

# BULLETIN DE LA S. M. F.

ED. MAILLET

## **Note sur les groupes de substitutions**

*Bulletin de la S. M. F.*, tome 24 (1896), p. 85-96

[http://www.numdam.org/item?id=BSMF\\_1896\\_\\_24\\_\\_85\\_0](http://www.numdam.org/item?id=BSMF_1896__24__85_0)

© Bulletin de la S. M. F., 1896, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

NOTE SUR LES GROUPES DE SUBSTITUTIONS;

Par M. ED. MAILLET.

Nous nous proposons de donner ici :

1° Quelques indications sur les sous-groupes transitifs des isomorphes holoédriques des groupes symétriques ou alternés;

2° Une relation entre le degré, la classe et l'ordre de certains groupes primitifs;

3° Quelques propriétés des groupes transitifs de classe  $ef$ ,  $e$  et  $f$  étant premiers et impairs.

I.

Soit  $D$  un groupe de substitutions, dérivé de deux de ses sous-groupes  $A$  et  $B$ , tous deux  $< D$  : supposons  $A$  et  $B$  échangeables <sup>(1)</sup>. Si  $d$ ,  $a$  et  $a'$ ,  $b$  et  $b'$  désignent des substitutions de  $D$ ,  $A$ ,  $B$  respectivement, on aura, quel que soit  $d$ , pour des valeurs de  $a$ ,  $a'$ ,  $b$ ,  $b'$  convenablement choisies :  $d = ab = b'a'$ . On peut donc écrire  $D = A \times B = B \times A$ , et dire que  $D$  est le produit de  $A$  par  $B$ ;  $D$  sera dit décomposable.

Si  $A$  ne contient aucun sous-groupe permutable aux substitutions de  $D$  (autrement dit aucun sous-groupe invariant de  $D$ ), on sait <sup>(2)</sup> que  $D$  possède un isomorphe holoédrique transitif  $D'$ ; de degré  $\frac{\Omega}{\mathfrak{A}} = \frac{\mathfrak{B}}{\mathfrak{C}}$ , où  $\Omega$ ,  $\mathfrak{A}$ ,  $\mathfrak{B}$  sont les ordres de  $D$ ,  $A$ ,  $B$ , et  $\mathfrak{C}$  celui du groupe  $E$  des substitutions communes à  $A$  et  $B$ , le groupe  $A'$ , qui correspond à  $A$  dans  $D'$ , étant formé des substitutions de  $D'$  laissant une même lettre de  $D'$  immobile; le groupe  $B'$ , correspondant à  $B$ , est transitif, puisqu'il est de degré  $\frac{\mathfrak{B}}{\mathfrak{C}}$ .

Réciproquement, si un isomorphe holoédrique transitif  $D'$  de  $D$  contient un sous-groupe transitif  $B'$  (de même degré que  $D'$  bien entendu), avec  $B' < D'$ , et si  $A'$  est le sous-groupe des substi-

---

(1) SERRET, *Algèbre supérieure*, t. II, p. 283.

(2) W. DYCK, *Math. Annalen*, t. XXII, et notre Thèse de Doctorat, p. 12.

tutions de  $D'$  qui laissent une même lettre de  $D'$  immobile, on aura  $D' = A' \times B'$ , ce qui entraîne  $D = A \times B$ ,  $A$  et  $B$  étant les sous-groupes de  $D$  correspondant à  $A'$  et  $B'$ . On peut donc dire :

*Le problème de la recherche des sous-groupes transitifs des isomorphes holoédriques et transitifs d'un groupe donné, est compris dans celui de la recherche des décompositions de ce groupe en un produit de deux sous-groupes. Il lui est équivalent quand le groupe donné est simple.*

Quand  $D$  est un groupe symétrique ou alterné de  $n$  éléments ( $n > 4$ ), les deux problèmes seront équivalents à condition d'exclure le cas où  $A$  ou  $B$  serait le groupe alterné de  $n$  éléments, lorsque  $D$  est symétrique; c'est ce que nous supposons dans la suite.

Ceci posé, considérons les isomorphes holoédriques et transitifs des groupes symétriques ou alternés de  $n$  éléments ( $n > 4$ ), et conservons les notations que nous avons adoptées dans le *Journal de Mathématiques* (1).

