

# Des groupes transitifs de classe (\*) $ef$ ( $e$ et $f$ étant premiers avec $5 \leq e \leq f$ ) et de degré $ef + k$ ( $k$ étant $< e$ ).

(Par ED. MAILLET, à Neuilly.)

---

Ces groupes peuvent contenir un sous-groupe d'ordre, de degré et de classe  $ef$ , ou n'en pas contenir : nous allons étudier successivement les deux cas.

## I.

### Groupes qui contiennent un sous-groupe d'ordre, de degré et de classe $ef$ .

Nous établissons le théorème suivant qui leur est applicable.

*Théorème.* — 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  $m + 1 = 2^v$ .

En effet, d'abord  $G$  est primitif. Car, s'il ne l'était pas, il admettrait une répartition de ses lettres  $u$  à  $u$  en systèmes de non-primitivité, avec  $u > 1$ . Soient  $\alpha_1, \alpha_2, \dots, \alpha_k$  les  $k$  lettres de  $G$  laissées immobiles par le groupe  $M$ , d'ordre, de degré et de classe  $m$ ;  $u$  divisera  $m + k < 2m$ , et sera par suite  $< m$ . Alors,  $M$  permutant exclusivement entre elles les lettres du système dont

---

(\*) D'après MM. JORDAN et NETTO la classe d'un groupe est le nombre de lettres minimum que déplace une substitution de ce groupe différente de l'unité; la classe d'une substitution est le nombre de lettres qu'elle déplace.

fait partie  $\alpha_i$ , ce système ne pourrait comprendre une des lettres de  $M$  sans les comprendre toutes, puisque  $M$  est transitif entre  $m$  lettres; dans ce cas il faudrait  $u > m$ , contrairement à ce qu'on a vu. Les lettres  $\alpha_1, \alpha_2, \dots, \alpha_k$  forment donc un certain nombre de systèmes, et  $u$  divise  $k$ ;  $u$  divisant  $k$  et  $m + k$  divise  $k$  et  $m$ , ce qui est absurde, puisque  $k < \varepsilon$  (\*).

Ceci posé, je dis que  $G$  est  $k + 1$  fois transitif.

En effet, cette propriété est vraie si  $k = 1$ . Admettons qu'elle le soit pour les degrés  $m + k'$  inférieurs à  $m + k$ , et montrons qu'elle a lieu pour le degré  $m + k$  ( $k' \geq 1, k > 1$ ).

Soit  $H_{\alpha_i}$  le groupe des substitutions de  $G$  qui laissent immobile  $\alpha_i$  par exemple. L'ordre de  $H_{\alpha_i}$  est  $> m$ , puisque  $G$  est primitif, car s'il était égal à  $m$ ,  $G$  admettrait une répartition de ses lettres  $k$  à  $k$  (\*\*). Dès lors, si  $H_{\alpha_i}$  permutait exclusivement entre elles les lettres  $\alpha_2, \dots, \alpha_k$ , ses substitutions seraient permutables à  $M$ , et  $H_{\alpha_i}$  ne renfermerait, comme il est facile de le voir, qu'un seul groupe d'ordre et de degré  $m$ , le groupe  $M$  lui-même. Donc, en considérant les transformés de  $H_{\alpha_i}$  par les substitutions de  $G$ , on voit que ces transformés sont en nombre  $m + k$ , puisque  $G$  est primitif, et que chacun des transformés de  $M$  par les substitutions de  $G$  est commun à  $k$  d'entre eux exactement, en sorte que  $k$  devrait diviser  $m + k$ , par suite  $m$ , ce qui est contraire à l'hypothèse  $k < \varepsilon$ .

On en conclut que  $H_{\alpha_i}$  contient une substitution permutant  $\alpha_i$  ( $i > 1$ ) avec une des lettres de  $M$ , et  $M$  n'est pas permutable à toutes les substitutions de  $H_{\alpha_i}$ . Soit  $M'$  un transformé de  $M$ , différent de  $M$ , par une substitution de  $H_{\alpha_i}$ :  $M'$  sera transitif entre  $m$  lettres, et d'ordre et de degré  $m$ ; parmi ces  $m$  lettres on en aura  $k'$ , par exemple, comprises parmi les lettres  $\alpha_2, \dots, \alpha_k$ , avec  $1 \leq k' \leq k - 1 < m$ , en sorte que  $M'$  permutera ces  $k'$  lettres avec des lettres de  $M$ . Le groupe  $(M, M')$  dérivé de  $M$  et de  $M'$  sera transitif, de degré  $m + k'$ , de classe  $m$ , et renfermera le groupe  $M$  d'ordre, de degré, et de classe  $m$ . Par hypothèse, il sera  $k' + 1$  fois transitif, avec  $k' + 1 \geq 2$ , c. à. d. primitif: donc, d'après un théorème connu (\*\*\*),  $G$  sera  $k + 1$  fois transitif.

(\*) Ce raisonnement peut même servir à montrer qu'un groupe transitif de degré  $m + k$ , avec  $k < m$ , contenant un sous-groupe transitif de degré  $m$ , ne peut exister que si  $k$  n'est pas premier à  $m$ , ou s'il est primitif.

(\*\*) Voir par exemple *Annales de la Faculté des Sciences de Toulouse*, 1895, D. 18.

(\*\*\*) JORDAN, *Journal de Liouville*, année 1871, p. 384.

D'après un théorème de M. JORDAN (\*), on sait que  $G$ , qui est  $k + 1$  fois transitif, de classe  $m$  et de degré  $m + k$ , ne peut exister,  $m$  étant impair et  $> 3$ , que si  $k \leq 2$ , et  $m + 1 = 2^v$ , ce qui démontre le théorème.

