BULLETIN DE LA S. M. F.

CAMILLE JORDAN

Sur la limite de transitivité des groupes non alternés

Bulletin de la S. M. F., tome 1 (1872-1873), p. 40-71

<http://www.numdam.org/item?id=BSMF_1872-1873__1__40_1>

Sur la limite de transitivité des groupes non alternés; par M. CAMILLE JORDAN.

(Séance du 8 janvier 1873)

Vers l'année 1845, époque où les travaux de M. Bertrand ramenèrent l'attention de Cauchy sur la théorie des substitutions, ce grand géomètre entreprit sur ce sujet une longue suite de recherches, dont il a consigné les résultats dans les *Comptes rendus*.

Le principal théorème qu'il ait obtenu est le suivant :

Tout groupe dont l'ordre est divisible par un nombre premier p contient une substitution d'ordre p.

L'importance de cette proposition est manifeste, et l'on peut s'étonner qu'elle n'ait donné lieu, jusqu'à ce jour, pour ainsi dire à aucune application. Mais le théorème de Cauchy vient enfin d'être complété et généralisé, de la manière la plus heureuse, par un géomètre norwégien, M. Sylow. Il vient en effet de formuler le théorème suivant (*Mathematische Annalen*, t. V) :

Soit G *un groupe dont l'ordre* O *soit divisible par* p^α, *sans l'être par* $p^{\alpha+1}$; *il contiendra des groupes d'ordre* p^α. *Ces groupes* H, H',... *seront tous semblables, et seront les transformés de l'un quelconque d'entre eux*, H, *par les substitutions de* G. *Enfin, leur nombre sera un entier de la forme* $np+1$. *Enfin l'on aura* $O = p^\alpha\nu(np+1)$, $p^\alpha\nu$ *étant l'ordre du groupe* I *formé par celles des substitutions de* G *qui sont permutables à* H.

Cette proposition mérite assurément par sa simplicité, sa netteté et sa généralité, d'être considérée comme fondamentale ; et nous ne doutons pas qu'elle ne donne lieu à d'importantes conséquences.

Nous en faisons, dans le mémoire ci-joint, une première application à la recherche de la limite de transitivité des groupes de substitutions.

On sait que M. Émile Mathieu a montré le premier qu'il existe une sorte de fossé entre le groupe alterné et les autres groupes de substitutions, ceux-ci ne pouvant être plus de $\frac{n}{2}$ fois transitifs (n étant le nombre des lettres), tandis que le groupe alterné l'est $n-1$ fois. Mais cette limite $\frac{n}{2}$, assignée à la transitivité des groupes qui ne contiennent pas le groupe alterné, est beaucoup trop élevée. Il est donc intéressant de la resserrer le plus possible; et si même on parvenait à démontrer que la véritable limite est une constante indépendante de n, on aurait atteint un résultat des plus importants.

Malheureusement cette question paraît d'une extrême difficulté; et nous avons dû recourir à des considérations très-compliquées pour arriver à réduire notablement la limite de M. Mathieu (*Traité des Substitutions*, nos 99 à 113).

Or, le théorème de M. Sylow permet d'établir avec une grande facilité les deux théorèmes suivants :

Théorème I. — *Soit p un nombre premier impair. Un groupe de degré $p+k$ ne pourra être plus de k fois transitif, si $k>2$, à moins de contenir le groupe alterné.*

Théorème II. — *Un groupe de degré $2p+k$ (p étant premier et >3) ne pourra être plus de k fois transitif, à moins de contenir le groupe alterné : 1° Si $k>2$, lorsque p est de la forme $3n-1$; 2° si $k>3$, lorsque p est de la forme $3n+1$.*

Le théorème suivant, beaucoup plus difficile à démontrer, et d'une utilité moins fréquente, mérite néanmoins d'être signalé à cause de sa généralité :

Théorème III. — *Soient p un nombre premier impair, q un entier premier à p et contenu entre p^m et p^{m+1}. Un groupe de degré $p^n q+k$ ne pourra être plus de k fois transitif, si l'un des trois systèmes de conditions ci dessous n'est pas satisfait : 1° $k<5$; 2° $k\leqslant q$; 3° $m+n\geqslant k-\frac{\log k}{\log 2}-3$.*

On remarquera que ce système de conditions est entièrement indépendant de p.

Cette troisième condition peut être remplacée par la suivante, qui donnera parfois une limite plus resserrée, $k<r+3$, r étant le plus petit nombre premier supérieur à $m+n+1$.

On voit immédiatement comment ces théorèmes peuvent être appliqués. Cherchons, par exemple, combien de fois un groupe de degré 100 peut être

transitif. Le plus grand nombre premier inférieur à $100-2$ est 97. Utilisant le théorème I, pour $p=97$, on voit que le groupe de degré $p+3=100$ ne peut être plus de 3 fois transitif.

Le plus grand nombre premier p, tel que $2p<100-3$ est 47. Appliquant à ce nombre le théorème II, on verrait que le groupe de degré $100=2p+6$ ne peut être plus de 6 fois transitif. On voit que, dans ce cas particulier, c'est le théorème I qui mérite la préférence; mais il n'en sera pas toujours ainsi.

Les nouvelles limites de transitivité que nous venons d'indiquer sont très-préférables à celles que nous avons données dans notre *Traité*. Non-seulement elles sont plus resserrées(*) (ce qu'il serait peut-être difficile de démontrer, vu le peu de notions que l'on a sur la loi de succession des nombres premiers), mais en outre ces nouvelles limites, au lieu d'être, comme les précédentes, des fonctions croissant régulièrement avec n, dépendent de la nature arithmétique de ce nombre, plutôt que de sa grandeur absolue. Il est donc vraisemblable qu'elles sont plus conformes à la réalité.

I

1. Théorème I. — *Soit p un nombre premier impair. Un groupe de degré $p+k$ ne pourra être plus de k fois transitif, si $k>2$ à moins de contenir le groupe alterné.*

Soit $\mathcal{G}$ un groupe de degré $p+k$ et plus de k fois transitif. Le groupe G formé par celles de ses substitutions qui ne déplacent que p lettres données $a_1,\ldots, a_p$ sera transitif, et contiendra une substitution circulaire d'ordre p. Les puissances de cette substitution S formeront un groupe H d'ordre p. Soient I le groupe formé par celles des substitutions de G qui sont permutables à H, $\Omega=p\nu$ son ordre : I étant contenu dans le groupe K, d'ordre $p(p-1)$, formé par toutes les substitutions entre les lettres $a_1,\ldots, a_p$ qui sont permutables à H, ν divisera $p-1$; enfin l'ordre O de G sera égal à $\Omega(np+1)$, d'après le théorème de M. Sylow ; on aura donc

$$\Omega\equiv 0 \bmod p^2.$$

Soient maintenant x, y deux autres lettres quelconques parmi celles qui figurent dans le groupe $\mathcal{G}$; G_2 le groupe au moins trois fois transitif formé par celles des substitutions de $\mathcal{G}$ qui ne déplacent que les lettres $a_1,\ldots, a_p, x, y$; $O_2=O(p+1)(p+2)$ son ordre ; I_2 le groupe formé par

(*) D'après ces anciennes formules, un groupe de degré 100 pourrait être 16 fois transitif.

celles des substitutions de G_2 qui sont permutables à H; Ω_2 son ordre : on aura, toujours d'après le théorème de M. Sylow,

$$\Omega_2 \equiv 0_2 \equiv 20 \equiv 2\Omega \bmod p^2. \tag{1}$$

Or Ω_2 est un multiple de Ω, car I_2 contient I. Soit donc $\Omega_2 = r\Omega$; Ω étant divisible par p, mais non par p^2, la relation (1) donnera

$$r \equiv 2 \bmod p. \tag{2}$$

D'ailleurs, les substitutions de Ω_2, étant permutables à H, permuteront exclusivement entre elles les deux lettres x, y que H ne déplace pas. Elles seront donc toutes de la forme A_φ ou de la forme $A_\varphi(xy)$, $A_1, \ldots, A_\varphi, \ldots$ désignant les diverses substitutions du groupe K, et (xy) une transposition opérée sur les lettres x, y. Si toutes les substitutions de I_2 étaient de la forme A_φ, elles appartiendraient à I ; on aurait donc $\Omega_2 = \Omega$, d'où $r = 1$, résultat incompatible avec la relation (2). Donc I_2 contiendra au moins une substitution de la forme $A_\varphi(xy)$, et l'on aura $r = 2$.

Soit maintenant $\mathfrak{I}$ le groupe formé par celles des substitutions de $\mathcal{G}$ qui sont permutables à H, tout en permutant exclusivement entre elles les lettres $a_1, \ldots, a_p$; ce groupe contiendra évidemment I_2; donc il contiendra la substitution $A_\varphi(xy)$. On voit de même qu'il contiendra une substitution $A_{\varphi'}(xz)$, z étant une nouvelle lettre quelconque, autre que $a_1, \ldots, a_p, x, y$.

Cela posé, K résulte de la combinaison du groupe H, formé des puissances de S, avec les puissances d'une certaine substitution circulaire B, d'ordre $p-1$, qui lui est permutable. Donc A_φ sera de la forme $S^\alpha B^\beta$, et de même $A_{\varphi'}$ sera de la forme $S^{\alpha'} B^{\beta'}$. Le groupe $\mathfrak{I}$, contenant évidemment la substitution S, et contenant d'autre part $A_\varphi(xy) = S^\alpha B^\beta(xy)$, contiendra $B^\beta(xy)$; de même il contiendra $B^{\beta'}(xz)$; il contiendra donc la substitution

$$[B^\beta(xy)]^{-1}[B^{\beta'}(xz)]^{-1} B^\beta(xy)\, B^{\beta'}(xz) = (xy)^{-1}(xz)^{-1}(xy)(xz) = (xzy),$$

laquelle est circulaire ternaire. Le groupe $\mathcal{G}$ contiendra *a fortiori* cette substitution, et comme il est plus de trois fois transitif, il contiendra le groupe alterné.

2. Théorème II. — *Soit p un nombre premier impair > 3. Un groupe $\mathcal{G}$ de degré $2p + k$ ne pourra être plus de k fois transitif, à moins de contenir le groupe alterné : 1° Si $k > 2$, lorsque p est de la forme $3n - 1$; 2° si $k > 3$, lorsque $p = 3n + 1$.*

En effet, le groupe G, formé de celles des substitutions de $\mathcal{G}$ qui ne déplacent que $2p$ lettres données $a_1, \ldots, a_p, b_1, \ldots, b_p$, sera transitif, par hypothèse. Donc son ordre sera divisible par p; s'il l'était par p^2, le groupe Γ d'ordre $2p$ fois moindre, formé par celles des substitutions de G qui ne dé-

placent que les $2p-1$ lettres $a_2,\ldots,b_p$, aurait son ordre divisible par p; il contiendrait donc une substitution d'ordre p qui ne pourrait être que circulaire; et G, contenant cette substitution, serait $p+1$ fois transitif (Note C de notre *Traité des Substitutions*); donc G contiendrait le groupe alterné et, par suite, contiendrait une substitution circulaire de trois lettres; le groupe $\mathcal{G}$ contenant *a fortiori* cette substitution, étant d'ailleurs plus de trois fois transitif, contiendrait le groupe alterné.

