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

CAMILLE JORDAN

Théorèmes sur les groupes primitifs

Journal de mathématiques pures et appliquées 2^e série, tome 16 (1871), p. 383-408.
<http://www.numdam.org/item?id=JMPA_1871_2_16__383_0>

Théorèmes sur les groupes primitifs;

PAR M. CAMILLE JORDAN,
Ingénieur des Mines.

1. Les principales difficultés de la théorie des substitutions se rencontrent dans la recherche des groupes primitifs. Les propriétés générales de ces groupes méritent donc une attention particulière. Mais on n'en connaît encore qu'un petit nombre.

L'une des plus utiles est la suivante, dont nous avons donné la démonstration dans notre *Traité des substitutions et des équations algébriques*, Note C.

Si un groupe G, *primitif et de degré n, contient une substitution circulaire de degré premier p, il sera au moins* $n-p+1$ *fois transitif.*

On sait d'ailleurs qu'un groupe de degré n, qui n'est pas symétrique ou alterné (nous appelons, pour abréger, *groupe symétrique* celui qui contient toutes les substitutions possibles), ne peut être plus de $\frac{n+4}{3}$ fois transitif (*Traité des substitutions*, n° **85**). Si donc G n'est pas symétrique ou alterné, on aura la relation

$$\frac{n+4}{3} \geqq n-p+1; \quad \text{d'où} \quad p \geqq \frac{2n-1}{3}, \quad n \leqq \frac{3p+1}{2}.$$

On a donc le corollaire suivant :

Si le groupe G, *primitif et de degré n, contient une substitution circulaire de degré p, il sera symétrique ou alterné, dès que n ne dépassera pas la limite* $\frac{3p+1}{2}$.

Ces propositions sont fort utiles dans les applications (*voir* l'ouvrage cité, n° **447** et Note C); il y a donc quelque intérêt à montrer qu'elles

peuvent être considérablement généralisées. Ce sera l'objet des pages suivantes.

2. THÉORÈME I. — *Si un groupe* G, *primitif et de degré n, contient un groupe* Γ *dont les substitutions ne déplacent que p lettres et les permutent transitivement* (*p étant un entier quelconque*), *il sera au moins* $n - p - 2q + 3$ *fois primitif, q étant le plus grand diviseur de p tel, que l'on puisse répartir les lettres de* Γ *de deux manières différentes en systèmes de q lettres jouissant de la propriété que chaque substitution de* Γ *remplace les lettres de chaque système par celles d'un même système.*

Si aucun des diviseurs de p ne jouit de cette propriété (*ce qui arrivera notamment si* Γ *est primitif, ou formé des puissances d'une seule substitution circulaire*), G *sera* $n - p + 1$ *fois transitif.*

Démonstration. — Si $n = p$, G étant primitif, et *a fortiori* transitif, ce théorème sera évident.

Supposons, au contraire, $p < n$. Soit H le groupe formé par celles des substitutions de G qui ne déplacent que les p lettres de Γ. Le groupe Γ étant transitif par rapport à ces lettres, H, qui le contient, le sera *a fortiori*. On pourra d'ailleurs partager les lettres de G en deux catégories, contenant, la première, les p lettres $a, b, \ldots$ que H déplace, la seconde, les $n - p$ lettres restantes $\alpha, \beta, \gamma, \ldots$.

Soient H, $H_1, \ldots$ les groupes transformés de H par les diverses substitutions de G. Le groupe $(H, H_1, \ldots)$, dérivé de leur combinaison, sera évidemment permutable à toutes les substitutions de G, et il faudra qu'il soit transitif pour que G soit primitif (*Traité des substitutions*, n° **53**). Or chacun des groupes H, $H_1, \ldots$ ne déplace que p lettres; et, pour que $(H, H_1, \ldots)$ soit transitif, il faudra évidemment que l'un au moins de ces groupes permute ensemble des lettres appartenant aux deux catégories $a, b, \ldots$ et $\alpha, \beta, \gamma, \ldots$.

Parmi les groupes de la suite H, $H_1, \ldots$ qui déplacent ainsi des lettres des deux catégories, soit H_1 l'un de ceux qui déplacent le nombre *minimum* de lettres de la seconde catégorie. Soient $\alpha, \beta, \ldots$ ces lettres et q leur nombre. Le groupe H_1 les permutant avec quelques-unes des p lettres $a, b, \ldots$ que H permute entre elles transitive-

ment, il est clair que le groupe $I = (H, H_1)$ permutera transitivement les $p + q$ lettres $\alpha, \beta, \ldots, a, b, \ldots$.

3. Cela posé, soient $1, S_1, \ldots$ les diverses substitutions de I; $s, s_1, \ldots$ les divers systèmes de q lettres que ces substitutions font respectivement succéder à $\alpha, \beta, \ldots$; chacune des lettres $a, b, \ldots, \alpha, \beta, \ldots$ figurera, d'après ce qui précède, dans l'un au moins de ces systèmes; mais, d'autre part, deux de ces systèmes ne peuvent avoir aucune lettre commune, sans se confondre entièrement. Supposons, en effet, que s_1 et s_2 eussent q' lettres communes, q' étant $< q$: la substitution $S_1 S_2^{-1}$ remplacerait $\alpha, \beta, \ldots$ par un système de q lettres, parmi lesquelles q' seulement appartiendraient à la suite $\alpha, \beta, \ldots$, et le groupe transformé de H_1 par $S_1 S_2^{-1}$, lequel fait évidemment partie de la suite $H, H_1, \ldots$, ne différerait du groupe H que par $q - q'$ lettres, résultat contraire à l'hypothèse d'après laquelle q est minimum.

Les $p + q$ lettres $\alpha, \beta, \ldots, a, b, \ldots$ peuvent donc se grouper q à q en systèmes n'ayant aucune lettre commune. D'ailleurs chaque substitution de I remplace les lettres de chaque système par celles d'un même système. Soient, en effet, T une de ces substitutions, et t l'ensemble des lettres qu'elle fait succéder à celles de s_1; les lettres de t, succédant à $\alpha, \beta, \ldots$ en vertu de la substitution $S_1 T$, appartiendront, par définition, à un même système.

Les substitutions de I, permutant transitivement les lettres $\alpha, \beta, \ldots$, $a, b, \ldots$ permutent *a fortiori* transitivement les systèmes $s, s_1, \ldots$. L'un de ces systèmes s étant d'ailleurs amené à une place quelconque, les substitutions de H, qui permutent transitivement les p lettres restantes, permuteront *a fortiori* transitivement les $\frac{p}{q}$ systèmes correspondants. Donc I est doublement transitif par rapport aux systèmes.

4. Deux cas seront ici à distinguer, suivant que le nombre q est supérieur ou égal à l'unité. Nous supposerons, en premier lieu, $q > 1$.

On aura, dans ce cas, $n > p + q$. Soit, en effet, $n = p + q$. Le groupe G, étant primitif, contiendra une substitution T qui ne remplace pas les lettres de chaque système par celles d'un même système. Supposons, par exemple, que T remplace les q lettres du système s_1

par de nouvelles lettres parmi lesquelles il y en ait un nombre $q' < q$ appartenant au système s_2. La substitution $S_1 T S_2^{-1} = U$ remplacera α, $\beta, \ldots$ par un système de q lettres parmi lesquelles q' appartiennent à la suite $\alpha, \beta, \ldots$; et le groupe transformé de H par U, lequel appartient à la suite $H, H_1, \ldots$, ne différera de H que par $q - q'$ lettres, résultat inadmissible.

5. Soit donc $n > p + q$. On pourra partager les lettres de G en deux catégories, formées, la première, des $p + q$ lettres que I déplace; la seconde, des lettres restantes. Puis, raisonnant sur I comme tout à l'heure sur H, on verra que, parmi les groupes $I, I_1, \ldots$, transformés de I par les diverses substitutions de G, il en existe au moins un qui permute ensemble des lettres de catégorie différente. Parmi les groupes qui jouissent de cette propriété, soit I_1 l'un de ceux qui déplacent le nombre *minimum* de lettres de la seconde catégorie. Soient $\alpha', \ldots$ ces lettres, et r leur nombre. Le groupe $J = (I, I_1)$ déplacera $p + q + r$ lettres, qu'il permute transitivement, et qu'on pourra grouper r à r en systèmes $\sigma, \sigma_1, \ldots$ tels, que chaque substitution de J remplace les lettres d'un même système par celles d'un même système; l'un de ces nouveaux systèmes sera formé des lettres $\alpha', \ldots$; enfin J sera doublement transitif par rapport à ces systèmes.