Ce résultat est applicable aux groupes transitifs de classe  $ef$  et de degré  $ef + k$  avec  $e$  et  $f$  premiers,  $0 < k < e \leq f$ , renfermant un sous-groupe de degré, d'ordre et de classe  $ef$ : on a forcément  $k \leq 2$ .

Comme exemple d'un pareil groupe on peut citer un groupe linéaire de degré 17 et d'ordre 17. 16. 15, et un groupe linéaire de degré 513, et d'ordre 513. 512. 511.

*Remarque.* — Après avoir établi que  $G$  est primitif, on abrégerait la démonstration en s'appuyant sur un théorème de M. JORDAN (\*\*).

## II.

### Groupes qui ne contiennent aucun sous-groupe d'ordre, de degré et de classe $ef$ .

Ces groupes contiendront un sous-groupe  $M$  d'ordre  $r$  et de degré  $ef$  ( $r$  étant égal à  $e$  ou à  $f$ ) maximum parmi les sous-groupes de degré et de classe  $ef$  qu'ils renferment.

Soit  $G$  un de ces groupes, d'ordre  $G$ , de degré  $ef + k$  avec  $0 < k < e \leq f$  et  $5 \leq e$ :  $G$  divise (\*\*\*)  $ef(ef + 1) \dots (ef + k)$ , et, par suite, est divisible par  $r$  sans l'être par  $r^2$ , même si  $e = f$ .

Soient  $\alpha_1, \alpha_2, \dots, \alpha_k$  les  $k$  lettres de  $G$  non déplacées par  $M$ ;  $H_{\alpha_1}$ , d'ordre  $H_{\alpha_1}$ , le groupe des substitutions de  $G$  qui laissent  $\alpha_1$  immobile;  $L$ , d'ordre  $L$ , le groupe des substitutions de  $H_{\alpha_1}$  permutables à  $M$ ;  $K$ , d'ordre  $K$ , le groupe des substitutions de  $G$  permutables à  $M$ , contenant  $L$ .

D'après un théorème de M. SYLOW (\*\*\*\*), on a :

$$H_{\alpha_1} = (1 + nr) L, \quad L = l \cdot r.$$

---

(\*) JORDAN, *Journal de Liouville*, année 1872.

(\*\*) D'après l'énoncé que nous en avons donné dans le *J. de Math.*, 1895, p. 20.

(\*\*\*) Voir par exemple *Annales de la Faculté des Sciences de Toulouse*, 1895, D. 9-10.

(\*\*\*\*) *Math. Ann.*, t. V, p. 584.

De plus,  $H_{\alpha_i}$  renferme  $1 + nr$  transformés de  $M$ , exactement.  $H_{\alpha_i}$  et ses transformés par les substitutions de  $G$  en renferment  $(1 + nr)(ef + k)$  qui, évidemment, sont identiques  $k$  à  $k$ , et le nombre des transformés distincts de  $M$  par les substitutions de  $G$  est  $\frac{(1 + nr)(ef + k)}{k}$ . Donc, d'après le même théorème de M. SYLOW :

$$G = \frac{(1 + nr)(ef + k)}{k} K = (ef + k) H_{\alpha_i},$$

$$K = k \cdot L = k \cdot l \cdot r > L.$$

$K$  déplace  $\alpha_i$ ; il permute exclusivement entre elles  $\alpha_1, \alpha_2, \dots, \alpha_k$ , puisque ses substitutions sont permutable à  $M$ , et les permute transitivement, puisque le groupe des substitutions de  $K$  laissant  $\alpha_i$  immobile est d'ordre  $L = \frac{K}{k}$ .

Je dis qu'aucune substitution de  $K$  ne peut être échangeable à une de  $M$  sans faire partie de  $M$ . En effet, une substitution de  $M$  déplace  $r$  lettres dans chacun de ses cycles; une substitution  $U$  qui lui serait échangeable ne pourrait laisser immobile une des lettres de  $M$  sans en laisser  $r > k$ , ce qui est impossible, puisqu'une substitution de  $G$  laisse au plus  $k$  lettres de  $M$  immobiles. Donc  $U$  déplace toutes les lettres de  $M$ ; de plus  $U$  opère entre elles une substitution régulière, sans quoi une de ses puissances, qui serait échangeable aux substitutions de  $M$ , laisserait des lettres de  $M$  immobiles, sans d'ailleurs les laisser toutes, puisqu'elle déplace au moins  $ef$  lettres avec  $ef > k$ . Cette substitution régulière est d'ordre diviseur de  $ef$ ; si elle déplace quelques unes des lettres  $\alpha_1, \dots, \alpha_k$ , en l'élevant à la puissance  $ef$ , on obtiendrait une substitution différente de l'unité, puisque  $f \geq e > k$ , et qui déplacerait au plus  $k$  lettres, tout en faisant partie de  $G$  qui est de classe  $ef$ , résultat absurde; si elle ne déplace aucune des lettres  $\alpha_1, \dots, \alpha_k$ , elle engendrera avec  $M$  un groupe contenant un sous-groupe d'ordre  $e^2$  ou  $ef$  contrairement à ce qu'on a vu ou à l'hypothèse, à moins qu'elle ne soit contenue dans  $M$ , ce qui montre le résultat annoncé.

On en conclut de suite que toute substitution de  $M$  a exactement  $kl$  transformées par les substitutions de  $K$  (à part l'unité), et, en considérant les  $r - 1$  substitutions de  $M$  différentes de l'unité, que :

$$r - 1 \equiv 0 \pmod{kl}. \quad (1)$$

Nous allons maintenant déterminer  $l$ .