Supposons au contraire que l'ordre de G ne soit divisible qu'une fois par p; il contiendra une substitution d'ordre p à deux cycles

$$S=(a_1\ldots a_p)(b_1\ldots b_p),$$

ses puissances formeront un groupe H d'ordre p. Soient, comme tout à l'heure, I le groupe formé par celles des substitutions de G qui sont permutables à H; K le groupe formé par toutes les substitutions possibles permutables à H, et ne déplaçant que les lettres $a_1,\ldots,b_p$. Soient de plus x, y deux lettres nouvelles quelconques, prises parmi celles de $\mathcal{G}$. On voit, comme au théorème I, que le groupe $\mathfrak{J}$, formé par celles des substitutions de $\mathcal{G}$ qui sont permutables à H, tout en permutant exclusivement entre elles les lettres $a_1,\ldots b_p$, contient une substitution de la forme $A_\varrho(xy)$, A_ϱ étant une substitution de K. On voit de même que $\mathfrak{J}$ contiendra des substitutions $A_{\varrho'}(xz)$, ..., $z,\ldots$ étant les autres lettres qui figurent dans $\mathcal{G}$.

En combinant ensemble ces substitutions, on obtiendra des substitutions contenues dans $\mathfrak{J}$, et permutant de toutes les manières possibles les lettres $x, y, z, u, \ldots$.

Les substitutions de $\mathfrak{J}$ étant donc représentées par $A_1\Theta_1$, $A_2\Theta_2,\ldots$, où $A_1, A_2,\ldots$, sont des substitutions de K, et Θ_1, $\Theta_2,\ldots$ des substitutions qui permutent ensemble les lettres $x, y, z,\ldots$, ces dernières substitutions formeront un groupe Θ contenant toutes les substitutions possibles entre $x, y, z,\ldots$.

3. Cela posé, les substitutions de K, étant permutables à H, remplaceront les lettres d'un même cycle de S par celles d'un même cycle; elles seront donc de la forme D ou de la forme CD, C étant la substitution qui remplace respectivement $a_1,\ldots,a_p$ par $b_1,\ldots,b_p$ et réciproquement, et D une nouvelle substitution permutable à H, mais ne déplaçant plus les deux cycles de S. La substitution D transformera d'ailleurs S en une de ses puissances que l'on pourra désigner par S^{g^s}, g étant une racine primitive de p. Or il existe une substitution B d'ordre $p-1$, à deux cycles, qui transforme S en S^g; on aura donc $D=B^sD'$, D' étant une nouvelle substitution, de même forme que D, mais échangeable à S. Il est clair que D' devra être de la forme $S_1^{\alpha_1}S_2^{\alpha_2}$, S_1 et S_2 désignant les deux substitutions circulaires partielles $(a_1\ldots a_p)$ et $(b_1\ldots b_p)$.

Donc les substitutions de K seront de la forme $C^{\gamma}B^{\beta}S_1^{\alpha_1}S_2^{\alpha_2}$, les indices γ, β, α_1, α_2 variant respectivement de 0 à 1, de 0 à $p-2$, et les deux derniers de 0 à $p-1$. L'ordre de K sera par suite égal à $2(p-1)p^2$.

4. Soit maintenant $p=3n-1$. L'ordre de K sera premier à 3, et, par suite, l'ordre de chacune de ses substitutions sera premier à 3. Mais on a vu que $\mathfrak{J}$ contient une substitution T de la forme $A(xyz)$, A étant une substitution de K. Soit ω l'ordre de A; $\mathfrak{J}$ contiendra la substitution $T^{\omega}=(xyz)^{\omega}$, laquelle ne se réduit pas à l'unité, ω étant premier à 3.

Donc $\mathfrak{J}$, et *a fortiori* $\mathfrak{G}$, contient une substitution circulaire ternaire; et comme $\mathfrak{G}$ est plus de trois fois transitif, il contiendra le groupe alterné.

5. Soit au contraire $p=3n+1$. Le groupe $\mathfrak{J}'$, formé par celles des substitutions $A'_1\Theta'_1$, $A'_2\Theta'_2$,... du groupe $\mathfrak{J}$ dont les premiers facteurs sont de la forme D, contiendra évidemment la moitié ou la totalité des substitutions de $\mathfrak{J}$. *A fortiori*, le groupe Θ' formé par les substitutions partielles Θ'_1, Θ'_2,... contiendra au moins la moitié des $1.2...k$ substitutions de Θ. Donc il contiendra le groupe alterné, et en particulier les deux substitutions circulaires ternaires xyz, xyu. Donc $\mathfrak{J}'$ contiendra deux substitutions telles que

$$A'_1(xyz),\quad A'_2(xyu),$$

et par suite la substitution

$$[A'_1(xyz)]^{-1}[A'_2(xyu)]^{-1}[A'_1(xyz)][A'_2(xyu)]=\mathfrak{H}(xuy),$$

en posant

$$\mathfrak{H}=A'^{-1}_1A'^{-1}_2A'_1A'_2.$$

Or A'_1, A'_2 sont de la forme $B^{\beta}S_1^{\alpha_1}S_1^{\alpha_2}$; S_1 et S_2 étant échangeables entre elles, et B les transformant respectivement en S_1^{q}, S_2^{q}, $\mathfrak{H}$ se réduira à la forme $S_1^{\alpha_1}S_2^{\alpha_2}$ et sera d'ordre p. Cela posé, $\mathfrak{J}'$ contiendra la substitution circulaire ternaire

$$[\mathfrak{H}(xuy)]^p=(xuy)^p,$$

et $\mathfrak{G}$, qui la contient *a fortiori* et qui est plus de trois fois transitif, contiendra le groupe alterné.

II

6. Nous allons déduire des mêmes principes un nouveau théorème, plus étendu que les précédents. Mais auparavant il sera bon de reprendre la démonstration d'une proposition auxiliaire que nous avons établie ailleurs dans ce qu'elle a de plus essentiel (*Traité des substitutions*, 394), mais par des voies indirectes et sous un énoncé qui ne serait pas commode dans la question actuelle. Les développements dans lesquels nous allons entrer, et

les définitions qui leur servent de base, nous semblent d'ailleurs de nature à simplifier notablement la démonstration de plusieurs propositions importantes.

7. *Définitions.* — Deux substitutions s et t, permutables à un groupe H, sont dites *congrues suivant le groupe* H, si l'on a une égalité de la forme

$$s = th,$$

h étant une substitution de H.

On peut exprimer cette relation par une formule analogue à celle des congruences ordinaires

$$s \equiv t \bmod H.$$

On peut multiplier deux congruences membre à membre. Soit en effet

$$\begin{aligned} s &\equiv t \bmod H = th, \\ s' &\equiv t' \bmod H = t'h', \end{aligned}$$

on aura

$$ss' = thth' = tt't'^{-1}ht'h',$$

et comme $t'^{-1}ht'$ appartient à H, par hypothèse,

$$ss' \equiv tt' \bmod H.$$

On dira qu'une suite de substitutions $s_1, s_2, \ldots$ (toutes permutables à un même groupe H) forme un *groupe suivant le module* H, si l'on a pour toutes valeurs de α et de β une relation de la forme

$$s_\alpha s_\beta \equiv s_\gamma \bmod H.$$

L'*ordre* de ce groupe sera le nombre des substitutions diverses, incongrues suivant le module H, qu'il contient.

Soit G le groupe dérivé des substitutions $s_1, s_2, \ldots$, lorsqu'on les combine entre elles à la manière ordinaire. Nous désignerons par $\frac{G}{H}$ le groupe formé par ces mêmes substitutions suivant le module H. Il est aisé de voir que l'ordre de G est égal au produit de l'ordre O de $\frac{G}{H}$ par l'ordre Ω du groupe I formé des substitutions communes à G et à H.

En effet, soit s une quelconque des O substitutions de $\frac{G}{H}$, et soient $1, t, t', \ldots$ les substitutions de I; G contiendra Ω substitutions $s, st, st', \ldots$ congrues à s mod H, mais il n'en contiendra pas davantage; car s'il en contenait une su, il contiendrait u, laquelle étant congrue à 1 mod H serait

aussi contenue dans H, quoique n'appartenant pas à I, ce qui est contraire à la définition de ce groupe.

On peut transporter aux substitutions et aux groupes pris suivant le module H toutes les définitions principales relatives aux groupes ordinaires. Ainsi deux substitutions S, T seront *échangeables* si l'on a $ST \equiv TS$. Une substitution T sera *permutable à un groupe* $(S_1, S_2, \ldots)$ si l'on a pour toute valeur de α une relation de la forme

$$T^{-1} S_\alpha T \equiv S_\beta.$$

Cette relation s'exprimera en langage ordinaire en disant que S_β est la *transformée* de S_α par T (suivant le module H).

Un groupe $\frac{G}{H}$ sera *isomorphe* à un autre groupe $\frac{G'}{H'}$, si l'on peut faire correspondre aux diverses substitutions de $\frac{G}{H}$ (incongrues suivant le module H) les diverses substitutions de $\frac{G'}{H'}$ (incongrues suivant le module H'), de telle sorte qu'à chaque substitution de $\frac{G'}{H'}$ corresponde une seule substitution de $\frac{G}{H}$, et qu'au produit de deux substitutions corresponde le produit de leurs correspondantes. L'isomorphisme sera dit mériédrique si, à une même substitution de $\frac{G}{H}$, correspondent plusieurs substitutions de $\frac{G'}{H'}$.

8. Soit maintenant G un groupe d'ordre O, ayant pour facteurs de composition $\nu_1, \nu_2, \ldots$; il existera par définition une suite de groupes $G, G_1, G_2, \ldots$, ayant respectivement pour ordres $O, \frac{O}{\nu_1}, \frac{O}{\nu_1\nu_2}, \ldots$, tels que chacun d'eux soit contenu dans le précédent et permutable à ses substitutions, mais ne soit contenu dans aucun groupe plus général jouissant de cette double propriété.

Soient $1, g_1, g'_1, \ldots$ les $\frac{O}{\nu_1}$ substitutions de G_1; on sait que les O substitutions de G seront données par le tableau

$$\begin{array}{cccc} 1 & g_1 & g'_1 & \cdots \\ g & gg_1 & gg'_1 & \cdots \\ g' & g'g_1 & g'g'_1 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{array},$$

$g, g', \ldots$ étant des substitutions en nombre ν_1, toutes incongrues suivant le module G_1. Donc le groupe $\frac{G}{G_1}$ contiendra ν_1 substitutions distinctes $1, g,$

g', ... mod G_1, correspondant respectivement à celles de G qui forment les diverses lignes du tableau ci-dessus. De même $\frac{G_1}{G_2}$ aura pour ordre ν_2, etc.

Nous dirons que *les groupes* $\frac{G}{G_1}, \frac{G_1}{G_2}, \ldots$ *sont les groupes composants de* G, *respectivement afférents aux facteurs de composition* $\nu_1, \nu_2, \ldots$; et nous dirons encore que *les groupes* $G_1, G_2, \ldots$ *se déduisent de* G *par la suppression successive des groupes composants* $\frac{G}{G_1}, \frac{G_1}{G_2}, \ldots$.