Considérons les $\frac{p+q}{r}$ nouveaux systèmes formés par les lettres que I déplace. L'un quelconque d'entre eux, σ_1, sera contenu en entier dans l'un des anciens systèmes $s, s_1, \ldots$, entre lesquels ces mêmes lettres se répartissaient q à q. Soient, en effet, $\alpha\beta, \ldots, a_1 b_1 \ldots a_2 b_2 \ldots, \ldots$ ces anciens systèmes; supposons que σ_1 contînt deux lettres a_1, a_2 appartenant respectivement à s_1 et à s_2, et voyons ce qui en résulterait. Le groupe $I = (H, H_1)$ contient le groupe H', transformé de H par S_1, lequel laisse immobiles les lettres de s_1 et permute transitivement les autres. Les substitutions de H', laissant immobile une des lettres a_1 du système σ_1, ne déplaceront pas ce système. Donc les p lettres α, $\beta, \ldots, a_2, b_2, \ldots$ qu'elles font succéder à a_2 appartiendront à σ_1; on voit de même que $a_1, b_1, \ldots$ lui appartiendront. Le nombre r des lettres de chaque système sera donc au moins égal à $p + q$, ce qui est absurde; car ce nombre est égal à celui des lettres $\alpha', \ldots$, c'est-à-dire

à $p+q-\rho$, ρ étant le nombre des lettres de la première catégorie que I_1 déplace.

Soit μ le nombre des systèmes de la suite $\sigma, \sigma_1, \ldots$ qui se trouvent ainsi contenus dans chacun des systèmes $s, s_1, \ldots$; on aura évidemment $q = \mu r$, et nous aurons deux cas à distinguer, suivant que μ est supérieur ou égal à l'unité.

6. Supposons d'abord $\mu > 1$. Soient $\sigma, \sigma', \ldots, \sigma^{\mu-1}; \sigma_1, \sigma'_1, \ldots, \sigma_1^{\mu-1}; \ldots$ les nouveaux systèmes dont la réunion forme respectivement $s, s_1, \ldots$; τ le dernier nouveau système formé par les lettres $\alpha', \ldots$. Le groupe J, étant doublement transitif par rapport à ces systèmes, contiendra une substitution T qui remplace σ par τ, et réciproquement. Les systèmes $\tau', \ldots, \tau^{\mu-1}; \tau_1, \tau'_1, \ldots, \tau_1^{\mu-1}; \ldots$ que T fait succéder à $\sigma', \ldots, \sigma^{\mu-1}; \sigma_1, \sigma'_1, \ldots, \sigma_1^{\mu-1}; \ldots$ se confondront, à l'ordre près, avec ces derniers.

Or le groupe H déplace tous les systèmes, sauf $\tau, \sigma, \sigma', \ldots, \sigma^{\mu-1}$; son transformé H' par T déplace tous les systèmes, sauf $\sigma, \tau, \tau', \ldots, \tau^{\mu-1}$. Le nombre des lettres déplacées par H' sans l'être par H sera donc égal à λr, λ étant le nombre des systèmes contenus dans la suite $\sigma', \ldots, \sigma^{\mu-1}$ sans l'être dans la suite $\tau', \ldots, \tau^{\mu-1}$, lequel est au plus égal à $\mu - 1$. Mais, par hypothèse, tous les groupes transformés de H par les substitutions de G qui ne se confondent pas avec lui en diffèrent au moins par $q = \mu r$ lettres. Donc $\lambda = 0$, et H' *se confond avec* H.

D'autre part, désignons par $t_1, t_2, \ldots$ les systèmes de q lettres que T fait succéder à $s_1, s_2, \ldots$. Il est clair que les lettres de chacun de ces systèmes seront remplacées par celles d'un même système dans chacune des substitutions du groupe $H' = H$. Donc *il existera deux modes de grouper les lettres de* H *en systèmes de q lettres*, de telle sorte que les substitutions de H, et *a fortiori* celles de Γ, remplacent les lettres de chaque système par celles d'un même système.

Ces deux modes de groupement seront essentiellement distincts. Supposons, en effet, qu'ils fussent identiques, et que les lettres de t_1, autrement dit celles des systèmes $\tau_1, \ldots, \tau_1^{\mu-1}$, se confondissent avec celles de s_2, par exemple. La substitution $S_1 T S_2^{-1}$ transformerait H en un groupe analogue H'', déplaçant toutes les lettres, sauf celles de s et celles que S_2^{-1} fait succéder à celles de σ, lesquelles sont en nombre r.

et font partie de s_2. Donc H'' ne différerait de H que par r lettres, nombre inférieur à $\mu r = q$, ce qui est contre l'hypothèse.

7. Supposons maintenant $\mu = 1$. Les $p + 2q$ lettres de J se grouperont en $\frac{p}{q} + 2$ systèmes, par rapport auxquels J sera trois fois transitif; car ses substitutions permettent de faire arriver le système σ à la place de l'un quelconque des autres systèmes $s, s_1, \ldots$, après quoi les substitutions de I, qui ne déplacent pas σ, permuteront ces derniers systèmes d'une manière deux fois transitive.

Cela posé, on verra, comme tout à l'heure, que $n > p + 2q$, et l'on partagera les lettres en deux catégories, formées respectivement des lettres que J déplace et de celles que J ne déplace pas. Parmi les groupes J, $J_1, \ldots$, transformés de J par les substitutions de G, il en existera qui permutent ensemble des lettres de catégorie différente. Parmi ces derniers groupes, soit J_1 l'un de ceux qui déplacent le nombre minimum r' de lettres de seconde catégorie. On trouvera, comme tout à l'heure, que les lettres du groupe $K = (J, J_1)$ se groupent r' à r' en systèmes; qu'on a $q = \mu' r'$, μ' étant le nombre des nouveaux systèmes dont la réunion forme chacun des anciens systèmes de q lettres $s, s_1, \ldots, \sigma$; et enfin que si $\mu' > 1$, les lettres de I pourront être groupées de deux manières distinctes en systèmes de q lettres.

Or I est deux fois transitif par rapport aux systèmes de q lettres s, $s_1, \ldots$ qu'il contient. Si donc ses lettres sont susceptibles de divers groupements en systèmes, chacun des nouveaux systèmes sera contenu en entier dans l'un des systèmes $s, s_1, \ldots$ (5). Donc il n'existe pas deux modes distincts de grouper les lettres de I en systèmes de q lettres. Donc $\mu' = 1$, et K contiendra $p + 3q$ lettres.

Continuant ce raisonnement, on aura successivement

$$n > p + 3q > p + 4q, \ldots$$

jusqu'à l'infini, ce qui est absurde.

Donc *μ ne peut se réduire à l'unité.*

8. Revenons donc à l'hypothèse $\mu > 1$. Si $r > 1$, on pourra raisonner sur I et J comme on l'avait fait sur H et I, de manière à établir que G contient un groupe K, déplaçant $p + q + r + s$ lettres (s étant

un sous-multiple de r), qu'il permute transitivement, et qui se groupent s à s en systèmes, par rapport auxquels K est deux fois transitif.

Si $s > 1$, on continuera de même, et l'on arrivera enfin à démontrer que G contient un groupe $\mathfrak{H}$ où chaque système ne contiendra plus qu'une seule lettre, et qui, par suite, sera deux fois transitif.

Soit d'ailleurs α le nombre des facteurs premiers de q. Le nombre $P = p + q + r + \ldots + 1$ des lettres déplacées par $\mathfrak{H}$ sera au plus égal à $p + q\left(1 + \frac{1}{2} + \ldots + \frac{1}{2^\alpha}\right) \leqq p + 2q - 1$.