Prenons dans  $K$  un des groupes  $F$  les plus généraux parmi ceux dont l'ordre  $F$  est premier à  $r$ , et qui n'ont avec  $M$  aucune substitution commune, et soit :

$$K = F \cdot \mu r.$$

Si un sous-groupe de  $F$  était permutable aux substitutions de  $K$ , on sait (\*), et l'on voit facilement,  $F$  n'ayant avec  $M$  aucune substitution commune, que les substitutions de ce sous-groupe seraient échangeables à celles de  $M$ , sans faire partie de  $M$ , ce que nous avons vu impossible. Dès lors,  $K$  est holoédriquement isomorphe (\*\*) à un groupe  $K'$  de degré  $\mu r$ , transitif, et où l'isomorphe  $F'$  de  $F$  est formé de l'ensemble des substitutions de  $K'$  laissant une même lettre de  $K'$ , convenablement choisie, immobile.

Soit  $\rho'$  une substitution d'ordre  $r$  de  $K'$  :

$$\rho' = (\beta_1 \beta_2 \dots \beta_r)(\gamma_1 \gamma_2 \dots \gamma_r) \dots,$$

$$\beta_1, \beta_2, \dots, \beta_r,$$

$$\gamma_1, \gamma_2, \dots, \gamma_r,$$

$$\dots \dots \dots$$

étant les lettres de  $K'$  qui ne renferme d'autres substitutions d'ordre  $r$  que  $\rho$  et ses puissances. Soit aussi  $F'_{\beta_i}$  celui des transformés de  $F'$  par les substitutions de  $K'$  qui laisse  $\beta_i$  immobile : une substitution de  $F'_{\beta_i}$  transforme  $\rho'$  en une de ses puissances, et ne peut laisser  $\beta_i$  (avec  $i > 1$ ) immobile que si elle est échangeable à  $\rho'$ , ce qui est impossible, comme on l'a vu, à cause de l'isomorphisme de  $K$  et de  $K'$ . Désignant alors par  $S$  une substitution déplaçant  $\beta_2, \dots, \beta_r$  et transformant la substitution  $(\beta_1 \beta_2 \dots \beta_r)$  en une de ses puissances, par  $T_1, T_2, \dots$  des substitutions entre  $\gamma_1, \gamma_2, \dots, \gamma_r, \dots$ , les substitutions de  $F'_{\beta_i}$  seront de la forme :

$$1, S T_1, S^2 T_2, \dots, S^{F-1} T_{F-1},$$

$S$  étant convenablement choisi, et d'ordre  $F$ . Cela résulte en effet facilement, d'une part de ce que  $F'_{\beta_i}$  doit permuter exclusivement entre elles  $\beta_2 \dots \beta_r$ , et de ce que chacune de ses substitutions déplace ces  $r - 1$  lettres et transforme  $\rho'$  en une de ses puissances ; d'autre part de ce que les substitutions

---

(\*) Voir par exemple *Annales de la Faculté des Sciences de Toulouse*, 1895, D. 17.

(\*\*) Voir par exemple notre *Thèse de Doctorat*, p. 12 et 15.

entre  $\beta_2, \dots, \beta_r$  qui transforment  $(\beta_1 \beta_2 \dots \beta_r)$  en ses puissances sont les puissances d'une même substitution.

On en conclut que  $F'_{\beta_1}$  est holoédriquement isomorphe à un groupe formé des puissances d'une même substitution, c. à d. est formé des puissances d'une même substitution.

Supposons maintenant qu'une substitution de  $F'_{\beta_1}$  laisse en même temps  $\gamma_1$  par exemple immobile.  $F'_{\beta_1}$  et  $F'_{\gamma_1}$  auraient une substitution commune différente de l'unité et échangeable à leurs substitutions, par suite à celles du groupe  $(F'_{\beta_1}, F'_{\gamma_1})$  dérivé de ces deux groupes. Ce groupe dérivé est alors d'ordre premier à  $r$ ; d'après l'hypothèse faite sur  $F$ , et en vertu de l'isomorphisme de  $F$  et de  $F'$ , on a :

$$(F'_{\beta_1}, F'_{\gamma_1}) = F'_{\beta_1} = F'_{\gamma_1};$$

c. à d. que si une substitution de  $F'_{\beta_1}$  laisse  $\gamma_1$  immobile, il en est de même de toutes les substitutions de  $F'_{\beta_1}$ , qui déplacent  $\gamma_2, \dots, \gamma_r$ , d'après ce qui précède.

Soit alors  $\mu_1$  le nombre des lettres laissées immobiles par une substitution de  $F'_{\beta_1}$ : toutes les substitutions de  $F'_{\beta_1}$  laissent ces  $\mu_1$  lettres immobiles et celles-ci appartiennent à  $\mu_1$  cycles différents de  $\rho'$ , en sorte que  $\mu_1 \leq \mu$ . Si  $\mu_1 > 1$ , on sait (\*) que  $K'$  contiendra un groupe  $\Phi'$  d'ordre  $\mu_1 F$  contenant  $F'_{\beta_1}$ : il en résulte sans peine que  $K$  contiendra un groupe  $\Phi$  d'ordre  $\mu_1 F$  contenant  $F$ . D'après l'hypothèse faite sur  $F$ ,  $\Phi$  aura des substitutions communes avec  $M$ , par suite contiendra  $M$ : les substitutions de  $\Phi'$  sont permutable à  $F'_{\beta_1}$ , et celles de  $\Phi$  à  $F$ , en sorte que les substitutions de  $M$  sont permutable à  $F$  et celles de  $F$  à  $M$ . Il en résulterait encore (\*\*) que les substitutions de  $F$  sont échangeables à celles de  $M$ , contrairement à ce qu'on a vu. Donc  $\mu_1 = 1$ .

