BULLETIN DE LA S. M. F.

CAMILLE JORDAN

Mémoire sur les groupes primitifs

Bulletin de la S. M. F., tome 1 (1872-1873), p. 175-221

<http://www.numdam.org/item?id=BSMF_1872-1873__1__175_1>

Mémoire sur les groupes primitifs ; par M. CAMILLE JORDAN.

(Séance du 30 avril 1873)

Nous avons démontré, dans un précédent mémoire (*Journal de Liouville*, 2e série, t. XVI), que le degré d'un groupe primitif G, ne contenant pas le groupe alterné, mais contenant une substitution donnée A qui déplace N lettres, ne saurait dépasser une certaine limite $L = N + M$. La quantité M est une fonction F(N) du nombre N.

Nous examinons, dans le mémoire qui suit, le cas où l'ordre de A est un nombre premier p. Tous les autres cas peuvent se ramener à celui-là ; car une substitution quelconque, élevée à une puissance convenable, donne une substitution d'ordre premier.

Nous arrivons à ce résultat remarquable, qu'*on peut assigner à* M *une valeur qui ne dépend pas du nombre p, mais seulement du nombre q des cycles de* A. Nous démontrons, en effet, qu'on peut assigner deux fonctions de q, $\varphi(q)$ et $f(q)$ jouissant de la propriété suivante :

Le degré d'un groupe primitif G, *ne contenant pas le groupe alterné, mais contenant une substitution* A *d'ordre premier p et à q cycles, ne peut dépasser* $pq + \varphi(q)$, *si l'on a* $p > f(q)$.

Donc, en appelant $\mathfrak{F}(q)$ la plus grande des quantités $F(2q)$, $F(3q)$, ..., $F(f(q)q)$, $\varphi(q)$, on pourra prendre pour limite $L = pq + \mathfrak{F}(q) = N + \mathfrak{F}(q)$.

Le premier paragraphe de notre mémoire est consacré à démontrer la proposition suivante, qui est le fondement de notre analyse :

Soit A une substitution d'ordre premier p à q cycles; si le groupe primitif G contient la substitution A, on pourra y déterminer une suite de substitutions A, B, C, ... semblables à A, et dont chacune déplace quelque lettre que les précédentes laissaient immobile, jusqu'à ce que l'on ait épuisé le nombre des lettres de A; mais si $p > q$, on pourra déterminer la suite A, B, C, ..., de telle sorte que chacune de ces substitutions successives ne puisse contenir dans aucun de ses cycles plus d'une lettre nouvelle.

Cela posé, notre théorème étant supposé démontré pour les nombres inférieurs à q (nous avons trouvé précédemment, p. 42, lorsque $q = 1$, $\varphi(q) = 2$, quel que soit p), nous le démontrons pour q, en établissant des formules récurrentes qui lient $\varphi(q)$ et $f(q)$ à $\varphi(q-1), \ldots, f(q-1), \ldots$. C'est là l'objet des sections II à VI.

Dans la section VII, nous discutons ces formules, et nous en déduisons les inégalités suivantes :

$$\varphi(q) \leqslant \frac{2}{\log 2} q \log q + 2q,$$

en prenant pour $f(q)$ la plus grande des quantités suivantes :

$$\frac{2}{\log 2} q \log q + q + 1, \quad 3q + 2, \quad 18.$$

Il est certain d'ailleurs, d'après notre mode d'opérer, que ces limites sont loin d'être assez resserrées. Une étude plus minutieuse (VIII) nous a en effet montré qu'on pouvait prendre pour limites

$$\varphi(q) = q + 1, \quad f(q) = q,$$

lorsque $q = 2, 3, 4$ ou 5; et nous avons de fortes raisons de croire qu'on arriverait au même résultat pour les valeurs suivantes de q.

I

1. Soient G un groupe primitif; A l'une de ses substitutions; A, A', ... les diverses substitutions semblables à A qui sont contenues dans G. Il est clair que toute substitution de G les transformera les unes dans les autres; donc le groupe $H = (A, A', \ldots)$ sera permutable à toutes les substitutions de G.

Le groupe H sera transitif; car, sans cela, on sait que G ne pourrait être primitif. Si donc A ne déplace qu'une partie des lettres, l'une au moins des autres substitutions A', ..., dont H est dérivé, contiendra réunies dans un de

ses cycles des lettres déplacées par A et quelques-unes des lettres restantes ; sans quoi H, permutant exclusivement entre elles les lettres que A déplace, ne serait pas transitif. Si la suite A′, ... contient plusieurs substitutions jouissant de la propriété ci-dessus, soit B l'une d'elles, choisie de telle sorte que G ne contienne aucune substitution qui jouisse des mêmes propriétés, tout en ne déplaçant qu'une partie des lettres nouvelles que B déplace.

S'il existe encore des lettres qui ne soient déplacées ni par A ni par B, l'une au moins des substitutions A′, ... devra de même mêler dans ses cycles quelques-unes de ces lettres à celles que déplaçaient déjà A et B. Si plusieurs de ces substitutions jouissent de cette propriété, on en choisira une C de telle sorte qu'il n'y en ait pas d'autre qui ne déplace qu'une partie des lettres nouvelles introduites dans C. On pourra continuer ainsi jusqu'à ce qu'on ait obtenu une suite de substitutions A, B, C, ..., telle que toute lettre se trouve déplacée au moins par l'une d'elles.

2. Nous admettrons, dans ce mémoire, que A soit une substitution d'ordre premier p et à q cycles, q étant un entier $< p$.

Les substitutions B, C, ..., étant successivement définies comme il vient d'être indiqué, nous aurons la proposition suivante, qui va servir de fondement à toute notre analyse.

THÉORÈME. — *Aucune des substitutions successives* B, C, ... *ne peut contenir dans aucun de ses cycles plus d'une lettre nouvelle.*

3. Nous allons démontrer d'abord cette proposition pour la substitution B. Pour y arriver, nous supposerons que l'un des cycles de B contienne plusieurs lettres nouvelles ; et nous en déduirons l'existence, dans la suite A, A′, ..., d'une substitution qui mêle dans ses cycles les lettres de A à des lettres nouvelles, tout en déplaçant moins de lettres nouvelles que B ; conséquence inadmissible, comme contraire à la définition même de B.

4. Soit I le groupe dérivé de celles A, A_1, ... des substitutions A, A′, ... qui ne déplacent aucune lettre nouvelle. Les pq lettres déplacées par les diverses substitutions de I pourront se répartir en classes, en groupant ensemble celles que les substitutions de I permettent de permuter entre elles. Si I permute transitivement les pq lettres, il n'y aura qu'une classe ; sinon il y en aura plusieurs ; mais dans aucun cas il n'y en aura plus de q, car chacune d'elles contient au moins p lettres, nombre des lettres associées dans chacun des cycles de A.

5. Soient maintenant x, y deux lettres nouvelles, contenues dans un même cycle de B. On peut admettre qu'elles s'y suivent immédiatement. Car si y suivait x à r rangs de distance, on n'aurait qu'à considérer, au lieu de la substitution B, la substitution B^r, qui lui est semblable, et dont l'un des cycles contient x suivi immédiatement de y.

Cela posé, les lettres nouvelles que B déplace seront de deux espèces ; les lettres y, ... que B fait succéder à des lettres nouvelles ; et les lettres

que B fait succéder à des lettres anciennes a, a', ... Il existe nécessairement des lettres de cette seconde espèce, puisque B contient au moins un cycle où les lettres nouvelles sont mêlées aux anciennes.

6. *Les lettres a, a', ..., auxquelles* B *fait succéder des lettres nouvelles, formeront par leur réunion une ou plusieurs des classes entre lesquelles nous avons réparti les lettres de* I. Supposons en effet qu'il en fût autrement, et qu'il y eût une classe contenant à la fois des lettres a, ... de la suite a, a', ..., et d'autres lettres α, ... non contenues dans cette suite. Le groupe I étant transitif par rapport aux lettres de cette classe, l'une au moins des substitutions A, A', ..., dont il est dérivé, mêlera dans ses cycles les lettres a, ... aux lettres α, ... Supposons, par exemple, que A contienne dans un même cycle les deux lettres a et α. La transformée de A par B sera semblable à A. Elle contiendra dans un de ses cycles la lettre que B fait succéder à a, laquelle est nouvelle, et celle que B fait succéder à α, laquelle est ancienne. Elle jouira donc comme B de la propriété de mêler dans ses cycles des lettres anciennes à des lettres nouvelles. Cependant elle déplace moins de lettres nouvelles que B, car elle laisse immobiles les lettres y, ... de première espèce que B déplaçait. Ce résultat est inadmissible, comme contraire à la définition de B.

7. On peut répartir d'une seconde façon les lettres nouvelles que B déplace en deux catégories : 1° les lettres x, ... auxquelles B fait succéder des lettres nouvelles; 2° celles auxquelles B fait succéder des lettres anciennes b, ... Et l'on verra de même que *les lettres b, ... formeront par leur réunion une ou plusieurs des classes de lettres de* I; car s'il en était autrement, l'une au moins des substitutions A, A', ..., étant transformée par B^{-1}, donnerait une nouvelle substitution jouissant de la même propriété que B, mais déplaçant moins de lettres nouvelles, ce qui est inadmissible.

8. Les classes de lettres qui constituent la suite a, ... peuvent appartenir en tout ou en partie à la suite b, ... Nous admettrons pour plus de généralité qu'elles ne lui appartiennent pas en totalité.

Soient a', ... celles des lettres a, ... qui n'appartiennent pas à b, ... Par la définition même de ces suites, B fera succéder a', ... à des lettres anciennes c, ...

9. *Les lettres c, ... formeront encore une ou plusieurs classes dans* I.

Cette proposition est le nœud de notre démonstration; pour l'établir, considérons le groupe $\mathfrak{I}$ transformé de I par B. Ses diverses substitutions laisseront immobiles les lettres que B fait succéder à des lettres nouvelles, c'est-à-dire les lettres nouvelles de première espèce, et les lettres anciennes de la suite b, ... Mais au contraire elles déplaceront les lettres nouvelles de seconde espèce, ainsi que les lettres a', ...

Les substitutions de I permutant exclusivement entre elles les lettres a, ..., celles de $\mathfrak{I}$ permuteront exclusivement entre elles les lettres nouvelles

de la seconde espèce, que B leur fait succéder. D'autre part, ces diverses substitutions remplaceront respectivement le système s' des lettres a', ... par divers systèmes de lettres s', s'', ..., dont chacun sera exclusivement formé de lettres anciennes.

10. En premier lieu, *chacun des systèmes s', s'', ... sera formé par l'ensemble des lettres d'une ou plusieurs classes.* En effet, soit S celle des substitutions de $\mathfrak{J}$ qui remplace les lettres de s' par celles de s''. La transformée B' de B par S sera une substitution semblable à B, dont les cycles contiendront les mêmes lettres nouvelles que ceux de B (puisque, parmi les lettres nouvelles que B contenait, les unes ne sont pas déplacées par S et les autres sont permutées ensemble). Soit d'ailleurs x' la lettre que S fait succéder à x; l'un des cycles de B contenant deux lettres nouvelles consécutives x, y, l'un des cycles de B' contiendra les deux lettres nouvelles consécutives x', y. Donc B' jouira des mêmes propriétés caractéristiques que B; et le raisonnement déjà fait sur B, étant appliqué à B', montrera que les lettres anciennes auxquelles B' fait succéder des lettres nouvelles doivent former par leur réunion une ou plusieurs classes. Mais ces lettres sont, d'une part, les lettres communes aux deux suites a, ... et b, ..., lesquelles forment une ou plusieurs classes, et, d'autre part, les lettres de s''. Donc ces dernières lettres, considérées isolément, formeront une ou plusieurs classes, ce qu'il fallait démontrer.

11. Deux cas pourront maintenant se présenter, suivant que les systèmes s', s'', ... seront tous formés des mêmes classes de lettres, ou différeront les uns des autres par quelques lettres.

Dans le premier cas, les substitutions de $\mathfrak{J}$ permuteront exclusivement entre elles les lettres a', ... du système s'; donc les substitutions de I, dont elles sont les transformées par B, permutaient exclusivement entre elles les lettres c, ..., que B remplaçait par a', ... Donc les lettres c, ... forment dans I une ou plusieurs classes, comme nous voulions l'établir.

12. Supposons au contraire que les systèmes s', s'', ... diffèrent par quelques classes; nous aboutirons à une absurdité.

On voit d'abord que chaque substitution de $\mathfrak{J}$ remplace les uns par les autres les systèmes s', s'', ... Supposons en effet que l'une d'elles S remplace s'' par un autre système de lettres s_1; $\mathfrak{J}$, contenant une substitution T qui remplace s' par s'', contiendra ST, qui le remplace par s_1; donc s_1 sera par définition l'un des systèmes de la suite s', s'', ...

Il résulte évidemment de là que, s'il existe des classes communes à tous les systèmes s', s'', ..., les lettres de ces classes seront permutées exclusivement entre elles par les substitutions de $\mathfrak{J}$. Si l'on supprime ces lettres communes dans chacun des systèmes s', s'', ..., les systèmes de lettres restantes σ', σ'', ... jouiront encore de la propriété d'être permutés entre eux par les substitutions de $\mathfrak{J}$.

13. Supposons, pour fixer les idées, qu'il existe des classes communes à μ systèmes de la suite σ', σ'', ..., mais qu'il n'en existe aucune commune à $\mu+1$ systèmes. Les classes communes à tous les systèmes ayant été supprimées, μ sera inférieur au nombre des systèmes; il se réduira à l'unité, si les systèmes pris deux à deux n'ont aucune classe commune.

Soient σ', σ'', ..., σ^{μ}, μ systèmes ayant des classes communes, et soient τ le système des lettres formant les classes communes à ces systèmes; τ, τ_1, τ_2, ... les systèmes de lettres que les diverses substitutions 1, S_1, S_2, ... du groupe $\mathfrak{I}$ font succéder à τ; τ_1, par exemple, sera formé des classes communes à ceux des systèmes σ'_1, ..., σ^{μ}_1 de la suite σ', ... que S_1 fait succéder à σ', ..., σ^{μ}. D'ailleurs deux quelconques des systèmes $\tau, \tau_1, \tau_2, \ldots$ ne peuvent avoir aucune classe commune sans être identiques. En effet, si τ_1 et τ_2, par exemple, avaient une classe commune, cette classe appartiendrait à la fois aux μ systèmes σ'_1, ..., σ^{μ}_1 que S_1 fait succéder à σ', ..., σ^{μ}, et aux μ systèmes σ'_2, ..., σ^{μ}_2 que S_2 leur fait succéder. Mais, par hypothèse, aucune classe n'appartient à plus de μ systèmes de la suite σ', ... Donc ces μ derniers systèmes se confondent avec les précédents; donc les lettres de τ_2, qui leur sont communes, se confondent avec celles de τ_1, communes aux précédents.

14. Nous remarquerons encore que *la suite* $\tau, \tau_1, \ldots$ *contient nécessairement plusieurs systèmes distincts*. Car $\mathfrak{I}$ contient une substitution S_1 qui remplace σ' par un système $\sigma^{\mu+1}$ différent de σ', ..., σ^{μ}; cette substitution remplacera τ par un nouveau système τ_1, dont les lettres appartiendront à $\sigma^{\mu+1}$, tandis que les lettres de τ ne lui appartenaient pas; donc τ_1 diffère de τ. Mais, d'un autre côté, *le nombre des systèmes distincts de la suite* $\tau, \tau_1, \ldots$ *ne peut dépasser* q, puisque chacun d'eux est formé d'une ou plusieurs classes de lettres, et que le nombre total des classes est au plus égal à q.

15. Cela posé, le groupe I étant dérivé des substitutions A, A', ... qui sont d'ordre p, son transformé $\mathfrak{I}$ par B sera dérivé des substitutions $\mathfrak{A}$, $\mathfrak{A}'$, ... transformées de celles-là par B, et qui seront aussi d'ordre p. Et puisque $\mathfrak{I}$ contient une substitution S_1 qui déplace les systèmes $\tau, \tau_1, \ldots$, l'une au moins $\mathfrak{A}$ des substitutions $\mathfrak{A}$, $\mathfrak{A}'$, ... dont il est dérivé déplacera ces systèmes. Soit $\mathfrak{A}^{\rho}$ la première des puissances successives de $\mathfrak{A}$ qui ne déplace plus les systèmes; ρ sera un entier >1 et qui divisera $1.2\ldots q$, le nombre des systèmes étant moindre que q. Il est évident d'ailleurs que celles des puissances de $\mathfrak{A}$ qui ne déplacent pas les systèmes sont $\mathfrak{A}^{\rho}$, $\mathfrak{A}^{2\rho}$, ..., $\mathfrak{A}^{m\rho}$, ... Mais $\mathfrak{A}^{p}$, se réduisant à l'unité, ne déplacera pas les systèmes. Donc p sera un multiple de ρ; et comme il est premier, on aura $p=\rho$; résultat absurde, p ne divisant pas $1.2\ldots q$.

16. Il est donc établi, ainsi que nous l'avions annoncé, que les lettres de la suite c, ... forment une ou plusieurs classes. Ces lettres pourront être contenues en tout ou en partie parmi celles de la suite b, ... Supposons

pour plus de généralité qu'elles n'y soient pas toutes contenues. Si, parmi les lettres de la suite c, ..., on efface celles qui lui sont communes avec la suite b, ..., les lettres restantes c', ... jouiront de la propriété que B les fait succéder à des lettres anciennes d, ...

Un raisonnement identique au précédent fera voir que les lettres d, ... forment une ou plusieurs classes.