9. Cela posé, si $n = P$, $\mathfrak{H}$ étant deux fois transitif, G le sera *a fortiori*, et le théorème sera démontré. Si $n > P$, on partagera les lettres de G en deux catégories, formées l'une des lettres que $\mathfrak{H}$ déplace, l'autre des lettres restantes. Parmi les groupes transformés de $\mathfrak{H}$ par les substitutions de G, et qui déplacent des lettres des deux catégories, soit $\mathfrak{H}_1$ l'un de ceux qui déplacent le moindre nombre u de lettres de seconde catégorie. Les lettres de $\mathfrak{H}$ pourront être groupées en systèmes u à u (**3**). Mais $\mathfrak{H}$, étant doublement transitif, sera évidemment primitif; donc u se réduit à l'unité, et le groupe $\mathfrak{H} = (\mathfrak{H}, \mathfrak{H}_1)$ déplacera $P + 1$ lettres, par rapport auxquelles il sera trois fois transitif. Si $n = P + 1$, G sera *a fortiori* trois fois transitif. Si $n > P + 1$, on verra de même que G contient un groupe $\mathfrak{K}$ déplaçant $P + 2$ lettres, par rapport auxquelles il sera quatre fois transitif, etc. Donc enfin G sera $n - P + 2$ fois transitif, ce qui démontre le théorème.

10. Nous avons supposé jusqu'à présent $q > 1$, ce qui suppose qu'il existe deux modes différents de répartir les lettres de H en systèmes de q lettres (**6**). Si l'on avait, au contraire, $q = 1$, I serait deux fois transitif par rapport aux $p + 1$ lettres qu'il déplace, et le raisonnement du numéro précédent serait applicable en y remplaçant P par $p + 1$. Donc G sera $n - p + 1$ fois transitif.

11. Corollaire. — *Si* G *n'est pas symétrique ou alterné, son degré n sera limité.* En effet, G ne peut être plus de $\frac{n+4}{3}$ fois transitif. On aura donc l'inégalité

$$\frac{n+4}{3} \geqq n - p - 2q + 3; \quad \text{d'où} \quad n \leqq \frac{3p + 6q - 5}{2} < 3p - 2,$$

en remarquant que q est un sous-multiple de p, au plus égal à $\frac{l'}{2}$. Si q se réduit à l'unité, on aura $n \leq \frac{3p+1}{2}$.

12. THÉORÈME II. — *Soit* A *une substitution quelconque, déplaçant* N *lettres. Un groupe primitif* G, *contenant la substitution* A, *sera nécessairement symétrique ou alterné, dès que son degré atteindra une certaine limite* A.

On peut supposer dans la démonstration de ce théorème que G ne contient aucune substitution qui déplace moins de N lettres. On peut admettre, en outre, que A est d'ordre premier p; car parmi les puissances de A, il en est une d'ordre premier, que G contiendra s'il contient A. On aura dans cette hypothèse $N = pl$, l étant le nombre des cycles de A.

Si A ne déplace que deux ou trois lettres, G sera symétrique ou alterné, et le théorème sera évident. Supposons qu'il reste vrai tant que A déplacera moins de N lettres. Soient L_1, L_2,... les limites correspondantes aux diverses formes que pourrait revêtir dans cette hypothèse la substitution A; L le plus grand des entiers L_1, L_2,..., $5N+4$. Nous allons démontrer que le théorème sera vrai si A déplace N lettres, et que G sera symétrique ou alterné, dès que son degré atteindra la limite $A = 3(Le - p)(N-1) + 1$, e étant le plus grand entier contenu dans $\frac{N}{2}$.

D'après le n° **11**, il nous suffira pour cela d'établir la proposition suivante :

LEMME. — *Le groupe* G *contient un groupe* Γ, *qui ne déplace pas plus de* $(Le - p)(N-1)+1$ *lettres, et les permute transitivement.*

13. Les N lettres que A déplace peuvent se répartir en l classes, en groupant ensemble les p lettres que les puissances de A permutent entre elles. Soit C l'une quelconque de ces classes. Parmi les substitutions A, A_1, A_2,... transformées de A par les substitutions de G, il en existe au moins une A_1 qui ne permute pas exclusivement entre elles les lettres de C, sans quoi, le groupe (A, A_1, A_2,...) n'étant pas transitif, le groupe G, qui lui est permutable, ne serait pas primitif.

Cela posé, A_1 déplaçant N lettres, dont une au moins était déjà déplacée par A, le nombre des lettres déplacées par les substitutions du groupe (A, A_1) sera au plus égal à $2N - 1$. Répartissons ces lettres en classes, en groupant ensemble celles que les substitutions de (A, A_1) permutent entre elles. Les lettres de C appartiendront évidemment à une même classe C_1, laquelle contiendra également les lettres que A_1 leur fait succéder, et dont une au moins, par hypothèse, ne faisait pas partie de C. Donc le nombre p_1 des lettres de C_1 ne pourra être $< p + 1$ ni $> 2N - 1$.

Le nombre des lettres de G, étant supposé égal ou supérieur à A, sera $> p_1$; et pour que G soit primitif il faudra que la suite $A_2, \ldots$ contienne au moins une substitution A_2 qui ne permute pas exclusivement entre elles les lettres de C_1. Le groupe (A, A_1, A_2) déplacera au plus $3N - 2$ lettres, qu'on pourra répartir en classes, en groupant ensemble celles que (A, A_1, A_2) permute entre elles; et celles de ces classes, C_2, qui contient C_3, contient un nombre de lettres p_2 au moins égal à $p + 2$, au plus égal à $3N - 2$.

Le nombre des lettres de G est $> p_2$; et continuant ainsi, on arrivera à montrer que G contient un groupe $H = (A, A_1, \ldots, A_{Le-p})$ déplaçant au plus $(Le - p)(N - 1) + 1$ lettres, qui pourront être groupées en classes, dont l'une C_{Le-p} contiendra au moins Le lettres.

S'il n'y a qu'une classe, notre lemme sera démontré, car H satisfera aux conditions que l'énoncé impose au groupe Γ.

14. Admettons donc qu'il y ait plusieurs classes. Chacune des substitutions de H est le produit de substitutions partielles permutant respectivement les lettres de chacune d'elles. Soit H_ρ le groupe formé par celles de ces substitutions partielles qui déplacent les lettres de la $\rho^{ième}$ classe, et soit m_ρ le nombre des lettres de cette classe. On pourra les répartir en systèmes tels, que chaque substitution de H_ρ remplace les lettres de chaque système par celles d'un même système. (Si H_ρ était primitif, chaque système se réduirait à une lettre.) S'il existe divers modes de répartition, adoptons l'un de ceux où le nombre k_ρ des lettres de chaque système est maximum. Les déplacements d'ensemble opérés sur ces systèmes par les substitutions de H_ρ formeront un groupe primitif K_ρ, car sans cela on pourrait grouper ces systèmes

en systèmes plus généraux et moins nombreux, contrairement à l'hypothèse.

Chaque système contiendra au plus e lettres. — En effet, parmi les substitutions $A, A_1, \ldots, A_{Le-p}$, il en existe une au moins qui permute les systèmes de la classe ρ. Elle déplacera au moins deux systèmes, dont elle déplacera toutes les lettres; mais elle ne déplace en tout que N lettres. Donc k_ρ est au plus égal à $\frac{N}{2}$, et comme il est entier, il sera au plus égal à e.

Cela posé, si l'une des substitutions $A, A_1, \ldots, A_{Le-p}$, par exemple A_1, déplace N systèmes, chacun d'eux ne contiendra qu'une lettre, et le groupe H_ρ, se confondant avec K_ρ, sera primitif. Le groupe Γ, dérivé de A_1 et de ses transformées par les substitutions de H_ρ (ou, ce qui revient au même, par celles de H), étant permutable aux substitutions de H_ρ, sera transitif par rapport aux m_ρ lettres qu'il déplace (*Traité des Substitutions,* n° **53**); et comme $m_\rho < (Le - p)(N - 1) + 1$, le lemme sera démontré.