En résumé,  $K'$  est transitif, de degré  $\mu r$ , de classe  $\mu r - 1$ , et le groupe  $F'_{\beta_1}$  des substitutions de  $K'$ , qui laissent une lettre  $\beta_1$  quelconque immobile, est formé des puissances d'une même substitution.

On sait alors (\*\*\*) que  $K'$  renferme  $\mu r - 1$  substitutions déplaçant  $\mu r$  lettres; parmi ces  $\mu r - 1$  substitutions sont comprises les  $r - 1$  substitutions

(\*) Voir par exemple *Ann. de la Fac. des Sc. de Toulouse*, D. 18-20 et notre *Thèse de Doctorat*, p. 18.

(\*\*) Voir par exemple *Ann. de la Fac. des Sc. de Toulouse*, D. 17.

(\*\*\*) Voir notre *Thèse de Doctorat*, p. 49 et suiv.

de  $M'$ , isomorphe de  $M$ , qui sont différentes de l'unité, puisqu'elles sont d'ordre  $r$  premier, et régulières. Je dis qu'on a  $\mu = 1$ .

En effet, soit  $\mu > 1$  : il y a dans  $K'$  des substitutions d'ordre premier à  $r$  et déplaçant  $\mu r$  lettres; les substitutions correspondantes de  $K$  ne sont comprises ni dans  $M$ , ni dans  $F$ , ni dans un de ses transformés par les substitutions de  $K$ . On peut donc partir d'une d'elles pour former un groupe  $E$  différent de  $F$  et de ses transformés par les substitutions de  $K$ , et maximum comme  $F$  parmi les groupes de  $K$  dont l'ordre est premier à  $r$ . On voit encore que  $E$  est formé des puissances d'une même substitution.

Les transformés de  $E$  par  $K$  sont différents des transformés de  $F$  par  $K$ ; de plus, si un transformé  $E_1$  de  $E$  avait une substitution autre que l'unité commune avec un transformé  $F_1$  de  $F$ , le groupe  $(E_1, F_1)$ , dérivé de  $E_1$  et  $F_1$ , qui serait  $> F_1$ , d'après ce qu'on vient de voir, aurait une substitution commune avec  $M$ , laquelle serait échangeable à une substitution de  $F_1$ , ce qui n'a pas lieu. Alors les transformés de  $F$  par les substitutions de  $K$  renferment  $(F-1)\mu r = K \frac{F-1}{F}$  substitutions distinctes, et distinctes de l'unité; les transformés de  $E$ , d'ordre  $E$ , renferment de même  $K \frac{E-1}{E}$  substitutions distinctes, et distinctes des précédentes et de l'unité : il faudrait donc :

$$K \left( \frac{F-1}{F} + \frac{E-1}{E} \right) < K,$$

ce qui est absurde, puisque  $\frac{F-1}{F} \geq \frac{1}{2}$ ,  $\frac{E-1}{E} \geq \frac{1}{2}$ . On en conclut que  $\mu = 1$ , comme nous l'avions annoncé.

Les groupes  $F$  et  $M$  sont échangeables (\*), et le groupe dérivé  $(F, M) = K$  est d'ordre  $K = F'r$ ;  $F$  ne contient aucune substitution (à part l'unité), laissant à la fois  $\alpha_1, \alpha_2, \dots, \alpha_k$  immobiles, d'après les hypothèses faites sur  $G$ . Les groupes des substitutions opérés par  $K$  et  $F$  entre  $\alpha_1, \alpha_2, \dots, \alpha_k$  coïncident : soit  $P$  ce groupe, d'ordre  $P = kl$ ; il est transitif et holoédriquement isomorphe à  $F$ , par suite formé des puissances d'une même substitution; une substitution de  $P$  laissant  $\alpha_1$  par exemple immobile est échangeable aux substitutions du groupe transitif  $P$ , et par suite laisse  $\alpha_2, \dots, \alpha_k$  immobiles. Donc :

$$P = k, \quad l = 1;$$

le groupe des substitutions de  $H_{\alpha_i}$  permutables à  $M$  se confond avec  $M$ .

---

(\*) D'après la définition de SERRET, *Algèbre supérieure*, t. II, pag. 283.

On en conclut immédiatement que, si  $G$  était deux fois transitif,  $H_{\alpha_i}$  serait transitif, et que la quantité désignée tout-à-l'heure par  $l$  devrait être égale à  $k-1$ , ce qui exige  $k \leq 2$ . En tenant compte de ce qui a été dit dans le § I, on peut dire :

*Théorème I.* — Un groupe  $G$  transitif, de classe  $ef$  ( $e$  et  $f$  premiers,  $5 \leq e \leq f$ ), de degré  $ef+k$  ( $0 < k < e$ ) n'est qu'une fois transitif (\*) si  $k > 2$ .

Quand  $k \leq 2$ ,  $G$  fait partie des groupes transitifs de degré  $N$  et de classe  $N-1$  ou  $N-2$ , que nous avons étudiés (\*\*). On sait en particulier qu'il n'existe aucun de ces groupes qui soit de classe  $4h+1$ , et que, pour les classes  $\leq 100$ ,  $G$  ne peut être primitif que si  $m+1=2^v$ .

Supposons  $k > 2$ ;  $H_{\alpha_i}$  ne peut se confondre avec  $M$ , sans quoi  $G$  admettrait (\*\*\*) une répartition de ses lettres  $k$  à  $k$ , les lettres  $\alpha_1, \alpha_2, \dots, \alpha_k$  formant un système et  $k$  diviserait  $ef+k$ , par suite  $e$  ou  $f$ , ce qui est absurde. Donc  $H_{\alpha_i} > M$ .

Je dis que  $H_{\alpha_i}$  déplace toutes les lettres de  $G$ , sauf  $\alpha_i$ .