17. Continuant ainsi, on arrive au résultat suivant : *Pour qu'il n'existe aucune substitution déplaçant moins de lettres nouvelles que* B *et les mêlant dans ses cycles aux lettres anciennes, il faut que les lettres anciennes* a, ..., *que* B *remplace par des lettres nouvelles, forment une ou plusieurs classes; de même pour les lettres anciennes* c, ..., *que* B *remplace par des lettres anciennes, mais que* B^2 *remplace par des lettres nouvelles; de même pour les lettres anciennes* d, *que* B *et* B^2 *remplacent par des lettres anciennes, mais que* B^3 *remplace par des lettres nouvelles, etc.*

18. Cela posé, considérons l'une des classes contenues dans la suite a, ... Elle contient au moins p lettres, toutes déplacées par B qui n'a que q cycles. Donc deux au moins de ces lettres, a, a_1, seront contenues dans un même cycle, où elles seront respectivement remplacées par deux lettres nouvelles z, z_1; on aura donc, en mettant ces lettres en évidence,

$$B = (az \dots a_1 z_1 \dots)(\dots)\dots,$$

et en élevant B à une puissance convenable on obtiendra une substitution semblable à B et de la forme

$$B^k = (aa_1 \dots zz_1 \dots)(\dots)\dots.$$

Cette substitution contient les mêmes lettres nouvelles que B, et son premier cycle contient deux lettres nouvelles consécutives; on peut donc raisonner sur elle comme sur B. D'ailleurs elle ne satisfait pas à la condition que nous venons de trouver (17). Car soit $m+2$ le rang de la première lettre nouvelle que renferme le cycle $(aa_1 \dots zz_1 \dots)$. La première puissance de B^k qui remplace a_1 par une lettre nouvelle sera la $m^{\text{ième}}$; si la condition était satisfaite, elle devrait remplacer a, qui appartient à la même classe, par une lettre nouvelle, ce qu'elle ne fait pas.

Donc on pourra déduire de B^k une substitution analogue, mais déplaçant moins de lettres nouvelles, ce qui est inadmissible.

19. Notre proposition est donc complétement démontrée pour la substitution B. Les mêmes principes serviront à l'établir pour la substitution suivante C, et de proche en proche pour toutes les autres.

Soit en effet I_1 le groupe formé par les substitutions A, A_1, ..., B, B_1, ... de la suite A, A', ... qui ne déplacent aucune lettre autre que celles déjà déplacées par A et B. On pourra y répartir les lettres en classes, en groupant ensemble celles que I_1 permute entre elles. Elles ne pourront former plus de

q classes. En effet, considérons d'abord les pq lettres anciennes que A déplaçait. Étant associées p à p dans les cycles de A, le nombre des classes distinctes entre lesquelles elles se répartissent ne pourra dépasser q. Passons maintenant aux lettres nouvelles introduites par la substitution B. Chacune d'elles se trouve dans un des cycles de B, associée à des lettres anciennes, et viendra s'adjoindre à la classe déjà formée par ces lettres. Donc l'introduction de ces lettres nouvelles ne pourra faire apparaître de nouvelles classes. Au contraire, le nombre des classes distinctes pourra se trouver réduit par l'adjonction des substitutions B, B_1, ...

Cela posé, les raisonnements que nous avons faits sur le groupe I et la substitution B deviennent identiquement applicables au groupe I_1 et à la substitution C. Ils le seront également au groupe I_2 formé par celles des substitutions semblables à A qui sont contenues dans G et ne déplacent que les lettres de A, B, C, et à la substitution suivante D; etc.

20. Nous remarquerons d'ailleurs que chacune des substitutions B, C, ..., ne pouvant contenir plus d'une lettre nouvelle dans chacun de ses cycles, le nombre total des lettres nouvelles introduites par l'une quelconque de ces substitutions ne pourra dépasser q, nombre des cycles.

II

21. Théorème. — *Un groupe primitif* G, *qui contient une substitution d'ordre p à q cycles, contient nécessairement le groupe alterné si son degré dépasse une certaine limite $pq + \varphi(q)$, toutes les fois que p surpassera lui-même une certaine limite $f(q)$.*

22. Pour démontrer ce théorème, et déterminer en même temps la forme des fonctions $\varphi(q)$, $f(q)$, nous admettrons que la proposition soit établie, et les limites déterminées pour toutes les valeurs de q inférieures à celles que l'on considère.

Nous admettrons en outre que l'on ait déterminé pour ces mêmes valeurs de q le degré maximum $pq + \psi(q)$ des groupes simplement transitifs que peut contenir un groupe primitif G dont une substitution est d'ordre p à q cycles, mais qui ne contient pas le groupe alterné (il est clair que $\psi(q)$ sera au plus égal à $\varphi(q)$; mais il pourra être moindre).

Cela posé, considérant les groupes qui contiennent une substitution d'ordre p à q cycles sans contenir de substitutions d'ordre p à moins de q cycles, nous assignerons les limites supérieures des trois quantités $\varphi(q)$, $f(q)$, $\psi(q)$, en fonction des quantités connues $\varphi(q-1)$, $\varphi(q-2)$, ..., $f(q-1)$, ..., $\psi(q-1)$, ...

23. Notre proposition sera dès lors démontrée; car nous avons établi le théorème dans le cas où $q = 1$ (même tome, p. 42) et trouvé pour ce cas les

limites $\varphi(1) = 2$, $f(1) = 1$. D'ailleurs un groupe primitif de degré n qui contient une substitution circulaire d'ordre p, étant au moins $n - p + 1$ fois transitif, ne pourra contenir un groupe simplement transitif de degré $> p$. On aura donc $\psi(1) = 0$.

Substituant ces valeurs dans les formules récurrentes qui donnent $\varphi(q)$, $f(q)$, $\psi(q)$, on trouvera facilement les limites suivantes :

$$\varphi(q) \leqslant \frac{2}{\log 2} q \log q + 2q, \qquad \psi(q) \leqslant \frac{2}{\log 2} q \log q + q,$$

et la valeur correspondante de $f(q)$ sera la plus grande des quantités $\psi(q) + 1$, $3q + 2$, 18.

On obtiendra d'ailleurs des limites plus étroites dans chaque cas particulier en serrant le problème de plus près, ainsi que nous le ferons voir dans la section VIII.

III

24. Considérons la suite des groupes I, I_1, ..., définis comme précédemment. Nous avons vu que, si l'on répartit en classes les lettres déplacées par chacun de ces groupes, en groupant ensemble celles qui sont permutées transitivement, aucun des groupes de la suite ne contiendra plus de classes que celui qui le précède. D'ailleurs la suite se termine par le groupe H, qui est transitif. Soit donc I_r le premier groupe transitif que contienne la suite; les groupes suivants I_{r+1}, ..., H seront tous transitifs.

Si $r = 0$, le groupe I sera lui-même transitif; nous laisserons provisoirement de côté ce cas, qui est relativement simple.

25. Soient x_1, ..., x_μ les lettres nouvelles que I_r déplace, mais que I_{r-1} ne déplaçait pas. Si $\mu > 1$, le *groupe* I_r *ne sera pas primitif; mais ses lettres se grouperont* μ *à* μ *en systèmes, dont l'un sera formé des lettres* x_1, ..., x_μ. En effet, considérons le groupe J formé de celles des substitutions de I_r qui ne déplacent pas x_1. Celles de ses substitutions qui sont semblables à A laissent immobiles les lettres x_2, ..., x_μ; car leur nombre $\mu - 1$ est inférieur à q (20) et par suite à p. Si donc il existait une substitution S semblable à A et déplaçant tout ou partie de ces lettres, elle les mêlerait dans ses cycles à des lettres anciennes, car ces lettres nouvelles sont en nombre insuffisant pour former à elles seules un cycle dans S. Mais, en vertu de la définition même des groupes successifs I, I_1, ..., il ne peut exister aucune substitution semblable à A, déplaçant moins de μ lettres nouvelles et les mêlant dans ses cycles avec celles de I_{r-1}. Donc S ne peut exister.

D'autre part, les substitutions semblables à A dont I_{r-1} est dérivé sont

contenues dans J, et déplacent toutes les lettres anciennes. Il résulte de là (voir notre *Traité des substitutions*, n° 399) que les lettres de I_r peuvent être réparties en systèmes, dont l'un sera formé des lettres $x_1, \ldots, x_\mu$, ce qu'il nous fallait démontrer.

26. Il se peut qu'il existe d'autres manières de répartir les lettres de I_r en systèmes (tels que chaque substitution de I_r remplace ces lettres de chaque système par celles d'un même système); mais, *dans chacune de ces répartitions diverses, les systèmes qui contiennent quelqu'une des lettres nouvelles* $x_1, \ldots, x_\mu$ *sont exclusivement formés de lettres nouvelles.*

Supposons en effet qu'il existât un système s contenant à la fois la lettre x_1 et l'une des anciennes lettres α. Les substitutions de I_{r-1}, laissant x_1 immobile, ne déplaceront pas ce système; donc les lettres $\alpha, \beta, \ldots$ qu'elles font succéder à α appartiennent toutes à ce système. Or I_{r-1} est dérivé de substitutions d'ordre p; soit S une de ces substitutions, laquelle déplace α; celui de ses cycles qui contient α contiendra p lettres distinctes, qui toutes appartiendront à la suite $\alpha, \beta, \ldots$. Donc s, contenant $x_1, \alpha, \beta, \ldots$, contiendra plus de p lettres.

Cela posé, I_r étant transitif, l'une au moins T des substitutions d'ordre p dont il est dérivé remplacera le système s par un autre. Mais T n'a que q cycles, et comme elle déplace toutes les lettres de s, en nombre $> p$, elle en contiendra deux au moins dans l'un de ses cycles. Supposons qu'elles s'y suivent à m rangs de distance; T^m, remplaçant une des lettres de s par une autre, ne déplacera pas ce système, et T, qui est une puissance de T^m, ne le déplacera pas non plus, comme nous l'avions supposé. Les μ lettres $x_1, \ldots, x_\mu$ formant à elles seules un certain nombre des systèmes de la nouvelle répartition, il est clair que chacun des anciens systèmes de μ lettres sera également formé de la réunion d'un certain nombre des systèmes de la nouvelle répartition.

27. Il résulte de là : 1° que *le nombre des lettres de chaque système de la nouvelle répartition divise* μ, puisque les μ lettres $x_1, \ldots, x_\mu$ forment à elles seules un ou plusieurs systèmes; 2° que *si* $\mu = 1$, I_r *sera primitif*, puisqu'il sera impossible d'y déterminer des systèmes contenant plus d'une seule lettre.

28. Les raisonnements que nous venons de faire pour le groupe I_r seront également applicables aux groupes suivants $I_{r+1}, \ldots, H$, qui sont également transitifs. On en tire de plus cette conséquence que H *est primitif.*

En effet, si H n'était pas primitif, le nombre λ des lettres déplacées par ce groupe et non déplacées par le précédent serait > 1. Et parmi les diverses manières qui peuvent exister de répartir les lettres de H en systèmes, il en existerait une seule où chaque système contînt λ lettres, à savoir celle où les systèmes formés par les lettres nouvelles se réduiraient à un seul contenant toutes ces lettres. Cela posé, les substitutions de G, étant per-

mutables à H, remplaceraient les systèmes de λ lettres ainsi déterminés dans H par de nouveaux systèmes de λ lettres jouissant également de la propriété que chaque substitution de H remplace les lettres de chaque système par celles d'un même système. Mais puisqu'il n'existe qu'une manière de déterminer dans H de semblables systèmes, les nouveaux systèmes se confondront avec les anciens, et les substitutions de G remplaçant ces anciens systèmes les uns par les autres, G ne sera pas primitif, comme on le suppose.

Revenons à la considération du groupe I_r. Deux cas seront à distinguer, suivant que l'on aura $\mu > 1$ ou $\mu = 1$.

IV

29. *Premier cas*, $\mu > 1$. — Soit $pq + k$ le nombre des lettres déplacées par I_r; nous allons déterminer une limite supérieure du nombre k.

Si $r = 1$, on obtiendra immédiatement la limite cherchée; en effet, I déplaçant pq lettres, I_1 en déplacera $pq + \mu$. On aura donc $k = \mu < q$.

30. Soit au contraire $r > 1$. Les lettres de I_r pourront se grouper μ à μ en systèmes $s, t, u, \ldots$. Les lettres déplacées par I_r sans l'être par I_{r-1} formeront l'un de ces systèmes s; *quant aux lettres déplacées par* I_{r-1} *sans l'être par* I_{r-2}, *elles formeront un ou plusieurs des systèmes de la suite* $t, u, \ldots$. Soit en effet α l'une de ces lettres, appartenant par exemple au système t; et soient $\beta, \ldots$ les autres lettres de cette sorte. Si I_{r-2} les déplaçait, l'une des substitutions d'ordre p dont I_{r-2} est dérivé les déplacerait. D'ailleurs cette substitution, laissant immobile α, ne déplacerait pas le système t; donc elle permuterait exclusivement entre elles les lettres $\beta, \ldots$; résultat absurde, car ces lettres, en nombre $< p$, ne peuvent former un cycle à elles seules.

31. *Les substitutions de* I_{r-1} *ne peuvent permuter les systèmes* $t, u, \ldots$ *les uns dans les autres d'une manière trois fois transitive.* Supposons en effet que cela eût lieu. Celles des substitutions de I_{r-1} qui ne déplacent pas t forment un groupe M deux fois transitif par rapport aux systèmes restants. Celles de ces substitutions qui sont d'ordre p, étant combinées ensemble, forment un groupe N, évidemment permutable aux substitutions de M, et par suite transitif. D'ailleurs les substitutions de M devant permuter exclusivement entre elles les μ lettres de t, celles d'entre elles qui sont d'ordre p laisseront ces lettres immobiles. D'ailleurs elles appartiendront à I_{r-2}; car si l'une d'elles S déplaçait quelqu'une des lettres nouvelles (en nombre $< q$) que I_{r-2} ne déplaçait pas, mais que I_{r-1} déplace, elle les mêlerait dans ses cycles avec les lettres de I_{r-2}; et, en transformant par S les substitutions semblables à A dont I_{r-2} est dérivé, on obtiendrait de nouvelles substitutions semblables

à A, mais contenant moins de lettres nouvelles que n'en déplace I_{r-1}; résultat inadmissible, comme contraire à la définition de ce groupe.

32. Donc I_{r-2} contient N, et par suite permute transitivement les systèmes restants u, ... D'ailleurs *le nombre de ces systèmes est au moins égal à* p. En effet, I_{r-2} contient la substitution A d'ordre p. Les lettres contenues dans chacun de ses cycles appartiendront nécessairement à p systèmes distincts. Supposons en effet qu'un même cycle c contînt deux lettres γ et δ d'un même système u, et que ces lettres se suivissent à m rangs de distance. A^m, remplaçant γ par δ, ne déplacerait pas le système u; il en serait de même de A, qui est une puissance de A^m; donc toutes les lettres du cycle qui contient γ et δ appartiendraient au système u; ce qui est absurde, le nombre μ des lettres du système étant $< p$.

33. On voit enfin qu'*il n'existera qu'une manière de répartir les lettres de* I_{r-1} *en systèmes de* μ *lettres*. Imaginons en effet qu'on ait opéré une semblable répartition, et soit t' celui de ces nouveaux systèmes qui contient une lettre α de t; il ne pourra contenir en même temps une lettre γ de l'un des systèmes restants u, ... En effet les substitutions de I_{r-2}, ne déplaçant pas α, ne déplaceraient pas le système t'; donc les lettres que ces substitutions permutent avec γ appartiendraient à t'; résultat absurde, leur nombre étant au moins égal à p. Donc t' doit se confondre avec t, et la nouvelle répartition avec l'ancienne.

34. Cela posé, I_r n'étant pas primitif, ne sera pas le dernier terme de la suite I, I_1, ..., H (28). Soient I_{r+1} le terme suivant, μ' le nombre des lettres nouvelles déplacées par I_{r+1} sans l'être par I_r. Des raisonnements analogues à ceux du n° 25 montrent que les lettres de I_{r+1} peuvent se répartir en systèmes de μ' lettres, l'un de ces systèmes ρ étant formé des lettres nouvelles qui viennent d'être introduites. Chacun des anciens systèmes de μ lettres s, t, ... sera formé par les lettres d'un ou plusieurs de ces nouveaux systèmes (26). Donc μ' sera égal à μ ou à un diviseur de μ.

35. Supposons d'abord $\mu' < \mu$; nous arriverons à une conséquence absurde.

Soient respectivement $\sigma, \sigma', \ldots; \tau, \tau', \ldots$; ... ceux des nouveaux systèmes dont la réunion forme $s, t, \ldots$; le groupe I_r, étant transitif, permutera transitivement ces systèmes, et I_{r+1} sera deux fois transitif par rapport aux systèmes $\rho, \sigma, \sigma', \ldots, \tau, \tau', \ldots$. Donc il contient une substitution S qui remplace le système ρ par le système σ et réciproquement.

36. *La substitution* S *est permutable à* I_{r-1}. En effet, I_{r-1} est dérivé de substitutions semblables à A et ne déplaçant ni les lettres de ρ ni celles de σ. Soit T l'une quelconque de ces substitutions. Sa transformée par S ne déplacera pas ces mêmes lettres. Elle ne pourra d'ailleurs déplacer aucune des lettres des systèmes $\sigma', \ldots$; car ces lettres, en nombre $\mu - \mu' < p$, ne pourraient y former un cycle entier; elles se trouveraient donc mêlées dans les

cycles de la transformée avec les lettres de I_{r-1}; on aurait ainsi une substitution semblable à A et mêlant dans ses cycles aux lettres de I_{r-1} des lettres nouvelles en nombre $< \mu$; résultat inadmissible comme contraire à la définition de I_r. Donc la transformée, ne déplaçant que les lettres de I_{r-1}, appartiendra à ce groupe.

37. Cela posé, les systèmes $t, u, \ldots$ jouissent de la propriété que chaque substitution de I_{r-1} remplace les lettres de chaque système par celles d'un même système. Les systèmes de lettres $t', u', \ldots$, que S leur fait succéder, jouiront de la même propriété dans le groupe transformé de I_{r-1} par S, lequel n'est autre que I_{r-1}. Mais il n'existe qu'une répartition des lettres de I_{r-1} en systèmes de μ lettres; donc $t', u', \ldots$ *se confondront, à l'ordre près, avec* $t, u, \ldots$.