15. Supposons, au contraire, que celles des substitutions de la suite $A, A_1, \ldots, A_{Le-p}$ qui déplacent les systèmes de H_ρ déplacent chacune moins de N systèmes, et cela, pour toutes les valeurs de l'indice ρ. Si le nombre q_ρ de ces systèmes atteint ou dépasse L, le groupe K_ρ, étant primitif, et contenant des substitutions qui déplacent moins de N systèmes, sera symétrique ou alterné, par hypothèse (**11**). Cette circonstance se présentera pour une valeur au moins de ρ, puisqu'il existe une classe contenant au moins Le lettres, et que chaque système n'en peut contenir plus de e.

16. Soit q le plus grand des nombres $q_1, q_2, \ldots$, et supposons, pour fixer les idées, que $q_1, \ldots, q_\beta$ soient égaux, et $q_{\beta+1}, \ldots$ inférieurs à q. Soit enfin I un groupe aussi général que possible parmi ceux qui sont contenus dans H et satisfont à la double condition suivante :

1° Faire subir aux systèmes de l'une au moins des β premières classes (par exemple à ceux de la classe ρ) un ensemble de déplacements dont la combinaison forme un groupe i_ρ symétrique ou alterné;

2° Subsidiairement, déplacer le moins de lettres possible.

Le groupe I, ainsi défini, existera toujours, car, à défaut de groupe déplaçant moins de lettres, on aurait toujours le groupe H, qui satisfait à la première condition. Il jouira de propriétés importantes, que nous allons développer.

17. Soient S, S',... les substitutions de I; s_σ, s'_σ,... les déplacements qu'elles font subir aux systèmes de l'une quelconque σ des classes dont elles déplacent les lettres.

A deux substitutions distinctes de la suite s_ρ, s'_ρ, ... *correspondront toujours deux substitutions distinctes dans la suite* s_σ, s'_σ,....

Supposons, en effet, qu'on ait $s_\sigma = s'_\sigma$, sans avoir $s_\rho = s'_\rho$. La substitution $S'S^{-1} = T$ ne déplace pas les systèmes de la classe σ, et fait subir à ceux de la classe ρ le déplacement $s'_\rho s_\rho^{-1} = t_\rho$. Les transformées de T par les substitutions de I forment un groupe J dont les substitutions ne déplaceront pas les systèmes de la classe σ et feront subir à ceux de la classe ρ des déplacements qui seront les transformés de t_ρ par s_ρ, s'_ρ,... et formeront un groupe j_ρ, contenu dans i_ρ et permutable à ses substitutions. Mais i_ρ est symétrique ou alterné; donc j_ρ le sera également (*Traité des Substitutions*, n^os^ **81** et **85**).

La suite t_ρ, t'_ρ,... des déplacements que les substitutions T, T',... de J font subir aux systèmes de la classe ρ contiendra donc $1.2...q$ ou $\frac{1.2...q}{2}$ termes distincts. Soit, d'autre part, α l'une des lettres de la classe σ, qui soit déplacée par les substitutions de I. Les substitutions T, T',... permutent exclusivement ensemble les lettres, en nombre $k_\sigma \leqq e$, qui appartiennent au même système que α. La suite θ, θ',... des déplacements que ces lettres éprouvent par les substitutions T, T',... contient donc au plus $1.2...k_\sigma$ termes distincts, nombre inférieur à $\frac{1.2...q}{2}$. On pourra donc trouver dans cette suite deux termes θ et θ' semblables entre eux et correspondant à des termes différents t_ρ et t'_ρ. Raisonnant alors comme précédemment, on voit que $T'T^{-1} = U$ et ses transformées par les substitutions de J forment un groupe contenu dans J et *a fortiori* dans I, qui satisfera encore à la première condition imposée à I, quoique ne déplaçant plus la lettre α; résultat inadmissible, vu la seconde condition à laquelle I est censé satisfaire.

18. *Les seules lettres que* I *puisse déplacer sont celles des* β *premières classes.* — Car si l'on avait $\sigma > \beta$, d'où $q_\sigma < q$, le nombre des substitutions distinctes de la suite $s_\sigma, s'_\sigma, \ldots$, lequel divise $1.2\ldots q_\sigma$, serait $< \frac{1.2\ldots q}{2}$, ce qui est inadmissible, d'après le numéro précédent.

On aura donc $\sigma \leqq \beta$. Il faut d'ailleurs que le groupe $i_\sigma = (s_\sigma, s'_\sigma, \ldots)$ contienne autant de substitutions que le groupe i_ρ. Donc, si i_ρ est symétrique, i_σ le sera; d'ailleurs la réciproque est vraie, car on peut échanger ρ et σ dans le raisonnement. Si au contraire i_ρ est alterné, i_σ le sera.

19. Soient $a_\rho, b_\rho, \ldots$ les q systèmes de la classe ρ; I_a le groupe formé par celles des substitutions de I qui laissent immobile le système a_ρ; ces substitutions font subir aux systèmes $b_\rho, \ldots$ des déplacements formant un groupe $i_{\rho a}$ d'ordre $1.2\ldots(q-1)$ ou $\frac{1.2\ldots(q-1)}{2}$, suivant que I_ρ est symétrique ou alterné. Les déplacements effectués par les mêmes substitutions sur les q systèmes de la classe σ formeront un groupe $i_{\sigma a}$ d'ordre $1.2\ldots(q-1)\left[\text{ou } \frac{1.2\ldots(q-1)}{2}\right]$. Or M. Bertrand a montré qu'un groupe ne peut avoir cet ordre que s'il est symétrique (ou alterné) par rapport à $q-1$ de ces systèmes. Donc les substitutions de $i_{\sigma a}$ laissent immobile un des systèmes de la classe σ; soit a_σ ce système.

Soit de même I_b le groupe formé par celles des substitutions de I qui laissent immobile le système b_ρ; elles laisseront immobile un des systèmes de la classe σ, que nous appellerons b_σ, etc.

Cela posé, *chaque substitution* S *du groupe* H *est permutable à* I, *et déplace les systèmes* $a_\sigma, b_\sigma, \ldots$ *de la même manière que les systèmes correspondants* $a_\rho, b_\rho, \ldots$. En effet, soit I' le groupe transformé de I par S. Si I' différait de I, le groupe (I, I') serait plus général que I, bien que déplaçant les mêmes lettres, et jouissant des mêmes propriétés caractéristiques, résultat contraire à notre hypothèse. Donc S est permutable à I. Supposons d'ailleurs que S remplace a_ρ par b_ρ, et a_σ par un système x. Il est clair que S transformera I_a en I_b, dont les substitutions laissent immobile le système b_σ; mais, d'autre part,

I_a laissant a_σ immobile, le système que son transformé laisse immobile sera x. Donc $x = b_\sigma$, ce qu'il fallait démontrer.

Soit $\gamma \gtreqless \beta$ le nombre des classes ρ, σ,... dont I déplace les lettres. Il est permis de supposer que ces classes sont les γ premières.

20. Nous allons maintenant établir la proposition suivante :

Si l'un des entiers k_1,..., k_γ, par exemple k_1, est plus grand que l'unité, H *contiendra une substitution* X, *qui déplace moins de* $2N$ *lettres, et qui déplace les lettres d'un système appartenant à l'une des γ premières classes, tout en laissant ce système immobile.*

Dans ce but, nous observerons que, parmi les substitutions A, A_1,..., A_{Le-p} dont H est dérivé, il en existe une au moins A qui déplace quelques-uns des systèmes de la première classe. Soit r le nombre de ces systèmes qu'elle déplace; elle déplacera d'une manière analogue les systèmes correspondants de chacune des γ premières classes. Ces systèmes contiennent en tout $r(k_1 + \ldots + k_\gamma)$ lettres, que A déplace toutes. Mais elle déplace en tout N lettres. Donc on aura $N \geqq r(k_1 + \ldots + k_\gamma)$, suivant que A déplace ou non d'autres lettres que celles-là.

Si elle en déplace d'autres, on peut admettre qu'elles appartiennent aux classes $\gamma + 1$,.... Car si l'une d'elles appartenait à l'une des γ premières classes, A laissant immobile son système satisferait à toutes les conditions imposées à X, et notre proposition se trouverait démontrée dès l'abord.