En effet, supposons que  $H_{\alpha_i}$  déplace seulement  $k_1-1$  des lettres  $\alpha_2, \dots, \alpha_k$ , avec  $k_1 < k$ : on sait (\*\*\*\*) que  $G$  admettra une répartition de ses lettres  $k-k_1+1$  à  $k-k_1+1$ . Si le système de cette répartition dont fait partie  $\alpha_i$  contenait quelques-unes des lettres de  $M$ , il contiendrait les  $r$  lettres d'un cycle d'une substitution de  $M$ , car  $M$  fait partie de  $H_{\alpha_i}$  qui permute exclusivement entre elles les lettres de ce système. On aurait :

$$k-k_1+1 > r, \quad \text{ou} \quad k > r,$$

contrairement à l'hypothèse. Les lettres  $\alpha_1, \dots, \alpha_k$  forment donc un certain nombre de systèmes, ainsi que les lettres de  $M$ , et  $k$  aurait un diviseur commun avec  $ef$ , ce qui est impossible. Il en résulte  $k_1 = k$ .

Je dis de plus que  $H_{\alpha_i}$  permute chacune des  $k-1$  lettres  $\alpha_2, \dots, \alpha_k$  exclusivement avec des lettres déplacées par  $M$ .

En effet, on sait (\*\*\*\*\*) que, si l'ordre du groupe des substitutions de  $H_{\alpha_i}$  permutable à  $M$  est  $vr$ , si  $v''$  est le nombre des lettres  $\alpha_2, \dots, \alpha_k$  que

(\*) Une propriété semblable a lieu pour les groupes de classe  $p_1 p_2 \dots p_i$  et de degré  $p_1 p_2 \dots p_i + k$ ; où  $k$  est  $> 2$  et plus petit que le plus petit des nombres premiers différents  $p_1, p_2, \dots, p_i$ .

(\*\*) *Thèse de Doctorat*, p. 49-104 et *Bull. Soc. Mat.*, 1897, t. 25, p. 16.

(\*\*\*) Voir par exemple *Ann. de la Fac. des Sc. de Toulouse*, 1895, D. 18-20.

(\*\*\*\*) Idem.

(\*\*\*\*\*) *Ann. de la Fac. des Sc. de Toulouse*, 1895, D. 20.



$H_{\alpha_1}$  substitue à  $\alpha_2$ , si  $H_{\alpha_1 \alpha_2}$  est le groupe des substitutions de  $H_{\alpha_1}$  qui laissent  $\alpha_2$  immobile,  $v'$  l'ordre du groupe des substitutions de  $H_{\alpha_1 \alpha_2}$  permutable à  $M$ , on a  $v = v' v''$ . Or ici  $v = 1$ , ce qui exige en particulier  $v'' = 1$ .

En résumé, si  $k > 2$ ,  $H_{\alpha_1}$  est de degré  $ef + k - 1$ , et permute exclusivement avec des lettres de  $M$  chacune des  $k - 1$  lettres que  $M$  laisse immobiles.

Ceci posé, considérons dans  $H_{\alpha_1}$  un des groupes minima  $D$  parmi ceux qui contiennent  $M$  et sont  $> M$ , ce qui est possible, puisque  $H_{\alpha_1} > M$ .

$D$  déplace  $k'$  des lettres  $\alpha_i$ , par exemple  $\alpha_2, \dots, \alpha_{k'+1}$ , avec  $k > k' > 0$ ; chacune de ces  $k'$  lettres est permutée transitivement avec des lettres de  $M$  exclusivement, d'après ce qui précède; l'une d'elles  $\alpha_j$ , par exemple, le sera avec  $qr$  lettres de  $M$ . Aucune substitution de  $D$  ne peut laisser simultanément ces  $qr$  lettres et  $\alpha_j$  immobiles sans se réduire à l'unité, en sorte que  $D$  est holoédriquement isomorphe au groupe  $D_{\alpha_j}$  des substitutions qu'il opère entre elles: de plus,  $M$  étant maximum dans  $D$ , par hypothèse, on sait (\*) que  $D_{\alpha_j}$  est primitif et d'ordre:

$$D_{\alpha_j} = D = r(1 + qr),$$

$D$  étant l'ordre de  $D$ ;  $q$  a donc la même valeur pour chacune des lettres  $\alpha_2, \dots, \alpha_{k'+1}$ .  $D_{\alpha_j}$  appartient aux groupes primitifs de degré  $N = 1 + qr$  et de classe  $N - 1$  dont nous avons déjà parlé, ce qui impose certaines conditions à la valeur de  $1 + qr$ . Ainsi il faut  $1 + qr \neq 4h + 2$ , et, comme  $1 + qr \leq ef + 1$ , on en conclut que pour  $ef < 200$ ,  $1 + qr$  est une puissance d'un nombre premier.

Les groupes  $D_{\alpha_2}, D_{\alpha_3}, \dots, D_{\alpha_{k'+1}}$  déplacent en tout  $k'(1 + qr)$  lettres. Les autres lettres de  $D$  sont toutes déplacées par  $M$ , s'il y en a: d'où deux cas à distinguer:

1.<sup>er</sup> cas. — Il n'y en a pas, c. à d.:

$$k'(1 + qr) = ef + k',$$

ou:

$$k'qr = ef.$$

Or  $k'$  divise  $ef$  et est  $< k < e$ : donc  $k' = 1$ .  $D$  est primitif et d'ordre  $r(ef + 1)$ : il est transitif entre  $ef + 1$  lettres, et d'après un théorème de M. JORDAN déjà utilisé,  $G$  serait  $k$  fois transitif, ce qui est impossible, d'après le théorème I, puisque  $k > 2$ . Il faut donc  $k'qr < ef$ .