Donc S *permute les uns dans les autres les systèmes* $t, u, \ldots$; et, par suite, elle permutera exclusivement ensemble les lettres de $\sigma', \ldots$.

38. Considérons maintenant le groupe I'_r transformé de I_r par S; les lettres s'y répartiront μ à μ en systèmes, respectivement formés des lettres que S fait succéder à celles de $s, t, u, \ldots$; ces nouveaux systèmes seront $(\rho, \sigma', \ldots), t, u, \ldots$, et I'_r les permutera d'une manière trois fois transitive. Il contiendra donc une substitution U qui remplace $(\rho, \sigma', \ldots)$ par t et réciproquement. Le groupe I'_{r-1}, transformé de I_{r-1} par U, déplacera toutes les lettres, sauf celles de σ et de t. Mais I_r, étant deux fois transitif par rapport aux systèmes $s = (\sigma, \sigma', \ldots), t, \ldots$, contient une substitution V qui remplace s par t et réciproquement. Le groupe I''_{r-1}, transformé de I'_{r-1} par V, ne déplacera pas les lettres de s. Donc les lettres nouvelles qu'il déplace, et que I_{r-1} ne déplaçait pas, se réduisent aux μ' lettres de ρ. Il dérive d'ailleurs de substitutions d'ordre p, comme I_{r-1} dont il est le transformé. Ces substitutions devront mêler dans leurs cycles les lettres nouvelles en nombre $\mu' < \mu$ avec les anciennes. Ce résultat est inadmissible, comme contraire à la définition du groupe I_r.

39. *On aura donc* $\mu' = \mu$; *donc les lettres de* I_{r+1} *se répartiront encore* μ *à* μ *en systèmes, et* I_{r+1} *ne sera pas primitif.*

40. Passons au groupe suivant I_{r+2}. Soit μ'' le nombre des lettres nouvelles déplacées par ce groupe; on verra de la même manière que $\mu'' = \mu$, et que I_{r+2} n'est pas primitif. De même pour I_{r+3}, etc. On pourra poursuivre indéfiniment, sans jamais arriver à un groupe primitif H qui puisse fermer la suite.

41. Il est donc établi, ainsi que nous l'avons annoncé (31), que I_{r-1} ne peut être plus de deux fois transitif par rapport aux systèmes $t, u, \ldots$; par suite I_r, qui est deux fois transitif par rapport à $s, t, u, \ldots$, le sera tout au plus trois fois.

42. Nous pouvons déduire de ce qui précède une limite pour le nombre k.

Considérons en effet les déplacements d'ensemble opérés sur les $\frac{pq+k}{\mu}$ systèmes $s, t, \ldots$ par les substitutions de I_r. Le groupe J_r formé par ces déplacements sera m fois transitif, m étant égal à 2 ou à 3; il sera donc primitif. Il contient d'ailleurs une substitution d'ordre p à $\frac{q}{\mu}$ cycles.

Considérons en effet la substitution A. Nous avons vu (32) que les lettres de chacun de ses cycles appartiennent à p systèmes différents, que A permute entre eux. D'ailleurs chacun de ces p systèmes contenant μ lettres, l'ensemble de leurs lettres formera μ cycles dans A. Donc A contiendra les lettres de $\frac{pq}{\mu}$ systèmes, formant $\frac{q}{\mu}$ classes telles que A permute circulairement entre eux les p systèmes de chaque classe.

43. Cela posé, si le groupe J_r contient le groupe alterné, on aura $k \leqslant 2\mu$. En effet, J_r devra être $\frac{pq+k}{\mu} - 2$ fois transitif; mais il l'est tout au plus trois fois. On aura donc $\frac{pq+k}{\mu} \leqslant 5$. Mais on a par hypothèse $\mu > 1$, $q \geqslant \mu$, $p > q$, d'où $p \geqslant 3$. La condition ci-dessus ne pourra donc être satisfaite qu'en posant $p = 3$, $q = \mu = 2$, $k \leqslant 2\mu$.

44. Si J_r ne contient pas le groupe alterné, soit L le groupe formé par celles de ses substitutions qui laissent immobile $m - 1$ systèmes donnés. Il sera simplement transitif par rapport aux systèmes restants. Il est d'ailleurs contenu dans J_r, qui est primitif, ne contient pas le groupe alterné, mais contient une substitution d'ordre p à $\frac{q}{\mu}$ cycles. Donc, en vertu de l'hypothèse admise (22), le nombre des systèmes que L déplace ne pourra dépasser $p\frac{q}{\mu} + \psi\left(\frac{q}{\mu}\right)$. Donc le nombre total des systèmes de J_r ne pourra dépasser $p\frac{q}{\mu} + \psi\left(\frac{q}{\mu}\right) + m - 1$; et chacun d'eux contenant μ lettres, le nombre des lettres déplacées par I_r aura pour limite supérieure

$$pq + \mu\psi\left(\frac{q}{\mu}\right) + (m-1)\mu.$$

On aura donc

$$k \leqslant \mu\psi\left(\frac{q}{\mu}\right) + (m-1)\mu,$$

ou, en remarquant que $m \leqslant 3$,

$$k \leqslant \mu\psi\left(\frac{q}{\mu}\right) + 2\mu. \qquad (1)$$

Cette limite, étant évidemment plus élevée que les limites μ et 2μ trouvées précédemment (29 et 43), s'appliquera à tous les cas et pourra être conservée seule.

45. Le groupe G, contenant un groupe transitif, mais non primitif I_r, de degré $pq+k$, contiendra un groupe deux fois transitif, K, et de degré $d=pq+k+q'+r'+s'+\ldots+1$, chacun des entiers $q',r',s'\ldots$ divisant le précédent, et q' étant un nombre tel, que les lettres de I_r puissent se répartir de deux manières différentes en systèmes de q' lettres. S'il n'existait aucun nombre q' jouissant de cette propriété, le degré de K se réduirait simplement à $pq+k+1$ (*Voir*, pour la démonstration, les nos 2 à 8 du mémoire intitulé *Théorèmes sur les groupes primitifs ; Journal de Liouville*, 2e série, t. XVI).

Or nous avons vu (26) qu'il n'existe qu'une seule répartition des lettres de I_r en systèmes de μ lettres, et que dans les autres répartitions, s'il en existe, le nombre des lettres de chaque système est un diviseur de μ ; donc q' divisera μ, et, si α désigne le nombre des facteurs premiers de μ, on aura

$$q'+r'+s'+\ldots+1\leqslant\mu\left(\frac{1}{2}+\frac{1}{4}+\ldots+\frac{1}{2^\alpha}\right)\leqslant\mu-1.$$

On aura donc

$$\Delta=d-pq\leqslant k+\mu-1\leqslant\mu\psi\left(\frac{q}{\mu}\right)+3\mu-1. \tag{2}$$

D'autre part $k\geqslant\mu$, puisque I_r déplace μ lettres nouvelles ; d'ailleurs $q'+r'+\ldots+1$ est au moins égal à 1 ; d'où la limite inférieure

$$\Delta\geqslant\mu+1\geqslant k. \tag{3}$$

46. Soit maintenant $n=d+e$ le degré de G ; ce groupe, contenant un groupe deux fois transitif de degré d, sera $e+2$ fois transitif, et le degré des groupes simplement transitifs qu'il peut contenir ne pourra dépasser la limite $d-1$. Car un groupe de degré $d-1+r$ contenu dans G serait $r+1$ fois transitif. On aura donc dans ce cas

$$pq+\psi(q)\leqslant d-1,$$

d'où

$$\psi(q)\leqslant\Delta-1\leqslant\mu\psi\left(\frac{q}{\mu}\right)+3\mu-2. \tag{4}$$

47. Cela posé, admettons que l'on ait

$$p>\mu\psi\left(\frac{q}{\mu}\right)+3\mu-1,\quad\text{d'où}\quad p>\Delta; \tag{5}$$

nous allons trouver une limite supérieure pour le nombre inconnu n.

En premier lieu, nous établirons que *l'ordre* Ω *de* K *ne peut être divisible par* p^2.

Soient $\alpha, \beta, \gamma, \ldots$ les Δ lettres déplacées par K sans l'être par I, et soient respectivement L le groupe formé par l'ensemble des substitutions de G qui ne déplacent que les lettres de K (ce groupe, contenant K, sera au moins deux fois transitif) ; $L_1, L_2, L_3, \ldots$ les groupes formés par celles des substitutions de L qui laissent immobile α; α et β; α, β et γ; etc. Soient $\Omega_1, \Omega_2, \Omega_3, \ldots$ les ordres respectifs de ces groupes ; O celui de I. Le groupe L étant deux fois transitif, on aura

$$\Omega = (pq + \Delta)\,\Omega_1 = (pq + \Delta)(pq + \Delta - 1)\,\Omega_2;$$

et, comme δ est > 2 et $< p$, Ω contiendra le facteur p à la même puissance que Ω_2.

On aura d'ailleurs

$$\Omega_2 = l\,\Omega_3,$$

l étant le nombre des lettres que L_2 permute avec γ. Ces lettres seront de deux sortes : les unes qui figuraient dans le groupe I; les autres nouvelles. Le nombre de ces dernières lettres sera au plus égal à $\Delta - 2$, et au moins égal à 1 (γ pouvant toujours être permuté avec lui-même) ; il sera donc premier à p. Au contraire, le nombre des lettres de la première sorte sera un multiple de p ; car L_2, contenant I, contiendra la substitution A dans les cycles de laquelle les lettres anciennes sont associées p à p ; et il est clair que si les substitutions de L_2 permutent γ avec une lettre ancienne quelconque ε, elles permettront de la permuter avec chacune des p lettres qui sont contenues dans le même cycle que celle-là. Donc l sera premier à p, et Ω_2 contiendra le facteur p à la même puissance que Ω_3.

Continuant ainsi, on verra que Ω contient le facteur p à la même puissance que O.

Or soient I' le groupe formé par celles des substitutions de I qui laissent immobile une lettre ε; O' son ordre ; l' le nombre des lettres avec lesquelles les substitutions de I permutent ε; on aura

$$O = l'O'.$$

Or l' est au plus égal à pq ; il est donc $< p^2$ et ne peut contenir qu'une fois le facteur p. D'autre part, O' est premier à p ; sans quoi I' contiendrait une substitution d'ordre p, laquelle aurait moins de q cycles, le nombre total des lettres de I' étant $pq - 1$; résultat inadmissible, car G, et *a fortiori* I', ne contient par hypothèse aucune semblable substitution (22).

48. Soient maintenant H, H_1, H_2 les groupes respectivement formés par celles des substitutions de L, L_1, L_2 qui sont permutables au groupe I

formé par les puissances de A ; $\omega, \omega_1, \omega_2$ les ordres de ces groupes ; on aura, d'après le théorème de M. Sylow,

$$\Omega \equiv \omega, \quad \Omega_1 \equiv \omega_1, \quad \Omega_2 \equiv \omega_2 \bmod p^2,$$

et, par suite,

$$\omega \equiv (pq + \Delta)\omega_1, \quad \omega_1 \equiv (pq + \Delta - 1)\omega_2. \tag{6}$$

Mais les substitutions de H_1, étant permutables à Γ, devront permuter exclusivement entre elles les $\Delta - 1$ lettres $\beta, \gamma, \ldots$ que Γ ne déplace pas ; et il est clair que l'on aura $\omega_1 = r\omega_2$, r étant le nombre de celles de ces lettres que les substitutions de H_1 permutent avec la lettre β, que les substitutions de H_2 ne déplacent pas. On aura par suite

$$r\omega_2 \equiv (pq + \Delta - 1)\omega_2 \bmod p^2,$$

et comme ω_2, diviseur de Ω_2, n'est pas divisible par p^2, on aura

$$r \equiv \Delta - 1 \bmod p,$$

et enfin, comme $r \leqslant \Delta - 1 < p$,

$$r \equiv \Delta - 1. \tag{7}$$

Donc les substitutions de H_1 permutent transitivement les lettres $\beta, \gamma, \ldots$.

On verra de la même manière que les substitutions de H permutent transitivement α avec $\beta, \gamma, \ldots$; il permutera donc les lettres $\alpha, \beta, \gamma, \ldots$ entre elles d'une manière deux fois transitive.

49. Soient maintenant $y, z, u, \ldots$ les lettres, en nombre e, que G déplace, mais que L ne déplaçait pas. Le groupe G, étant $e + 2$ fois transitif, contiendra une substitution S qui laisse immobiles $e - 1$ lettres $z, \ldots$, et qui remplace y par α et réciproquement. Cette substitution sera permutable à L_1 ; car les transformées des substitutions de L_1 par S appartiendront à G ; d'autre part, elles laissent immobiles les lettres $y, z, \ldots, \alpha$ que L_1 ne déplace pas et que S permute exclusivement entre elles ; donc elles appartiendront à L_1, en vertu de la définition de ce groupe. Quant au groupe L, S le transformera en un groupe semblable L', où la lettre y jouera le même rôle que α jouait dans le groupe L. Cela posé, le groupe L', contenant L_1, contiendra la substitution A, dont les puissances forment le groupe Γ ; et, en appliquant à L' les mêmes raisonnements qu'à L, on voit que le groupe H' formé par celles des substitutions de L' qui sont permutables à Γ permutera exclusivement entre elles, et d'une manière deux fois transitive, les lettres $y, \beta, \gamma, \ldots$ que Γ ne déplace pas.

Les substitutions de H et de H' combinées ensemble permettront évidemment d'amener y à la place de l'une quelconque des lettres $\alpha, \beta, \gamma, \ldots, y$; puis,

sans déplacer y, d'amener α et β à deux quelconques des places restantes; donc le groupe (H, H') sera trois fois transitif par rapport à ces lettres.

50. On voit de la même manière que G contient un groupe H'', dont les substitutions sont permutables à Γ, laissent immobiles les lettres y, u,..., et permutent entre elles, d'une manière deux fois transitive, les lettres z, β, γ,..., etc.; et que le groupe (H, H', H'') sera quatre fois transitif par rapport aux lettres α, β, γ,..., y, z. On pourra continuer ainsi jusqu'à ce qu'on ait épuisé le nombre des lettres y, z, ...

51. Soit maintenant $\mathfrak{G}$ le groupe formé par celles des substitutions de G qui sont permutables à Γ et permutent exclusivement entre elles les $e+\Delta$ lettres α, β, γ,..., y, z, ... Ce groupe, contenant évidemment H, H', H'', ..., sera au moins $e+2$ fois transitif par rapport à ces lettres. Ses substitutions seront d'ailleurs de la forme XY, X étant une substitution entre les lettres ci-dessus et Y une substitution entre les lettres anciennes que Γ déplace.

La substitution partielle X étant échangeable à Γ, la substitution Y lui sera permutable. Donc elle remplacera les lettres de chaque cycle de A, lesquelles sont permutées entre elles par les substitutions de Γ, par d'autres lettres jouissant de cette propriété, et appartenant par suite à un même cycle de A. On aura donc $Y = ZU$, Z étant une substitution qui permute entre eux les cycles de A en remplaçant les unes par les autres les lettres correspondantes, et U une substitution qui ne déplace plus les cycles. Cette substitution U, étant permutable à Γ, transformera A en une de ses puissances, telle que A^{g^ε} (g désignant une racine primitive de p). Or, si l'on désigne par a_{11},..., a_{1p},..., a_{q1},..., a_{qp} les diverses lettres de A, on pourra la mettre sous la forme

$$A = | a_{uv} \; a_{u+1,v} |,$$

et la substitution

$$V = | a_{uv} \; a_{gu,v} |$$

la transformera en A^g. On aura donc $U = V^\varepsilon W$, W étant une nouvelle substitution qui ne déplace pas les cycles et qui soit échangeable à A; on voit sans peine qu'elle devra être de la forme

$$W = | a_{uv} \; a_{u+\varphi(v),v} |.$$

Il est donc établi que les substitutions de $\mathfrak{G}$ seront toutes de la forme $XZV^\varepsilon W$.

52. Ici divers cas seront à distinguer :

1° Parmi les substitutions du groupe $\mathfrak{G}$, il en existe deux $S_1 = X_1 Z_1 V^{\varepsilon_1} W_1$, $S_2 = X_2 Z_2 V^{\varepsilon_2} W_2$, pour lesquelles on aura $Z_1 = Z_2$, sans avoir en même temps

$X_1 = X_2$. Dans ce cas, $\mathfrak{G}$ contiendra la substitution $S_1 S_2^{-1}$, qui se réduit évidemment à la forme XV^rW, X différant de l'unité.

Soient $X'V^{\varrho'}W'$, $X''V^{\varrho''}W''$,....les substitutions de $\mathfrak{G}$ qui se réduisent à cette forme. Elles forment un groupe évidemment permutable aux substitutions de $\mathfrak{G}$. *A fortiori*, les substitutions partielles X', X'',... formeront un groupe permutable au groupe partiel formé par les déplacements X_1, X_2,... que les substitutions de $\mathfrak{G}$ font éprouver aux $e+\Delta$ lettres $\alpha, \beta, \gamma, \ldots, x, y, \ldots$.

Mais le groupe $(X_1, X_2, \ldots)$ est $e+2$ fois transitif. Donc le groupe $(X', X'', \ldots)$, qui est permutable à ses substitutions, sera au moins $e+1$ fois transitif, si $e > 1$ (même tome, *Sur la limite de transitivité des groupes non alternés*, p. 69). Donc ses substitutions ne seront pas toutes échangeables entre elles. Supposons, par exemple, que X' ne soit pas échangeable à X''.

Des deux substitutions $S' = X'V^{\varrho'}W'$, $S'' = X''V^{\varrho''}W''$, on déduira la substitution $S'^{-1}S''^{-1}S'S''$ qui se réduit à la forme XW (X différant de l'unité).