9. Ces définitions posées, soit G un groupe non transitif, groupons ses lettres en classes en réunissant ensemble celles que G permute entre elles. Les substitutions de G seront de la forme :

$$s_1 = a_1 b_1 c_1 \ldots, \quad s_2 = a_2 b_2 c_2 \ldots, \quad \ldots,$$

$a_1, a_2, \ldots$ étant des substitutions opérées entre les lettres de la première classe, $b_1, b_2, \ldots$ des substitutions opérées entre celles de la seconde classe, etc. Soient respectivement A, B, ... les groupes formés par les substitutions partielles $a_1, a_2, \ldots$; $b_1, b_2, \ldots$; .... Soient enfin ν_1 le premier facteur de composition de A; $\frac{A}{A_1}$ le groupe afférent à ce facteur; G_1 le groupe formé par celles des substitutions de G

$$a_\lambda b_\lambda c_\lambda, \ldots,$$

dont les premiers facteurs $a_\lambda, \ldots$ appartiennent à A_1; B_1 le groupe formé par les seconds facteurs $b_\lambda, \ldots$; etc. Le groupe B_1 sera évidemment permutable aux substitutions de B, et, s'il n'en contient qu'une partie, les deux groupes $\frac{A}{A_1}$ et $\frac{B}{B_1}$ seront isomorphes sans mériédrie.

En effet, aux diverses substitutions $s_1, s_2, \ldots$ de G correspondent des substitutions $\alpha_1, \alpha_2, \ldots, \beta_1, \beta_2, \ldots$ dans chacun des groupes $\frac{A}{A_1}$ et $\frac{B}{B_1}$, ce qui établit une correspondance entre les substitutions de ces deux groupes. Il reste à prouver que cette correspondance est telle que chaque substitution de $\frac{A}{A_1}$ correspond à une seule substitution de $\frac{B}{B_1}$, et réciproquement.

Supposons d'abord que l'on pût avoir $\alpha_1 \equiv \alpha_2 \bmod A_1$, sans avoir en même temps $\beta_1 \equiv \beta_2 \bmod B_1$. La substitution $t \equiv s_1 s_2^{-1} = a_\varrho b_\varrho \ldots$ aurait pour correspondante dans $\frac{A}{A_1}$ la substitution $\alpha_1 \alpha_2^{-1} \equiv 1$; donc a_ϱ appar-

tiendrait à A_1 ; mais t aurait pour correspondante dans $\frac{B}{B_1}$ la substitution $\beta_1\beta_2^{-1}$, laquelle diffère de 1 mod B_1 ; donc b_ρ n'appartiendrait pas à B_1, ce qui est contraire à la définition de ce groupe.

Supposons au contraire que l'on eût $\beta_1 \equiv \beta_2 \bmod B_1$ et $\alpha_1 \gtrless \alpha_2 \bmod A_1$; t aurait pour correspondante l'unité dans $\frac{B}{B_1}$, et une substitution α_ρ autre que l'unité dans $\frac{A}{A_1}$. Cela posé, G contient le groupe dérivé des transformées $s_1^{-1}ts_1$, $s_2^{-1}ts_2$, ... de t par les substitutions de G. A ces transformées et à leurs dérivées correspondraient dans $\frac{B}{B_1}$ la substitution 1, et dans $\frac{A}{A_1}$ les substitutions $\alpha_1^{-1}\alpha_\rho\alpha_1$, $\alpha_2^{-1}\alpha_\rho\alpha_2$, ... et leurs dérivées. Ces dernières substitutions reproduisent tout le groupe $\frac{A}{A_1}$. Supposons en effet qu'elles formassent un groupe moindre $\frac{\mathfrak{A}}{A_1}$ d'ordre $\nu' < \nu_1$. Ce groupe serait évidemment permutable aux substitutions α_1, α_2, ... Le groupe $\mathfrak{A}$, formé par celles des substitutions de A dont les correspondantes appartiennent à $\frac{\mathfrak{A}}{A_1}$ serait évidemment contenu dans A et permutable à ses substitutions. D'ailleurs, il serait plus général que A_1, groupe formé par les substitutions de A qui ont pour correspondante l'unité. Ce résultat est contraire aux propriétés caractéristiques par lesquelles nous avons défini A_1.

Soit donc α_σ une substitution quelconque de $\frac{A}{A_1}$; G contiendra une substitution u_σ ayant respectivement pour correspondantes dans $\frac{A}{A_1}$ et dans $\frac{B}{B_1}$ les substitutions α_σ et 1. Mais, d'autre part, B_1 ne contenant par hypothèse qu'une portion des substitutions de B, G contiendra une substitution v ayant pour correspondante dans $\frac{B}{B_1}$ une substitution β_σ différente de l'unité ; soit α_σ sa correspondante dans $\frac{A}{A_1}$; G contiendra $vu_\sigma^{-1} = a_\tau b_\tau \ldots$, à laquelle correspondent, dans $\frac{A}{A_1}$ l'unité, dans $\frac{B}{B_1}$, β_σ, qui diffère de l'unité ; résultat absurde, car il faudrait pour cela que a_τ appartînt à A_1, sans que b_τ appartînt à B_1, ce qui est contraire à la définition de ce dernier groupe.

Le groupe B_1 étant encore supposé $< B$, le groupe $\frac{B}{B_1}$, qui est isomorphe sans mériédrie, comme nous venons de le voir, au groupe simple

$\frac{A}{A_1}$, sera lui-même simple, et $\frac{B}{B_1}$ sera le premier groupe composant de B. En effet, s'il en était autrement, il existerait un groupe B′ plus général que B_1, contenu dans B et permutable à ses substitutions. Les substitutions correspondantes du groupe $\frac{B}{B_1}$ formeraient évidemment un groupe $\frac{B'}{B_1}$, contenu dans $\frac{B}{B_1}$ et permutable à ses substitutions; cela est impossible, $\frac{B}{B_1}$ étant simple.

10. On déduit de ce qui précède la conséquence suivante, qui est fort utile :

Si l'un des groupes composants du groupe B, *par exemple, n'est isomorphe à aucun des groupes composants des autres groupes* A, C, ..., G *contiendra un groupe ne déplaçant que les lettres de* B, *et dans la composition duquel figurera encore le groupe en question.*

En effet, nous avons vu que G contient le groupe G_1, et que les groupes partiels A_1, B_1, C_1, ... relatifs à ce groupe ne pourront différer des groupes analogues A, B, C,... que par la suppression de groupes composants isomorphes à $\frac{A}{A_1}$. Soit $\frac{A_1}{A_2}$ le second groupe composant de A; on verra de même que G_1 contient un groupe G_2, tel que les groupes partiels A_2, B_2, C_2, ... qui y sont relatifs ne diffèrent de A_1, B_1, C_1, ... que par la perte de groupes composants isomorphes à $\frac{A_1}{A_2}$. Continuant ainsi, on arrivera à un groupe G′ dont les substitutions ne déplacent plus les lettres de la classe A. Soient B′, C′, ... les groupes partiels formés par les déplacements que Il fait subir aux lettres des autres classes; ces groupes conserveront encore tous ceux des groupes composants de B, C, ... qui ne sont pas isomorphes à ceux de A.

De G′ on déduira de même un groupe G″, dont les substitutions ne déplacent plus les lettres de C, et ainsi de suite. On arrivera enfin à un groupe $\mathfrak{B}$ dont les substitutions ne déplacent plus que les lettres de B; et ce groupe retiendra toujours ceux des groupes composants de B qui ne sont pas isomorphes à ceux de A, C, ...

III

11. Théorème III. — *Soit p un nombre premier impair, q un nombre quelconque premier à p et compris entre p^n et p^{n+1}. Un groupe $\mathfrak{G}$ de degré $p^m q + k$ ne pourra être plus de k fois transitif sans contenir le groupe alterné, à moins qu'une des trois conditions ci-dessous ne soit satisfaite :* 1° $k < 5$;

2° $k \leqslant q$; 3° *le groupe linéaire de degré* p^{m+n} *contient un groupe admettant parmi ses groupes composants un groupe isomorphe au groupe alterné de degré* k.

12. *Démonstration.* — Supposons qu'aucune des conditions ci-dessus ne soit satisfaite. Considérons $p^m q$ lettres quelconques a, b, ... parmi celles de $\mathcal{G}$; celles des substitutions de $\mathcal{G}$ qui ne déplacent que ces lettres forment un groupe transitif G. Soient O l'ordre de G; p^l la plus haute puissance de p par laquelle O est divisible. D'après le théorème de M. Sylow, G contiendra un groupe H d'ordre p^l.

Groupons les lettres de G en classes, en réunissant entre elles celles de ces lettres que les substitutions de H permutent entre elles.

Le nombre des lettres de chaque classe sera une puissance de p au moins égale à p^m. Considérons en effet une lettre quelconque a, et soit r le nombre des lettres de sa classe : l'ordre de H sera évidemment égal à rs, s étant l'ordre du groupe H′ formé par celles des substitutions de H qui ne déplacent pas a. Or l'ordre de H est une puissance de p; donc r et s sont des puissances de p. D'ailleurs, H′ est contenu dans le groupe G′, formé par celles des substitutions de G qui ne déplacent pas a; O′, ordre de G′, est égal à $\frac{O}{p^m q}$, et par suite ne contient p qu'à la puissance $l-m$; s, ordre de H′, divisant O′, sera au plus égal à p^{l-m}; donc $r = \frac{p^l}{s}$ sera au moins égal à p^m.

Le nombre total des lettres de G étant $p^m q$, et chaque classe en contenant au moins p^m, *le nombre des classes sera au plus égal à* q.

13. Cela posé, soit $\mathfrak{I}$ le groupe formé par celles des substitutions de $\mathcal{G}$ qui sont permutables à H et qui permutent exclusivement entre elles les lettres a, b, ... d'une part, et les k lettres restantes x, y, ... d'autre part. Ces substitutions seront de la forme

$$A_1\Theta_1,\ A_2\Theta_2,\ \ldots.$$

A_1, A_2, ... étant des substitutions entre les lettres a, b, ..., lesquelles devront être permutables à H, et Θ_1, Θ_2, ... des substitutions entre les lettres $x, y, \ldots$. On verra, comme au théorème précédent, que le groupe Θ, formé des substitutions Θ_1, Θ_2, ..., contiendra toutes les substitutions possibles entre les lettres x, y, ...

Ce point établi, chacune des substitutions A_1, A_2, ... étant permutable à H, devra remplacer les lettres d'une même classe, lesquelles sont permutées entre elles par les substitutions de H, par d'autres lettres jouissant de cette même propriété, lesquelles appartiendront par suite à une même classe. Donc chacune des substitutions A_1, A_2, ... sera de la forme BC, B

étant une certaine substitution exécutée sur les classes, et C une nouvelle substitution qui ne déplace pas les classes.

Le nombre des classes ne pouvant dépasser q, le nombre des déplacements qu'on peut leur faire subir ne saurait dépasser $1.2...q$, nombre inférieur à $1.2...k$, nombre des substitutions distinctes du groupe Θ. Donc, parmi les substitutions de $\mathfrak{J}$, on en trouvera au moins deux, $A_1\Theta$ et $A_2\Theta_2$ qui permuteront les classes de la même manière, sans permuter x, y, ... de la même manière; et $\mathfrak{J}$ *contiendra la substitution* $(A_1\Theta_1)^{-1}A_2\Theta_2$, *laquelle ne déplace plus les classes, mais déplace encore les lettres* x, y, ...