$S$  désignant le groupe symétrique ou alterné de  $n$  éléments,  $G$  un isomorphe holoédrique et transitif de  $S$ , nous avons montré que  $G$  ne peut contenir de substitution circulaire pour  $n > 6$ , si  $S$  est symétrique, et pour  $n > 8$  si  $S$  est alterné. Une démonstration à peu près identique suffira pour établir cette propriété :

**THÉORÈME.** — *Un isomorphe holoédrique et transitif  $G$  d'un groupe symétrique ou alterné  $S$  de  $n$  éléments ne peut contenir aucun groupe régulier (2) formé de substitutions échangeables, et de degré égal ou inférieur à celui de  $G$ , sauf pour  $n \leq 6$  si  $S$  est symétrique, ou pour  $n \leq 8$  si  $S$  est alterné.*

On s'appuie encore sur ce qu'un sous-groupe de  $S$  formé de substitutions échangeables est d'ordre  $\leq e^{\frac{n}{e}}$ , et sur ce lemme :

**LEMME.** — *Un groupe transitif ne peut renfermer de groupe régulier d'ordre  $h$ , formé de substitutions échangeables que*

---

(1) P. 5 à 34; 1895.

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

*s'il est primitif ou composé avec un sous-groupe d'ordre non premier à  $h$ .*

Si  $S = A \times B$  est une décomposition de  $S$ ,  $G$  l'isomorphe holoédrique de  $S$  issu de  $A$ , c'est-à-dire où  $A'$  correspondant à  $A$  est formé de l'ensemble des substitutions de  $G$  laissant une même lettre de  $G$  immobile, le sous-groupe  $B'$  de  $G$  correspondant à  $B$  est transitif, et réciproquement.

Si, en particulier,  $G$  est primitif et appartient à la première ou à la troisième catégorie, on sait que  $A$  est transitif entre les  $n$  éléments de  $S$ . On peut prendre pour  $B$  évidemment un groupe symétrique ou alterné de  $n - 1$  éléments, suivant que  $S$  est symétrique ou alterné.

De même, si  $A$  est  $k$  fois transitif, avec  $k > 1$ , on peut prendre pour  $B$  un groupe symétrique ou alterné respectivement de  $n - k'$  éléments, avec  $k' \leq k$ ; si de plus  $G$  est primitif, il appartiendra à la troisième catégorie, puisque  $A$  est primitif. On aura ainsi en particulier :

**THÉORÈME.** — *Dans les isomorphes holoédriques primitifs  $G$  des groupes symétriques (alternés)  $S$  de  $n$  éléments :*

1° *Les sous-groupes correspondant aux sous-groupes de  $S$  symétriques (alternés) entre  $n - 1$  éléments sont transitifs, quand  $G$  est de la première catégorie;*

2° *Les sous-groupes correspondant aux sous-groupes de  $S$  symétriques (alternés) entre  $n - k'$  éléments sont transitifs, quand  $G$  est de la troisième catégorie et est issu d'un sous-groupe  $T$  de  $S$ ,  $k$  fois transitif entre les  $n$  éléments de  $S$ , avec  $k \geq k' \geq 1$ .*

A peine est-il besoin de faire remarquer qu'un sous-groupe de  $S$  contenant un sous-groupe symétrique (alterné) entre  $n - k'$  éléments, donnera lieu à une remarque analogue, quand  $G$  est de la troisième-catégorie.

Si l'on prend pour  $A$  un groupe intransitif, on voit encore :

**THÉORÈME.** — *Dans un isomorphe holoédrique et primitif  $G$  de la deuxième catégorie d'un groupe symétrique ou alterné  $S$ , formé par les substitutions opérées par  $S$  entre les combi-*

naisons  $\alpha$  à  $\alpha$  des  $n$  lettres de  $S$  ( $1 < \alpha < \frac{n}{2}$ ), à tout sous-groupe de  $S$   $k$  fois transitif entre les  $n$  lettres, correspondra dans  $G$  un sous-groupe transitif <sup>(1)</sup> dès que  $\alpha \leq k$ .

$G$  étant un isomorphe holoédrique et primitif quelconque de  $S$  contenant un sous-groupe transitif  $B'$  correspondant à un sous-groupe  $B$  de  $S$ , ne peut-on assigner certaines conditions auxquelles doive satisfaire  $B$  ?

