BULLETIN DE LA S. M. F.

E. MAILLET

Des groupes transitifs de substitutions de degré N et de classe $N - 1$

Bulletin de la S. M. F., tome 26 (1898), p. 249-259

<http://www.numdam.org/item?id=BSMF_1898__26__249_0>

DES GROUPES TRANSITIFS DE SUBSTITUTIONS DE DEGRÉ N ET DE CLASSE N — 1.

Par M. E. MAILLET.

I.

Comme suite à ce que nous avons établi, soit dans notre Thèse de Doctorat, soit dans le *Bulletin de la Société mathématique* (1) au sujet de ces groupes, nous nous proposons d'indiquer ici quelques propriétés, parmi lesquelles nous mentionnerons le lemme I et les théorèmes suivants :

Soit G un groupe transitif de classe N — 1 et de degré N, H le sous-groupe des substitutions de G laissant une même lettre de G immobile :

I. *Si* G *est primitif et* $N = p^m r$ (*p et r premiers différents*), *on a* $r - 1 \equiv 0 \pmod p$, *et* $r \geq 11$ *quand* $p = 2$.

II. *Si* $N = \rho p$ (*p premier et premier à* $\rho > 1$), *on a* $\mathfrak{K} < \frac{p\delta}{p-1} \leq p$, δ *étant le plus grand commun diviseur de* $p - 1$ *et* $\mathcal{G}$, *en sorte que* $p \geq 3$. *Si, de plus,* G *est primitif, on a* $p - 1$ *non premier à* ρ, $\rho \geq p + 1$, $p > 5$; $p - 1$ *et* $\rho(\rho - 1)$ *ont un diviseur commun* > 2.

III. *Si* $N = \rho p^2$ (*p premier et premier à* $\rho > 1$), *on a* $\mathfrak{K} < \frac{p^2\delta}{p^2-1} < p^2(p-1)$, δ *étant le plus grand commun diviseur de* $(p-1)(p^2-1)$ *et* $\mathcal{G}$. *Quand* $p = 2$, G *est imprimitif et d'ordre* 12ρ *avec* $\rho = 3l + 1$. *Si, de plus,* G *est primitif, on a* $p^2 - 1$ *non premier à* ρ, $\rho \geq p^2 + 1$, *et, quand* $p = 3$, ρ *est pair.*

IV. *Si* G *est primitif et* $N \leq 401$, *on a* $N = p^m$ (*p premier*), *et* G *est un groupe linéaire à m indices réels.*

II.

THÉORÈME I. — *Un groupe* G *transitif de classe* N — 1 *et de*

(1) T. XXV, p. 16 et suiv.; 1897.

degré $N = p^m r$ (p *et* r *premiers différents*), *d'ordre* $\mathcal{G} = N\mathfrak{H}$, *ne peut exister que si* $\mathfrak{H} < \frac{2r-p-1}{2r-2}\nu' < \nu'$, *avec* $r - 1 \equiv 0 \pmod p$, *ou s'il est non primitif et renferme un sous-groupe invariant d'ordre* p^m, $r\nu_1\nu'$ *et* $r\nu_1$ *étant les ordres des groupes de substitutions de* G *permutables et échangeables respectivement à un sous-groupe d'ordre* r *de* G.

Soit

$$\mathcal{G} = r\nu_1\nu'(1 + nr),$$

d'après la formule de M. Sylow (1), G renfermant $1 + nr$ sous-groupes d'ordre r, et $r\nu_1$ étant l'ordre du sous-groupe des substitutions de G échangeables à une substitution d'ordre r. G renferme

$$\mathcal{G}\frac{r-1}{r\nu'}$$

substitutions d'ordre divisible par r, par suite de classe N et de plus (2) au moins $\frac{p+1}{2}(p^m + p - 2)$ substitutions d'ordre > 1 diviseur de p^m; par suite aussi de classe N, en supposant que G ne renferme pas un sous-groupe invariant d'ordre p^m. Il faudra donc

$$\mathfrak{H}p^m r\frac{r-1}{r\nu'} + \frac{p+1}{2}(p^m + p - 2) < p^m r$$

$$\mathfrak{H}\frac{r-1}{\nu'} + \frac{p+1}{2} < r,$$

$$\mathfrak{H} < \frac{2r-p-1}{2r-2}\nu' < \nu' < \delta, \tag{1}$$

car ν' divise δ, plus grand commun diviseur de $r - 1$ et $\mathcal{G}$.

On retrouve d'abord la condition connue (3) $r > \frac{p+1}{2}$. De plus, ν' n'est pas premier à p, puisque $\mathfrak{H} < \nu'$, et $r - 1 \equiv 0 \pmod p$.