Celles des substitutions de $\mathfrak{J}$ qui ne déplacent pas les classes forment évidemment un groupe $\mathfrak{J}'$, contenant H et permutable à toutes les substitutions de $\mathfrak{J}$. Soient

$$C_1\Theta'_1,\ C_2\Theta'_2,\ \ldots,$$

les substitutions de $\mathfrak{J}'$. Les substitutions de Θ seront évidemment permutables au groupe Θ', formé des substitutions partielles Θ'_1, Θ'_2, ... Mais k étant > 4, les seuls groupes contenus dans le groupe Θ et permutables à ses substitutions sont, comme on sait, le groupe Θ lui-même et le groupe alterné. Donc Θ' *contient dans tous les cas le groupe alterné.*

On peut d'ailleurs admettre que Θ' *ne contient aucune substitution autre que celle du groupe alterné.* Car, s'il en était autrement, nous n'aurions qu'à appliquer les raisonnements qui vont suivre non plus aux groupes Θ' et $\mathfrak{J}'$, mais au groupe alterné Θ'' et au groupe $\mathfrak{J}''$, formé par celles des substitutions de $\mathfrak{J}'$ dont les seconds facteurs appartiennent à Θ''.

14. Ce point établi, celles des lettres a, b, ... qui appartiennent à la première classe, à la seconde, etc., sont respectivement en nombre $p^{\alpha'}, p^{\alpha''}, \ldots$, $\alpha', \alpha'', \ldots$ *étant au plus égaux à* $m+n$; car le nombre total des lettres a, b, ... est $p^m q$, nombre $< p^{m+n+1}$ par hypothèse.

15. Considérons maintenant les substitutions $C_1, C_2, \ldots$ qui forment les premiers facteurs des substitutions de $\mathfrak{J}'$. On aura

$$C_1 = C'_1C''_1\ldots,\quad C_2 = C'_2C''_2\ldots,\quad \ldots,$$

$C'_1, C'_2, \ldots$ étant des substitutions opérées entre les lettres de la première classe, $C''_1, C''_2, \ldots$ des substitutions opérées entre les lettres de la seconde classe, etc.

En particulier, les substitutions de H seront respectivement

$$H'_1H''_1\ldots,\quad H'_2H''_2\ldots,\quad \ldots,$$

$H'_1, H'_2, \ldots$ étant des substitutions opérées entre les lettres de la première classe, $H''_1, H''_2, \ldots$ des substitutions opérées entre les lettres de la seconde classe, etc. Le groupe H' de degré $p^{\alpha'}$, formé par les substitutions partielles

$H'_1, H'_2, \ldots$, sera transitif par hypothèse. D'ailleurs l'ordre de H, lequel est p^l, est évidemment le produit de l'ordre de H′ par l'ordre du nouveau groupe formé par celles des substitutions de H qui ne déplacent plus les lettres de la première classe. Donc *l'ordre de* H′, divisant p^l, *sera une puissance de* p, *telle que* $p^{l'}$.

16. Soit maintenant C′ le groupe formé par les substitutions $C'_1, C'_2, \ldots$. Nous allons montrer que *tous les groupes composants de* C′ *appartiennent à des groupes contenus dans le groupe linéaire de degré* p^{m+n}. Et d'abord, nous remarquerons que les substitutions $C_1, C_2, \ldots$ étant permutables à H, les substitutions partielles $C'_1, C'_2, \ldots$ le seront *a fortiori* à celles de H′.

Or il résulte d'un théorème de M. Sylow que le groupe H′, dont l'ordre est une puissance de p, contient au moins une substitution d'ordre p échangeable à toutes les autres (n° 3 du mémoire cité). Mais il pourra en contenir plusieurs. Réunissons-les toutes ensemble; nous obtiendrons un groupe F′, formé de substitutions d'ordre p, échangeables entre elles. *Toutes les substitutions de* C′ *seront permutables à* F′; en effet, soit Φ' le groupe transformé de F′ par l'une quelconque C'_1 de ces substitutions; les substitutions de Φ' seront d'ordre p et échangeables à toutes celles du groupe transformé de H′ par C'_1, lequel groupe n'est autre que H′; donc, par définition, les substitutions de Φ' appartiendront à F′.

Le groupe F′ pourra être transitif ou non. Supposons pour plus de généralité qu'il ne le soit pas ; et groupons les $p^{\alpha'}$ lettres de la classe considérée en systèmes, en réunissant ensemble celles que F′ permute entre elles. Chaque substitution de C′, étant permutable à F′, remplacera les lettres de chaque système par celles d'un même système.

En particulier, H′ étant transitif, ses substitutions déplaceront *a fortiori* les systèmes d'une manière transitive; donc *chacun d'eux contiendra un même nombre de lettres*, $p^{\beta'}$, et ils seront en nombre $p^{\alpha'-\beta'} = p^{\gamma'}$.

17. Considérons maintenant les déplacements d'ensemble que les substitutions de C′ font éprouver aux systèmes. Ils forment un groupe transitif D, isomorphe à C′, et les groupes composants de C′ seront ceux de D, joints à ceux du groupe E formé par celles des substitutions de C′ qui ne déplacent pas les systèmes (*Traité des substitutions*, note B.). Les substitutions de E sont d'ailleurs de la forme

$$E'_1 E''_1 \ldots, \quad E'_2 E''_2 \ldots, \quad \ldots,$$

$E'_1, E'_2, \ldots$ étant des substitutions opérées entre les lettres du premier système, $E''_1, E''_2, \ldots$ des substitutions entre les lettres du second système, etc.

Les substitutions partielles $E'_1, E'_2, \ldots$ forment évidemment un groupe E′ isomorphe à E; et E aura pour groupes composants ceux de E′, joints à ceux du groupe Γ formé par celles des substitutions de E qui ne déplacent pas les lettres du premier système.

Soit de même Γ'' le groupe formé par les déplacements que les substitutions de Γ font subir aux lettres du second système, lequel groupe sera évidemment contenu dans $E'' = (E''_1, E''_2, \ldots)$. Le groupe Γ aura pour groupes composants ceux de Γ'' et ceux du groupe Δ formé par celles de ses substitutions qui ne déplacent pas les lettres des deux premiers systèmes. Soit de même Γ''' le groupe formé par les déplacements que les substitutions de Δ font éprouver aux lettres du troisième système, lequel groupe est contenu dans $E''' = (E'''_1, E'''_2, \ldots)$; Δ aura pour groupes composants ceux de Γ''', plus ceux du groupe formé par celles des substitutions de Δ qui ne déplacent pas les lettres des trois premiers systèmes. Continuant ainsi, on voit que G' *a pour groupes composants ceux des groupes* D, E', Γ'', Γ''',...; Γ'', Γ''',... *étant des groupes respectivement contenus dans* E'', E''', ...

18. Or il est aisé de voir que *les groupes* E', E'', E''',... *et a fortiori les groupes* E',Γ'',Γ''', ... *sont respectivement contenus dans les groupes linéaires de degré* $p^{\beta'}$ (et *a fortiori* dans le groupe linéaire du degré p^{m+n}; car le groupe linéaire de degré $p^{\beta'}$ est formé par celles des substitutions du groupe linéaire de degré p^{m+n} qui laissent $m+n-\beta'$ indices immobiles).

En effet, les substitutions de E

$$E'_1 E''_1 \ldots, \quad E'_2 E''_2, \ldots, \quad \ldots,$$

sont permutables à F, formé des substitutions

$$F_1 = F'_1 F''_1 \ldots, \quad F_2 = F'_2 F''_2 \ldots;$$

a fortiori les substitutions partielles E'_1, E'_2,... opérées entre les lettres du premier système, seront permutables au groupe partiel

$$F' = (F'_1, F'_2, \ldots),$$

formé des déplacements que les substitutions de F font subir aux lettres du premier système.

Mais les substitutions de F sont d'ordre p et échangeables entre elles; *a fortiori* celles de F' seront d'ordre p et échangeables entre elles; de plus, elles permutent transitivement les $p^{\beta'}$ lettres du premier système. On pourra donc (*Traité des substitutions*, n° 408) caractériser ces lettres par β' indices choisis de telle sorte que les substitutions de F' soient de la forme

$$| \; x, y, \ldots \quad x + \delta, y + \delta', \ldots \; |$$

et les substitutions de E', qui leur sont permutables, de la forme linéaire

$$| \; x, y \quad ax + by + \ldots + \delta, a'x + b'y + \ldots + \delta', \ldots \; |$$

La même démonstration s'applique aux groupes F'' et E'', etc.

Il est donc établi que *les derniers groupes composants de* G' *sont ceux de*

certains groupes E', Γ'', Γ''',... *contenus dans le groupe linéaire de degré* $m+n$. Il reste à démontrer que les premiers groupes composants, à savoir ceux de D, jouissent de la même propriété.

19. Soit Λ le groupe formé par les déplacements que les substitutions de H' font subir aux $p^{\gamma'}$ systèmes. L'ordre de H', $p^{\mu'}$, est évidemment égal à l'ordre de Λ, multiplié par l'ordre du groupe formé par celles des substitutions de H' qui ne déplacent pas les systèmes; donc Λ a pour ordre une puissance de p, et pour degré $p^{\gamma'}$, γ' étant $< m+n$. D'ailleurs les substitutions de C' étant permutables à H', celles de D le sont *a fortiori* à Λ. Cela posé, on raisonnera sur D et Λ comme nous l'avons fait sur C' et H', pour prouver que les derniers groupes composants de D sont ceux de groupes contenus dans le groupe linéaire de degré p^{m+n}. Continuant ainsi, on arrivera à prouver que tous les groupes composants de C' jouissent de cette propriété.

Il résulte de là que si, comme nous le supposons, la troisième condition du théorème III n'est pas satisfaite, aucun des groupes composants de C' ne sera isomorphe au groupe alterné Θ'; de même pour les facteurs de composition des groupes $C''=(C''_1, C''_2,\ldots)$, ...

20. Cela posé, k étant >4, le groupe Θ' sera simple, et par suite n'aura d'autre groupe composant que lui-même; donc d'après la proposition démontrée au n° 10, celles des substitutions du groupe $\mathfrak{I}'$ qui ne déplacent pas les lettres $a, b,\ldots$ permuteront encore d'une manière alternée les lettres x, $y,\ldots$. Donc $\mathfrak{I}'$, et *a fortiori* $\mathfrak{C}'_3$, contiendra une substitution circulaire ternaire; et comme il est au moins 5 fois transitif, il contiendra le groupe alterné.

Notre théorème est ainsi démontré.

IV

21. Nous nous trouvons ainsi conduits à examiner la question suivante :

Problème. — *Déterminer la valeur que k ne doit pas dépasser pour qu'on puisse déterminer un groupe* Γ, *contenu dans le groupe linéaire de degré* p^n, *et dont l'un des groupes composants soit isomorphe au groupe alterné* Θ *de degré* k.

(Dans cet énoncé, nous avons pour abréger désigné par n la quantité précédemment représentée par $m+n$ et par Θ le groupe que nous appelions Θ'.)

Tout d'abord, le groupe Γ étant contenu dans le groupe linéaire, ses facteurs de composition divisent ceux du groupe linéaire; mais ceux-ci sont premiers, à l'exception d'un seul, égal à $\frac{(p^n-1)(p^n-p)\ldots(p^n-p^{n-1})}{\delta(p-1)}$, δ étant le plus grand commun diviseur de n et de $p-1$ (*Traité des sub-*

stitutions, 135). Or Γ, par hypothèse, a l'un de ses facteurs de composition égal à $\frac{1.2\ldots k}{2}$. On aura donc la condition

$$\frac{(p^n-1)\ldots(p^n-p^{n-1})}{\delta(p-1)} \equiv 0 \mod \frac{1\,2\ldots k}{2},$$

laquelle pourra servir à limiter la valeur de k.