D'abord, si  $A'$  est le sous-groupe des substitutions de  $G$  laissant une même lettre immobile,  $A$  le sous-groupe correspondant de  $S$ , on a  $G = A' \times B'$ ,  $S = A \times B$ .

Mais l'on peut préciser davantage pour les deux premières catégories.

**THÉORÈME.** — *Quand  $G$  est un isomorphe primitif et holoédrique de la première catégorie du groupe symétrique ou alterné  $S$  de  $n$  éléments, tout sous-groupe transitif  $B'$  de  $G$  correspond à un sous-groupe  $B$  de  $S$  transitif entre  $n$  ou  $n - 1$  éléments.*

En effet,  $G$  est formé de l'ensemble des substitutions opérées par  $S$ , entre les hypersystèmes constitués chacun par  $\frac{n}{l}$  systèmes de  $l$  lettres de  $S$ , et  $2 \leq l \leq \frac{n}{2}$ . Si  $B$  est intransitif entre les  $n$  lettres de  $S$ , il permute exclusivement entre elles  $\lambda$  lettres, avec  $\lambda \leq \frac{n}{2}$ . Dès lors,  $B$  permute exclusivement entre eux les hypersystèmes dont les systèmes ont respectivement  $\lambda_1, \lambda_2, \dots$  lettres communes avec ces  $\lambda$  lettres,  $\lambda_1 + \lambda_2 + \dots$  étant égal à  $\lambda$ . Donc  $B'$ , qui est précisément le groupe des substitutions opérées par  $B$  entre tous les hypersystèmes, ne pourra être transitif que si l'on n'a qu'une seule combinaison de nombres  $\lambda_1, \lambda_2, \dots$ , tous  $\leq l$ , et dont la somme soit égale à  $\lambda$ . Or on aura toujours au moins deux combinaisons dès que  $\lambda \geq 2$ , puisqu'on peut toujours prendre, par exemple,  $0 < \lambda_1 \leq \lambda_2 < l$ , et considérer les deux combinaisons  $\lambda_1, \lambda_2, \dots$  et  $\lambda_1 - 1, \lambda_2 + 1, \dots$ , où tous les nombres, sauf les deux

---

<sup>(1)</sup> Parmi ces sous-groupes, on trouve même une série étendue de groupes primitifs; nous y reviendrons.

premiers, coïncident. On pourra d'ailleurs toujours prendre  $\lambda \geq 2$  quand A n'est pas transitif entre  $n$  ou  $n - 1$  éléments.

C. Q. F. D.

**THÉORÈME.** — *Quand G est un isomorphe primitif et holoédrique de la deuxième catégorie du groupe symétrique ou alterné S entre n éléments, tout sous-groupe transitif B' de G correspond à un sous-groupe B de S transitif entre n éléments.*

En effet, G est formé de l'ensemble des substitutions opérées par S entre les combinaisons des  $n$  lettres de S  $\alpha$  à  $\alpha$ , et  $2 \leq \alpha < \frac{n}{2}$ . Si B n'est pas transitif, il permute exclusivement entre elles  $\lambda$  lettres, avec  $0 < \lambda \leq \frac{n}{2}$ . Dès lors, il permute exclusivement entre elles les combinaisons ayant  $\lambda_1$  lettres communes avec ces  $\lambda$  lettres et, par suite, B' n'est pas transitif, puisqu'on peut choisir  $\lambda_1 = 0$  et  $\lambda_1 > 0$ .

**THÉORÈME.** — *Si G<sub>2</sub> et G<sub>3</sub> sont les isomorphes primitifs et holoédriques de la deuxième catégorie du groupe symétrique ou alterné S de n éléments, formés respectivement par les substitutions que S opère entre les combinaisons 2 à 2 et 3 à 3 de ces n éléments, G<sub>2</sub> et G<sub>3</sub> sont isomorphes, et à tout sous-groupe de G<sub>3</sub> transitif entre les lettres de G<sub>3</sub> correspond dans G<sub>2</sub> un sous-groupe transitif entre les lettres de G<sub>2</sub>.*

Soient B'<sub>3</sub> un sous-groupe de G<sub>3</sub> transitif entre les lettres de G<sub>3</sub>, B'<sub>2</sub> et B les sous-groupes correspondants de G<sub>2</sub> et S : nous savons déjà que B est transitif entre les  $n$  lettres de S.