53. Soient $x'w'$, $x''w''$,... les substitutions de cette dernière forme que contient $\mathfrak{G}$. Elles forment un groupe évidemment permutable aux substitutions de $\mathfrak{G}$; et les substitutions partielles x', x''... formeront un groupe permutable à X_1, X_2,...; il sera donc $e+1$ fois transitif, et ses substitutions ne seront pas toutes échangeables entre elles. Supposons, par exemple, que x' ne le soit pas à x'' ; les substitutions w', w'',... de la forme W étant évidemment échangeables entre elles, $\mathfrak{G}$ contiendra la substitution $(x'w')^{-1}(x''w'')^{-1}(x'w')(x''w'')$, qui se réduira à la forme X.

Donc $\mathfrak{G}$ contiendra des substitutions de la forme X. Elles constitueront un groupe évidemment permutable à X_1, X_2,..., et qui, par suite, sera $e+1$ fois transitif. D'ailleurs, il ne déplace que les $e+\Delta$ lettres α, β, γ,..., x, y,.... Le groupe G, de degré n, contenant ce dernier groupe, sera $n-\Delta+1$ fois transitif. Mais il ne peut l'être plus de $\frac{n+4}{3}$ fois (*Traité des substitutions*, 83) ; on aura donc

$$n < \frac{3\Delta+1}{2} < \frac{3p+1}{2},$$

résultat absurde, car $n \geqslant qp+\Delta+2$ et $q > 1$ par hypothèse.

54. Si l'on avait $e=1$, il pourrait se faire que le groupe $(X', X'', \ldots)$, permutable aux substitutions du groupe $(B_1, B_2, \ldots)$, ne fût qu'une fois transitif, ce qui infirmerait le raisonnement. Mais cette circonstance ne peut se présenter (*loc. cit.*) que si le degré $e+\Delta$ de ce groupe est une puissance de 2, et ses substitutions de la forme

$$| \; u, v, \ldots \quad u+\sigma, \; v+\sigma', \ldots \; | \bmod 2.$$

Comme $e+\Delta$ est au moins égal à 3, il y aura plusieurs indices, et les substitutions X', X'',... ne seront pas des puissances d'une même substitu-

tion. Supposons, par exemple, que X'' ne soit pas une puissance de X'; $\mathfrak{H}$ contiendra la substitution $X'V^{\rho'}W'(X''V^{\rho''}W'')^{-\frac{\rho'}{\rho''}}$, qui se réduit à la forme XW, X différant de l'unité. D'ailleurs X, appartenant au groupe (X',X'',...), sera d'ordre 2, tandis que W est d'ordre p; et $\mathfrak{H}$ contiendra la substitution $(XW)^p = X$.

Donc $\mathfrak{H}$ contient des substitutions de la forme X. Ces substitutions forment un groupe permutable aux substitutions de $\mathfrak{H}$, et par suite transitif. Il a d'ailleurs pour degré $1+\Delta$. Donc G contiendra un groupe transitif de degré $1+\Delta$; si donc il n'est pas alterné, son degré n sera inférieur à $3(1+\Delta)-2$ (*Théorèmes sur les groupes primitifs*, n° 2). Ce résultat est absurde, car $n = qp+\Delta+1$, où $q>1$ et $p>\Delta$.

55. Donc, dans l'hypothèse que nous traitons, il faudra nécessairement admettre $e=0$, d'où

$$n \leqslant pq + \mu\psi\left(\frac{q}{\mu}\right) + 3\mu - 1,$$

et enfin

$$\varphi(q) = n - pq \leqslant \mu\psi\left(\frac{q}{\mu}\right) + 3\mu - 1. \tag{8}$$

56. 2° Il nous reste à discuter l'hypothèse où, parmi les substitutions de $\mathfrak{H}$, $X_1Z_1V^{\rho_1}W_1, X_2Z_2V^{\rho_1}W_2, \ldots$, il n'en existe point où l'on ait $Z_1 = Z_2$, sans avoir en même temps $X_1 = X_2$. Dans ce cas, à chacune des substitutions du groupe $Z_1,Z_2,\ldots)$ correspondra une seule substitution du groupe $(X_1,X_2,\ldots)$; ce dernier groupe sera donc isomorphe au précédent, et si l'on désigne par ξ et ζ leurs ordres respectifs, par Θ le nombre des substitutions de $(Z_1,Z_2,\ldots)$ auxquelles correspond l'unité dans l'autre groupe, on aura

$$\zeta = \Theta\xi \equiv 0 \mod \xi.$$

D'ailleurs $(Z_1,Z_2,\ldots)$ étant un groupe de substitutions opérées entre q cycles, son ordre ζ divisera $1.2\ldots q$. D'un autre côté, le groupe $(X_1,X_2,\ldots)$, étant $e+2$ fois transitif entre $e+\Delta$ lettres, aura pour ordre un multiple de $(e+\Delta)(e+\Delta-1)\ldots(\Delta-1)$. On aura donc

$$1.2\ldots q \equiv 0 \mod \xi \equiv 0 \mod (e+\Delta)(e+\Delta-1)\ldots(\Delta-1), \tag{9}$$

et *a fortiori*

$$1.2\ldots q \geqslant (e+\Delta)(e+\Delta-1)\ldots(\Delta-1), \tag{10}$$

ou, comme $\Delta \geqslant 3$,

$$1.2\ldots q \geqslant 2.3\ldots(e+3),$$

d'où

$$e \leqslant q-3, \tag{11}$$

d'où l'on conclut

$$n = e + \Delta + pq \leqslant q - 3 + \mu\psi\left(\frac{q}{\mu}\right) + 3\mu - 1 + pq,$$

et enfin

$$\varphi(q) = n - pq \leqslant \mu\psi\left(\frac{q}{\mu}\right) + q + 3\mu - 4. \tag{12}$$

V

57. *Second cas*, $\mu = 1$. — Nous avons vu (27) que I_r sera primitif; mais I_{r-1} n'est pas transitif, et l'on pourra répartir ses lettres en classes, en réunissant ensemble celles qui sont permutées entre elles. Chaque classe sera formée des lettres d'un ou plusieurs cycles de A, seules, ou jointes à des lettres nouvelles. Soient respectivement $b, c, d, \ldots$ le nombre des cycles de A dont les lettres appartiennent à la première classe, à la seconde, à la troisième, etc.; $bp + b'$, $cp + c', \ldots$ les nombres de lettres de ces classes. Chaque substitution de I_{r-1} sera de la forme $BC \ldots, B, C, \ldots$ étant des substitutions partielles respectivement opérées sur les lettres des diverses classes.

Soient donc $B_1C_1 \ldots, B_2C_2 \ldots, \ldots$ les diverses substitutions semblables à A dont I_{r-1} est dérivé. Considérons les groupes respectivement dérivés des substitutions partielles $B_1, B_2, \ldots; C_1, C_2, \ldots; \ldots$.

58. Le groupe $(B_1, B_2, \ldots)$ a pour degré $bp + b'$, et contient une substitution d'ordre p à b cycles; à savoir la substitution partielle B_1 formée par les b premiers cycles de la substitution $A = B_1C_1 \ldots$.

Répartissons les lettres de ce groupe en systèmes tels que les substitutions de $(B_1, B_2, \ldots)$ remplacent les lettres de chaque système par celles d'un même système; et, s'il existe plusieurs semblables répartitions, choisissons une de celles où le nombre β des lettres de chaque système est maximum. Si $(B_1, B_2, \ldots)$ est primitif, chaque système sera formé d'une seule lettre et l'on aura $\beta = 1$; mais *dans tous les cas on aura* $\beta < p$. Supposons en effet qu'un des systèmes, s, contienne au moins p lettres. Le groupe $(B_1, B_2, \ldots)$ étant transitif, l'une au moins des substitutions dont il dérive, par exemple B_2, doit déplacer le système s; donc elle déplacera toutes ses lettres. Mais leur nombre est supérieur au nombre des cycles de B_2, lequel est au plus égal à q. Donc B_2 contiendra deux de ces lettres, α et α', dans un même cycle. Si elles s'y suivent à m rangs de distance, la substitution B_2^m, remplaçant α par α', ne déplacera pas s; et B_2, qui en est une puissance, ne le déplacera pas non plus, contrairement à notre supposition.

Les lettres contenues dans chacun des cycles de l'une quelconque des substi-

tutions $B_1, B_2, \ldots$, *telle que* B_2, *appartiendront toutes à des systèmes différents;* car si l'un de ces cycles contenait deux lettres de s, α et α', se suivant à m rangs d'intervalle, B_2^m et par suite B_2, qui en est une puissance, ne déplacerait pas s; donc elle permuterait exclusivement entre elles les lettres de ce système, résultat absurde, puisqu'elles sont en nombre insuffisant pour former un cycle dans B_2.

Donc chacune des substitutions $B_1, B_2, \ldots$ permutera les systèmes p à p. Donc le groupe $\mathfrak{B}$, formé par les déplacements que les substitutions du groupe $(B_1, B_2, \ldots)$ font éprouver aux systèmes, sera dérivé de substitutions d'ordre p; p étant impair, ces substitutions seront toutes contenues dans le groupe alterné. $\mathfrak{B}$ aura pour degré $\frac{bp+b'}{\beta}$. D'ailleurs il sera primitif; car autrement on pourrait grouper les systèmes en hypersystèmes contenant plus de β lettres, contrairement à notre hypothèse.

Enfin la substitution B_1 déplace bp lettres, appartenant à $\frac{bp}{\beta}$ systèmes, qu'elle permute p à p. Donc β divise b, et la substitution de $\mathfrak{B}$ correspondant à B_1 sera d'ordre p à $\frac{b}{\beta}$ cycles.

59. On verra de même que les lettres du groupe $(C_1, C_2, \ldots)$ peuvent être réparties en systèmes contenant chacun γ lettres, γ étant un diviseur de c qui peut se réduire à l'unité; et que les déplacements opérés sur les systèmes par les substitutions $(C_1, C_2, \ldots)$ forment un groupe primitif $\mathfrak{C}$ de degré $\frac{cp+c'}{\gamma}$, contenu dans le groupe alterné, et contenant une substitution d'ordre p à $\frac{c}{\gamma}$ cycles. De même pour chacun des groupes suivants $(D_1, D_2, \ldots), \ldots$.

Ici deux cas seront à distinguer :

60. *Première hypothèse. — Aucun des groupes* $\mathfrak{B}$, $\mathfrak{C}$, ... *ne contient le groupe alterné.*

Notre théorème étant supposé établi pour les nombres $\frac{b}{\beta}, \frac{c}{\gamma}, \ldots$ qui sont tous $< q$, on aura

$$\frac{b'}{\beta} \leqslant \varphi\left(\frac{b}{\beta}\right), \quad \frac{c'}{\gamma} \leqslant \varphi\left(\frac{c}{\gamma}\right), \ldots, \tag{13}$$

d'où

$$\begin{aligned} pq + \Delta &= 1 + bp + b' + cp + c' + \ldots \\ &= 1 + qp + b' + c' + \ldots \leqslant 1 + qp + \beta\varphi\left(\frac{b}{\beta}\right) + \gamma\varphi\left(\frac{c}{\gamma}\right) + \ldots \end{aligned} \tag{14}$$

Or supposons d'abord que $\frac{b}{\beta}, \frac{c}{\gamma}, \ldots$ soient tous $\leqslant \frac{q}{2}$; $\beta\varphi\left(\frac{b}{\beta}\right) + \gamma\varphi\left(\frac{c}{\gamma}\right) + \ldots$ est évidemment l'une des valeurs que peut prendre l'expression

$$\varphi(s) + \varphi(t) + \ldots, \tag{15}$$

où s, t, ... sont des entiers variables, assujettis aux conditions

$$s + t + \ldots = b + c + \ldots = q, \quad \frac{q}{2} \geqslant s \geqslant t \geqslant \ldots. \tag{16}$$

On aura donc, en désignant par $\mathfrak{M}$ la valeur maximum de cette expression,

$$\Delta \leqslant 1 + \mathfrak{M}. \tag{17}$$

61. Soit au contraire $\frac{b}{\beta} > \frac{q}{2}$, d'où $\beta = 1$; $(B_1, B_2, \ldots)$ sera primitif; mais nous allons montrer que ce groupe sera simplement transitif, si p est suffisamment grand. Dès lors on aura, en outre de l'hypothèse admise,

$$b' \leqslant \psi(b), \tag{18}$$

et, par suite,

$$\Delta \leqslant 1 + \psi(b) + \gamma\varphi\left(\frac{c}{\gamma}\right) + \ldots, \tag{19}$$

et *a fortiori*

$$\Delta \leqslant 1 + \mathfrak{N}, \tag{20}$$

$\mathfrak{N}$ désignant le maximum de l'expression

$$\psi(b) + \varphi(s) + \varphi(t) + \ldots \quad \left(s + t + \ldots = q - b,\ b > \frac{q}{2}\right). \tag{21}$$

62. Supposons en effet que $(B_1, B_2, \ldots)$ fût plusieurs fois transitif, et soient : x la lettre déplacée par I_r sans l'être par I_{r-1}; J le groupe formé par celles des substitutions de I_r qui laissent x immobile. Le groupe I_{r-1} est dérivé, par définition, de celles des substitutions de J qui sont semblables à A; et les substitutions de J, les transformant évidemment les unes dans les autres, seront permutables à I_{r-1}; donc elles remplaceront les lettres de chaque classe par celles d'une même classe. Mais les classes contiennent respectivement $bp + b'$, $cp + c'$, ... lettres; et, comme on a par hypothèse $b > \frac{q}{2}$ et $b + c + \ldots = q$, on aura $b > c > \ldots$. Si donc on a

$$p > 1 + \mathfrak{N}, \tag{22}$$

d'où *a fortiori*

$$p > 1 + \gamma\varphi\left(\frac{c}{\gamma}\right) + \ldots > 1 + c' + \ldots, \tag{23}$$

la première classe contiendra plus de lettres que toutes les autres et ne pourra, par suite, être permutée avec elles ; donc J permutera exclusivement entre elles les $bp + b'$ lettres de la première classe, d'une part, et les $(q - b)p + c' + \ldots$ lettres restantes, d'autre part.

63. Soient maintenant O l'ordre de J, et y, z deux quelconques des lettres de ce groupe. L'ordre du groupe L, formé par celles des substitutions de I_r qui laissent immobiles x, y, z, sera évidemment égal à $\frac{O}{mm'}$, m étant le nombre des lettres que les substitutions de J permutent avec y, et m' le nombre des lettres que celles des substitutions de J qui ne déplacent plus y permutent avec z. Par hypothèse, le groupe I_{r-1}, et *a fortiori* le groupe J, permute d'une manière deux fois transitive les lettres de la première classe. Donc si y et z appartiennent à cette classe, on aura $mm' = (bp + b')(bp + b' - 1)$. Si y appartient à la première classe et z aux autres classes, on aura encore $m = bp + b'$, et $m' \leqslant (q - b)p + c' + \ldots$ quantité moindre que $bp + b - 1$, car on a par hypothèse $q - b < b$, et $p > 1 + c' + \ldots$. Si enfin y et z n'appartiennent ni l'un ni l'autre à la première classe, m et m' seront tous deux moindres que $bp + b' - 1$. Donc mm' atteint son maximum lorsque y et z appartiennent à la première classe.

64. Cela posé, soient y, z, u, ... les lettres de la première classe ; v, w, ... les autres. Toute substitution S du groupe I_r qui remplace x par une des lettres y, z, ..., telle que y, permutera exclusivement entre elles les lettres x, y, z, ... En effet, soit J' le groupe transformé de J par S ; il ne déplacera pas y ; et les autres lettres s'y grouperont en classes, de telle sorte que l'ordre du groupe formé par celles des substitutions de J' qui laissent immobiles deux de ces lettres sera $\frac{O}{(bp + b)(bp + b' - 1)}$ si les deux lettres sont de la première classe, et sera plus grand dans le cas contraire. Or cet ordre sera $\frac{O}{(bp + b')(bp + b' - 1)}$ si les deux lettres données sont x et l'une des lettres z, u, ... Donc la première classe sera formée des lettres x, z, u, ... Mais elle est formée des lettres que S fait succéder à y, z, u, ... Donc S permute exclusivement entre elles les lettres x, y, z, u, ..., comme nous l'avons annoncé.

On déduit aisément de là (*Traité des substitutions*, n° 396) que le groupe I_r ne pourrait être primitif, ainsi que nous l'avons supposé, mais que ses lettres devraient se répartir en systèmes, dont l'un serait formé des lettres x, y, z, u, ...

Il est donc absurde d'admettre que $(B_1, B_2, \ldots)$ soit plusieurs fois transitif.

65. Soit maintenant $n = pq + \Delta + e$ le nombre des lettres que contient le groupe G. Il contient le groupe primitif et simplement transitif I_r; il sera donc $e+1$ fois transitif; et le degré $pq + \psi(q)$ des groupes simplement transitifs qu'il peut contenir ne pourra dépasser $pq + \Delta$; on aura donc ici

$$\psi(q) \leqslant \Delta, \tag{24}$$

Δ étant déterminé comme ci-dessus.

66. Supposons maintenant p supérieur à la plus grande des deux limites $1 + \mathfrak{N}$, $1 + \mathfrak{M}$, trouvées ci-dessus pour Δ.

On verra comme précédemment (47 à 55) : 1° que le groupe $\mathfrak{G}$ formé par celles des substitutions de G qui sont permutables au groupe formé des puissances de A et qui permutent exclusivement entre elles les lettres de A d'une part, et les lettres nouvelles d'autre part, est $e+1$ fois transitif par rapport à ces lettres nouvelles; 2° que ses substitutions sont de la forme $XZV^{\gamma}W$; 3° que si, dans deux de ces substitutions $X_1Z_1V^{\gamma_1}W_1$, $X_2Z_2V^{\gamma_2}W_2$, on a $Z_1 = Z_2$ sans avoir $X_1 = X_2$, et si l'on suppose $e > 2$, G contiendra un groupe de substitutions de la forme X, qui sera e fois transitif et de degré $e + \Delta$. Par suite, G sera $n - \Delta$ fois transitif; et comme il ne peut l'être plus de $\frac{n+4}{3}$ fois, on aura

$$n - \Delta \leqslant \frac{n+4}{3}, \text{ d'où } n \leqslant \frac{3\Delta + 4}{2},$$

résultat absurde, n étant égal à $pq + \Delta + e$, où $q > 1$, $p > \Delta$, $e > 2$.