On a d'ailleurs $q > N + 1 > r + 1$. Donc il existe dans la première classe deux systèmes au moins x_1, y_1, que A ne déplace pas. Soient, au contraire, a_1, b_1,... ceux qu'elle déplace. Le groupe I, permutant les systèmes de la première classe d'une manière symétrique ou alternée, contiendra une substitution B qui permute circulairement les trois systèmes a_1, x_1, y_1, sans déplacer les autres systèmes de cette classe; H contiendra la substitution $B^{-1}AB$, transformée de A par B, laquelle déplace N lettres, parmi lesquelles celles de b_1,..., et déplace les lettres des classes $\gamma + 1$,... de la même manière que A; il contiendra également la substitution $U = A^{-1}B^{-1}AB$, laquelle déplace moins de $2N$ lettres, appartenant toutes aux γ premières classes, et laisse

immobiles tous les systèmes de la première classe, sauf a_1, x_1, b_1 qu'elle permute circulairement. Elle déplace d'ailleurs de la même manière les systèmes correspondants de chacune des γ premières classes; et, par suite, elle déplacera au moins $3(k_1 + \ldots + k_\gamma) = N'$ lettres. Si elle en déplace d'autres, ce sera sans déplacer les systèmes auxquels elles appartiennent, et par suite U satisfera à toutes les conditions que l'énoncé impose à la substitution X dont nous voulons prouver l'existence.

Admettons, au contraire, que U ne déplace que N' lettres; ce nombre ne pouvant être inférieur à N, par hypothèse, r se réduira à 2 ou à 3.

21. Supposons, par exemple, que $r = 3$; et soient a_1, b_1, c_1 les trois systèmes de la première classe que A permute entre eux; on pourra évidemment établir entre les lettres de ces trois systèmes une correspondance telle, que A fasse succéder à chaque lettre de a_1 sa correspondante du système b_1, et à celle-ci sa correspondante du système c_1. D'ailleurs A^p se réduisant à l'unité ne déplace aucun système; donc p est un multiple de 3, et comme il est premier, il se réduira à 3; donc $A^3 = 1$, et par suite A remplacera chaque lettre de c_1 par sa correspondante de a_1.

Cela posé, I étant alterné, et *a fortiori* trois fois transitif par rapport aux systèmes a_1, b_1, c_1,... de la première classe, contient une substitution C qui remplace les systèmes a_1, b_1, c_1 par les systèmes b_1, c_1, d_1; et H contiendra la substitution $A' = C^{-1}AC$, qui permute circulairement les trois systèmes b_1, c_1, d_1. Si A' ne remplace pas chaque lettre de b_1 par sa correspondante de c_1, H contiendra la substitution $A'A^{-1}$, laquelle satisfera aux conditions imposées à X, car elle déplace moins de 2N lettres et permute ensemble les lettres de b_1. Dans le cas contraire, on pourra faire correspondre à chaque lettre de c_1 celle des lettres de d_1 que A' lui fait succéder, et que A' remplacera elle-même par sa correspondante de b_1. On verra de même (en continuant à exclure les hypothèses desquelles résulte l'existence de la substitution cherchée X) que H contient une substitution A'' qui permute les trois systèmes c_1, d_1, e_1 en remplaçant les unes par les autres les lettres correspondantes, etc. Des substitutions A, A', A'',...

combinées ensemble, on déduira par une suite de transformations une substitution $\mathfrak{A}$ qui permute entre eux trois systèmes quelconques de la première classe, x_1, y_1, z_1, en remplaçant les unes par les autres les lettres correspondantes. D'ailleurs A, A', A'',..., $\mathfrak{A}$, étant les transformées successives d'une même substitution A, déplaceront chacune N lettres.

Cela posé, H permutant transitivement les lettres de la première classe, l'une au moins des substitutions A, A_1,... de degré N dont il est dérivé, déplacera quelqu'une de ces lettres sans lui faire succéder une de ses correspondantes. Si cette substitution A_1 ne déplace pas le système x_1 auquel cette lettre appartient, elle satisfera aux conditions imposées à X. Si au contraire elle fait succéder le système x_1 au système y_1, H contiendra $A_1 \mathfrak{A}^{-1}$ qui satisfait à ces conditions.

Si l'on avait $r = 2$, la démonstration serait la même.

22. L'existence de la substitution X étant ainsi démontrée, formons avec les systèmes des γ premières classes le tableau suivant :

$$(1) \qquad \left| \begin{array}{cccccc} a_1 & b_1 & \dots & f_1 & g_1 & \dots \\ a_2 & b_2 & \dots & f_2 & g_2 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_\gamma & b_\gamma & \dots & f_\gamma & g_\gamma & \dots \end{array} \right|$$

Les lettres déplacées par X, et *a fortiori* celles de ces lettres qui appartiennent aux γ premières classes sont en nombre inférieur à 2N. Le nombre des colonnes distinctes du tableau (1) où figurent les systèmes dont ces lettres font partie sera *a fortiori* inférieur à 2N. Supposons, pour fixer les idées, que ces lettres appartiennent toutes aux systèmes des premières colonnes $a,\dots,f$. Le nombre ν des colonnes suivantes $g,\dots$ sera supérieur à $q - 2N$. Soit, d'autre part, f_1 le système dont X déplace les lettres tout en laissant le système lui-même immobile.

Le groupe I, permutant d'une manière symétrique ou alternée les diverses colonnes de systèmes du tableau (1), contiendra un groupe partiel I' dont les substitutions laissent immobiles les colonnes a,

$b, \ldots$, et permutent d'une manière symétrique ou alternée les colonnes $f, g, \ldots$.

23. Soit J un groupe aussi général que possible parmi ceux qui sont contenus dans I' et satisfont à la double condition suivante :

1° Permuter d'une manière symétrique ou alternée les colonnes $f, g, \ldots$;

2° Subsidiairement, déplacer le moins de lettres possible.

Nous allons démontrer que J laisse immobiles les lettres de tous les systèmes appartenant aux colonnes $a, b, \ldots$.

Supposons, en effet, que J déplace les lettres de a_1. Le nombre des positions distinctes que ses substitutions permettent d'assigner à ces lettres sera un diviseur de $1.2\ldots k_1$. Celui des déplacements différents que ces substitutions impriment aux $\nu+1$ colonnes $f, g, \ldots$ est un multiple de $\frac{1.2\ldots(\nu+1)}{2}$, nombre supérieur au précédent, car on a

$$\nu+1 > q-2\mathrm{N}+1 > \mathrm{L}-2\mathrm{N}+1 > e > k_1.$$

Donc J contient deux substitutions s et s', qui permutent de même les lettres de a_1 sans permuter de même les colonnes $f, g, \ldots$; il contiendra la substitution $t = s^{-1}s'$ qui permute ces colonnes sans déplacer les lettres de a_1. Les transformées de t par les substitutions de J formeront évidemment un groupe J' dont les substitutions permuteront les colonnes $f, g, \ldots$ d'une manière symétrique ou alternée, sans déplacer les lettres de a_1, que J déplaçait, résultat inadmissible, comme contredisant la seconde propriété du groupe J.

24. Cela posé, J contient une substitution Y qui permute circulairement les trois colonnes f, g, h. Et il est clair que la substitution $\mathrm{Z} = \mathrm{X}\mathrm{Y}^{-1}\mathrm{X}^{-1}\mathrm{Y}$ ne déplace aucun système, et laisse immobiles toutes les lettres, sauf celles des colonnes f, g; qu'elle déplace les lettres de f de la même manière que X, et qu'elle déplace en outre celles des lettres de g que Y fait succéder à celles des lettres de f que X déplace. Le nombre des lettres déplacées par Z est donc au plus égal à $2(k_1+\ldots+k_\gamma)$, nombre total des lettres des deux colonnes f, g. Mais il ne peut être moindre que $\mathrm{N} \geqq r(k_1+\ldots k_\gamma)$. Il faudra, pour que cela soit possible : 1° qu'on ait $r=2$; 2° que N ne surpasse pas

$2(k_1 + \ldots + k_\gamma)$ et, par suite, que A ne déplace aucune lettre autre que celles des deux colonnes qu'elle permute entre elles; 3° que Z déplace toutes les lettres des colonnes f, g, et, par suite, que X déplace toutes celles de f.