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

2.<sup>ème</sup> cas. — Il y en a.

Ces lettres sont au nombre de  $ef - k'qr$ . Une d'elles sera permutée transitivement par  $D$  avec  $\lambda r$  lettres; aucune substitution de  $D$  ne peut laisser simultanément immobiles ces  $\lambda r$  lettres, puisque  $k < \lambda r$ , et les substitutions opérées entre elles par  $D$  forment un groupe  $D'$ , de degré  $\lambda r$ , transitif, holédriquement isomorphe à  $D$ , d'ordre :

$$D' = D = B' . \lambda r, .$$

$B'$ , d'ordre  $B'$ , étant le groupe des substitutions de  $D'$  qui laissent immobile une de ces  $\lambda r$  lettres. Aucune des substitutions de  $B'$  ou de ses transformés par  $D'$  ne fait partie de  $M'$ , isomorphe de  $M$  dans  $D'$ , ni des transformés de  $M'$  par  $D'$ , puisque  $B'$  est premier à  $r$ .

En considérant successivement toutes les lettres qui font partie des  $ef - k'qr$  en question, on obtiendra un certain nombre de groupes  $D', D'_1, \dots$  analogues à  $D'$ , et :

$$ef - k'qr = r . \sum \lambda. \quad (2)$$

Deux circonstances pourront alors se présenter :

1.<sup>o</sup> — Il pourra se faire qu'une des valeurs  $B', B'_1, \dots$  qui correspondent respectivement à  $D', D'_1, \dots$  soit  $> 1$ . Soit par exemple  $B' > 1$ .

On a :

$$B' \lambda = 1 + qr.$$

$D'$  sera de classe  $\lambda r - t$ , avec  $0 < t \leq k'$ , et de degré  $\lambda r$ .

Soit  $n_i$  le nombre des substitutions de  $B'$  qui laissent immobiles  $i$  des lettres de  $D'$ ; on sait (\*) que  $D'$  contient :

$$\lambda r \left( \frac{n_1}{1} + \frac{n_2}{2} + \dots + \frac{n_t}{t} \right),$$

substitutions qui laissent quelques lettres immobiles, avec :

$$n_1 + n_2 + \dots + n_t = B' - 1.$$

$D'$  contient d'ailleurs, d'après ce qui précède,  $\frac{r-1}{r} D$  substitutions faisant partie de  $M'$  ou de ses transformés par  $D'$ , et déplaçant toutes les lettres de  $D'$ . Donc :

$$\frac{r-1}{r} D + \lambda r \left( \frac{n_1}{1} + \frac{n_2}{2} + \dots + \frac{n_t}{t} \right) < D,$$

---

(\*) JORDAN, *J. de Math.*, 1872.

ou, a fortiori :

$$\frac{r-1}{r} + \frac{B'-1}{tB'} < 1,$$

ce qui donne :

$$e > k > k' \geq t > r \frac{B'-1}{B'} \geq \frac{r}{2}. \quad (3)$$

Or d'après la congruence (1),  $k$  divise  $r-1$ , ce qui donne  $k = r-1$ ; d'après l'hypothèse  $k < e \leq f$ , il faut :

$$r = e, \quad k = e - 1. \quad (4)$$

L'un des ordres  $B', B'_1, \dots$  ne peut être  $> 1$  que si  $r = e = k + 1$ .

Supposons donc  $r = e = k + 1$ . Si l'on a  $k' = t$ ,  $D$  contiendra une substitution de classe  $ef$  déplaçant toutes les lettres de  $D_{a_2}, D_{a_3}, \dots, D_{a_{k'+1}}$  et régulière, puisque  $G$  est de classe  $ef$ . Son ordre divise  $ef$  et  $B'$ , et par suite est égal à  $f$  : ses puissances forment un groupe  $Q$  sur lequel on peut raisonner comme on l'a fait sur  $M$ . On sera encore conduit à des groupes analogues à  $B', B'_1, \dots$  dont les ordres seront tous égaux à 1, d'après ce qui précède; on verra tout-à-l'heure que leurs ordres ne peuvent pas non plus être tous égaux à 1, et par suite que  $k' > t$ . L'inégalité (3) deviendra :

$$e - 1 = k > k' > t > e \frac{B'-1}{B'} \geq \frac{e}{2}, \quad (5)$$

d'où :

$$e \geq t + 3 > \frac{e}{2} + 3, \quad (6)$$

et :

$$e \geq 7. \quad (7)$$

Enfin, d'après (2) :

$$\lambda \leq f - k'q,$$

$$B'\lambda = 1 + qe \leq (f - k'q)B',$$

ou :

$$B' \geq \frac{1 + qe}{f - k'q};$$

mais, d'après (5) :

$$B' < \frac{e}{e-t},$$

en sorte que :

$$\frac{e}{e-t} > \frac{1 + qe}{f - k'q},$$

ou :

$$ef > qe(k' - t) + qe^2 + e - t,$$

ou, d'après (5) et (6):

$$ef \geq qe(e + 1) + 4,$$

ce qui donne :

$$f > q(e + 1). \quad (8)$$

Il y aura intérêt, pour chaque valeur particulière de  $e$ , à déterminer une limite inférieure de  $q$ , d'après ce que nous avons dit de  $D$  et des groupes primitifs de classe  $N - 1$  et de degré  $N$ . Ainsi on ne pourra avoir  $q = 1$  que si  $e + 1 = 2^r < f$ ; si  $e + 1 \neq 2^r$ , il faudra  $q \geq 2$ , et:

$$f \geq 2e + 3. \quad (9)$$

En résumé, l'un des ordres  $B', B'_1, \dots$  ne peut être  $> 1$  que si l'on a:

$$r = e = k + 1, \quad (4)$$

$$e \geq 7, \quad (7)$$

$$e + 1 = 2^r < f, \quad \text{ou} \quad f \geq 2e + 3. \quad (10)$$

2.° — Toutes les valeurs  $B', B'_1, \dots$  sont  $= 1$ .