Supposons au contraire qu'on ne puisse avoir $Z_1 = Z_2$ sans avoir $X_1 = X_2$. On verra, comme précédemment (56), que l'on a

$$1.2 \ldots q \equiv 0 \mod (e+\Delta)(e+\Delta-1)\ldots\Delta, \tag{25}$$

d'où, en donnant à Δ sa valeur minimum 1,

$$e \leqslant q, \tag{26}$$

limite au moins égale à la limite $e = 2$ trouvée dans l'autre hypothèse.

On aura donc, pour la limite supérieure de $e + \Delta$, l'une des deux expressions

$$\varphi(q) \leqslant q + \varphi(s) + \varphi(t) + \ldots \quad \left(s + t + \ldots = q,\ \frac{q}{2} \geqslant s \geqslant t \ldots\right), \tag{27}$$

ou

$$\varphi(q) \leqslant q + \psi(b) + \varphi(s) + \varphi(t) + \ldots \quad \left(s + t + \ldots = q - b,\ b > \frac{q}{2}\right). \tag{28}$$

67. *Seconde hypothèse. — Le groupe $\mathfrak{B}$ est alterné.*

Ce groupe sera simple et aura pour ordre $\omega = 3.4 \ldots p_1$, en posant, pour abréger, $p_1 = \frac{bp + b'}{\beta}$. Ce sera d'ailleurs le premier groupe composant de $(B_1, B_2, \ldots)$.

68. Lemme. — *Chacun des groupes* $(C_1, C_2, \ldots)$, $(D_1, D_2, \ldots)$, ... *aura l'un au moins de ses groupes composants isomorphe à* $\mathfrak{B}$.

Supposons en effet, pour fixer les idées, que le groupe $(C_1, C_2, \ldots)$ jouisse de cette propriété, à l'exclusion des autres groupes de la suite. Il a pour groupes composants ceux du groupe $\mathfrak{C}$, suivis de ceux du groupe formé par celles des substitutions de $(C_1, C_2, \ldots)$ qui ne déplacent pas les systèmes de γ lettres entre lesquels se répartissent les lettres de $(C_1, C_2, \ldots)$. Mais chacun de ces derniers groupes composants a évidemment pour ordre un diviseur de $1.2 \ldots \gamma$, nombre $< \omega$ (car $\gamma < q < p < p_1$). Donc l'un des groupes composants de $\mathfrak{C}$ sera isomorphe à $\mathfrak{B}$.

Cela posé, soient B'C', B''C'', ... celles des substitutions de I_{r-1} qui se réduisent à la forme BC. Le groupe $(B', B'', \ldots)$ sera évidemment contenu dans $(B_1, B_2, \ldots)$ et permutable à ses substitutions; d'ailleurs il aura conservé celui des facteurs de composition de $(B_1, B_2, \ldots)$ qui est afférent au groupe $\mathfrak{B}$ (*Sur la limite de transitivité des groupes non alternés*, n° 10). De même $(C', C'', \ldots)$ sera contenu dans $(C_1, C_2, \ldots)$ et permutable à ses substitutions, et le groupe $\mathfrak{C}'$ formé par celles des substitutions de $\mathfrak{C}$ qui correspondent à celles de $(C', C'', \ldots)$ aura conservé le facteur de composition ω.

69. Ici deux cas seront à distinguer, suivant que $\mathfrak{C}$ sera ou non alterné.

1° Si $\mathfrak{C}$ n'est pas alterné, ce groupe étant d'ordre $\frac{cp + c'}{\gamma}$ et contenant une substitution d'ordre p à $\frac{c}{\gamma}$ cycles, on aura par hypothèse

$$\frac{c'}{\gamma} < \varphi\left(\frac{c}{\gamma}\right), \quad c' < \gamma\varphi\left(\frac{c}{\gamma}\right) < p, \quad cp + c' < (c+1)p,$$

à cause de la relation (23).

Cela posé, le groupe alterné $\mathfrak{B}$ contient une substitution circulaire d'ordre p; la substitution correspondante du groupe $(B', B'', \ldots)$ sera de la forme MN, M permutant circulairement p systèmes et N permutant ensemble les lettres des autres systèmes, sans déplacer ces systèmes eux-mêmes. Le nombre β des lettres de chaque système étant $< p$, l'ordre de N sera évidemment premier à p. Donc, en élevant MN à une puissance convenable, on obtiendra une substitution, contenue dans $(B', B'', \ldots)$ et ne déplaçant que les lettres de p systèmes, en nombre βp. Soient B' cette substitution, B'C' la substitution correspondante dans le groupe $(B'C', B''C'', \ldots)$. Le nombre total des lettres que C' peut déplacer étant $< (c+1)p$, le nombre k des cy-

cles d'ordre p que C′ peut contenir ne saurait dépasser c. Mais il est clair qu'en élevant B′C′ à une puissance convenable, on obtiendra une substitution d'ordre p à $\beta+k$ cycles. Ce résultat est absurde ; car β divisant b, on aura $\beta \leqslant b$, et

$$\beta+k \leqslant b+c < b+c+d+\ldots < q,$$

et, par hypothèse, G ne contient aucune substitution d'ordre p à moins de q cycles.

70. 2° Si C est alterné, il sera simple, et aura pour ordre $3.4\ldots\frac{cp+c'}{\gamma}$; ce nombre devant être égal à ω, on aura $\frac{cp+c'}{\gamma}=p_1$.

Cela posé, à chaque substitution du groupe (B′C′, B″C″, ...) correspondent une substitution de $\mathfrak{B}$ et une de C. Si à deux substitutions différentes B′C′, B″C″ correspondaient dans $\mathfrak{B}$ deux substitutions différentes $\mathfrak{B}'$ et $\mathfrak{B}''$, et dans C une seule substitution C′, à la substitution $[B'C']^{-1}B''C''$ correspondraient dans C l'unité, et dans $\mathfrak{B}$ la substitution $\mathfrak{B}'^{-1}\mathfrak{B}''$ qui diffère de l'unité. Celles des substitutions de (B′C′, B″C″, ...), auxquelles correspond dans C l'unité, forment évidemment un groupe permutable aux substitutions B′C′, B″C″, ... ; leurs correspondantes dans $\mathfrak{B}$ formeront un groupe contenu dans $\mathfrak{B}$ et permutable à ses substitutions ; mais $\mathfrak{B}$ est simple ; donc ce nouveau groupe contiendra toutes les substitutions de $\mathfrak{B}$. Il contiendra en particulier une substitution circulaire d'ordre p. La substitution correspondante dans (B′C′, B″C″, ...) sera de la forme MNP, M permutant circulairement p des systèmes de β lettres, N permutant les lettres des autres systèmes de $\mathfrak{B}$ sans déplacer ces systèmes, et P permutant les lettres des systèmes de C sans déplacer ces systèmes ; d'ailleurs il est clair que N et P ont leur ordre premier à p ; donc MNP, élevé à une puissance convenable, donnera une substitution d'ordre p, à β cycles seulement ; résultat absurde.

71. Il faut donc admettre que la correspondance établie entre les substitutions de $\mathfrak{B}$ et de C est telle qu'à chaque substitution de C réponde une seule substitution de $\mathfrak{B}$. Or soient $s, s', \ldots$ les divers systèmes de β lettres que $\mathfrak{B}$ déplace ; $t, t', \ldots$ les divers systèmes de γ lettres que C déplace. *Deux substitutions correspondantes $\mathfrak{B}'$ et C′ déplaceront de la même manière les systèmes $s, s', \ldots$ et leurs homologues $t, t', \ldots$.*

En effet, celles des substitutions de $\mathfrak{B}$ qui laissent immobile s forment un groupe contenu dans $\mathfrak{B}$ et renfermant $3\ldots(p_1-1)$ substitutions. Les substitutions correspondantes de C devront former un groupe homologue Γ, d'ordre $3\ldots(p_1-1)$. Mais, en vertu d'un théorème de M. Bertrand, tout groupe de degré p_1 et d'ordre $3\ldots(p_1-1)$ (caractérisant une fonction à $2p_1$ valeurs) sera alterné par rapport à p_1-1 lettres, pourvu toutefois qu'on ait $p_1>7$;

on vérifie d'ailleurs aisément que cela est encore vrai pour $p_1 = 7$. Mais $p_1 \geqslant p$, et p est premier; donc cette condition sera satisfaite si l'on a

(29) $$p > 5.$$

Cette inégalité étant admise, le groupe Γ sera alterné par rapport à $p_1 - 1$ systèmes de la suite $t, t', \ldots$; et ses substitutions laisseront immobile le système restant t.

Donc à chacun des systèmes $s, s', \ldots$ sera associé un des systèmes $t, t', \ldots$, de telle sorte qu'à celles des substitutions de $\mathfrak{B}$ qui ne déplacent pas l'un des systèmes $s, s', \ldots$ correspondent des substitutions qui ne déplacent pas son associé.

72. Cela posé, soient s, s', s'', s''' quatre quelconques des systèmes de $\mathfrak{B}$; t, t', t'', t''' leurs correspondants dans $\mathfrak{C}$; $\mathfrak{B}$, étant alterné, contient les substitutions $S = (ss's'')$ et $S_1 = (ss's''')$; à la première correspond dans $\mathfrak{C}$ une substitution ternaire T, ne déplaçant que t, t' et t''; ce sera donc $(tt't'')$ ou $(tt''t')$; à la seconde correspondra de même une substitution T_1 de l'une des deux formes $(tt't''')$, $(tt'''t')$. Mais $S_1 S^{-1}$ laisse s invariable; donc $T_1 T^{-1}$ doit laisser t invariable; il faut évidemment pour cela qu'on ait $T = (tt't'')$, $T_1 = (tt't''')$.

Donc à chacune des substitutions circulaires ternaires telles que $(ss's'')$, dont $\mathfrak{B}$ est dérivé, correspondra dans $\mathfrak{C}$ une substitution analogue $(tt't'')$. Donc chaque substitution de $\mathfrak{C}$ déplacera les t de la même manière que sa correspondante dans $\mathfrak{B}$ déplace les s.

73. Cela posé, $\mathfrak{B}$ contient une substitution circulaire σ d'ordre p; son homologue dans $\mathfrak{C}$ sera circulaire et d'ordre p; et la substitution correspondante dans le groupe (B'C', B''C'', ...) sera de la forme MNM'N', M étant une substitution qui permute circulairement p des systèmes de $\mathfrak{B}$, N une substitution qui permute les lettres dans l'intérieur des autres systèmes, M' une substitution circulaire entre p systèmes de $\mathfrak{C}$, N' une substitution qui permute les lettres dans l'intérieur des autres systèmes. D'ailleurs N et N' ont leur ordre évidemment premier à p. Donc la substitution considérée, élevée à une puissance convenable, donnera une nouvelle substitution de la forme MM' et déplaçant seulement $(\beta + \gamma)p$ lettres; résultat absurde, $\beta + \gamma$ étant $< q$.

Notre lemme est donc établi.

74. Pour continuer notre recherche, nous distinguerons deux cas.

Premier cas. — Les groupes $\mathfrak{B}$, $\mathfrak{C}$,... sont tous alternés.

Nous admettrons, pour fixer les idées, que cette suite ne contient que deux groupes $\mathfrak{B}$ et $\mathfrak{C}$.

D'après ce que nous avons vu, on aura $p_1 = \frac{bp + b'}{\beta} = \frac{cp + c'}{\gamma}$. De plus, I_{r-1} contiendra une substitution d'ordre p déplaçant $(\beta + \gamma)p$ lettres; or

il ne peut par hypothèse en contenir aucune déplaçant moins de $qp=(b+c)p$ lettres. On aura donc nécessairement $\beta=b$, $\gamma=c$ $\left(\frac{b}{\beta}\right.$ et $\left.\frac{c}{\gamma}\right.$ devant être entiers).

D'ailleurs, chacun des systèmes s, s',... de $\mathfrak{S}$ doit être associé à un des systèmes t, t',... de $\mathfrak{C}$. En joignant ensemble les lettres des systèmes associés, on obtiendra des systèmes de $\beta+\gamma=q$ lettres, tels que les substitutions de I_{r-1} remplacent chacune les lettres d'un système par celles d'un même système, et permutent d'ailleurs les systèmes d'une manière alternée. Si donc on fait correspondre d'une manière arbitraire les lettres de chaque système avec celles d'un autre système, chaque substitution de I_{r-1} sera de la forme $\mathfrak{M}\mathfrak{N}$, $\mathfrak{M}$ étant une substitution qui permute les systèmes en remplaçant chaque lettre par sa correspondante, et $\mathfrak{N}$ une substitution qui permute exclusivement entre elles les lettres d'un même système.

75. Supposons maintenant que l'on ait la condition

$$p \geqslant 3q+2. \tag{30}$$

On pourra trouver un nombre premier π, supérieur à q, et inférieur à $\frac{p}{2}+1$. On le vérifie aisément par les tables de nombres premiers, si q est petit, et par les formules de M. Tchébychef, si q est grand. Cela posé, nous allons voir que la correspondance entre les lettres des divers systèmes peut être établie de telle sorte que celles des substitutions de I_{r-1} qui se réduisent à la forme $\mathfrak{M}$ permutent encore les systèmes d'une façon alternée.

Soient σ_0, σ_1, ..., ... les systèmes ; I_{r-1} contient une substitution $\mathfrak{M}'\mathfrak{N}'$ qui permute circulairement σ_0, ..., $\sigma_{\pi-1}$, sans déplacer les autres systèmes. Son ordre sera évidemment multiple de π ; et, en l'élevant à une puissance convenable, on obtiendra une substitution $\mathfrak{M}_1\mathfrak{N}_1$ d'ordre π, qui permute encore circulairement ces π systèmes.

La substitution $\mathfrak{N}_1$ sera le produit de deux autres, dont l'une $\mathfrak{L}$ déplace les lettres des systèmes σ_0, ... $\sigma_{\pi-1}$ et l'autre $\mathfrak{Q}_1$ celles des autres systèmes. Cette dernière substitution étant échangeable à $\mathfrak{M}_1\mathfrak{L}_1$, son ordre divisera π, ordre de $\mathfrak{M}_1\mathfrak{L}_1\mathfrak{Q}_1$; mais $\mathfrak{Q}_1$ permute exclusivement entre elles les lettres de chaque système, en nombre $q<\pi$. Donc son ordre est premier à π, et se réduit à l'unité. Donc $\mathfrak{M}_1\mathfrak{N}_1$ se réduit à $\mathfrak{M}_1\mathfrak{L}_1$.

Cela posé, faisons correspondre à chaque lettre de σ_0 la lettre de σ_1 que $\mathfrak{M}_1\mathfrak{L}_1$ lui fait succéder ; puis celle de σ_2 que $\mathfrak{M}_1\mathfrak{L}_1$ fait succéder à cette dernière, etc. La substitution $\mathfrak{M}_1\mathfrak{L}_1$, étant d'ordre π, fera succéder à chacune des lettres de $\sigma_{\pi-1}$ la lettre correspondante de σ_0. Donc elle se réduira à la forme $\mathfrak{M}_1$.

76. On verra de même que I_{r-1} contient une substitution $\mathfrak{M}_2$, d'ordre π et

permutant entre eux, et d'une manière circulaire, les systèmes $\sigma_0, \sigma_\pi, \ldots, \sigma_{2\pi-2}$.

Les substitutions $\mathfrak{M}_1$ et $\mathfrak{M}_2$, combinées entre elles, fourniront un groupe transitif de déplacements entre les systèmes $\sigma_0, \ldots, \sigma_{2\pi-2}$. Ce groupe $\mathcal{G}$, de degré $2\pi-1$ et dérivé de substitutions circulaires d'ordre π, sera alterné. Ses substitutions, remplaçant d'ailleurs chaque lettre par sa correspondante, seront de la forme $\mathfrak{M}$; et celle d'entre elles, S, qui permute circulairement les trois systèmes $\sigma_0, \sigma_1, \sigma_2$ sans déplacer les autres, déplacera en tout $3q$ lettres.

77. Cela posé, on a $p_1 \geqslant p \geqslant 2\pi-1$. Si l'on a $p_1 = 2\pi-1$, notre proposition sera démontrée. Si au contraire $p_1 > 2\pi-1$, on peut admettre que la différence de ces deux nombres est paire. Sans quoi, au lieu de raisonner sur le groupe $\mathcal{G}$ comme nous allons le faire, on raisonnerait sur le groupe $\mathcal{G}_1$ formé des substitutions de $\mathcal{G}$ qui laissent immobile le système $\sigma_{2\pi-2}$. Ce groupe contient S, et il est alterné comme $\mathcal{G}$; mais il ne déplace que $2\pi-2$ systèmes, nombre dont la différence avec p_1 sera paire.

Soit donc $p_1 - 2\pi + 1 =$ un nombre pair; les systèmes non déplacés par $\mathcal{G}$ pourront se répartir en couples. Soient σ_μ, σ_ν les deux systèmes d'un même couple; le groupe I_{r-1}, permutant les systèmes d'une manière alternée, contient une substitution T qui permute σ_μ avec σ_1 et σ_ν avec σ_2 sans déplacer les autres systèmes; il contiendra $T^{-1}ST = S'$ laquelle permute les trois systèmes $\sigma_0, \sigma_\mu, \sigma_\nu$ et ne déplace aucune autre lettre. Faisons maintenant correspondre à chaque lettre de σ_0 celle des lettres de σ_μ que S' lui fait succéder, puis celles des lettres de σ_ν que S' fait succéder à ces dernières; S' étant d'ordre 3, comme S dont elle est transformée, remplacera chaque lettre de σ_ν par sa correspondante de σ_0.