Celles des substitutions de la suite A, $A_1, \ldots, A_{Le-p}$ qui déplacent les lettres des γ premières classes seront donc de deux sortes : 1° celles qui déplacent des systèmes; celles-là permuteront deux colonnes, et ne déplaceront aucune autre lettre; 2° celles qui ne déplacent pas de systèmes; celles-là déplaceront toutes les lettres d'une colonne dès qu'elles en déplacent une seule; elles déplaceront donc chacune les lettres de deux colonnes, ou celles d'une seule colonne avec des lettres des classes $\gamma + 1, \ldots$.

25. Soit A_{ab} une des substitutions de la première sorte, qui permute ensemble les colonnes a et b, par exemple. Les substitutions de I permutent les colonnes d'une manière alternée; donc parmi les transformées de A_{ab} par ces substitutions, il en existera une A_{bc} qui permute les colonnes b et c, une cd qui permute les colonnes c et d, etc. On pourra d'ailleurs établir entre les lettres de ces colonnes une correspondance telle, que chacune de ces substitutions échange entre elles les lettres correspondantes des systèmes qu'elle déplace (**21**). Ces substitutions $A_{ab}, A_{bc}, \ldots$, combinées ensemble par voie de transformation, fourniront une substitution A_{xy} permutant les lettres correspondantes de deux colonnes quelconques x, y.

Désignons maintenant par $B_a, B'_a, \ldots$ des substitutions opérées sur les lettres de la colonne a, par $B_b, B'_b, \ldots$ les substitutions analogues opérées sur les lettres correspondantes de b, etc., par M, M', ... des substitutions qui ne déplacent pas les lettres des γ premières classes. Celles des substitutions de la suite A, $A_1, \ldots, A_{Le-p}$ qui déplacent les lettres de deux colonnes x et y seront évidemment de la forme $A^{\mu}_{xy} B_x B'_y$, μ étant égal à zéro ou à 1, suivant que la substitution considérée laisse les colonnes immobiles ou les permute entre elles; et celles qui ne déplacent les lettres que d'une colonne z seront de la forme MB''_z.

Cela posé, le groupe $H = (A, A_1, \ldots, A_{Le-p})$ étant transitif, celles de ses substitutions qui ne déplacent pas la colonne a permutent transitivement les lettres de chacun des systèmes $a_1, a_2, \ldots, a_\gamma$. *A fortiori*,

ces lettres seront permutées transitivement par les substitutions du groupe plus général $\mathfrak{H}$ dérivé des substitutions $A_{ab},\ldots, A_{xy},\ldots, B_a, B'_a, B''_a,\ldots, B_x, B'_x, B''_x,\ldots, M,\ldots$.

26. Nous pouvons maintenant établir la proposition suivante, but des développements précédents :

Le groupe $\mathfrak{H}$ formé par celles des substitutions de I *qui ne déplacent que les lettres de deux colonnes a, b permute transitivement les lettres de chacun des systèmes $a_1, a_2,\ldots, b_1, b_2,\ldots$.*

Car I contient la substitution $A_{xy}^{-\mu}.A_{xy}^{\mu}B_xB'_y = B_xB'_y$ dont $\mathfrak{H}$ contiendra les transformées $B_aB'_b$ et $B_bB'_a$ par les substitutions $A_{ax}A_{by}$ et $A_{ay}A_{bx}$ qui sont contenues dans I. De même $\mathfrak{H}$ contiendra la substitution $A_{az}^{-1}MB''_zA_{az}.A_{bz}(MB''_z)^{-1}A_{bz}^{-1} = B''_aB''^{-1}_b$. Donc les substitutions de $\mathfrak{H}$ font subir aux lettres de a les mêmes déplacements $B_a, B'_a, B''_a,\ldots$ que celles de $\mathfrak{H}$; donc elles permutent transitivement les lettres de chacun des systèmes $a_1, a_2,\ldots$. De même évidemment pour celles des systèmes $b_1, b_2,\ldots$.

27. Cela posé, les transformées $A, A_1,\ldots, A_{Le-p}, A_{Le-p+1},\ldots$ de A par les substitutions de G formant un groupe transitif, l'une d'elles au moins, A_{Le-p+1}, permutera les lettres de la première classe avec d'autres lettres, dont chacune pourra, soit appartenir à l'une des $\gamma-1$ autres classes de lettres que I déplace, soit n'être pas déplacée par I. Cette substitution, jointe à I, donnera un groupe H'. Réunissons dans une même classe toutes les lettres que ce dernier groupe permute entre elles. Ces nouvelles classes pourront être de deux sortes : 1° celles qui sont formées par les lettres d'une ou plusieurs des classes de I, jointes ou non à des lettres nouvelles, que I ne déplaçait pas; 2° celles qui sont formées exclusivement de lettres nouvelles. Ces dernières contiendront moins de N lettres, la substitution A_{Le-p+1} ne déplaçant en tout que N lettres, qui ne sont pas toutes nouvelles.

Considérons l'une quelconque Θ des classes de la première sorte, et supposons-la formée des lettres des δ premières classes de I, jointes à m lettres nouvelles, m étant $< N$ et pouvant se réduire à zéro. Le groupe H'_1, formé par les déplacements que les substitutions de H' font subir aux lettres de Θ, pourra n'être pas primitif; mais, dans ce

cas, adoptons parmi les divers modes de répartition de ces lettres en systèmes celui où chaque système contient le nombre *maximum* de lettres, sans toutefois contenir toutes celles de Θ; le groupe K'_1 formé par les déplacements d'ensemble de ces systèmes sera primitif. D'ailleurs *les lettres de chacune des colonnes du tableau suivant*

$$(2)\qquad \begin{cases} a_1 & b_1 & c_1 & \dots \\ a_2 & b_2 & c_2 & \dots \\ \vdots & \vdots & \vdots & \vdots \\ a_\delta & b_\delta & c_\delta & \dots \end{cases}$$

formeront à elles seules un ou plusieurs systèmes.

Soient, en effet, α une quelconque des lettres d'un système a_i appartenant à la colonne a, γ_ρ une lettre quelconque de l'un c_ρ des systèmes d'une autre colonne c, ε une lettre nouvelle; nous allons démontrer que α ne peut être contenu dans le même système que γ_ρ ou ε.

Si α était contenu dans le même système que γ_ρ, les substitutions de $\mathfrak{H}$, ne déplaçant pas γ_ρ, ne déplaceront pas ce système, et, comme elles permutent α avec toutes les lettres de a_i, ce système contiendra toutes ces lettres. D'autre part, un raisonnement identique à celui du n° **23** montre que I contient un groupe dont les substitutions laissent immobiles les lettres de la colonne c, et permutent les autres colonnes a, b, d,... d'une manière symétrique ou alternée. Ces substitutions, ne déplaçant pas γ_ρ, ne déplaceront pas son système; donc les lettres de b_i, d_i,..., qu'elles font succéder à celles de a_i, appartiendront à ce système. De même, les substitutions de I qui permutent ensemble les colonnes b, c, d,... d'une manière symétrique ou alternée, sans déplacer les lettres de la colonne a, laisseront le système immobile, puisqu'elles ne déplacent pas a_i. Donc les lettres de c_i qu'elles font succéder à celles de b_i appartiennent à ce système. Ce système contiendra donc toutes les lettres de la première classe de I, en nombre qk_i. La substitution A_{Le-p+1}, ne déplaçant que N lettres, laissera invariables une partie de celles-là; donc elle ne déplacera pas le système considéré. De même pour les substitutions de I, qui permutent ensemble les lettres de la première classe de I. Donc aucune des sub-

stitutions de H' ne déplacera ce système ; donc ce système contiendrait, contrairement à l'hypothèse, toutes les lettres de Θ, que H' permute avec α.

Si α était contenu dans le même système que ε, ce système ne serait pas déplacé par les substitutions de I, qui ne déplacent pas ε; il contiendrait donc les lettres de la première classe de I, que ces substitutions permutent avec α; et l'on voit, comme tout à l'heure, qu'il contiendrait toutes les lettres de Θ.