On a toujours  $\lambda = 1 + qr$ , et, d'après (2):

$$ef = k'qr + (1 + qr)r \cdot \varphi,$$

$\varphi$  désignant le nombre des groupes analogues à  $D'$ . On a  $\varphi > 0$ ,  $q > 0$ , et, par suite,  $r = e$ , et:

$$f = k'q + (1 + qe)\varphi \geq 1 + q(e + k'). \quad (11)$$

Mais  $H_{\alpha_1}$  est de degré  $m + k - 1$  et permute chacune des lettres  $\alpha_2, \dots, \alpha_k$  avec des lettres de  $M$  exclusivement. Chacune des lettres  $\alpha_i$  non déplacées par  $D$  ( $i > 1$ ) sera permutée par  $H_{\alpha_1}$  avec au moins  $e(1 + qe)$  lettres de  $M$ ; il faut donc  $\varphi \geq k - 1 - k'$ , et:

$$f \geq k'q + (1 + qe)(k - 1 - k'). \quad (12)$$

Les inégalités (11) et (12) montrent, en remarquant que  $q$  satisfait aux conditions précédemment indiquées, que l'on ne pourra avoir  $f < 2e + 3$  que si:

$$\left. \begin{aligned} q = 1, \quad \varphi = 1, \quad f = k' + e + 1, \quad k - 1 - k' \leq 1, \\ k = k' + 2, \quad \text{ou} \quad k = k' + 1. \end{aligned} \right\} \quad (13)$$

par suite :

Si  $k = k' + 2$ ,  $f = e + k - 1$ , ce qui est impossible,  $f$  étant premier, et  $k > 1$  divisant  $e - 1$ , d'après (1).

Si  $k = k' + 1$ ,  $D$  et  $H_{\alpha_i}$  sont tous deux de degré  $ef + k - 1$ ; on ne peut avoir  $D = H_{\alpha_i}$ , car on en conclurait :

$$G = (ef + k) D = (ef + k)(e + 1)e,$$

et  $G$  contenant le sous-groupe désigné antérieurement par  $K$ , d'ordre  $ke$ ,  $k < e$  devrait diviser  $e + 1$  et  $e - 1$ , d'après (1), ce qui exigerait  $k \leq 2$ , contrairement à l'hypothèse. Soit donc  $D < H_{\alpha_i} : \alpha_i (i > 1)$  est permutée par  $H_{\alpha_i}$  avec au moins  $e$  lettres de  $M$ , puisqu'elle l'est déjà par  $D$ ; mais elle ne pourra l'être aussi avec les  $e(e + 1)$  lettres permutées exclusivement entre elles par  $D$  que pour une valeur de  $i$  au plus, puisque  $H_{\alpha_i}$  permute chacune des lettres  $\alpha_2, \dots, \alpha_k$  avec des lettres de  $M$  exclusivement. Donc, puisque  $k > 2$ , il y a au moins une des lettres  $\alpha_2, \dots, \alpha_k$ , par exemple  $\alpha_2$ , que  $H_{\alpha_i}$  permute exclusivement avec  $e$  lettres de  $M$ . Le groupe  $H_{\alpha_i, \alpha_2}$ , formé des substitutions de  $H_{\alpha_i}$  laissant  $\alpha_2$  immobile, est d'ordre :

$$\frac{H_{\alpha_i}}{e + 1} > e,$$

puisque :

$$H_{\alpha_i} > (e + 1)e = D.$$

$H_{\alpha_i, \alpha_2}$  contient alors un sous-groupe  $\Delta$  analogue à  $D$ , minimum parmi ceux qui contiennent  $M$  et sont  $> M$ ; mais ce groupe  $\Delta$  est de degré  $< ef + k - 1$ , c. à d. de degré plus petit que celui de  $H_{\alpha_i}$ , et le cas exceptionnel que nous venons d'étudier pour  $D$  ne pourra se présenter pour  $\Delta$ . En raisonnant sur  $\Delta$  comme nous l'avons fait sur  $D$ , on sera donc conduit, soit aux conditions (4), (7) et (10), soit à la condition :

$$f \geq 2e + 3. \quad (14)$$

Nous concluons, en tenant compte du théorème I et du § I :

**Théorème 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.° —  $k \leq 2$ ,  $ef = 4k + 3$ ;
- 2.° —  $f > e + 1 = 2^r$ ;
- 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  $f$ .

Si en particulier  $e=f$ , on a :

*Corollaire.* — Un groupe transitif de classe  $e^2$  est de degré  $e^2$  ou  $\geq e^2 + e$ ,  $e$  étant premier impair.

### III.

#### Application aux groupes transitifs des 100 premières classes.

Si  $ef \leq 100$ , il faut  $e$  égal à 5 ou 7.

1.° —  $e=5$ .

On a  $e+1=6 \neq 2r$ ,  $f \geq 13$ .

De plus, d'après (7), les quantités  $B'$ ,  $B'_1, \dots$  sont toutes égales à 1. Appliquant alors (11) :

$$f = k'q + (1 + 5q)\varphi,$$

$\varphi > 0$ ,  $k-1-k' \leq \varphi$ ,  $3 \geq q \geq 2$ , puisque  $ef \leq 100$ ,  $k=4$  si  $k > 2$ , puisque  $k$  divise  $e-1=4$ .

Pour  $f=13$ ,  $q=2$ ,  $\varphi=1$ ,  $k'=1$ ,  $k-1-k'=2 > \varphi=1$ , ce qui implique contradiction.