Soit de même $\sigma_{\mu'}$, $\sigma_{\nu'}$ un autre couple de systèmes; on pourra faire correspondre leurs lettres à celles de σ_0, de telle sorte que I_{r-1} contienne une substitution S'' qui permute entre eux ces trois systèmes, en remplaçant les unes par les autres les lettres correspondantes, sans déplacer aucune autre lettre.

Cela posé, il est clair qu'en adjoignant à $\mathcal{G}$ les substitutions S', S'', ..., on obtiendra un groupe résultant J dont les substitutions seront de la forme $\mathfrak{M}$, et permuteront les systèmes d'une façon alternée.

78. Soient $u_0 v_0 \ldots$ les q lettres du système σ_0, $u_m v_m \ldots$ leurs correspondantes dans σ_m. En groupant ensemble celles de ces lettres que J permute entre elles, on les répartira en q classes, $u_0 u_1 \ldots$, $v_0 v_1 \ldots$, ...

Soit S une de celles des substitutions de G qui déplacent le moins de lettres; N le nombre de ses lettres; on aura $N \leqslant 3q$, J étant dérivé de substitutions ternaires à q cycles.

Le groupe G étant primitif, le groupe K, dérivé de celles de ses substitutions qui sont semblables à S, sera transitif. Si donc G contient plus de qp_1

lettres, ce que nous supposerons pour plus de généralité, l'une au moins S des substitutions de K mêlera dans ses cycles les lettres de J à des lettres nouvelles $x, y, \ldots$. Or celles des lettres de J que S déplace sont en nombre inférieur à N, et *a fortiori* à $3q$. Donc, parmi les systèmes $\sigma_0, \sigma_1, \ldots$ en nombre $p_1 \geqslant 3q+2$, il en existe au moins deux, σ_0 et σ_1, dont S ne déplace aucune lettre. Soit au contraire σ_2 un quelconque des systèmes dont S déplace des lettres; et soit ν le nombre de lettres de σ_2 que contient S. Le groupe J contient une substitution T qui permute circulairement les trois systèmes $\sigma_0, \sigma_1, \sigma_2$; et G contiendra $S^{-1}T^{-1}ST$, qui laisse toutes les lettres immobiles, sauf les ν lettres de σ_2 que S déplace, celles que S leur fait succéder, et les lettres correspondantes de σ_0; en tout 3ν lettres, qui même peuvent n'être pas toutes distinctes; mais elle en déplace au moins N; donc on aura

$$\nu \geqslant \frac{N}{3}.$$

Par suite, *les lettres de* J *que* S *déplace ne peuvent appartenir à plus de trois systèmes différents*. Supposons, pour fixer les idées, qu'elles appartiennent toutes à l'un des trois systèmes $\sigma_2, \sigma_3, \sigma_4$.

79. Considérons le groupe (J, S) obtenu en adjoignant S aux substitutions de J; et groupons ensemble celles de ses lettres qu'il permute transitivement entre elles; on obtiendra ainsi une ou plusieurs catégories de lettres, dont chacune pourra contenir, avec les lettres d'une ou plusieurs des classes $u_0u_1 \ldots, v_0v_1 \ldots, \ldots$, une ou plusieurs lettres nouvelles. En particulier, si une catégorie était uniquement formée de lettres nouvelles, elles fourniraient un cycle dans S; et les déplacements que (J, S) leur fait subir se réduiraient évidemment aux puissances d'une seule substitution circulaire. D'ailleurs, S mêlant dans ses cycles les lettres anciennes aux nouvelles, l'une au moins des catégories contiendra à la fois ces deux sortes de lettres.

Enfin chaque substitution de (J, S), telle que S, est le produit de substitutions partielles $S_1, S_2, \ldots$ respectivement opérées entre les lettres de chaque catégorie. Soit (J_1, S_1) le groupe formé par les déplacements ainsi opérés entre les lettres de la première catégorie par les substitutions (J, S).

Admettons, pour fixer les idées, que la première catégorie contienne les lettres des b_1 premières classes $u, v, \ldots$ et b_1' lettres nouvelles $x, y, \ldots$. Ce groupe (J_1, S_1) peut être primitif ou non; mais, dans ce dernier cas, *le nombre des lettres de chaque système sera nécessairement un diviseur de* b_1.

En effet, s'il en était autrement, les b_1 lettres $u_0v_0 \ldots$ de σ_0 que (J_1, S_1) déplace ne fourniraient pas à elles seules un nombre entier de systèmes; donc l'une d'elles, u_0, appartiendrait au même système qu'une autre lettre,

laquelle pourrait être une des lettres de la même classe que u, telle que u_1, ou une lettre d'une autre classe, telle que v_2, ou enfin une lettre nouvelle, telle que x.

Si u_0 était dans le même système que v_2 ou que x, il serait dans le même système que u_1; car J contient une substitution qui permute circulairement $\sigma_0\sigma_1\sigma_2$. Cette substitution, laissant v_2 et x immobiles, ne déplacera pas le système qui les contient; donc u_1 qu'elle fait succéder à u_0 appartiendra à ce système.

Il faut donc admettre que u_0 est dans le même système que u_1; mais alors ce système contiendra les p_1 lettres $u_0u_1\ldots$. En effet, soit u_ρ l'une d'elles. J contient une substitution qui permute circulairement $\sigma_0\sigma_1\sigma_\rho$. Cette substitution, remplaçant u_0 par u_1, ne déplacera pas le système qui les contient; donc u_ρ qu'elle fait succéder à u_1 appartiendra à ce système.

Donc chaque système contiendrait au moins p_1 lettres. Mais (J_1, S_1) étant primitif, l'une au moins des substitutions dont il est dérivé déplacerait les systèmes, et par suite déplacerait au moins $2p_1$ lettres; résultat absurde, car (J_1, S_1) est dérivé de substitutions ternaires à q cycles, et de la substitution partielle S_1 formée par ceux des cycles de S qui déplacent les lettres de la première catégorie, lesquels cycles contiennent un nombre de lettres $\leqslant N \leqslant 39$.

Parmi les diverses répartitions possibles des lettres de (J_1, S_1) en systèmes, choisissons l'une de celles où le nombre β_1 des lettres de chaque système est maximum. Les déplacements des systèmes par les substitutions de (J_1, S_1) formeront un groupe primitif $\mathfrak{B}_1$ de degré $\frac{b_1p_1+b_1'}{\beta_1}$.

Cela posé, la substitution S ne déplaçant par hypothèse que des lettres appartenant aux trois systèmes σ_2, σ_3, σ_4, et les autres substitutions dont J est dérivé remplaçant les lettres de chacun des systèmes σ_0, σ_1, ... par les lettres correspondantes d'un même système, il faudra évidemment, pour que (J, S) permute transitivement entre elles les lettres de la première catégorie, que le groupe dérivé de la substitution S et de celle U des substitutions de J qui permute circulairement les trois systèmes σ_2, σ_3, σ_4 soit transitif par rapport aux $3b_1+b_1'$ lettres de première catégorie qu'il déplace.

Le groupe (U_1, S_1) formé par les déplacements que (U, S) fait éprouver à ces lettres sera donc transitif, et contenu dans (J_1, S_1). D'ailleurs ces lettres formeront $\frac{3b_1+b_1'}{\beta_1}$ systèmes; et les déplacements d'ensemble opérés sur ces systèmes par les substitutions de (J_1, S_1) formeront un groupe transitif, de degré $\frac{3b_1+b_1'}{\beta_1}$ et contenu dans $\mathfrak{B}_1$.

Le groupe $\mathfrak{B}_1$ sera donc alterné (*Théorèmes sur les groupes primitifs,*

n° 11), si son degré $\frac{b_1 p_1 + b'_1}{\beta_1}$ surpasse $3\left(\frac{3b_1 + b'_1}{\beta_1}\right) - 2$, ce qui aura lieu si p_1, et *a fortiori* si p, est supérieur à la limite

$$9 + \frac{2b'_1}{b_1} - \frac{2\beta_1}{b_1}.$$

Or le nombre total N des lettres déplacées par S est $\leqslant 3q$, parmi lesquelles $\frac{N}{3}$ au moins sont des lettres anciennes; donc $b'_1 \leqslant 2q$, ce qui réduit la limite de p à

$$9 + \frac{4q}{b_1} - \frac{2\beta_1}{b_1}.$$

Mais nous avons déjà supposé $p \geqslant 3q + 2$; et cette ancienne limite sera supérieure à celle que nous trouvons ici, à moins qu'on n'ait

$$b_1 = 1,$$

ou

$$b_1 = 2 \text{ et } q < 6,$$

ou

$$b_1 = 3 \text{ et } q < 4.$$

Mais si $b_1 = 1$, d'où $\beta_1 = 1$, le groupe J_1 sera alterné, et le groupe $\mathfrak{B}_1$, qui se confond ici avec (J_1, S_1), étant primitif et contenant J_1, sera alterné.

Dans les autres cas d'exception, on aura pour maximum de la limite

$$p > 18, \tag{31}$$

inégalité que nous supposerons satisfaite. Dès lors il sera établi que $\mathfrak{B}_1$ est alterné.

80. Soit de même $c_1 p + c'_1$ le nombre des lettres de la seconde catégorie. Elles pourront se répartir en $\frac{c_1 p_1 + c'_1}{\gamma_1}$ systèmes, γ_1 étant un diviseur de c_1; et les déplacements de ces systèmes par les substitutions de (J, S) formeront un groupe alterné $\mathfrak{C}_1$. De même pour chacune des autres catégories qui renferment des lettres anciennes.

81. Supposons, pour fixer les idées, que toutes les catégories, sauf les deux premières ci-dessus, soient exclusivement formées de lettres nouvelles. Les déplacements de ces lettres nouvelles par les substitutions de (J, S) se réduiront aux déplacements opérés par S et ses puissances; et le groupe L, formé par celles des substitutions de (J, S) qui ne déplacent que les lettres des deux premières catégories, sera contenu dans (J, S) et permutable à ces substitutions. Il aura d'ailleurs évidemment conservé tous ceux des groupes

composants de (J, S) qui ne sont pas des puissances d'une même substitution; et notamment ceux qui sont afférents aux groupes $\mathfrak{B}_1, \mathfrak{C}_1$.

82. Cela posé, on verra comme plus haut (68 à 73) que G contiendrait une substitution d'ordre p à moins de q cycles (ce qui est absurde), à moins qu'on ne suppose $\frac{b_1 p_1 + b'_1}{\beta_1} = \frac{c_1 p_1 + c'_1}{\gamma_1}$, $\beta_1 = b_1$, $\gamma_1 = c_1$, et qu'on n'admette en outre que les groupes $\mathfrak{B}_1, \mathfrak{C}_1$ se correspondent de telle sorte qu'à chaque substitution de $\mathfrak{B}_1$ en corresponde une seule de $\mathfrak{C}_1$, et réciproquement. Mais, si ces conditions sont satisfaites, on pourra poser, pour abréger, $\frac{b_1 p_1 + b'_1}{\beta_1} = p_2$; et l'on verra : 1° que les $p_2 q$ lettres déplacées par L y forment p_2 systèmes tels, que les substitutions de L remplacent les lettres de chaque système par celles d'un même système ; 2° que G contient un groupe J_1 de degré $p_2 q$, dont les lettres se grouperont q à q en p_2 systèmes, que J_1 permute d'une manière alternée, en remplaçant les unes par les autres les lettres correspondantes.

On aura d'ailleurs $p_2 > p_1$; car S mêlant dans ses cycles des lettres nouvelles avec les lettres anciennes que J déplaçait, on ne pourra pas avoir à la fois $b'_1 = 0$, $c'_1 = 0$.

83. Si le nombre des lettres de G était supérieur à $p_2 q$, on verrait de même que G contient un groupe J_2 analogue à J_1, mais de degré $p_3 q$, p_3 étant $> p_2$.

Continuant ainsi, on voit que le nombre des lettres de G sera un multiple de q, tel que $p_m q$, et que G contient un groupe J_{m-1} dans lequel ces lettres forment p_m systèmes, $u_0, v_0, \ldots$; $u_1, v_1, \ldots$; ... que J_{m-1} permute d'une manière alternée, en remplaçant les unes par les autres les lettres correspondantes.

Il n'existe d'ailleurs aucune autre manière de répartir les lettres de J_{m-1} en systèmes de q lettres. En effet, supposons qu'un de ces nouveaux systèmes s contint les deux lettres u_0 et u_1 par exemple; et soit u_2 une quelconque des $p_m - 2$ lettres $u_2, u_3, \ldots$; J_{m-1} contient une substitution qui permute circulairement u_0, u_1, u_2. Cette substitution ne déplace pas le système s; donc u_2 appartient à ce système, qui contiendra dès lors au moins p_m lettres, nombre $> q$, contrairement à l'hypothèse.

En second lieu, si s contenait u_0 et v_1, J_{m-1} contient des substitutions qui laissent u_0 immobile et permutent ensemble $v_1, v_2, \ldots$. Ces lettres appartiendraient à s, qui contiendrait encore au moins p_m lettres.

84. Soit maintenant Σ une quelconque des substitutions de G qui ne déplacent que N lettres. On peut supposer que son ordre k est un nombre premier; car, au besoin, on considérerait à sa place une quelconque de ses puissances. Adjoignons-la au groupe J_{m-1}. Raisonnant sur Σ et sur J_{m-1} comme tout à l'heure sur S et sur J, on voit que G contiendra une substitu-

tion d'ordre p à moins de q cycles (résultat absurde), à moins que les lettres de (J_{m-1}, Σ) ne puissent se répartir en systèmes de q lettres. Mais il n'y a qu'une manière de grouper les lettres de J_{m-1} en systèmes de q lettres. Donc Σ remplacera les lettres de chaque système par celles d'un même système. Les substitutions semblables à Σ forment un groupe K qui ne sera pas primitif, d'après ce qui précède; il est permutable à G, et par suite transitif. Donc l'une au moins de ses substitutions, Σ par exemple, déplacera les systèmes.

Soit d'ailleurs σ l'un des systèmes qu'elle déplace; C l'un des cycles de Σ, qui contienne une des lettres de Σ. Les k lettres de ce cycle appartiendront à k systèmes distincts; car si deux d'entre elles appartenaient à un même système σ_1, et se suivaient à ρ rangs de distance dans C, il est clair que Σ^ρ et par suite Σ, qui en est une puissance, ne déplacerait pas ce système. Donc les lettres de C appartiendraient toutes à σ_1, contrairement à l'hypothèse.

Donc Σ déplace au moins k systèmes; elle déplacera toutes leurs lettres, en nombre kq; d'où $N \geqslant kq$. Mais J_{m-1} contient des substitutions d'ordre 3 à q cycles; donc $N \leqslant 3q$ et par suite $k \leqslant 3$.

La substitution Σ ne déplaçant ainsi que deux ou trois systèmes, ses transformées par les diverses substitutions de J_{m-1}, qui permute les systèmes d'une manière alternée, formeront évidemment un groupe $\mathfrak{H}$ qui permute les systèmes d'une manière alternée si $k = 3$, de toutes les manières possibles si $k = 2$. On en conclut comme précédemment (75 à 77 et 83) : 1° que l'on pourrait établir entre les lettres des divers systèmes une correspondance telle, que $\mathfrak{H}$ contînt un groupe $\mathfrak{H}_1$ permutant les systèmes d'une manière alternée, en remplaçant les unes par les autres les lettres correspondantes; 2°. qu'il n'existe qu'une manière de répartir les lettres q à q en systèmes dans le groupe $\mathfrak{H}_1$, et *a fortiori* dans le groupe K, qui contient $\mathfrak{H}_1$.

Cela posé, soit T une substitution quelconque de G; elle remplace les divers systèmes de q lettres que renferme K par de nouveaux systèmes tels que les substitutions du groupe transformé de K par T, lequel groupe n'est autre que K, remplacent les lettres de chaque système par celles d'un même système. Comme il n'y a qu'une répartition possible des lettres de K en systèmes de q lettres, les nouveaux systèmes se confondront avec les anciens. Donc T remplacera les lettres de chaque système par celles d'un même système. Donc G ne pourra être primitif, comme on l'a supposé. Nous nous trouvons ainsi conduits à une absurdité.

85. *Second cas. — L'un des groupes* C, ..., *par exemple* C, *n'est pas alterné.*

Ici encore nous allons démontrer qu'on arrive à une impossibilité si p satisfait aux inégalités (30) et (31) et à la suivante

$$p > \varphi(s) \quad (s = 1, 2, \ldots, q-1). \tag{32}$$

86. Et d'abord, si $\mathcal{C}$ était simple, il serait isomorphe à $\mathfrak{B}$; mais c'est impossible. En effet, si cela était, on sait (*Traité des substitutions*, 69 à 73) qu'il existerait une fonction Φ des p_1 systèmes permutés par $\mathfrak{B}$ dont les déplacements par les substitutions de $\mathfrak{B}$ formeraient un groupe semblable à $\mathcal{C}$. Le nombre des valeurs distinctes que prend cette fonction par les substitutions de $\mathfrak{B}$ serait donc égal à $\frac{cp+c'}{\gamma}$, degré de $\mathcal{C}$; et suivant qu'elle serait altérée ou non par une transposition effectuée entre deux systèmes, elle prendrait $2\frac{cp+c'}{\gamma}$ ou $\frac{cp+c'}{\gamma}$ valeurs distinctes par toutes les substitutions possibles opérées sur les p_1 systèmes. Or, d'après un théorème de M. Bertrand, une fonction quelconque des p_1 systèmes prendra p_1 valeurs si elle est symétrique par rapport à p_1-1 systèmes; $2p_1$ si elle est alternée par rapport à p_1-1 systèmes; au moins $\frac{p_1(p_1-1)}{2}$ valeurs dans tous les autres cas. D'ailleurs on a $\frac{c'}{\gamma} \leqslant \varphi\left(\frac{c}{\gamma}\right) < p$ et, par suite,

$$\frac{p_1(p_1-1)}{2} \geqslant \frac{p(p-1)}{2} \geqslant pq \geqslant (c+1)p > \frac{cp+c'}{\gamma}.$$

Il faut donc admettre que Φ est symétrique ou alternée par rapport à p_1-1 systèmes; mais alors elle prendra p_1 valeurs distinctes par les déplacements des systèmes; et si l'on fait correspondre à chacune de ces p_1 fonctions $\Phi, \Phi', \ldots$ celui des systèmes qui y figure d'une manière dissymétrique, il est clair que les diverses fonctions $\Phi, \Phi', \ldots$ seront permutées les unes dans les autres par les substitutions de $\mathfrak{B}$ de la même manière que les systèmes correspondants ; le groupe formé par les déplacements de ces fonctions sera donc alterné comme $\mathfrak{B}$, et le groupe $\mathcal{C}$, qui lui est semblable, le sera aussi, contrairement à l'hypothèse.