Le nombre des lettres de chaque colonne étant $k_1 + \ldots + k_\delta$, sera au plus égal à $k_1 + \ldots + k_\gamma = \frac{N}{2} = e$. *Le nombre de lettres de chaque système sera donc au plus égal à e.*

Soient ζ le nombre des systèmes de Θ formés par chacune des q colonnes $a, b, c, \ldots$; η le nombre des systèmes restants formés par les m lettres nouvelles; Θ contiendra $q\zeta + \eta$ systèmes, nombre au moins égal à q.

28. Le nombre total des lettres déplacées par A_{Le-p+1} étant N, celles de ces lettres qui sont contenues dans les colonnes du tableau (2) ne pourront se trouver dans plus de N colonnes distinctes; et, l'ordre des colonnes étant indifférent, on peut admettre qu'elles se trouvent dans les $N+1$ premières colonnes $a, b, \ldots, d$ du tableau (2). Un raisonnement identique à celui du n° **23** montrera d'ailleurs que I contient un groupe dont les substitutions permutent d'une manière symétrique ou alternée les $N+1$ colonnes considérées sans déplacer les lettres des autres colonnes. Ce groupe, combiné avec $\mathfrak{H}$, donnera un groupe $\mathfrak{H}_1$, contenu dans I et permutant transitivement entre elles les lettres de $a_\rho, b_\rho, \ldots, d_\rho$ sans déplacer celles de $e_\rho, f_\rho, \ldots$ pour toute valeur de l'indice ρ comprise entre 1 et γ.

29. La substitution A_{Le-p+1} et ses puissances permutant ensemble des lettres qui appartiennent aux classes $1, \ldots, \delta$, et dont aucune n'appartient aux colonnes $e, f, \ldots$, jointes à des lettres nouvelles en nombre m, cette substitution, jointe à $\mathfrak{H}_1$, donnera un nouveau groupe Γ, permutant transitivement les lettres de $a_1, b_1, \ldots, d_1$; $\ldots$; $a_\delta, b_\delta, \ldots, d_\delta$ et les m lettres nouvelles sans déplacer les autres lettres

de e. *A fortiori,* les déplacements que ces substitutions font subir aux $(N+1)\zeta+\eta$ systèmes formés par ces lettres constituent un groupe transitif Δ.

Le groupe K'_1, contenant le groupe Δ, sera symétrique ou alterné (**11**) si l'on a la relation

$$q\zeta+\eta \geqq 3[(N+1)\zeta+\eta)]-2,$$

laquelle devient évidente, en remarquant que l'on a

$$\eta \leqq m < N < N\zeta \quad \text{et} \quad q \geqq L > 5N+3.$$

Nous obtenons donc ce résultat :

Si dans chacune des classes de la première sorte on répartit les lettres en systèmes, on aura au moins q systèmes, que les substitutions de H' *permuteront d'une manière symétrique ou alternée. Le nombre de lettres de chaque système ne pourra surpasser e.*

Considérons, au contraire, une classe de la seconde sorte. Le nombre des lettres qu'elle déplace sera inférieur à N, et par suite à q.

30. Cela posé, de même que du groupe H on a déduit le groupe I, on déduira de H' un autre groupe I', dont les substitutions ne déplacent que les lettres de celles des classes de première sorte où le nombre des systèmes est *maximum ;* ce groupe I' jouira de toutes les propriétés de I.

On doit remarquer que les classes de I', étant formées chacune des lettres d'une ou plusieurs classes de I, auxquelles peuvent s'ajouter des lettres nouvelles, seront en nombre au plus égal à celui de ces dernières classes. De plus, la première classe de I' contient au moins une lettre de plus que la première de I. Si l'on admet, ce qui est permis, que parmi les classes de I la première est une de celles où le nombre des lettres est maximum, on voit que I' contiendra au moins une classe où ce maximum sera dépassé.

Raisonnant sur I' comme sur I, on en déduira un nouveau groupe I'', où le nombre des classes ne sera pas plus grand que dans I', et où l'une d'elles sera plus nombreuse que la plus nombreuse de I'.

Poursuivant ainsi, comme le nombre de lettres de la classe la plus nombreuse s'accroît constamment, on arrivera enfin à un groupe Γ^{ν} dans lequel cette classe contient toutes les lettres de G. Tous les raisonnements qui ont servi à établir les propriétés de I s'appliquent à chacun des groupes successifs $\Gamma', \ldots, \Gamma^{\nu}$. Donc chacun des systèmes a^{ν}, $b^{\nu}, \ldots$ entre lesquels se répartissent les lettres de Γ^{ν} contiendra au plus e lettres; et Γ^{ν} contiendra un groupe $\mathfrak{H}_1^{\nu}$ dont les substitutions permutent transitivement les lettres des $N+1$ systèmes $a^{\nu}, b^{\nu}, \ldots, d^{\nu}$, sans déplacer les autres lettres. Ce groupe contenant au plus $(N+1)e$ lettres, nombre inférieur à $(Le-p)(N-1)+1$, notre théorème est démontré.

31. L'examen de chaque cas particulier permettra de resserrer considérablement la limite A résultant de la démonstration précédente. Pour en donner un exemple, nous allons examiner le cas où la substitution A est d'ordre premier impair p, et contient deux cycles.

Soit $A=(a_1 a_2 \ldots a_p)(b_1 b_2 \ldots b_p)$. Parmi les substitutions transformées de A par les substitutions de G, il en existe une au moins A' qui ne permute pas exclusivement entre elles les lettres $a_1, a_2, \ldots, a_p$. Ici divers cas seront à discuter.

32. *Premier cas.* — A' ne déplace aucune des lettres $b_1, b_2, \ldots, b_p$. Si A' ne déplace qu'une portion des lettres $a_1, a_2, \ldots, a_p$, la substitution $A'^{-1}AA'=B$ aura pour second cycle $b_1 b_2 \ldots b_p$, et son premier cycle sera formé d'une portion des lettres $a_1, a_2, \ldots, a_p$ jointes à des lettres nouvelles $\alpha, \ldots$. Soit ν le nombre de ces dernières lettres. Soient encore Γ le groupe (A, B), Δ le groupe formé par les déplacements que ces substitutions font subir aux lettres $a_1, \ldots, a_p, \alpha, \ldots$. Ce groupe Δ sera $\nu+1$ fois transitif (théorème I). Cela posé, celles des substitutions de Γ qui laissent immobiles les lettres $b_1, \ldots, b_p$ forment un groupe Γ' évidemment permutable à toutes les substitutions de Γ, ou, ce qui revient au même, à celles de Δ. Il sera donc au moins ν fois transitif. Le groupe formé par celles de ses substitutions qui ne déplacent que $p+1$ lettres sera donc transitif. Donc G, contenant un groupe transitif de degré $p+1$, aura son degré au plus égal à $3p+1$ (**11**).

Si A′ déplace toutes les lettres $a_1,\ldots, a_p$, deux au moins de ces lettres, telles que a_1 et a_2, appartiendront au même cycle de A′, lequel contiendra encore des lettres nouvelles $\alpha,\ldots$. Supposons que a_1 et a_2 se suivent de q rangs dans ce cycle. On prendra $B = A'^{-q}AA'^{q}$, et cette substitution jouira des mêmes propriétés qu'à l'alinéa précédent.

33. *Deuxième cas.* — A′ déplace au moins une lettre de chacun des cycles de A (et réciproquement). Supposons d'abord que l'un des cycles de A′ contienne deux lettres, a_1, b_1, appartenant à des cycles différents dans A, et admettons que ces deux lettres se suivent de q rangs dans le cycle considéré.

Si A′ déplace les mêmes lettres que A, G contiendra le groupe (A, A′) transitif et de degré $2p$.

Si A′ laisse immobile une des lettres de A, telle que a_ρ, le groupe (A, A′) sera transitif, et son degré égal à $2p + m$, m étant le nombre de lettres déplacées par A′ sans l'être par A.