Pour  $f=17$ ,  $q=2$ ,  $\varphi=1$ ,  $k'=3=k-1$  :  $D$  et  $H_{a_i}$  seraient tous deux de degré  $ef+k-1$ , et un raisonnement fait précédemment montre que  $H_{a_i}$  contiendrait un sous-groupe  $\Delta$ , analogue à  $D$ , mais de degré  $< ef+k-1$ , ce qui conduit à une contradiction.

Pour  $f=19$ ,  $q=2$  exigerait  $\varphi=1$ ,  $k'=4$ , ce qui est impossible, puisque  $k' \leq k-1=3$ ;  $q=3$  donne  $\varphi=1$ ,  $k'=1$ ,  $k-1-k'=2 > \varphi=1$ , ce qui implique contradiction.

2.° —  $e=7$ .

On a  $e+1=8=2^3$ . Nous savons qu'alors l'hypothèse  $B' = B'_1 = \dots = 1$  conduit à la condition  $f \geq 2e+3=17$ ,  $ef > 100$ , à moins qu'on ne puisse trouver dans  $H_{a_i}$  un groupe analogue à  $D$  pour lequel les quantités analogues à  $B'$ ,  $B'_1, \dots$  ne soient pas toutes égales à 1.

Supposant donc qu'a priori on ait pris pour  $D$  ce groupe et que  $B' > 1$ , les conditions (8) et  $ef \leq 100$  donnent  $q=1$ . De plus (5) et (6) donnent

$k' = 5 = k - 1$ ,  $t = 4 > 7 \cdot \frac{B' - 1}{B'}$ ,  $B' = 2$ , et d'après (2) où l'on remplace  $r$  par  $e$ :

$$f = 5 + \sum \lambda. \quad (15)$$

Ce qui précède montre d'ailleurs que si, par exemple  $B'_1 > 1$ , il faut  $B'_1 = 2$ , et, d'après  $B'_i \lambda_i = 8$ , que les quantités  $\lambda$  sont toutes égales à 4 ou 8, l'une d'elles étant égale à 4, à cause de  $B' = 2$ . Mais  $ef \leq 100$  donne  $f$  égal à 11 ou 13, et, par suite, il y a dans (15) au plus deux quantités  $\lambda$ , dont une égale à 4, l'autre égale à 4 ou à 8. Ceci exige immédiatement:

$$f = 13, \quad \lambda = 4, \quad \lambda_1 = 4, \quad B' = B'_1 = 2.$$

Dans ce cas on ne peut avoir  $H_{\alpha_1} = D$ , sans quoi:

$$G = (ef + k)(e + 1)e = 97 \cdot 8 \cdot 7,$$

et  $k = 6$  devrait diviser  $G$ , à cause de l'existence du groupe  $K$ , ce qui n'a pas lieu. Soit donc  $H_{\alpha_1} > D$ .

$D$  est de même degré que  $H_{\alpha_1}$ , puisque  $k' = k - 1 = 5$ ; il permute chacune des lettres  $\alpha_2, \dots, \alpha_6$  avec  $e = 7$  lettres de  $M$  exclusivement, et permute exclusivement entre elles les 28 lettres de chacun des deux groupes  $D'$ ,  $D'_1$ , correspondant à  $B'$ ,  $B'_1$ .  $H_{\alpha_1}$  permutant chacune des lettres  $\alpha_2, \dots, \alpha_6$  avec des lettres de  $M$  exclusivement, il y en aura au moins 3 permutées par  $H_{\alpha_1}$  chacune avec 7 lettres de  $M$  seulement: soit  $\alpha_2$  l'une d'elles. Le groupe  $H_{\alpha_1 \alpha_2}$  des substitutions de  $H_{\alpha_1}$  laissant  $\alpha_2$  immobile est alors d'ordre  $\frac{H_{\alpha_1}}{8} > 7$ , et contient un sous-groupe  $\Delta'$  analogue à  $D$ , mais pour lequel la quantité  $k'$  est  $\leq 4$ .

Les quantités qui pour  $\Delta'$  sont analogues à  $B'$ ,  $B'_1, \dots$  seront ici toutes égales à 1, sans quoi on trouverait, en raisonnant comme sur  $D$ ,  $k' = 5$ . Mais, puisque  $f < 2e + 3$ , (13) doit avoir lieu et  $f = k' + e + 1 \leq 12$ , ce qui est contradictoire.

Nous pouvons donc conclure:

*Théorème III.* — Les groupes transitifs de classe  $ef \leq 100$  ( $e$  et  $f$  premiers,  $5 \leq e \leq f$ ) sont de degré  $ef + k$ , avec  $k \leq 2$ , ou  $k \geq e$ .

*Corollaire.* — Ceux de ces groupes qui sont primitifs sont de degré  $\geq ef + e$ .

Car il suffit de tenir compte des résultats que nous avons obtenus pour les groupes primitifs de degré  $N$  et de classe  $N - 1$  ou  $N - 2$ .

D'autre part, on connaît (\*) l'existence d'un groupe primitif au moins de classe  $ef$  et de degré  $ef + e$  pour les 100 premières classes, à savoir un groupe primitif de classe 55, de degré 60, d'ordre  $\overline{60}^2$ , dérivé de l'isomorphe régulier du groupe alterné de 5 éléments, et de son conjoint. Néanmoins, ainsi que nous le montrerons ultérieurement, ces raisonnements sont susceptibles d'extensions quand on ne considère que des groupes renfermant une substitution d'ordre  $f$  à  $e$  cycles, avec  $f > e$ .

Neuilly-sur-Marne, 17 avril 1897.

---

(\*) Voir par ex. notre *Thèse de Doctorat*, p. 35.