87. Supposons donc que $\mathcal{C}$ soit composé. Nous remarquerons d'abord que *son ordre est divisible par p* (puisqu'il dérive de substitutions d'ordre p), *mais non divisible par* p^2. En effet, les systèmes qu'il permute sont en nombre $\frac{c}{\gamma}p+\frac{c'}{\gamma}$; et l'on voit comme précédemment (47) que l'ordre Ω du groupe $\mathcal{C}$ contient le facteur p à la même puissance que l'ordre 0 du groupe formé par celles de ses substitutions qui ne déplacent que les $\frac{c}{\gamma}p$ systèmes que A déplace ; de plus, si 0 était divisible par p^2, $\mathcal{C}$ contiendrait une substitution d'ordre p à moins de $\frac{c}{\gamma}$ cycles. Soit $\frac{c}{\gamma}-k$ le nombre de ces cycles. $\mathcal{C}$ étant primitif et ne contenant pas le groupe alterné, on aurait par hypothèse la relation

$$\varphi\left(\frac{c}{\gamma}-k\right)\geqslant kp+\frac{c'}{\gamma};$$

ce qui est absurde, en vertu de l'inégalité (32).

88. En second lieu, soit $\mathcal{C}'$ le groupe le plus général parmi ceux qui sont contenus dans $\mathcal{C}$ et permutables à ses substitutions; *le nombre p divisera l'ordre de* $\frac{\mathcal{C}}{\mathcal{C}'}$, *premier groupe composant de* $\mathcal{C}$. Supposons en effet que p divisât au contraire l'ordre de $\mathcal{C}'$. Ce groupe contiendrait un groupe d'ordre p. Étant permutable aux substitutions de $\mathcal{C}$, il contiendrait tous les groupes transformés de celui-là par les substitutions de $\mathcal{C}$. Mais, d'une part, tous les groupes d'ordre p contenus dans $\mathcal{C}$ sont les transformés de l'un quelconque d'entre eux par les substitutions de $\mathcal{C}$ (théorème de M. Sylow); d'autre part, $\mathcal{C}$ est dérivé de substitutions d'ordre p (respectivement correspondantes à $C_1, C_2, \ldots$); donc $\mathcal{C}'$, contenant toutes ces substitutions, se confondrait avec $\mathcal{C}$.

Si donc $\mathcal{C}$ a, comme on le suppose, un groupe composant isomorphe à $\mathcal{B}$, dont l'ordre $\omega = 3.4 \ldots p_1$ est divisible par p, ce groupe composant ne pourra être que le premier $\frac{\mathcal{C}}{\mathcal{C}'}$.

89. Cela posé, soient $M_1, \ldots, M_\pi$ les substitutions de $\mathcal{C}'$. On pourra déterminer dans $\mathcal{C}$ des substitutions $N_1, \ldots, N_\omega$ en nombre ω, incongrues (mod $\mathcal{C}'$); et les substitutions de $\mathcal{C}$ seront données par le tableau

$$\begin{array}{c} M_1N_1, \ \ldots, \ M_1N_\pi \\ \cdots\cdots\cdots \\ M_\omega N_1, \ \ldots, \ M_\omega N_\pi. \end{array}$$

Posons pour abréger $\frac{cp+c'}{\gamma}=\lambda_1$, $\frac{c'}{\gamma}=\varepsilon$, et admettons, pour plus de généralité, que l'on ait $\varepsilon > 0$. Le groupe $\mathcal{C}_1$ formé par celles des substitutions de $\mathcal{C}$ qui laissent immobile un des ε systèmes qui figurent dans $\mathcal{C}$, mais que A ne déplaçait pas, a pour ordre celui de $\mathcal{C}$, divisé par λ. Celles des lignes du tableau précédent dont quelque substitution est contenue dans $\mathcal{C}_1$ forment donc au moins la $\lambda^{\text{ième}}$ partie du nombre total; donc l'ordre ω_1 du groupe $\frac{\mathcal{C}_1}{\mathcal{C}'}$ formé par les substitutions correspondantes du groupe $\frac{\mathcal{C}}{\mathcal{C}'}$ sera au moins égal à $\frac{\omega}{\lambda}$. Le groupe $\mathcal{B}$, étant isomorphe à $\frac{\mathcal{C}}{\mathcal{C}'}$, devra de même contenir un groupe $\mathcal{B}_1$, isomorphe à $\frac{\mathcal{C}_1}{\mathcal{C}'}$, et d'ordre ω_1. Mais, d'après le théorème de M. Bertrand, si $\omega_1 < \omega$, il sera égal à $\frac{\omega}{p_1}$, ou au moins égal à $\frac{2}{p_1(p_1-1)}\omega$.

Cette dernière hypothèse est absurde, $\frac{cp+c'}{\gamma}$ étant $< \frac{p_1(p_1-1)}{2}$. D'ailleurs, en vertu du même théorème, si $\omega_1 = \frac{\omega}{p_1}$, $\mathfrak{B}_1$ sera le groupe d'une fonction alternée par rapport à $p_1 - 1$ systèmes, et sera un groupe simple, d'ordre $3.4...(p_1-1)$. Enfin, si $\omega_1 = \omega$, $\mathfrak{B}_1$ se confond avec $\mathfrak{B}$, et par suite sera simple, et d'ordre $3.4...p_1$. Donc le groupe $\frac{\mathfrak{C}_1}{\mathfrak{C}'}$ sera simple, et isomorphe au groupe alterné de degré $p_1 - \theta_1$, θ_1 étant égal à 0 ou à 1.

90. D'ailleurs $p_1 - \theta_1 \geqslant p$. En effet, s'il en était autrement, $\frac{\mathfrak{C}_1}{\mathfrak{C}'}$ n'aurait pas son ordre divisible par p; les autres groupes composants de $\mathfrak{C}_1$, étant contenus dans $\mathfrak{C}'$, leur ordre ne sera pas non plus divisible par p. Donc l'ordre de $\mathfrak{C}_1$ serait premier à p; résultat absurde, car il contient une substitution d'ordre p, correspondant à la substitution A.

91. Soient $\mathfrak{C}_2$, $\mathfrak{C}_3$, ... les groupes respectivement formés par celles des substitutions de $\mathfrak{C}$ qui laissent immobiles deux, trois, etc., des ε systèmes que A ne déplaçait pas; on voit de la même manière que $\frac{\mathfrak{C}_2}{\mathfrak{C}'}$, $\frac{\mathfrak{C}_3}{\mathfrak{C}'}$, ... sont isomorphes aux groupes alternés de degrés $p_1 - \theta_2$, $p_1 - \theta_3$, ..., $\theta_\rho + 1$ étant égal à θ_ρ ou à $\theta_\rho + 1$, et par suite contenu entre 0 et ρ; $p_1 - \theta_\rho$ étant d'ailleurs au moins égal à p. Donc enfin $\frac{\mathfrak{C}_\varepsilon}{\mathfrak{C}'}$ *sera isomorphe à un groupe alterné de degré* $p_1 - \theta_\varepsilon$, θ_ε *étant compris entre* 0 *et* ε, *et* $p_1 - \theta_\varepsilon$ *au moins égal à* p.

92. Donc l'un des groupes composants de $\mathfrak{C}_\varepsilon$ est isomorphe à un groupe alterné de degré $p' \geqslant p$. Le groupe X, dérivé de celles des substitutions de $\mathfrak{C}_\varepsilon$ qui sont d'ordre p, jouira de la même propriété. En effet, il est évidemment permutable aux substitutions de $\mathfrak{C}_\varepsilon$; donc il possédera comme groupes composants une partie de ceux de $\mathfrak{C}_\varepsilon$, et notamment celui dont l'ordre est divisible par p, puisque l'ordre de X est divisible par p.

93. Le groupe X déplace $\frac{cp}{\gamma}$ systèmes, et dérive de substitutions qui les permutent p à p. Si donc X ne les permute pas transitivement, on pourra, en groupant ensemble ceux que X permute entre eux, les répartir en classes, contenant respectivement $k_1 p$, $k_2 p$, ... systèmes, avec la condition $k_1 + k_2 + ... = \frac{c}{\gamma}$. Soient $X_1, X_2, ...$ les groupes partiels formés par les déplacements que les substitutions de X font éprouver aux systèmes des diverses classes. Ils seront respectivement dérivés de substitutions d'ordre p, à k_1 cycles, à k_2 cycles, etc.

94. Considérons l'un de ces groupes X_1. Il est transitif et de degré $k_1 p$; donc son ordre est divisible par p; donc un au moins de ses facteurs de composition est divisible par p. Mais les facteurs de composition de X_1 sont tous des facteurs de composition de X, lequel a un facteur de composition divisible par $3.4...p$, les autres étant tous premiers à p (car l'ordre de X, divisant celui de $\mathcal{C}$, ne sera pas divisible par p^2). Donc X_1 n'a qu'un groupe composant dont l'ordre soit divisible par p, et cet ordre sera $3.4... p'$. D'ailleurs X_1, étant dérivé de substitutions d'ordre p, ce groupe composant sera nécessairement le premier (88).

95. Parmi les diverses répartitions possibles des systèmes que X_1 déplace en hypersystèmes (tels que chaque substitution de X_1 remplace les systèmes de chaque hypersystème par celles d'un même hypersystème), choisissons celle où le nombre μ des systèmes contenus dans chaque hypersystème est maximum (si X_1 était primitif, on aurait $\mu = 1$). On aura $\mu \leqslant k_1$. En effet, X_1 est dérivé de substitutions d'ordre p à k_1 cycles. Si donc une de ses substitutions S déplace l'un des systèmes, s, elle déplacera ses μ lettres. Si μ était $> k_1$, deux au moins de ces lettres se trouveraient dans un même cycle de S; et par suite S ne déplacerait pas ce système, ainsi qu'on l'a supposé. D'ailleurs μ divise $k_1 p$, nombre total des systèmes; et comme il est $\leqslant k_1$, il sera $< p$, et divisera k_1.

Mais on aura $\mu = k_1$. En effet, soit Y_1 le groupe primitif de degré $\frac{k_1 p}{\mu}$ formé par les déplacements que X_1 fait éprouver aux hypersystèmes; X_1 aura pour premier facteur de composition le premier facteur de composition de Y_1, lequel sera, par suite, $3.4... p'$. Soit maintenant Z_1 le groupe dérivé de Y_1 par la suppression de ce facteur de composition. L'ordre de Z_1 n'étant plus divisible par p, ce groupe ne sera plus transitif; donc il se réduira à la seule substitution 1, sans quoi Y_1 ne serait pas primitif comme il doit l'être. Donc Y_1 est simple, et a pour ordre $3.4... p'$. Mais son degré $\frac{k_1 p}{\mu} < \frac{p'(p'-1)}{2}$. Donc, d'après le théorème de M. Bertrand, il se réduira à p'; d'ailleurs $3.4 .. p'$ n'étant pas divisible par p^2 (87), p' sera $< 2p$; on aura donc $p' = p$ et $\mu = k_1$. De plus, Y_1 sera alterné.

Donc *les systèmes de* X_1 *se groupent* k_1 *à* k_1 *en* p *hypersystèmes, que* Y_1 *permute d'une manière alternée.*

96. On verra de même que les systèmes de X_2 se groupent k_2 à k_2 en p hypersystèmes, et que les déplacements que X_2 fait subir à ces hypersystèmes forment un groupe alterné Y_2, etc.

Cela posé, à chaque substitution de X correspond une substitution dans chacun des groupes Y_1, Y_2, ...; et cette correspondance doit être telle, qu'à chaque substitution de l'un des groupes Y_1, Y_2, ... corresponde une seule substitution dans chacun des autres groupes. Car si à deux substitutions S et

T du groupe X correspondaient deux substitutions distinctes S_2 et T_2 dans Y_2 et une seule S_1 dans Y_1, à la substitution $S^{-1}T$ correspondrait l'unité dans Y_1 et une autre substitution $S_2^{-1}T_2$ dans Y_2. Ses transformées par les substitutions de X donneraient des substitutions auxquelles correspondraient dans Y_1 l'unité, et dans Y_2 les transformées de $S_2^{-1}T_2$ par les substitutions de Y_2, lesquelles reproduisent tout le groupe Y_2, ce groupe étant simple. Cela posé, l'ordre de X serait évidemment égal à $3.4\ldots p$, ordre de Y_1, multiplié par $3.4\ldots p$, ordre de Y_2, multiplié par l'ordre du groupe formé par celles des substitutions de X auxquelles correspond l'unité dans Y_1 et dans Y_2. Donc X aurait son ordre divisible par p^2, ce qui est impossible.

97. Cela posé, on verra comme précédemment (74 à 84) : 1° que chacun des hypersystèmes de X_1 peut être associé à l'un des hypersystèmes de X_2, etc., de manière à former des hypersystèmes de $\frac{c}{\gamma}$ systèmes, que X permute d'une manière alternée ; 2° que l'on peut faire correspondre les uns aux autres les systèmes de ces hypersystèmes, de telle sorte que X contienne un groupe J qui permute les hypersystèmes d'une manière alternée en remplaçant les uns par les autres les systèmes correspondants ; 3° que la supposition d'après laquelle C, qui contient J, serait primitif sans contenir le groupe alterné, est absurde.

VI

98. Il nous reste à examiner le cas où le groupe I, dérivé de celles des substitutions semblables à A qui ne déplacent que les pq lettres de A, est transitif. Ce cas n'offre aucune difficulté.

Si I est primitif, et si l'on désigne par $pq + \varphi(q)$ le nombre des lettres de G, G sera $\varphi(q)+1$ fois transitif ; ce qui ne sera possible que si l'on a

$$\varphi(q) \leqslant q, \tag{33}$$

ou

$$\varphi(q) < 5 \tag{34}$$

(*Sur la limite de transitivité des groupes non alternés*, même tome, p. 50).

Quant à $\psi(q)$, il sera égal à zéro.

99. Supposons au contraire I non primitif. Répartissons les lettres en systèmes contenant le plus grand nombre possible de lettres ; on aura $\mu \leqslant q$. Car si l'on avait $\mu > q$, une au moins S des substitutions semblables à A dont I est dérivé déplacerait un système s. Elle déplacerait toutes ses lettres, en nombre $> q$; donc elle contiendrait plusieurs de ces lettres dans un même cycle, et par suite ne pourrait pas déplacer s comme on le suppose.

Cela posé, G contenant un groupe I de degré pq et transitif, où les lettres se répartissent μ à μ en systèmes, contiendra un groupe deux fois transitif de degré d au plus égal à $pq+2\nu-1$, ν étant un diviseur de μ (*Théorèmes sur les groupes primitifs ; Journal de Liouville*, 2e série, t. XVI, nos 2 à 8). On aura par suite

$$\Delta = d - pq \leqslant q - 1.$$

D'ailleurs Δ sera au moins égal à 1, I n'étant pas primitif.

Raisonnant maintenant comme plus haut (nos 47 à 55), on trouvera la relation

$$1.2...q \equiv 0 \mod (e+\Delta)(e+\Delta-1)...\Delta,$$

d'où l'on déduira, dans le cas le plus défavorable, où $\Delta = 1$,

$$e \leqslant q.$$

On aura par suite, pour la limite $\varphi(q)$ de la somme $e+\Delta$,

(35) $$\varphi(q) \leqslant 2q - 1.$$

On aura d'ailleurs

(36) $$\psi(q) \leqslant q - 1$$

VII

100. En récapitulant les résultats précédents, on voit que $\varphi(q)$ aura pour limite supérieure la plus grande des quantités suivantes :

(37) $\Delta = \mu\psi\left(\frac{q}{\mu}\right) + 3\mu - 1$ (μ diviseur de q et > 1),

(38) $\Delta + q - 3$, (39) $q + \mathfrak{M}$, (40) $q + \mathfrak{N}$,

$\mathfrak{M}$ étant le maximum de l'expression

$$\varphi(s) + \varphi(t) + \ldots \quad \left(s + t + \ldots = q,\ \frac{q}{2} \geqslant s \geqslant t \geqslant \ldots\right),$$

et $\mathfrak{N}$ le maximum de l'expression

$$\psi(b) + \varphi(s) + \ldots \quad \left(s + t + \ldots = q - b,\ b > \frac{q}{2}\right);$$

(41) 4, (42) $2q - 1$;

et que $\psi(q)$ aura pour limite supérieure la plus grande des quantités

$$\Delta - 1,\ 1 + \mathfrak{M},\ 1 + \mathfrak{N},\ q - 1,$$

pourvu que p soit supérieur à la plus grande $f(q)$ des quantités suivantes :

$$\Delta,\ 1 + \mathfrak{M},\ 1 + \mathfrak{N},\ 3q + 2,\ 18,\ \varphi(s)\ (s = 1, 2, \ldots, q - 1).$$

101. Or il est aisé de voir que, quelles que soient celles des inégalités précédentes dont on se serve pour déterminer $\varphi(q)$ et $\psi(q)$, on aura

$$\psi(q) \leqslant \frac{2}{\log 2} q \log q + q, \quad \varphi(q) \leqslant \frac{2}{\log 2} q \log q + 2q.$$

En effet, ces inégalités sont satisfaites pour $q = 1$; et nous allons montrer qu'elles le seront, pour une valeur quelconque de q, si elles le sont pour les valeurs inférieures.