Supposons que B'<sub>2</sub> ne soit pas transitif : B et B'<sub>2</sub> permutent exclusivement entre elles  $\lambda$  combinaisons 2 à 2 des  $n$  lettres de S, avec  $\lambda < C_n^2$ . Or, une combinaison de 3 lettres renferme  $C_3^2 = 3$  combinaisons de 2 lettres ; si elle a  $\lambda_1$  combinaisons de 2 lettres communes avec les  $\lambda$  précédentes, une substitution de B ou B'<sub>2</sub> la remplace par une autre ayant  $\lambda_1$  combinaisons de 2 lettres communes avec les  $\lambda$  précédentes. Donc, B permutant transitivement les combinaisons de 3 lettres, chacune de ces dernières contiendra le même nombre  $\lambda_1$  des  $\lambda$  combinaisons de 2 lettres précitées. Enfin, si l'on avait  $\lambda_1 = 3$ , B'<sub>3</sub> étant transitif, il faudrait  $\lambda = C_n^2$ ,

et  $B'_2$  serait transitif, contrairement à l'hypothèse; si l'on a  $\lambda_1 = 2$ , chaque combinaison de 3 lettres en renferme une et une seule de 2 lettres ne faisant pas partie des  $\lambda$  précédentes; B permute exclusivement entre elles les combinaisons ne faisant pas partie de ces  $\lambda$ , et l'on peut trouver un nombre  $\lambda'$  de combinaisons de 2 lettres, analogue à  $\lambda$ , et pour lequel le nombre  $\lambda'_1$ , analogue à  $\lambda_1$ , est  $= 1$ . On peut donc supposer, si l'on veut,  $\lambda_1 = 1$ .

Ceci posé, considérons la combinaison  $a_1 a_2 a_3$  : elle contiendra une et une seule combinaison de deux lettres, par exemple  $a_1 a_2$ , faisant partie des  $\lambda$  précitées. Alors  $a_1 a_2 a_i$ , avec  $i = 3, 4, \dots, n$ , sera dans le même cas. Donc  $a_1 a_i$ , avec  $i = 3, 4, \dots, n$ , n'est pas contenue dans ces  $\lambda$ ; de même pour  $a_2 a_i$ . La considération de  $a_1 a_3 a_4$  et de  $a_1 a_3 a_5$  montre, par suite, que  $a_3 a_4$  et  $a_3 a_5$  sont contenues dans les  $\lambda$  précitées.

Mais la considération de  $a_3 a_4 a_5$  montre aussi que l'une des combinaisons  $a_3 a_4$  et  $a_3 a_5$  n'est pas contenue dans les  $\lambda$  précitées. On est ainsi conduit à une contradiction et l'on en conclut que  $B'_2$  est transitif.

En terminant ce paragraphe, nous allons examiner si, pour certains cas particuliers, on peut avoir dans les groupes G des sous-groupes réguliers.

**THÉORÈME.** — *La condition nécessaire et suffisante pour qu'un isomorphe holoédrique et primitif G d'un groupe symétrique ou alterné S de n lettres, formé des substitutions opérées par S entre les  $C_n^2$  combinaisons 2 à 2 des n lettres (n étant premier), renferme un groupe régulier, de degré  $C_n^2$ , est que n soit de la forme  $4h + 3$ .*

Soit  $B'$  le sous-groupe régulier de G, d'ordre  $C_n^2$ , et B le sous-groupe correspondant de S : B est linéaire et dérivé des substitutions

$$U = |x; x + 1|, \quad V = |x; b^2 x| \pmod n.$$

où  $b$  racine primitive  $(\pmod n)$ . La substitution la plus générale de B est

$$W = |x; p^2 x + q| \pmod n,$$

où  $p^2$  est résidu quadratique de  $n$ . Les  $n$  lettres sont ici représentées par  $0, 1, 2, \dots, n-1 \pmod{n}$  et  $W$  remplace la combinaison  $l, m$  par la combinaison  $p^2 l + q, p^2 m + q$ .

La condition nécessaire et suffisante pour que  $B'$  soit régulier est évidemment qu'aucune substitution  $W \neq 1$  de  $B$  ne laisse une seule combinaison immobile, c'est-à-dire qu'aucun des deux systèmes de congruences

$$l \equiv p^2 l + q, \quad m \equiv p^2 m + q, \quad (\text{mod } n),$$

ou

$$l \equiv p^2 m + q, \quad m \equiv p^2 l + q, \quad (\text{mod } n),$$

ne soit possible.