On peut admettre que m est au plus égal à $p - 1$. Soit, en effet, $m > p - 1$. La substitution $A'' = A'^{-q}AA'^{q}$, qui contient dans un de ses cycles les deux lettres b_1 et a_ρ, peut être comparée à A de la même manière que l'était la substitution A′. D'ailleurs le nombre μ des lettres nouvelles qu'elle contient est égal au nombre des lettres appartenant à A que A'^{q} remplace par des lettres nouvelles, nombre qui ne peut évidemment pas dépasser $2p - m - 1$, et serait $\leqq p - 1$, si m était supérieur à ce nombre.

Donc G contiendra un groupe transitif, dont le degré ne dépassera pas $3p - 1$. Nous allons démontrer que, si ce groupe Γ n'est pas primitif, ses lettres ne pourront être réparties en systèmes que d'une seule manière; d'où cette conclusion que le degré de G ne peut dépasser $\frac{9p}{2} - 1$ (**11**).

Considérons, en effet, un groupement quelconque en systèmes. Si deux des lettres $a_1,\ldots, a_p$, telles que a_1 et a_ρ, appartenaient au même système, toutes y appartiendraient; car, la substitution A^ρ ne déplaçant pas ce système, les p lettres a_1, a_ρ, $a_{2\rho}$, $a_{3\rho},\ldots$, qu'elle remplace les unes par les autres, feraient partie de ce système, que A ne déplace

pas. Cela posé, A′ laisserait immobiles quelques-unes des lettres ci-dessus ou contiendrait plusieurs de ces lettres dans un seul cycle. Dans l'un ou l'autre cas, elle ne déplacerait pas le système; donc toutes les substitutions de (A, A′) ne déplaceraient pas ce système, et, comme elles permutent transitivement les lettres, il n'y aurait qu'un système, contrairement à l'hypothèse.

D'autre part, si a_1 faisait partie du même système qu'une lettre α non déplacée par A, A ne déplacerait pas ce système, qui contiendrait par suite $a_1, a_2, \ldots, a_p$, ce qui est inadmissible. Donc le système qui contient a_1 ne contiendra qu'une autre lettre, prise dans le cycle $b_1 b_2 \ldots b_p$. Soit $b_{\sigma+1}$ cette lettre; A permutera transitivement p systèmes $a_1 b_{\sigma+1}$, $a_2 b_{\sigma+2}, \ldots, a_x b_{\sigma+x}$. D'après l'analogie des deux substitutions A, A′, il est clair que, si A′ contient dans l'un de ses cycles l'une des lettres a_x, $b_{\sigma+x}$, elle contiendra l'autre dans son autre cycle.

Supposons maintenant qu'il existe une seconde décomposition en systèmes, et soient $a_1 b_{\tau+1}, \ldots, a_x b_{\tau+x}, \ldots$ ceux de ces nouveaux systèmes qui sont formés par les lettres de A. La substitution A′, contenant a_1 dans son premier cycle, contiendra $b_{\tau+1}$ dans le second; donc elle contiendra $a_{\tau-\sigma+1}$ dans le premier, puis $b_{2\tau-\sigma+1}$ dans le second, etc. Donc $a_1, a_2, \ldots, a_p$ appartiendraient à son premier cycle, et $b_1, b_2, \ldots, b_p$ au second, ce qui est inadmissible, a_1 et b_1 appartenant au même cycle, par hypothèse.

34. Il nous reste à considérer le cas où la substitution A′ ne permet pas de permuter ensemble les lettres des deux cycles de A. Le premier cycle de A′ sera formé, dans cette hypothèse, des lettres $a_1, \ldots, a_p$, ou de quelques-unes seulement, jointes à de nouvelles lettres $a_{p+1}, \ldots, a_{p+q}$; son second cycle sera formé des lettres $b_1, \ldots, b_p$, ou d'une partie de ces lettres, jointes à de nouvelles lettres $b_{p+1}, \ldots, b_{p+r}$.

Parmi les transformées de A par les substitutions de G, il pourra en exister encore une A″, permutant, d'une part, les lettres $a_1, \ldots, a_{p+q}$ exclusivement entre elles, ou avec des lettres nouvelles $a_{p+q+1}, \ldots, a_{p+q+q'}$; d'autre part, les lettres $b_1, \ldots, b_{p+r}$ exclusivement entre elles, ou avec des lettres nouvelles $b_{p+r+1}, \ldots, b_{p+r+r'}$; puis une nouvelle substitution A‴ jouissant de propriétés analogues, etc. Tant que nous aurons de ces nouvelles substitutions, nous nous les adjoindrons, et

nous obtiendrons un groupe $H = (A, A', A'', \ldots)$ dont les lettres forment deux catégories $a_1, \ldots, a_s$ et $b_1, \ldots, b_t$, en réunissant ensemble celles que H permute entre elles.

Cela posé, parmi les substitutions transformées de A par les substitutions de G, il existe une substitution au moins A_1 qui ne permute pas exclusivement ensemble les lettres $a_1, \ldots, a_s$.

Supposons qu'elle remplace a_σ, par exemple, par une lettre autre que celles de cette catégorie; a_σ est déplacé par l'une au moins des substitutions A, A', A'',..., par exemple par A', dont le second cycle sera formé de lettres de la catégorie b. Si A_1 ne déplaçait aucune de ces dernières lettres, on pourrait la comparer avec A', et retomber ainsi sur le premier cas examiné plus haut. Donc A_1 déplacera quelqu'une des lettres $b_1, \ldots, b_t$. D'ailleurs elle contiendra dans un même cycle des lettres des deux catégories a et b; car, si elle ne permutait les a d'une part et les b d'autre part qu'avec des lettres nouvelles, on pourrait la joindre à A, A', A'',... pour former un nouveau groupe H' analogue à H, ce qu'on suppose n'être plus possible.

Admettons donc que A_1 contienne dans un même cycle a_σ et b_τ. Nous allons démontrer que H contient une substitution S, semblable à A, et qui déplace à la fois ces deux lettres. En effet, si t n'est pas $> p$, chacune des substitutions A, A', A'',... déplacera tous les b, et celle de ces substitutions qui déplace a_ρ pourra être prise pour S. Si $t > p$, H permute ensemble les lettres $b_1, \ldots, b_t$ d'une manière $t - p + 1$ fois transitive (théorème I), et dérivera évidemment de la combinaison d'une substitution quelconque A', prise parmi celles de la suite A, A', A'',... qui déplacent b_τ, avec le groupe H' formé de celles des substitutions de H qui ne déplacent pas b_τ. Le groupe H permutant transitivement les lettres de la suite $a_1, \ldots, a_s$, le groupe H' contiendra au moins une substitution B qui fait succéder a_σ à l'une des lettres de cette suite que A' déplaçait (si A' déplaçait a_σ, on prendrait pour B la substitution unité), et H contiendra la substitution $S = B^{-1}A'B$, qui déplace a_σ et b_τ.

Cela posé, si A_1 contient un cycle entier de lettres non déplacées par S, on pourra appliquer à ces deux substitutions le raisonnement du n° **32**, sinon on leur appliquera celui du n° **33**. Nous obtenons donc le théorème suivant :

THÉORÈME III. — *Soit* A *une substitution d'ordre premier p et conte-*

nant deux cycles. Tout groupe primitif G, *contenant la substitution* A, *sera symétrique ou alterné dès que son degré dépassera* $\frac{9p}{2} - 1$.

Ce théorème n'est démontré par ce qui précède que si p est impair; mais on vérifiera aisément qu'il est encore exact pour $p = 2$.

35. Nous conviendrons de dire qu'un groupe de substitutions appartient à la $N^{ième}$ classe, si celle de ses substitutions qui déplace le moins de lettres (l'unité exceptée) en déplace précisément N.

Cela posé, les résultats exposés dans ce Mémoire conduisent immédiatement à cette conséquence remarquable, que *chaque classe ne contient qu'un nombre limité de groupes primitifs* (sauf les classes 2 et 3 qui contiennent les groupes symétriques et alternés de tous les degrés).

En effet, les groupes primitifs de la classe N ont leur degré limité (théorème II); et chaque degré ne peut d'ailleurs fournir qu'un nombre limité de groupes.