Mais on peut assigner à cette quantité une limite plus étroite, et *indépendante de p*. Nous allons en effet établir les deux inégalités suivantes

$$n \geqslant q-1, \tag{3}$$

q étant le plus grand nombre premier autre que p et inférieur à $k-1$

$$n \geqslant k - \frac{\log k}{\log 2} - 3. \tag{4}$$

Pour les démontrer, nous pourrons admettre qu'il existe un groupe contenu dans un groupe linéaire à n indices, et dont un groupe composant soit isomorphe à Θ, mais qu'il n'existe aucun semblable groupe contenu dans un groupe linéaire à moins de n indices. En suivant les conséquences de cette hypothèse, nous arriverons aux inégalités (3) et (4).

Nous embrasserons d'ailleurs dans notre démonstration pour plus de généralité, et pour éviter toute difficulté, le cas où les n indices x, y,... au lieu d'être des entiers réels, seraient des entiers imaginaires de la forme $a+bi+\ldots+ri^{\nu-1}$, i étant une racine d'une congruence irréductible de degré ν suivant le module p.

22. En premier lieu, faisons correspondre à chaque substitution

$$\gamma = |\ x, y, \ldots\ \ ax+by+\ldots+\alpha,\ a'x+b'y+\ldots+\alpha',\ \ldots\ |$$

du groupe Γ, la substitution linéaire

$$g = |\ x, y, \ldots\ \ ax+by+\ldots,\ a'x+b'y+\ldots,\ \ldots\ |$$

qui n'a plus de termes constants. Il est clair : 1° que les substitutions g, g_1,..., correspondantes aux diverses substitutions γ, γ_1,... du groupe Γ, formeront un groupe G isomorphe à Γ ; 2° que Γ aura pour premiers groupes composants ceux de G, ses autres groupes composants étant ceux du groupe Γ', formé par celles des substitutions de Γ dont la correspondante se réduit à l'unité. Ces dernières substitutions se réduisant à la forme

$$|\ x, y, \ldots\ \ x+\alpha,\ y+\alpha',\ \ldots\ |$$

les facteurs de composition de Γ' seront tous premiers ; et ne pourront être

égaux à $\frac{1.2...k}{2}$. C'est donc parmi les groupes composants de G que devra se trouver le groupe isomorphe à Θ.

23. Soient $\frac{G}{G_1}$, $\frac{G_1}{G_2}$,... les groupes composants de G, et admettons que Θ soit isomorphe au groupe $\frac{G_2}{G_{2+1}}$. Le groupe G_2 étant contenu dans G, a ses substitutions linéaires sans termes constants; et $\frac{G_2}{G_{2+1}}$, isomorphe à Θ, est le premier de ses groupes composants. On raisonnerait au besoin sur G_2, au lieu de raisonner sur G; on peut donc admettre sans nuire à la généralité de la question, que Θ est isomorphe à $\frac{G}{G_1}$, premier groupe composant de G.

Ici se présenteront deux cas, suivant que G_1 contient ou non des substitutions qui ne multiplient pas tous les indices par un même facteur constant.

24. *Premier cas.* — Nous allons montrer qu'on peut admettre, sans diminuer la généralité de la question, que *toutes les substitutions de* G *sont permutables à un groupe partiel* H, *ayant pour ordre une puissance d'un nombre premier, et contenant des substitutions qui ne multiplient pas tous les indices par un même facteur.*

Soit en effet $O = \pi^\alpha \pi'^{\alpha'}...$ l'ordre de G_1, π, π',... étant des nombres premiers; G_1 contiendra, d'après M. Sylow, un groupe H d'ordre π^α, un groupe H' d'ordre $\pi'^{\alpha'}$, etc., et dérivera de la combinaison de ces groupes. Si chaque substitution de chacun de ces groupes multipliait tous les indices par un même facteur constant, chacune des $\pi^\alpha \pi'^{\alpha'}...$ substitutions qui résultent de leur combinaison et qui reproduisent toutes celles de G_1, multiplierait tous les indices par un même facteur, contrairement à notre supposition.

On peut donc admettre que les substitutions de H, par exemple, ne multiplient pas toutes tous les indices par un même facteur. Si celles de H', etc. jouissaient au contraire de cette propriété, elles seraient échangeables à celles de H. Donc le groupe G_1, dérivé de la combinaison des groupes H, H',... aura toutes ses substitutions permutables à H; donc H sera le seul groupe d'ordre π^α que G_1 contienne. Cela posé, les substitutions de G, permutables à G_1, le seront évidemment à H, ce qui démontre notre proposition.

Supposons au contraire que deux au moins H, H' des groupes de la suite H, H',... contiennent des substitutions qui ne multiplient pas tous les indices par un même facteur; l'un au moins π des deux nombres π, π' sera > 2. Cela posé, soient I le groupe formé par celles des substitutions de G_1, qui sont permutables à H, M son ordre; on aura d'après M. Sylow

$$O \equiv M \bmod \pi M \equiv M \bmod \pi^{\alpha+1}.$$

Soient $1, g_1, g'_1, \ldots$ les substitutions de G_1 ; $1, s, s', \ldots$ les substitutions de $\frac{G}{G_1}$; celles de G seront données par le tableau suivant :

$$(5) \qquad \begin{array}{llll} 1 & g_1 & g'_1, & \ldots \\ s & sg_1 & sg'_1, & \ldots \\ s' & s'g_1 & s'g'_1, & \ldots \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

dont les diverses lignes sont formées de substitutions congrues mod G_1 aux diverses substitutions de $\frac{G}{G_1}$.

Nous allons montrer que chaque ligne de ce tableau contient au moins une substitution permutable à H.

Soient en effet $a, b, c, d, \ldots$ les lettres de Θ, dont le nombre est par hypothèse supérieur à 4. Soient a, b, c, d quatre quelconques d'entre elles ; Θ contiendra la substitution linéaire $S = (ab)(cd)$, laquelle aura pour homologue dans $\frac{G}{G_1}$ une substitution s, satisfaisant à la relation $s^2 \equiv 1 \bmod G_1$.

Les substitutions des deux premières lignes du tableau (5) formeront un groupe $\mathcal{G}$ d'ordre 20 contenant G_1. Le groupe $\mathfrak{I}$, formé par celles des substitutions de $\mathcal{G}$ qui sont permutables à H, contiendra I et aura pour ordre $\mathfrak{N} = rM$, r étant un entier. D'ailleurs $r = 1$ ou 2. En effet, si aucune des substitutions de la suite $s, sg_1, \ldots$ n'est permutable à H, $\mathfrak{I}$ se réduira à I et son ordre $\mathfrak{N}$ sera égal à M. Au contraire, si l'une σ des substitutions de cette suite est permutable à H, cette suite contiendra M substitutions permutables à H, lesquelles s'obtiendront en multipliant successivement σ par les M substitutions $1, i_1, i'_1, \ldots$ du groupe I. On aura donc $\mathfrak{N} = 2M$.

Ce dernier cas sera nécessairement réalisé. En effet, le théorème de M. Sylow, appliqué à $\mathcal{G}$, donnera

$$20 \equiv rM \bmod \pi^{\alpha+1},$$

et comme $0 \equiv M$, on aura

$$(2 - r)\,0 \equiv 0 \bmod \pi^{\alpha+1}, \quad \text{d'où} \quad 2 - r \equiv 0 \bmod \pi = 0.$$

Donc G contient des substitutions permutables à H et congrues mod G_1 à la substitution s.

Soient maintenant S, T, ... les diverses substitutions semblables à S que contient le groupe Θ. Ces substitutions, combinées entre elles, reproduisent tout ce groupe. Leurs correspondantes $s, t, \ldots$ dans le groupe isomorphe $\frac{G}{G_1}$ reproduiront tout ce groupe ; et les substitutions $\sigma, \tau, \ldots$ congrues à celles-là et contenues dans G, combinées entre elles de la même manière,

donneront des substitutions permutables à H et congrues à toutes les substitutions du groupe $\frac{G}{G_1}$.

Le groupe I′, formé par celles des substitutions de G qui sont permutables à H, contiendra donc des substitutions congrues à chacune de celles de $\frac{G}{G_1}$; il aura donc pour groupes composants ce groupe $\frac{G}{G_1}$, suivi des groupes composants du groupe I formé par celles de ses substitutions qui appartiennent à G_1.

Donc, dans le cas que nous traitons, *s'il existe un groupe* G *contenu dans le groupe linéaire et tel que l'un de ses groupes composants soit isomorphe à* Θ, *on pourra déterminer un autre groupe* I′ *jouissant de cette même propriété, et dont les substitutions soient en outre permutables à un groupe partiel* H *dont l'ordre soit une puissance de nombre premier et dont toutes les substitutions ne multiplient pas tous les indices par un même facteur constant.*

On peut donc sans nuire à la généralité de la question, imposer cette nouvelle condition au groupe G; car s'il n'y satisfaisait pas, on appliquerait tous les raisonnements qui vont suivre au groupe I′ lequel y satisfait.

25. Ce point établi, parmi les substitutions de H, autres que l'unité, il en est qui sont échangeables à toutes les autres (mémoire cité de M. Sylow, n° 5). Soit F le groupe formé par leur réunion. Il sera permutable aux substitutions de G. En effet, chacune d'elles transforme F en un groupe formé de substitutions contenues dans H, et échangeables à toutes celles de H; ce groupe transformé se confondra donc avec F.

26. Cela posé, soit d'abord $\pi \gtrless p$. Les substitutions de F, étant échangeables entre elles, et d'ordre premier à p, pourront être ramenées simultanément par un changement d'indices convenable à la forme canonique monôme

$$| x, y, \ldots \quad ax, by, \ldots |$$

Si l'on réunit ensemble dans une même classe tous les indices qui sont multipliés par un même facteur dans chacune des substitutions de F, le nombre m de ces classes ne pourra surpasser le nombre n des indices.

27. Supposons d'abord qu'il y ait plusieurs classes.

Les substitutions de G, étant permutables à F, remplaceront les indices de chaque classe par des fonctions linéaires des indices d'une même classe. Si elles déplacent les classes, elles seront de la forme $P_1Q_1, P_2Q_2, \ldots; P_1, P_2, \ldots$ étant des déplacements opérés entre les classes, en remplaçant chaque indice par un indice correspondant, et $Q_1, Q_2, \ldots$ des substitutions qui remplacent chaque indice par une fonction linéaire des indices de la même classe.

Celles des substitutions de G qui ne déplacent pas les classes forment un groupe K auquel toutes les substitutions de G sont évidemment permutables, et dont l'ordre est égal à $\frac{0}{\Omega}$, 0 étant l'ordre de G, et Ω l'ordre du groupe formé par les substitutions $P_1, P_2, \ldots$, lequel divisera évidemment $1.2 \ldots m$, m étant le nombre des classes. Soit d'ailleurs G_1 le groupe le plus général parmi ceux qui contiennent K, sont contenus dans G et permutables aux substitutions de G. Son ordre sera un multiple de $\frac{0}{\Omega}$, tel que $q\frac{0}{\Omega}$; et G aura pour premier facteur de composition $\frac{\Omega}{q}$. Mais ce premier facteur de composition doit être $\frac{1.2 \ldots k}{2}$; on aura donc

$$\frac{1.2 \ldots k}{2} = \frac{\Omega}{q} \leqslant 1.2 \ldots m, \quad \text{d'où} \quad k \leqslant m \leqslant n,$$

inégalité qui entraîne *a fortiori* les relations (3) et (4).