Le premier exigerait  $(l-m)(p^2-1) \equiv 0 \pmod{n}$  et le second  $(l-m)(p^2+1) \equiv 0 \pmod{n}$ , pour  $l \neq m$ . La première condition entraîne  $W = 1$ , la seconde  $p^2 \equiv -1 \pmod{n}$ , d'où  $n = 4h + 1$ . Si d'ailleurs  $n$  est de cette forme, la substitution  $|x; -x|$  laisse immobile les combinaisons  $l, m$ , pour lesquelles  $l + m \equiv 0 \pmod{n}$ , et  $B'$  n'est pas régulier. C. Q. F. D.

**THÉORÈME.** — *Un isomorphe holoédrique et primitif  $G$  d'un groupe symétrique ou alterné  $S$  de  $n$  lettres, formé des substitutions opérées par  $S$  entre les combinaisons 3 à 3 des  $n$  lettres ( $n$  étant premier et  $\geq 7$ ), ne renferme aucun sous-groupe régulier de même degré  $C_n^3$  que celui de  $G$ .*

Car si  $G$  renfermait un pareil sous-groupe  $B'$  d'ordre  $C_n^3$ , soit  $B$  le sous-groupe correspondant de  $S$  :  $B$  serait transitif entre les  $n$  lettres de  $S$  et d'ordre  $C_n^3 = \frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3}$ . Ici  $\frac{(n-1)(n-2)}{6}$  ne divise pas  $n-1$ ; donc, d'après un théorème de MM. Mathieu <sup>(1)</sup> et Sylow <sup>(2)</sup>, on a

$$C_n^3 = n \nu (bn + 1) \quad \text{avec} \quad b > 0, \quad \nu \geq 1,$$

$bn + 1$  étant le nombre des groupes d'ordre  $n$  contenus dans  $B$ ;

<sup>(1)</sup> *Journal de Liouville*, 1861.

<sup>(2)</sup> *Math. Ann.*, t. V, p. 584.



par suite,

$$\begin{aligned} \nu(bn + 1) &= \frac{(n-1)(n-2)}{6}, \\ 3\nu &= \beta n + 1 \quad \text{avec} \quad \beta > 0, \\ 2(\beta n + 1)(bn + 1) &= (n-1)(n-2), \end{aligned}$$

ce qui est absurde, puisque  $b > 0$ ,  $\beta > 0$ . c. q. f. d.

*Remarque.* — On peut même, en remarquant que  $\nu$  doit diviser  $n - 1$ , établir un théorème analogue pour les isomorphes holoédriques et primitifs  $G$  des groupes symétrique ou alterné  $S$  de  $n$  lettres, formés des substitutions opérées par  $S$  entre les combinaisons  $\alpha$  à  $\alpha$  des  $n$  lettres ( $n$  étant premier et  $\geq 2\alpha + 1$ ), quand  $\alpha$  est impair ou quand il est pair sans diviser  $n - 1$ .

## II.

M. Jordan a montré <sup>(1)</sup> que tout groupe primitif  $G$  de degré  $n$ , qui ne contient pas le groupe alterné de  $n$  éléments, mais renferme une substitution d'ordre premier  $p$  à  $q$  cycles, contient un groupe  $\Gamma$ , transitif entre les lettres qu'il permute, et pour le degré duquel on peut trouver une limite supérieure en fonction de  $u = pq$ .

Reportons-nous à la démonstration en question. Le degré de  $\Gamma$  ne peut être inférieur à celui de  $G$  que si  $G$  est deux fois transitif; dans ce cas, on a <sup>(2)</sup>

$$(1) \quad u \geq \frac{1}{4}n - 1.$$

Si  $G$  n'est qu'une fois transitif, son degré est égal à celui de  $\Gamma$ , et cette remarque permet d'améliorer légèrement la limite la plus exacte <sup>(3)</sup> trouvée par M. Jordan pour  $n$  en fonction de  $p$  et  $q$ .

Mais on peut déduire facilement de sa démonstration une limite plus avantageuse dans certains cas particuliers. En effet, supposons que  $G$  ne soit qu'une fois transitif : pour former  $\Gamma$ ,

<sup>(1)</sup> *J. für Math.*, t. LXXIX, p. 248-258; 1875.