En effet, on aura

$$(43)\quad \Delta - 1 = \mu\psi\left(\frac{q}{\mu}\right) + 3\mu - 2 \leqslant \mu \frac{2}{\log 2} \frac{q}{\mu} \log \frac{q}{\mu} + \mu \frac{q}{\mu} + 3\mu - 2$$
$$\leqslant \frac{2}{\log 2} q \log q + q - \frac{2q}{\log 2} \log \mu + 3\mu - 2 \leqslant \frac{2}{\log 2} q \log q + q,$$

car les trois termes négligés auront évidemment une somme négative, sauf dans le cas le plus défavorable où l'on aura $\mu = q = 2$, auquel cas la somme s'annulera.

On aura, d'autre part,

$$1 + \mathfrak{M} = 1 + \varphi(s) + \varphi(t) + \ldots \leqslant 1 + \frac{2}{\log 2} (s \log s + t \log t + \ldots) + 2(s + t + \ldots),$$

et comme on a d'une part $s + t + \ldots = q$, et d'autre part $\log s \leqslant \log q - \log 2$, $\log t \leqslant \log q - \log 2$, etc.,

$$(44)\quad 1 + \mathfrak{M} \leqslant 1 + \frac{2}{\log 2} q \log q - \frac{2}{\log 2} q \log 2 + 2q < \frac{2}{\log 2} q \log q + q.$$

En troisième lieu, on a

$$(45)\quad 1 + \mathfrak{N} = 1 + \psi(b) + \varphi(s) + \ldots \leqslant 1 + \frac{2}{\log 2} b \log b + b + \frac{2}{\log 2} s \log s + 2s + \ldots$$
$$\leqslant 1 + \frac{2}{\log 2} b \log q + b + \frac{2}{\log 2} s (\log q - \log 2) + 2s + \ldots$$
$$\leqslant 1 + b + \frac{2}{\log 2} (b + s + \ldots) \log q \leqslant q + \frac{2}{\log 2} q \log q.$$

Enfin il est clair que $q - 1$ est inférieur à cette même limite. On aura donc nécessairement

$$\psi(q) \leqslant \frac{2}{\log 2} q \log q + q.$$

D'ailleurs les limites que les relations (37), (38), (39), (40), (41), (42) donnent pour $\varphi(q)$ seront évidemment inférieures à

$$\frac{2}{\log 2} q \log q + 2q.$$

Enfin $f(q)$, limite inférieure de p, sera évidemment égale à la plus grande des quantités

$$\frac{2}{\log 2} q \log q + q + 1, \quad 3q + 2, \quad 18 \text{ (*)}.$$

On voit d'ailleurs, d'après la manière dont les limites ci-dessus ont été trouvées, qu'elles sont trop élevées. En serrant la question de plus près, on en trouvera de plus rapprochées, pour chaque valeur de q.

Nous allons en donner un exemple.

VIII

102. Proposons-nous d'étudier les groupes primitifs qui contiennent une substitution circulaire d'ordre p à 2 cycles. On aura par suite $q = 2$.

103. Les groupes I, I_1, ... étant définis comme ci-dessus, soit I_r le premier groupe transitif de cette suite.

On peut admettre que G ne contient aucune groupe transitif dérivé de substitutions semblables à A, et déplaçant moins de lettres que I_{r-1}. Supposons en effet que l'on eût un pareil groupe J. Le groupe K dérivé de toutes les substitutions semblables à A qui ne déplaçent que les lettres de J, sera *a fortiori* transitif. Soient B′ celle des substitutions d'ordre p dont il est dérivé qui déplace le moins de lettres parmi celles que A ne déplaçait pas ; C′ celle qui déplace le moins de lettres parmi celles que A et B′ ne déplaçaient pas; etc. ; soient de plus E′ celle des substitutions d'ordre μ contenues dans G qui déplace le nombre minimum de lettres nouvelles, autres que celles de J ; etc. Il est clair que la suite A, B′, C′, ..., E′, ... jouira des propriétés imposées au n° 1 à la suite A, B, C, ...; mais elle permettra d'arriver à la transitivité après adjonction d'un moindre nombre de lettres nouvelles à celles que A déplaçait.

Or, il est clair qu'on peut admettre que, parmi les diverses manières de déterminer la suite A, B, C, ..., on ait choisi dès l'abord celle qui permettait

(*) On peut admettre toujours la limite $\frac{2}{\log 2} q \log q + q + 1$. En effet, si $q > 5$, cette quantité sera supérieure aux deux autres; et si $q < 5$, il résulte de nos recherches que la vraie limite de p est égale à q (Voir la section suivante).

d'arriver le plus tôt à la transitivité. Si l'on s'est imposé cette condition, l'existence de la nouvelle suite A, B', C', ..., E', ... sera impossible.

104. 1° Si I_r n'est pas primitif, ses lettres se grouperont en systèmes μ à μ; et μ, étant > 1 et divisant q, sera égal à 2. Le groupe I_{r-1} n'étant pas transitif, par hypothèse, ses lettres formeront deux classes. Ceux des systèmes de deux lettres que I_{r-1} déplace auront une de leurs lettres dans chaque classe. Considérons en effet l'une de ces classes, et soit $p+\alpha$ le nombre de lettres qu'elle contient. Le groupe partiel formé par les déplacements que I_{r-1} fait subir aux lettres de cette classe, étant dérivé de substitutions circulaires d'ordre p, sera $\alpha+1$ fois transitif. Si donc deux de ces lettres a et b appartenaient à un même système, I_{r-1} contiendrait une substitution S d'ordre p permutant ces deux lettres; et le système qui les contient n'étant pas déplacé par S, les p lettres contenues dans le même cycle de S appartiendraient à ce système, qui contiendrait ainsi plus de deux lettres, contrairement à notre supposition.

Donc les deux classes contiendront le même nombre de lettres; et les substitutions de I_{r-1}, remplaçant les deux lettres de chaque système par celles d'un même système, permuteront de la même manière les lettres correspondantes des deux classes.

105. Si $\alpha = 0$, et si l'on désigne par $p+k$ le nombre des lettres de G, soient comme précédemment Γ le groupe formé par les puissances de A; $\mathfrak{H}$ le groupe formé par celles des substitutions de G qui sont permutables à Γ et qui permutent exclusivement entre elles les k lettres nouvelles; ses substitutions seront de la forme $X_1Y_1, X_2Y_2, \ldots, X_1, X_2, \ldots$ étant des substitutions entre ces k lettres, et $Y_1, Y_2, \ldots$ des substitutions entre les $2p$ lettres de A; ces dernières, étant permutables à Γ, remplaceront les lettres de chaque cycle par celles d'un même cycle. On verra d'ailleurs comme précédemment que la groupe $X_1, X_2, \ldots$ contiendra toutes les substitutions possibles entre les k lettres nouvelles.

Soient $\mathfrak{H}'$ le groupe formé par celles des substitutions de $\mathfrak{H}$ qui ne déplacent pas les cycles de A; $X'Y', X''Y'', \ldots$ ses substitutions. Il est clair que leurs premiers facteurs $X', X'', \ldots$ formeront un groupe contenu dans $(X_1, X_2, \ldots)$ et renfermant au moins la moitié de ses substitutions. Donc le groupe $(X', X'', \ldots)$ contiendra le groupe alterné. On aura d'ailleurs $Y' = V^{\varepsilon'}W', Y'' = V^{\varepsilon''}W'', \ldots$, V, W', W'', ... étant des substitutions de même forme qu'à l'endroit cité.

Cela posé, si $k > 3$, le groupe alterné $(X', X'', \ldots)$ contiendra au moins deux substitutions non échangeables entre elles. En combinant entre elles les substitutions correspondantes de $\mathfrak{H}'$, on obtiendra une substitution qui se réduit à la forme XW.

Soient $x'w', x''w'', \ldots$ les substitutions de cette forme que contient $\mathfrak{H}$; le groupe $(x', x'', \ldots)$ sera évidemment permutable à $(X_1, X_2, \ldots)$; donc il con-

tiendra des substitutions binaires à 2 cycles (il en contient si $k=4$; et si $k>4$, il contient le groupe alterné).

Supposons donc que x' soit une substitution binaire à 2 cycles; w' étant d'ordre p, G contiendra $(x'w')^p$, substitution binaire à 2 cycles. Mais son degré $2p+k>9$; donc G contiendra le groupe alterné.

Si $k\leqslant 3$, l'ordre de G sera $0(2p+2)\ldots(2p+k)$, 0 étant l'ordre du groupe formé par celles de ses substitutions qui ne déplacent que $2p$ lettres.

106. Il resterait à discuter l'hypothèse $\alpha>0$. Mais ce cas doit être exclu. En effet, I_r étant transitif, parmi les substitutions S, T, ... d'ordre p dont il est dérivé, il en est une S qui mêlera dans ses cycles les lettres des deux classes. Car s'il en pouvait être autrement, soient x, y les deux lettres nouvelles contenues dans I_r et que I_{r-1} ne déplaçait pas. Pour que I_r fût transitif, il faudrait qu'une des substitutions S, T, ... contînt dans un de ses cycles x et des lettres de la première classe, et dans l'autre y et des lettres de la seconde classe; tandis qu'une autre de ces substitutions, U, permuterait x avec des lettres de seconde classe, et y avec des lettres de première classe. Mais il est clair que $T^{-1}UT=S$ mêlerait dans ses cycles les lettres des deux classes. Donc la substitution S existe nécessairement. Elle laisse immobiles $\alpha+1$ systèmes de lettres. Soient s l'un d'eux, t celui de ces systèmes que I_{r-1} déplace, mais que I_{r-2} ne déplaçait pas : I_{r-1} contient une substitution T qui remplace le système s par le système t, sans mêler ensemble les lettres des deux classes; $T^{-1}ST$ laissera immobiles les lettres de t, tout en mêlant encore les lettres de deux classes. En l'adjoignant à I_{r-2}, on obtiendra un groupe J ne déplaçant que $2p+2\alpha$ lettres, mais transitif; résultat inadmissible (103).

107. 2° Si I_r est primitif, les lettres de I_{r-1} formeront deux classes, contenant respectivement $p+\alpha$ et $p+\beta$ lettres.

Si $\alpha>2$, les déplacements que I_{r-1} font subir aux lettres de la première classe formeront un groupe alterné (*Sur la limite de transitivité des groupes non alternés*, théorème I); et, d'après l'analyse précédente, G contiendra le groupe alterné, à moins qu'on n'ait $\alpha=\beta$, et que les substitutions de I_{r-1} ne permutent de la même manière les lettres correspondantes des deux classes.

Soient respectivement $a_1\ldots a_p x_1\ldots x_\alpha$, $b_1\ldots b_p y_1\ldots y_\alpha$ ces lettres; $x_\alpha y_\alpha$ le dernier couple de lettres introduit dans le passage de I_{r-2} à I_{r-1}.

Soit z la nouvelle lettre introduite dans le passage au groupe suivant I_r. Ce groupe, étant transitif, contiendra une substitution S qui mêle dans ses cycles les lettres des deux classes. Parmi les $2\alpha+1$ lettres qu'elle laisse immobiles, on peut admettre que se trouve l'une des deux lettres x_α, y_α, par exemple y_α. Car si elle laissait immobile b_ρ, il suffirait de considérer au lieu de S sa transformée par une substitution de I_{r-1} qui remplace b_ρ par y_α.

Cela posé, si S mêlait dans ses cycles les lettres $a_1\ldots a_p x_1\ldots x_{\alpha-1}$ aux

lettres $b_1 \ldots b_p y_1 \ldots y_{\alpha-1}$, il est clair qu'en l'adjoignant à I_{r-1} on aurait un groupe transitif, de degré moindre que I_r, résultat inadmissible. Donc S devra déplacer x_α et celui de ses cycles qui contient cette lettre ne pourra renfermer que des lettres de la suite $b_1 \ldots b_p y_1 \ldots y_{\alpha-1} z$.

Mais si z faisait partie de ce cycle, et y suivait x_α à m rangs de distance, par exemple, le groupe transformé de I_{r-1} par S^m, ne déplaçant plus z, serait contenu dans I_r; et ces substitutions déplaceraient x_α sans déplacer sa correspondante y_α, ce qui est inadmissible.

Il faut donc admettre que le premier cycle de S ne contient avec x_α que des lettres de la suite $b_1 \ldots b_p y_1 \ldots y_{\alpha-1}$. Le second devra contenir z avec des lettres de cette même suite, ou des lettres de l'autre suite $a_1 \ldots x_{\alpha-1}$.

Mais si ce cycle contenait z avec des lettres $b_1 \ldots y_{\alpha-1}$, le groupe dérivé de S et de I_{r-1} permuterait d'une manière alternée les $p+\alpha+1$ lettres $b_1 \ldots y_{\alpha-1} z x$ d'une part, les $p+\alpha-1$ lettres $a_1 \ldots x_{\alpha-1}$ d'autre part. Ce groupe, réduit à celles de ses substitutions qui ne déplacent pas ces dernières lettres, permuterait encore les autres d'une manière alternée, et G qui le contient serait alterné.

Donc le second cycle de S ne contiendra aucune des lettres $b_1 \ldots y_{\alpha-1}$; et S laissera immobiles α de ces lettres. Soit s l'une de ces lettres immobiles; I_{r-1}, étant $\alpha+1$ fois transitif, contiendra une substitution T d'ordre p qui remplace s par y_α; et $T^{-1}ST$, qui ne déplace pas y_α, contiendra dans son premier cycle la lettre que T fait succéder à x_α, laquelle est de la suite $a_1 \ldots x_{\alpha-1}$, et celles que T fait succéder aux autres lettres du cycle, lesquelles sont de la suite $b_1 \ldots y_{\alpha-1}$: on retombe ainsi sur un cas où l'impossibilité est démontrée.

108. Il faut donc supposer $\alpha \leqslant 2$, $\beta \leqslant 2$. D'ailleurs I_{r-1} ne doit contenir qu'une lettre de plus que I_{r-2}, sans quoi, les lettres de I_{r-1} se groupant deux à deux en systèmes, on pourrait appliquer le raisonnement qui précède.

109. Supposons d'abord $\alpha > 0$, $\beta > 0$; et soient $a_1 \ldots a_p x_1 \ldots x_\alpha$, $b_1 \ldots b_p y_1 \ldots y_\beta$ les lettres des deux classes; x_α la dernière lettre introduite. Le groupe I_r contiendra une substitution S semblable à A et mêlant dans ses cycles les lettres des deux classes. Comme elle ne déplace que $2p$ lettres, elle laissera immobiles $\alpha+\beta+1$ lettres de ces classes.

Si elle laisse immobile une lettre de la première classe, on peut admettre que c'est x_α; mais alors il est clair qu'en adjoignant S à I_{r-2} on obtiendrait un groupe transitif contenu dans G, dérivé de substitutions d'ordre p et déplaçant moins de lettres que I_r, ce qui ne peut être, par hypothèse.

Si au contraire les $\alpha+\beta+1$ lettres que S laisse immobiles appartiennent toutes à la seconde classe, on pourra admettre que dans le nombre se trouvent les β lettres $y_1, \ldots, y_\beta$ que A ne déplaçait pas; et celles des lettres $b_1 \ldots b_p$ que S déplace, en nombre $p-\alpha-1$ (on suppose $p > 3$ et $\alpha \leqslant 2$), ne pourront former un cycle à elles seules. Si l'une de ces lettres figure

dans le même cycle de S que l'une des lettres $a_1 \dots a_p$, ce cycle ne contiendra qu'une partie des lettres $a_1 \dots a_p$, et les autres seront contenues dans l'autre cycle. Dès lors il est clair que le groupe dérivé de A et de S, qui déplace moins de lettres que I_r, serait transitif, résultat inadmissible.

Supposons au contraire que S eût un de ses cycles formé des lettres $a_1 \dots a_p$ et l'autre des lettres $zx_1 \dots x_\alpha$ jointes à des lettres b. Le groupe I_{r-1} contient une substitution T d'ordre p qui déplace x_α; son premier cycle sera formé de lettres de la première classe, parmi lesquelles $p - \alpha$ au moins seront des a; son second cycle contiendra p lettres de seconde classe; les autres resteront immobiles, et l'on peut admettre que y_β est de ces dernières. Mais alors le groupe dérivé de S et de T sera transitif, quoique déplaçant moins de lettres que I_r, ce qui est inadmissible.

110. Il faut donc admettre que $\beta = 0$; mais alors le raisonnement des n^{os} 63-64 montre que α doit être nul aussi pour que I_r soit primitif.

111. On aura donc $\alpha = \beta = 0$; et l'on en conclut, comme au n° 105, que si $2p + k$ est le nombre des lettres de G, on aura $k \leqslant 3$. De plus, l'ordre de G sera $0(2p+1)\dots(2p+k)$.

On aura donc dans tous les cas $k < 3$.

Notre démonstration suppose que p est supérieur à 3. Mais on s'assure aisément, en traitant directement le cas où $p = 3$, qu'on obtiendra pour k la même limite 3.

112. En raisonnant d'une manière analogue sur les cas où l'on a $q = 3$, 4 ou 5, nous avons obtenu des résultats tout semblables, qui peuvent se formuler dans le théorème suivant.

Théorème. — *Soit q un nombre inférieur à 6; p un nombre premier quelconque supérieur à q; l'ordre d'un groupe primitif* G *qui contient une substitution d'ordre p à q cycles (sans contenir le groupe alterné) ne peut dépasser* $pq + q + 1$.