28. Supposons en second lieu que les substitutions de G ne déplacent pas les classes. Elles seront de la forme $a_1 b_1 \ldots$, $a_2 b_2 \ldots$, ..., $a_1, a_2, \ldots$ étant des substitutions linéaires (*) opérées sur les indices de la première classe; $b_1, b_2, \ldots$ des substitutions sur les indices de la seconde classe, etc.

Considérons les groupes

$$A = (a_1, a_2, \ldots), \quad B = (b_1, b_2, \ldots), \quad \ldots.$$

L'un au moins d'entre eux, A par exemple, contiendra des substitutions autres que l'unité; et il est clair que G aura pour groupes composants les groupes composants de A, suivis des groupes composants du groupe partiel G′ formé par celles des substitutions de G qui se réduisent à la forme $b \ldots$.

Le premier groupe composant de A étant en même temps le premier groupe composant de G devra être isomorphe à Θ. Résultat inadmissible, par hypothèse (21); A ayant ses substitutions linéaires avec un nombre n' d'indices inférieur à n.

29. Admettons maintenant qu'il n'y ait qu'une classe. Les substitutions de F se réduiront à la forme

$$| \; x, y, \ldots \; ax, ay, \ldots \; |$$

On pourra déterminer dans le groupe H *un groupe partiel* Φ *plus général*

(*) Si la réduction des substitutions de F à la forme canonique a nécessité l'introduction d'imaginaires, les substitutions $Q'_1, Q'_2, \ldots$ pourront avoir leurs coefficients imaginaires.

que F, *et dont les substitutions soient échangeables* mod F *à toutes les substitutions de* H.

Soit en effet π^β l'ordre de F, celui de H étant π^α comme ci-dessus. Une fonction z invariable par les substitutions de F et variable par toute autre substitution prendra par les substitutions de H un nombre de valeurs distinctes $z, z', \ldots$ égal à $\pi^{\alpha-\beta}$. Les déplacements opérés sur ces fonctions par les substitutions de H formeront un groupe $\mathfrak{G}$ de substitutions S, S', ... isomorphe à H et d'ordre $\pi^{\alpha-\beta}$. On pourra (Sylow, n° 3) y déterminer un faisceau Ψ de substitutions échangeables entre elles. Soit π^γ son ordre. A chacune des substitutions S, S', ... correspondent π^β substitutions dans H; et l'ensemble des substitutions correspondantes à celles de Ψ donnera un groupe Φ d'ordre $\pi^{\beta+\gamma}$, dont les substitutions seront échangeables mod F à toutes celles de H. Soient en effet s une d'entre elles, t une substitution de H, S et T leurs corrélatives dans $\mathfrak{G}$. La substitution $s^{-1}t^{-1}st$, ayant pour corrélative $S^{-1}T^{-1}ST$, qui se réduit à l'unité, appartiendra à F.

30. L'une quelconque u des substitutions de Φ, étant contenue dans H dont l'ordre est une puissance de π, aura pour ordre une puissance de π; et l'exposant de la première de ses puissances successives qui appartient à F étant évidemment un diviseur de l'ordre de u, sera lui-même une puissance de π, telle que π^δ; et Φ contiendra la substitution $u^{\pi^\delta-1}$, dont la puissance π appartient à F.

Celles des substitutions de Φ *dont les* $\pi^{\text{ièmes}}$ *puissances appartiennent ainsi à* F, *forment un groupe* $\mathfrak{F}$. En effet, soient u, v deux d'entre elles; comme elles sont échangeables mod F, on aura

$$(uv)^\pi \equiv u^\pi v^\pi \bmod \mathrm{F},$$

et u^π, v^π appartenant à F, il en sera de même de $(uv)^\pi$.

Les substitutions de G *sont permutables à* $\mathfrak{F}$; car elles le sont à F et à H; donc elles transformeront chaque substitution de $\mathfrak{F}$ en une substitution contenue dans H, permutable à F, et dont la $\pi^{\text{ième}}$ puissance appartiendra à F; donc cette transformée appartiendra à $\mathfrak{F}$.

Deux substitutions quelconques de $\mathfrak{F}$, u et v, satisfont par hypothèse à la relation

$$v^{-1}uv = \tau u,$$

τ étant une substitution de F. On en déduit

$$v^{-2}uv^2 = v^{-1}\tau uv = \tau v^{-1}uv = \tau^2 u,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$v^{-\pi}uv^\pi = \tau^\pi u.$$

Mais v^π, appartenant à F, est échangeable à u; on aura donc

$$\tau^\pi = 1$$

et par suite τ *sera une puissance de la substitution*

$$| x, y, \ldots \quad \theta x, \theta y, \ldots |$$

où θ est une racine primitive de la congruence

$$\theta^{\tau} \equiv 1 \mod p.$$

Nous désignerons cette dernière substitution par θ.

31. Celles des substitutions de $\mathfrak{F}$ qui sont échangeables à toutes les autres forment d'ailleurs un groupe partiel F_1, auquel les substitutions de G sont évidemment permutables. Si F_1 est plus général que F, il contiendra des substitutions qui ne sont pas échangeables à toutes celles de H, et qui par suite ne multiplieront pas tous les indices par un même facteur. Le raisonnement des nos 26 à 28 étant appliqué aux groupes G et F_1 mènera à une conséquence inadmissible.

32. Supposons donc que F_1 se réduise à F. Soit A_1 une substitution quelconque de $\mathfrak{F}$, autre que celles de F; $\mathfrak{F}$ contiendra une substitution u non échangeable à A_1; supposons qu'elle transforme A_1 en $\theta^{\xi}A_1$; et soit

$$\tau \equiv \frac{1}{\xi} \mod \pi.$$

La substitution $u^{\tau} = B_1$ transformera A_1 en θA_1; et $\mathfrak{F}$ résultera de la combinaison de A_1 et de B_1 avec des substitutions échangeables à A_1 et à B_1. Soit en effet v une substitution de $\mathfrak{F}$ qui transforme A_1 et B_1 en $\theta^{\alpha}A_1$, $\theta^{\beta}B_1$; on aura

$$v = A_1^{-\alpha}B_1^{\lambda}w,$$

w étant une nouvelle substitution de $\mathfrak{F}$, échangeable à A_1 et à B_1.

Cela posé, celles des substitutions de $\mathfrak{F}$ qui sont échangeables à A_1 et B_1 forment évidemment un groupe $\mathfrak{F}_1$. Si $\mathfrak{F}_1$ contient une substitution A_2 qui n'appartienne pas à F, il contiendra une substitution B_2 qui transforme A_2 en θA_2, et résultera de la combinaison de A_2 et de B_2 avec un groupe $\mathfrak{F}_2$ de substitutions échangeables à A_1, B_1, A_2, B_2. Poursuivant ainsi, on voit que $\mathfrak{F}$ *résulte de la combinaison de* F *avec une double suite de substitutions*

$$A_1, A_2, \ldots, A_\sigma,$$
$$B_1, B_2, \ldots, B_\sigma,$$

toutes échangeables entre elles, sauf deux substitutions correspondantes A_r *et* B_r, *lesquelles satisferont à la relation*

$$B_r^{-1}A_rB_r = \theta A_r.$$

33. Les substitutions de la première ligne $A_1, \ldots, A_\sigma$ sont échangeables entre elles ; d'ailleurs leur puissance $\pi^{\text{ième}}$ appartient à F ; donc leur ordre est premier à p ; et ces substitutions pourront être ramenées simultanément par un choix d'indices convenable à la forme canonique monôme. Réunissons dans une même classe, que nous désignerons par $C_{0\ldots0}$, ceux des nouveaux indices $y, z, \ldots$ que $A_1, \ldots, A_\sigma$ multiplient respectivement par une même série de facteurs constants $a_1, \ldots, a_\sigma$; *on aura quels que soient les entiers* $\xi_1, \ldots \xi_\sigma \bmod \pi$ *une classe* $C_{\xi_1\ldots\xi_\sigma}$ *contenant un nombre égal d'indices* $y', z', \ldots$ *que* $A_1, \ldots, A_\sigma$ *multiplieront par* $a_1\theta^{\xi_1}, \ldots, a_\sigma\theta^{\xi_\sigma}$.

En effet, soit μ le nombre des indices de la classe $y, z, \ldots$. La substitution $B_1^{\xi_1} \ldots B_\sigma^{\xi_\sigma}$ transformant $A_1, \ldots, A_\sigma$ en $\theta^{\xi_1}A_1, \ldots, \theta^{\xi_\sigma}A_\sigma$ remplacera ces indices par μ fonctions distinctes $\varphi, \psi, \ldots$ des indices tels que $A_1, \ldots, A_\sigma$ les multiplient respectivement par $a_1\theta^{\xi_1}, \ldots, a_\sigma\theta^{\xi_\sigma}$. Mais A_1 multipliant chaque indice par un facteur constant ne pourra multiplier une fonction de ces indices par $a_1\theta^{\xi_1}$ que si cette fonction contient seulement les indices que A_1 multiplie par ce facteur. On peut faire un raisonnement analogue pour A_2, etc. Les indices $y', z', \ldots$ qui figurent dans les fonctions $\varphi, \psi, \ldots$ appartiendront donc à la classe $C_{\xi_1\ldots\xi_\sigma}$. Leur nombre μ' devra être au moins égal au nombre μ de ces fonctions. Par un raisonnement inverse, on verrait que μ est au moins égal à μ' ; donc $\mu = \mu'$.

En faisant varier successivement $\xi_1, \ldots, \xi_\sigma$ de 0 à $\pi - 1$, on voit qu'à la classe $C_{0\ldots0}$ sont associées π^σ classes également nombreuses. Donc *le nombre total n des indices est un multiple de* π^σ.

34. Cela posé, considérons une substitution quelconque S du groupe G. Elle transforme les substitutions

$$A_1, A_2, \ldots, A_\sigma$$
$$B_1, B_2, \ldots, B_\sigma$$

en substitutions du groupe $\mathfrak{F}$, lesquelles seront de la forme

$$f_1 A_1^{a'_1} B_1^{b'_1} A_2^{a'_2} B_2^{b'_2} \ldots, \quad f_2 A_1^{a''_1} B_1^{b''_1} A_2^{a''_2} B_2^{b''_2} \ldots, \ldots,$$
$$g_1 A_1^{c'_1} B_1^{d'_1} A_2^{c'_2} B_2^{d'_2} \ldots, \quad g_2 A_1^{c''_1} B_1^{d''_1} A_2^{c''_2} B_2^{d''_2} \ldots, \ldots$$

$f_1, f_2, \ldots, g_1, g_2, \ldots$ étant des substitutions de F, et si l'on fait correspondre à la substitution S la substitution linéaire suivante de degré $\pi^{2\sigma}$

$$\begin{vmatrix} x_1, y_1 & a'_1x_1 + c'_1y_1 + a''_1x_2 + c''_1y_2 + \ldots, b'_1x_1 + d'_1y_1 + b''_1x_2 + d''_1y_2 + \ldots \\ x_2, y_2 & a'_2x_1 + c'_2y_1 + a''_2x_2 + c''_2y_2 + \ldots, b'_2x_1 + d'_2y_1 + b''_2x_2 + d''_2y_2 + \ldots \end{vmatrix} \bmod \pi$$

on verra sans difficulté que les substitutions correspondantes aux diverses substitutions de G forment un groupe Γ, isomorphe à G.