<sup>(2)</sup> A. BOCHERT, *Math. Ann.*, t. XL, p. 176.

<sup>(3)</sup> *Loc. cit.*, p. 255.

qui est de degré  $n$ , on forme une suite de groupes

$$(2) \quad \Gamma_0, \Gamma_1, \dots, \Gamma_\mu,$$

tels que si  $\Gamma_i$  permute transitivement entre elles  $M_i$  lettres convenablement choisies,  $\Gamma_{i+1}$ , qui contient  $\Gamma_i$ , en permute de même au moins  $e_i M_i$  comprenant les  $M_i$  précédentes, avec  $e_i = \frac{p}{E\left(\frac{p}{2}\right)}$ ,

ainsi que des lettres non déplacées par  $\Gamma_i$ . L'ordre de  $\Gamma_{i+1}$  est dès lors au moins égal à celui de  $\Gamma_i$  multiplié par  $e_i M_i$ . Or  $M_i \geq e_i^i p$ , en sorte que les groupes (2) sont d'ordres respectifs au moins égaux à

$$(3) \quad p, e_1 p^2, e_1^3 p^3, \dots, e_1^{\frac{\mu(\mu+1)}{2}} p^{\mu+1}.$$

On forme ensuite une seconde série de groupes

$$(4) \quad \Gamma_\mu, \Gamma_{\mu+1}, \Gamma_{\mu+2}, \dots, \Gamma_{\mu+\tau} = \Gamma,$$

avec

$$\tau \leq K_\mu - 1 \leq (\mu + 1)q - e_1 \frac{e_1^\mu - 1}{e_1 - 1} - 1,$$

et tels que chacun d'eux contienne le précédent, et au moins une substitution d'ordre  $p$  à  $q$  cycles non contenue dans ce précédent; en sorte que l'ordre de  $\Gamma_{\mu+j+1}$  est au moins égal à celui de  $\Gamma_{\mu+j}$  multiplié par  $p$ . Les groupes (4) sont donc d'ordres respectifs au moins égaux à

$$(5) \quad e_1^{\frac{\mu(\mu+1)}{2}} p^{\mu+1}, e_1^{\frac{\mu(\mu+1)}{2}} p^{\mu+2}, \dots, e_1^{\frac{\mu(\mu+1)}{2}} p^{\mu+\tau+1}.$$

On a de plus

$$e_1^{\mu-1} p \leq q E\left(\frac{p}{2}\right),$$

ou

$$(6) \quad e_1^\mu \leq q.$$

$\Gamma_\mu$  étant de degré

$$(7) \quad N_\mu \leq (\mu + 1) p q - p \frac{e_1^\mu - 1}{e_1 - 1},$$

$\Gamma$  est de degré

$$(8) \quad n \leq N_\mu + \tau q,$$

et il en est de même de  $G$  qui contient  $\Gamma$ . Dès lors, si  $\mathcal{G}$  est l'ordre de  $G$ , (5) donne

$$\mathcal{G} \geq e_1^{\frac{\mu(\mu+1)}{2}} p^{\mu+\tau+1},$$

$$\tau \leq \frac{\log \mathcal{G}}{\log p} - \frac{\mu(\mu+1)}{2} \frac{\log e_1}{\log p} - (\mu+1),$$

et, d'après (7) et (8),

$$n \leq (\mu+1)pq - p \frac{e_1^\mu - 1}{e_1 - 1} + q \left[ \frac{\log \mathcal{G}}{\log p} - \frac{\mu(\mu+1)}{2} \frac{\log e_1}{\log p} - \mu - 1 \right].$$

Sans chercher à discuter complètement cette formule, nous remarquerons qu'elle donne de suite

$$n - \frac{q \log \mathcal{G}}{\log p} \leq (\mu+1)(p-1)q \leq (p-1)q \frac{\log(qe_1)}{\log 2},$$

d'après (6); ou, *a fortiori*, puisque  $qe_1 \leq pq = u$ ,

$$\log \mathcal{G} \geq p \log p \left( \frac{n}{u} - \frac{p-1}{p} \frac{\log u}{\log 2} \right).$$