Corollaire I. — Si $p = 2$, G ne peut être primitif que si le plus grand commun diviseur de $r - 1$ et $2^m(2^m - 1)$ est 8 ou ≥ 10. En particulier, on a $r \geq 11$.

---

(1) *Bull. Soc. Math.*, t. XXV, p. 193; 1897.
(2) *Bull. Soc. Math.*, t. XXV, p. 27-29; 1897.
(3) *Ibid.*

En effet, ν' divise $2^m(2^m r-1)$ et $2^m \cdot 2^m(r-1)$, par suite $2^m(2^m r-1-2^m r+2^m)=2^m(2^m-1)$ et $r-1$. Si $\mathfrak{K}$ est premier, on ne peut avoir $\nu_1 \nu' \equiv 0 \pmod{\mathfrak{K}}$, puisque (1) H est maximum dans G; donc $\nu'=2^\alpha$. On a d'ailleurs $\mathfrak{K} \neq 3$; donc $\mathfrak{K} \geqq 5$, $2^\alpha > 5\frac{2r-2}{2r-3}$, c'est-à-dire $\nu' \geqq 8$. Si $\mathfrak{K}$ n'est pas premier, on a $\nu' > \frac{2r-2}{2r-3}\mathfrak{K} > 9$.

Exemple : Si G est primitif, on n'a pas $N = 320 = 2^6 . 5$.

Remarque. — Quand $p=3$ et que G est primitif, ν' doit diviser $3^m(3^m-1)$ et $r-1$. Si $\mathfrak{K}$ est premier, on a $\nu'=3^\alpha$, avec $3^\alpha > 5\frac{2r-2}{2r-4}$. Si $\mathfrak{K}$ n'est pas premier, ou bien $\mathcal{G}$ est impair, et $\mathfrak{K} \geqq 25$, $\nu' > \frac{2r-2}{2r-4}25$, c'est-à-dire $\nu' \geqq 26$, ou bien $\mathcal{G}=4h+2$, $\mathfrak{K} \geqq 10$, $\nu' > 10$, ou bien $\mathcal{G}=4h$ et $3^m r \equiv 1 \pmod 4$ avec $\mathfrak{K} \geqq 4$, $\nu' > 4$.

Des remarques semblables ont lieu quand $p > 3$.

THÉORÈME II. — *Soit* $N=\rho p$ (p *premier et premier à* $\rho > 1$) : *un groupe* G *transitif de degré* N, *de classe* $N-1$, *d'ordre* $\mathcal{G}=N\mathfrak{K}$, *ne peut exister que si* $\mathfrak{K} < \frac{p\delta}{p-1} \leqq p$, δ *étant le plus grand commun diviseur de* $p-1$ *et* $\mathcal{G}$, *en sorte que* $p \geqq 3$; *si* $\mathcal{G}$ *est primitif, on a* $p-1$ *non premier à* ρ, $\rho \geqq p+1$ *et* $p > 5$.

En effet, on aura encore, d'après la formule de M. Sylow

$$\mathcal{G} = N\mathfrak{K} = \rho p \mathfrak{K} = p\nu_1\nu'(np+1), \tag{2}$$

ν_1, ν' ayant même signification qu'au théorème I. On aura

$$N\mathfrak{K}\frac{p-1}{p\nu'} < N, \qquad \mathfrak{K} < \frac{p\nu'}{p-1} \leqq \frac{p\delta}{p-1}. \tag{3}$$

Si G est primitif, on n'a pas $p-1$ premier à ρ, sans quoi ν' qui divise $p-1$ devrait diviser $\mathfrak{K}$ et l'on aurait $p \geqq 3$, $\mathfrak{K} < \frac{3}{2}\nu'$,

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

d'où $\mathfrak{K} = \nu'$, c'est-à-dire G non primitif (1). De plus, si G est primitif, on sait (2) que $\rho \geq p + 1$. Enfin, si $p = 3$, il faut $\mathfrak{K} = 2$ et $N - 1$ pair, et G n'est pas primitif; si $p = 5$, G ne pourrait être primitif (3) que si $\mathfrak{K} > 3$, par suite, d'après (3) si $\mathfrak{K} = 4$, c'est-à-dire $N - 1$ pair; mais l'on aurait ici, d'autre part, $p - 1 = 4$, par suite ρ et N pairs. On en conclut que G ne peut être primitif si $p = 5$.

Exemple : Si G est primitif, on n'a pas $N = 297 = 3^3.11$, parce que $11 - 1 = 10$ est premier à 3^3, ni $N = 315 = 3^2.5.7$ ni $N = 375 = 3.5^3$.

Corollaire I. — Si N est pair et a un diviseur premier p inférieur à tous les diviseurs de $N - 1$, G ne peut être transitif que si $N \equiv 0 \pmod{p^2}$.

Corollaire II. — Si N est impair, soit p son plus petit diviseur premier : G ne peut être primitif à moins que $N \equiv 0 \pmod{p^2}$.

