitif : les seules exceptions, correspondant à des groupes connus, ont lieu quand* $n \leq 8$, *pour des valeurs de* ρ *égales à* 15, 10 *et* 6.

La discussion des cas particuliers que ne permettent pas d'écarter la relation de M. Bochert et la relation (13) du lemme I se fait assez facilement en s'appuyant sur les propriétés connues des groupes primitifs.

Que S soit symétrique ou alterné, on voit, en effet, quand T est primitif :

Que, si p est un nombre premier $\leq n - 3$, p divisera ρ ;

Que, si n est premier, ρ sera premier à n ;

Que n divisera $\frac{n!}{\rho}$ ou $\frac{n!}{2\rho}$ respectivement.

On a également cette propriété :

THÉORÈME V. — G *ne peut contenir un groupe* K, *de degré* $< \rho$, *transitif entre les lettres qu'il déplace, quand* $n > 8$.

Enfin, on peut dire également :

THÉORÈME VI. — G *ne peut renfermer de substitution circulaire quand* $n > 8$.

(¹) C'est-à-dire contenues dans le groupe alterné.

Si G renferme une substitution circulaire, d'après le lemme II, il doit être primitif puisque le groupe alterné est simple, et cette substitution circulaire est d'ordre et de degré p, quand $n > 8$, d'après le théorème V.

Quand G est primitif, la marche à suivre est la même que dans le cas où S est le groupe symétrique.

Pour $n = 8$, il existe un groupe G deux fois transitif, de degré 15, d'ordre $15.14.12.8$, renfermant une substitution circulaire d'ordre 15, correspondant à la substitution $(a_1 a_2 a_3 a_4 a_5)(a_6 a_7 a_8)$ du groupe alterné de huit éléments. Ce groupe G est le groupe linéaire (1) du degré 2^4 (mod. 2).

Pour $n = 7$, il n'existe aucun groupe G renfermant une substitution circulaire.

---

(1) JORDAN, *Traité des substitutions*, p. 380-382.