Si  $n \log 2 \geq u \log u$ , le second membre est fonction croissante de  $p$ , qui est  $\geq 2$ , et, par suite,

$$\log \mathcal{G} \geq \left( \frac{n}{u} - \frac{\log u}{2 \log 2} \right) 2 \log 2,$$

ou

$$(9) \quad \mathcal{G} u \geq 2^{\frac{n}{u}}.$$

Or, si  $n \log 2 < u \log u$ , on a

$$2 \frac{n \log 2}{u} - \log u < \log u,$$

et la condition (9) est satisfaite, puisque  $n \geq u$ ,  $\mathcal{G} > n$ ,  $G$  étant primitif. Donc

**THÉORÈME.** — Si  $G$  est un groupe primitif, une seule fois transitif, d'ordre  $\mathcal{G}$ , de degré  $n$  et de classe  $u$ , on a

$$(9) \quad \mathcal{G} u \geq 2^{\frac{n}{u}}.$$

*Corollaire I.* — Si l'on sait que  $G$  est d'ordre  $G \leq n^k$ , on aura

$$u \geq \frac{n}{\log n} \frac{\log 4}{k+1}.$$

Car, d'après  $u < n$ , (9) donne

$$n^{k+1} \geq 4^{\frac{n}{u}}.$$

*Corollaire II.* — Un isomorphe holoédrique et primitif  $G$  de la troisième catégorie, de degré  $\rho$ , d'un groupe symétrique ou alterné  $S$  de  $n$  éléments, est de classe au moins égale à

$$\frac{\rho}{\log \rho} \frac{\log 4}{4},$$

sauf peut-être pour quelques petites valeurs de  $n$ .

$G$  étant issu d'un sous-groupe  $T$  de  $S$  primitif, ne contenant pas de substitution circulaire d'ordre 3, on a, d'après un théorème (1) de M. Bochert, et suivant que  $S$  est symétrique ou alterné,

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

On voit sans peine, soit à l'aide de la formule connue

$$\left( \frac{p}{e} \right)^{p+\frac{1}{2}} \sqrt{2\pi e} < p! < \left( \frac{p}{e} \right)^{p+\frac{1}{2}} \sqrt{2\pi e} e^{\frac{1}{12p}},$$

soit directement, qu'on a

$$G < \rho^3,$$

sauf pour de petites valeurs de  $n$ ; il ne reste plus qu'à appliquer le corollaire I.

### III.

Nous nous contenterons ici d'énoncer les propriétés suivantes (2) :

(1) *Math. Ann.*, t. XXXIII, p. 584.

(2) Elles seront établies en détail dans les *Mémoires de l'Académie des Sciences, Inscriptions et Belles-Lettres de Toulouse* pour 1896.

I. Soit  $m$  un nombre impair quelconque,  $k$  un nombre plus petit que le plus petit diviseur  $\varepsilon$  de  $m$ ; un groupe  $G$  transitif, de classe  $m$ , de degré  $m + k$ , avec  $0 < k < \varepsilon$ , renfermant un sous-groupe  $M$  d'ordre, de degré et de classe  $m$ , ne peut exister que si  $k \leq 2$  et  $m + 1 = 2^\nu$ .

II. Un groupe transitif de classe  $ef$  ( $e$  et  $f$  premiers,  $5 \leq e \leq f$ ), de degré  $ef + k$  (avec  $0 < k < e$ ), ne peut exister qu'à l'une des conditions suivantes :

1°  $k \leq 2$  avec  $ef = 4h + 3$ ;

2°  $f > e + 1 = 2^\nu$ ;

3°  $f \geq 2e + 3$ .

De plus, dans les deux derniers cas, le groupe ne sera qu'une fois transitif et aura son ordre premier à  $f$ .

III. Un groupe transitif de classe  $e^2$  ( $e$  premier impair) est de degré  $e^2$  ou  $\geq e^2 + e$ .

IV. Les groupes transitifs de classe  $ef < 100$  ( $e$  et  $f$  premiers,  $5 \leq e \leq f$ ) sont de degré  $ef + k$ , avec  $k \leq 2$ , ou  $k \geq e$ . Ceux de ces groupes qui sont primitifs sont de degré  $\geq ef + e$ .

On doit noter qu'il existe un groupe de classe  $55 = 5 \cdot 11$  et de degré  $60$  primitif (1).

---

(1) Voir notre Thèse de Doctorat, p. 35.