35. Supposons d'abord que Γ contienne des substitutions autres que l'unité. Son premier groupe composant sera isomorphe au premier groupe

composant de G, et par suite isomorphe à Θ. Ce résultat est inadmissible par hypothèse (21) ; car Γ est de degré $\pi^{2\sigma}$ et l'exposant 2σ est moindre que n, multiple de π^{σ}.

36. Si Γ se réduisait à la seule substitution 1, toutes les substitutions de G transformeraient A_1 en substitutions de la forme $f_1 A_1^{\alpha'_1}$. Elles seraient donc permutables au groupe F′ dérivé de F et de A_1. Ce groupe contient une substitution A_1 qui ne multiplie pas tous les indices par un facteur constant. Donc les indices pourront s'y répartir en plusieurs classes. Et l'on verra comme aux nos 27 et 28 que *si* G *contient des substitutions qui déplacent les classes, on aura* $k \leqslant n$; dans le cas contraire, on aurait un groupe contenu dans le groupe linéaire de degré $p^{n'}$, n' étant $< n$ et dont le premier groupe composant serait isomorphe à Θ ; résultat inadmissible, par hypothèse (21).

37. Soit en dernier lieu $\pi = p$. On pourra (*Traité des Substitutions*, 179-182) choisir les indices indépendants de telle sorte qu'un certain nombre d'entre eux, x, x',... restent inaltérés par toutes les substitutions de F; les autres indices étant désignés par y,... les substitutions de G seront de la forme suivante (*Ibid.*, 188).

$$\left| \begin{array}{ll} x, x', .. & f(x, x', \ldots), f'(x, x', ..).. . \\ y, .., & ay + .. + \varphi(x, x', \ldots), \ldots \end{array} \right|$$

et il aura pour groupes composants :

1° Les composants du groupe isomorphe J formé par les altérations

$$| x, x', \ldots \quad f(x, x', \ldots), f'(x, x', . .). \ldots |$$

que les substitutions de G font subir aux indices x, x', ...

2° Ceux du groupe formé par celles des substitutions de G qui n'altèrent pas les indices x, x',... et se réduisent en conséquence à la forme

$$\left| \begin{array}{ll} x, x', \ldots & x, x', \ldots \\ y, . . & ay + \ldots + \varphi(x, x', . .), \ldots \end{array} \right|$$

Ceux-ci seront à leur tour de deux sortes :

1° Les composants du groupe isomorphe K formé des substitutions

$$| y, \ldots \quad ay + \ldots, \ldots |$$

2° Ceux du groupe L formé par celles des substitutions de G qui se réduisent à la forme

$$\left| \begin{array}{ll} x, x', \ldots & x, x', . . \\ y, y', \ldots & y + \varphi(x, x', \ldots), y' + \varphi'(x, x', \ldots), \ldots \end{array} \right|$$

Or L ayant ses substitutions d'ordre p et échangeables entre elles, ses composants ont tous pour ordre p et ne peuvent être isomorphes à Θ.

D'autre part, J et K sont contenus dans des groupes linéaires à moins de n indices ; ils ne peuvent donc être isomorphes à Θ.

38. *Second cas.* — Supposons que G_1 ne contienne aucune substitution autre que celles qui multiplient tous les indices par un même facteur constant.

Soit q un nombre premier impair quelconque, différent de p et inférieur à $k-1$. Soient $\alpha, \beta, \ldots, \lambda$ les k lettres que déplace Θ. Ce groupe contient une substitution circulaire S entre les q premières de ces lettres, $\alpha, \beta, \ldots, \gamma$. Elle aura pour homologue dans $\frac{G}{G_1}$ une substitution linéaire s, dont la puissance q appartiendra à G_1. Cette substitution pourra se mettre sous la forme canonique

$$| x, y, \ldots \quad ax, by, \ldots |$$

avec la condition $a^q \equiv b^q \equiv \ldots \bmod p$. On aura donc $b = a\theta^\rho, \ldots$, θ étan une racine primitive de la congruence $\theta^q \equiv 1 \bmod p$. On pourra grouper le indices en classes, en réunissant ensemble, comme appartenant à la classe ρ, ceux que s multiplie par $a\theta^\rho$.

Cela posé, soit g une racine primitive de q. Il existe une substitution circulaire entre les $q-1$ lettres $\beta, \ldots, \gamma$ qui transforme S en S^g. En y joignant une transposition opérée sur deux des lettres suivantes, on obtiendra une substitution T qui transforme S en S^g et qui sera contenue dans Θ. Son homologue t dans G transformera s en $s^g m$, m étant une substitution de G_1, laquelle multipliera par suite tous les indices par un même facteur m.

Les deux substitutions s et $s^g m$, étant transformables l'une dans l'autre, auront la même forme canonique. Or l'une multiplie les diverses classes d'indices par $a, a\theta, a\theta^2, \ldots$; l'autre les multiplie par ma^g, $ma^g\theta^g$, $ma^g\theta^{2g}, \ldots$, nombres qui doivent être égaux à l'ordre près aux précédents. On aura donc une égalité de la forme

$$ma^g = a\theta^\rho,$$

d'où l'on déduira

$$ma^g a\theta^{\sigma g} = a\theta^{\rho + \sigma g}.$$

Donc autant il y a d'indices dans la classe σ, autant il y en a que $t^{-1}st$ multiplie par $a\theta^{\rho+\sigma g}$. Mais $t^{-1}st$ est semblable à s; donc le nombre des indices multipliés par un même facteur est le même dans les deux substitutions. Donc la classe σ contient autant d'indices que la classe $\rho + \sigma g = \sigma_1$, celle-ci autant que la classe $\rho + \sigma_1 g$, etc.

Posons $\sigma \equiv \frac{\rho}{1-g} + 1 \bmod q$; on aura $\sigma_1 \equiv \frac{\rho}{1-g} + g$, $\sigma_2 \equiv \frac{\rho}{1-g} + g^2$, ... ; et comme la suite $1, g, g^2, \ldots$ contient tous les nombres mod q, sauf zéro, on voit qu'il y aura $q-1$ classes contenant un même nombre μ

d'indices. Ce nombre ne peut être nul, car si tous les indices étaient contenus dans la même classe, s appartiendrait à G_1, ce qui est absurde. Quant à la dernière classe, elle contiendra $\mu' = n - (q-1)\mu$ indices.

On voit déjà que n *est au moins égal à* $q-1$, ce qui démontre l'inégalité (3).

39. On remarquera en outre que *le nombre maximum d'indices que chaque classe puisse posséder est égal à* $n-q+1$, *ou à* 1. En effet, il doit y avoir plusieurs classes, donc $\mu > 0$, et si $q=2$, $\mu' > 0$, et la plus grande valeur que μ' puisse posséder sera, pour $\mu = 1$, $\mu' = n-q+1$. Quant à $\mu = \frac{n-\mu'}{q-1}$, sa plus grande valeur sera, si $q=2$, $n-1 = n-q+1$, cas répondant à $\mu' = 1$; si $q > 2$, on pourra poser $\mu' = 0$; et si $n < 2(q-1)$, le maximum sera égal à l'unité ; si $n \geqslant 2(q-1)$, il ne pourra dépasser $n-q+1$.

40. Posons maintenant $k-q=k'$ et supposons cette quantité supérieure à 4. Dans le groupe Θ sera contenu un groupe Θ', ne déplaçant pas les lettres $\alpha, \beta, \ldots, \gamma$ et alterné par rapport aux k' lettres restantes. Ce groupe sera simple, et d'ordre $\frac{1.2 \ldots k'}{2}$. De plus ses substitutions U, U', ... seront échangeables à S. Leurs homologues dans G formeront un groupe G', dont les substitutions $u, u', \ldots$ transformeront s en substitutions congrues à s mod G_1, lesquelles seront, par suite, de la forme $sm, sm', \ldots, m, m', \ldots$ désignant les substitutions qui multiplient tous les indices par un même facteur respectivement égal à $m, m', \ldots$.

Pour que la substitution sm, qui multiplie les diverses classes d'indices respectivement par $ma, ma\theta, \ldots$ soit semblable à la substitution s, qui les multiplie par $a, a\theta, \ldots$, il faudra que m soit une puissance de θ, telle que θ^ρ. D'ailleurs, pour que u transforme s en sm, il faudra qu'elle remplace les indices de la classe σ, que s multiplie par $a\theta^\sigma$, par des fonctions que s multiplie par $ma\theta^\sigma = a\theta^{\sigma+\rho}$, c'est-à-dire par des fonctions des indices de la classe $\sigma+\rho$.

On aura de même $m' = \theta^{\rho'}$, et u' remplacera les indices d'une classe quelconque σ par des fonctions de ceux de la classe $\sigma+\rho'$; etc.

41. Nous allons montrer que l'on aura $\rho \equiv \rho' \equiv \ldots \equiv 0 \bmod q$, de telle sorte qu'*aucune des substitutions de* G' *ne déplace les classes d'indices*. Supposons en effet $\rho \gtrless 0 \bmod q$, et soit δ' un entier satisfaisant à la congruence $\delta'\rho \equiv \rho' \bmod q$. On aura $u' = u^{\delta'}t'$, t' étant une substitution qui ne déplace plus les classes ; de même $u'' = u^{\delta''}t''$, etc. Donc G' résultera de la combinaison de u avec des substitutions qui ne déplacent plus les classes. Celles-ci forment un groupe H', évidemment permutable à toutes les substitutions de G' ; il contiendra d'ailleurs la $q^{\text{ième}}$ partie des substitutions de G' ; car $u, u^2, \ldots, u^{q-1}$ déplacent les classes, mais u^q ne les déplace plus. Cela

posé, le groupe Θ' étant isomorphe à G', le groupe formé par celles de ses substitutions qui sont homologues à celles de H' sera permutable aux substitutions de Θ' et contiendra la $q^{\text{ième}}$ partie de ces substitutions; résultat absurde, Θ' étant simple, et d'ordre $\frac{1.2\ldots k'}{2}$.

42. Donc toutes les substitutions $u, u', \ldots$ du groupe G' remplaceront les indices de chaque classe par des fonctions de ces mêmes indices. D'ailleurs *il existe au moins une classe dont toutes les substitutions* $u, u', \ldots$ *ne multiplient pas chacune tous les indices par de simples facteurs constants;* sans quoi $u, u', \ldots$ seraient échangeables entre elles, et leurs homologues U, U', ... le seraient aussi, ce qui est absurde.

Cette classe σ contiendra nécessairement plusieurs indices; mais leur nombre n' ne pourra dépasser $n-q+1$, ainsi que nous l'avons vu.

43. Soient $v, v', \ldots$ les altérations que les substitutions $u, u', \ldots$ font subir aux indices de la classe σ; $\mathcal{G}$ le groupe formé par ces altérations; $\mathcal{G}_1$ un groupe aussi général que possible parmi ceux qui sont contenus dans $\mathcal{G}$ et permutables à ses substitutions. Celles des substitutions de G' qui font subir aux indices de la classe σ une altération contenue dans $\mathcal{G}_1$ forment évidemment un groupe contenu dans G' et permutable à ses substitutions. Leurs homologues dans Θ' formeront un groupe contenu dans Θ' et permutable à ses substitutions. Mais Θ' est simple; donc ce nouveau groupe se réduit à la substitution 1.

Il est clair d'ailleurs que le groupe Θ' de degré $k-q$ sera isomorphe à $\frac{\mathcal{G}}{\mathcal{G}_1}$, premier groupe composant de $\mathcal{G}$. Or $\mathcal{G}$ a ses substitutions linéaires entre $n' \leqslant n-q+1$ indices. Et l'on pourra raisonner sur $\mathcal{G}$ et Θ' comme sur G et Θ. On aura donc, en désignant par q' un nombre premier $\geqslant p$ et $< k'-1$,

$$n' \geqslant q'-1, \quad \text{d'où} \quad n' \geqslant (q-1)+(q'-1).$$

On voit de même que, si $k'' = k'-q' > 4$, on aura, en désignant par n'' un entier au plus égal à $n'-q'+1$ et par q'' un nombre premier différent de p et $< k''-1$,

$$n'' \geqslant q''-1, \quad \text{d'où} \quad n \geqslant (q-1)+(q'-1)+(q''-1),$$

etc.

Soient donc $q, q', q'', \ldots$ des nombres premiers quelconques différents de 1 et de p, et tels que l'on ait

$$k = q + q' + q'' + \ldots + q^{(\mu-1)} + \rho, \tag{6}$$

$$\rho > 1 \quad \text{et} \quad q^{(\mu-1)} + \rho > 4, \tag{7}$$

on aura

$$n \geqslant q-1+q'-1+\ldots \geqslant k-\rho-\mu. \tag{8}$$

44. Pour achever de déterminer la limite inférieure de n correspondant à chaque valeur de k, il ne restera plus qu'à opérer de la manière la plus avantageuse la décomposition de $k-\rho$ en une somme de nombres premiers. Très-peu de nombres premiers suffiront en général.

45. Les théorèmes de M. Tchébychef sur la fréquence des nombres premiers permettent d'assigner à n une limite indépendante de toute recherche arithmétique. Supposons en effet que k soit contenu entre 2^m et 2^{m+1}. On sait qu'il existe un nombre premier q contenu entre $k-2$ et $\frac{k}{2}$. Si $q \gtrless p$, on pourra poser

$$k = q + k', \quad n = q - 1 + n',$$

k' étant $< \frac{k}{2}$, et par suite au plus égal à 2^m. On aura d'ailleurs

$$k - n = 1 + k' - n',$$

et, par suite, la limite de $k-n$ se déduira de celle de $k'-n'$.

Si $p=q$ (cas qui ne peut se présenter que lorsque p est contenu lui-même entre k et $\frac{k}{2}$), on aura un nombre premier q_1 compris entre $\frac{k}{2}$ et $\frac{k}{4}$, et l'on posera

$$k = 2q_1 + k', \quad n = (q_1 - 1) + (q_1 - 1) + n',$$

d'où

$$k - n = 2 + k' - n',$$

k' étant encore $< \frac{k}{2}$.

On aura de même

$$k' - n' = \lambda + k'' - n'',$$

k'' étant $< \frac{k''}{2}$, et λ étant égal à 1, sauf dans le cas où p serait contenu entre k' et $\frac{k'}{2}$.

On opérera une suite de réductions analogues, jusqu'à ce qu'on arrive à un nombre $k^{(r)}$ inférieur à 8, et l'on aura

$$k - n = r + k^{(r)} - n^{(r)},$$

ou

$$k - n = r + 1 + k^{(r)} - n^{(r)},$$

suivant qu'on aura été ou non obligé d'éviter le nombre premier p dans la suite des opérations.

Le nombre r des réductions à faire sera d'ailleurs au plus égal à $m-2$; on aura donc

$$k-n\leqslant m-1+k^{(r)}-n^{(r)},$$

formule où le nombre $m-1$ doit être remplacé par $m-2$, si l'on n'a pas eu à éviter p, et notamment si $p<8$.

Cela posé, on aura

$$m-1\leqslant\frac{\log k}{\log 2}-1;$$

il reste à évaluer $k^{(r)}-n^{(r)}$ pour chacune des valeurs de $k^{(r)}$ inférieure à 8.

46. 1° Soit $k^{(r)}=7$.

Si $p>5$, on pourra, dans les formules générales (6), (7), (8), poser $k^{(r)}=5+2$, $n^{(r)}\geqslant 4$, $k^{(r)}-n^{(r)}\leqslant 3$.

Si $p=5$, on posera $k^{(r)}=3+2+2$, $n^{(r)}\geqslant 2+1$, $k^{(r)}-n^{(r)}\leqslant 4$.

2° Si $k^{(r)}<7$ et >3, on aura $n^{(r)}\geqslant 2$. En effet, si $n^{(r)}$ était égal à 1, le groupe linéaire correspondant n'ayant qu'un indice, ses substitutions seraient échangeables entre elles. Il ne pourrait donc être isomorphe au groupe alterné Θ, qui ne jouit pas de cette propriété. On aura donc, suivant que $r^{(k)}=6$, 5 ou 4, $k^{(r)}-n^{(r)}\geqslant 4$, 3 ou 2.

3° Enfin si $k^{(r)}=3$, on aura $k^{(r)}-n^{(r)}\leqslant 2$.

On aura donc dans tous les cas

$$k^{(r)}-n^{(r)}\leqslant 4,$$

d'où la formule définitive

$$k-n\leqslant\frac{\log k}{\log 2}+3,$$

qui n'est autre que l'inégalité (4) que nous voulions établir.

V

Nous profitons de cette occasion pour rectifier la proposition suivante, que nous avons donnée dans notre *Traité des substitutions* (n° 84) :

Un groupe G *permutable aux substitutions d'un groupe n fois transitif* H *est au moins* $n-1$ *fois transitif.*

Cet énoncé doit être complété par l'exception suivante :

Néanmoins, si G *est un groupe simplement transitif de degré* 2^m, *formé par les substitutions*

$$| x_1,\ldots, x_m \quad x_1+\alpha_1,\ldots, x_m+\alpha_m | \bmod 2,$$

H *pourra être trois fois transitif.*

La nécessité de cette exception est évidente ; car on sait que le groupe linéaire de degré 2^m, formé par l'ensemble des substitutions permutables à G, est trois fois transitif.

Nous allons montrer que cette exception est la seule, en reprenant la démonstration de l'endroit cité, dont l'insuffisance ressortira d'elle-même chemin faisant.

Soient S l'une des substitutions de G; $C_1,\ldots, C_k$ ses divers cycles, y compris ceux qui ne contiennent qu'une lettre. Prenons un nombre de cycles $C_1,\ldots, C_\rho$, tel, qu'ils contiennent au moins n lettres, mais qu'en supprimant l'un d'entre eux, les précédents en contiennent seulement $n-\nu$, ν étant >0. Nous admettrons en premier lieu que l'on puisse choisir les cycles $C_1,\ldots, C_\rho$ de telle sorte que l'on ait $\nu>1$.

Soient, dans cette hypothèse, a, b,... les $n-\nu$ lettres de $C_1,\ldots, C_{\rho-1}$, d, e, ..., g les ν premières lettres de C_ρ. Le groupe H, étant n fois transitif, contient une substitution T qui laisse immobiles a, b, c,..., d, e,... et remplace g par une autre lettre arbitraire p; G, étant permutable à T, contiendra la substitution $T^{-1}ST$, et par suite la substitution $U=S^{-1}T^{-1}ST$, laquelle laisse immobiles les $n-2$ lettres a, b,..., e,... et remplace g par p. Mais H renferme une substitution V qui remplace les n lettres a, b,..., e,..., g, p par n lettres arbitraires α, β,..., ε,..., γ, π; et G contiendra $V^{-1}UV$, qui laisse immobiles $n-2$ lettres arbitraires α, β,..., ε,... et remplace l'une des lettres restantes, γ, par l'une quelconque des autres lettres restantes, π. Donc G est $n-1$ fois transitif.

Il reste à examiner le cas, omis dans notre ancienne démonstration, où l'on a nécessairement $\nu=1$. Suivons les conséquences de cette hypothèse, pour voir l'étendue de l'exception.

Tous les cycles de S *contiennent un même nombre* μ *de lettres.* En effet, supposons-les écrits plus haut, de manière à être ordonnés d'après le nombre décroissant de leurs lettres. Si le dernier cycle C_k contenait moins de lettres que le premier C_1, les cycles $C_1, C_2,\ldots, C_{\rho-1}$, contenant par hypothèse $n-1$ lettres, les cycles C_k, $C_2,\ldots, C_{\rho-1}$ en contiendraient $n-\nu$, ν étant >1. D'autre part, C_k contenant au moins une lettre, les cycles C_k, $C_2,\ldots, C_{\rho-1}$, C_1 en contiendraient au moins n. On voit donc qu'on pourrait, contrairement à l'hypothèse, faire en sorte que ν fût >1. On a d'ailleurs, par hypothèse, $\mu(\rho-1)=n-1$, donc μ *divise* $n-1$.

La substitution S étant l'une quelconque de celles de G, on voit que *toutes*

les substitutions de G (*l'unité exceptée*) *doivent être régulières, et déplacer toutes les lettres : de plus leur ordre doit diviser* $n-1$.

Cela posé, si le groupe G n'est pas transitif, le groupe H, dont les substitutions lui sont permutables, sera non primitif; il ne pourra donc être qu'une fois transitif, et le théorème sera vrai.

Soit au contraire G transitif, il ne pourra l'être qu'une fois; car toutes ses substitutions (sauf l'unité) déplaçant toutes les lettres, celles d'entre elles qui laissent une lettre immobile se réduisent à l'unité.

D'autre part, G est $n-2$ fois transitif; car H l'étant n fois, l'est *a fortiori* $n-1$ fois; et les cycles $C_1,\ldots, C_{\varrho-1}$ contiennent $n-1$ lettres, tandis que les cycles $C_1,\ldots, C_{\varrho-2}$ n'en contiennent que $n-1-\mu$; S étant choisie différente de l'unité, μ sera évidemment >1; en raisonnant sur $n-1$ comme précédemment sur n, on ne tombera donc pas sur le cas d'exception que nous discutons en ce moment.

Il résulte de là que n est au plus égal à 3. Mais si $n<3$, le théorème sera vérifié. Si $n=3$, les substitutions de G, dont l'ordre divise $n-1$, auront toutes pour ordre 2. Donc l'ordre du groupe G sera une puissance de 2, telle que 2^m. D'ailleurs il est transitif, et toutes ses substitutions déplacent toutes les lettres; donc le nombre des lettres qu'il contient est 2^m.

Soient maintenant $S=(ab)(cd)\ldots$ l'une des substitutions de G; S_1 une autre substitution de G, qui remplace a par une autre lettre quelconque c. La substitution SS_1 remplace b par c; mais elle est d'ordre 2; donc elle remplacera c par b; et comme S le remplace par d, S_1 remplacera d par b; on aura donc $S_1=(ac)(bd)\ldots$ et S_1 sera échangeable à S.

Donc les substitutions de G sont échangeables entre elles; donc (*Traité des substitutions*, 408) on pourra les mettre sous la forme

$$\left| x_1,\ldots, x_m \quad x_1+\alpha_1,\ldots, x_m+\alpha_m \right| \bmod 2.$$