Corollaire III. — G ne peut être primitif : 1° si $\nu' \leq 3$ ou si $\delta \leq 3$, *a fortiori* si $p - 1$ et $\rho(\rho - 1)$ ont pour plus grand commun diviseur 2, en particulier si $\rho = 4h + 3$ et $p - 1 = 2^m$, si $\rho = 12h' - 1$ et $p - 1 = 2^m 3^{m'}$, etc.; 2° si $\nu' \leq 4$ ou si $\delta \leq 4$.

En effet, le plus grand commun diviseur Δ de $p - 1$ et $\rho p(\rho p - 1)$ est celui de $p - 1$ et $\rho(\rho - 1)$: Δ est pair et l'on n'a $\Delta \leq 3$ que si $\Delta = 2$.

Quand $\nu' \leq 3$ ou $\delta \leq 3$, on a $p > 5$, et, d'après (3), $\mathfrak{K} \leq 3$, en sorte que G n'est pas primitif.

Quand $\nu' \leq 4$ ou $\delta \leq 4$, on a, d'après (3), $\mathfrak{K} \leq 4$, et

$$\mathfrak{K} < \frac{p\nu'}{p-1} \leq \frac{7\nu'}{6};$$

G ne pourrait être primitif que si $\mathfrak{K} \geq 4$, ce qui exige $\mathfrak{K} = 4 \leq \frac{7\nu'}{6}$,

---

(1) Alors, en effet, G renfermerait un groupe d'ordre $p\nu_1\nu'$ renfermant H ou un de ses transformés par les substitutions de G.

(2) *Bull. Soc. Math.*, t. XXV, p. 18; 1897.

(3) *Voir* notre Thèse de Doctorat, p. 65.

d'où $\nu' = 4$; H ne serait pas maximum dans G, ce qui est impossible.

Exemples : Quand G est primitif, on n'a pas

$$N = 260 = 2^2.5.13. \qquad \text{ni} \qquad N = 280 = 2^3.5.7.$$

III.

Lemme I. — Soit G un groupe quelconque d'ordre

$$\mathcal{G} \equiv 0 \pmod{p^2}, \qquad \text{avec} \qquad \mathcal{G} \not\equiv 0 \pmod{p^3},$$

p étant premier, et $\mathcal{G} = p^2\nu_1\nu'(1 + np)$, $p^2\nu_1\nu'$ et $p^2\nu_1$ étant respectivement les ordres des groupes H' et K des substitutions de G qui sont permutables à un sous-groupe H d'ordre p^2 de G ou échangeables aux substitutions de H. Si $\nu_1\nu' = \nu'_1\nu_2$, $p^2\nu'_1$ étant le plus grand commun diviseur des ordres des groupes des substitutions de H' échangeables à une substitution d'ordre p, G contient au moins

$$\mathcal{G}\frac{p^2-1}{p^2\zeta} \geq \mathcal{G}\frac{p^2-1}{p^2\delta} \tag{4}$$

substitutions d'ordre $\equiv 0 \pmod{p}$, ζ étant égal à ν' ou ν_2, et δ étant le plus grand commun diviseur de $\mathcal{G}$ et $p-1$ ou $(p-1)(p^2-1)$ respectivement, suivant que G contient ou non une substitution d'ordre p^2.

Il nous suffit, pour le voir, de généraliser un lemme que nous avons donné (1) antérieurement. Nous conservons, en principe, les mêmes notations que dans sa démonstration.

On a encore ici $1 + np = 1 + n_1p + n_2p^2$. Formant le groupe L des substitutions de G échangeables à une substitution S d'ordre p de H, on a $\mathcal{L} = p^2\nu''(1 + hp)$, $1 + hp$ étant le nombre des transformés de H qui contiennent S. Si $h > 0$, L est isomorphe à un groupe L' d'ordre $\frac{\mathcal{L}}{p}$ et de degré $\frac{\mathcal{L}}{p^2}$, où la substitution 1 correspond au sous-groupe (S) de L; L' contient (2) $\lambda \geq (1 + hp)\nu''$ substitutions d'ordre premier à p. On peut former un tableau Θ

(1) *Bull. Soc. Math.*, t. XXV, p. 20.
(2) *Bull. Soc. Math.*, t. XXV, p. 18; 1897.

de $(p-1)\lambda$ substitutions distinctes appartenant à L et d'ordre $\equiv 0 \pmod{p}$ et $\not\equiv 0 \pmod{p^2}$, tableau que l'on fait correspondre à (S).

De même, au groupe (S_1) des puissances d'une substitution S_1 d'ordre p non contenue dans (S), on fait correspondre un tableau ou ensemble Θ_1 de $(p-1)\lambda_1 \geqq (p-1)(1+h_1 p)\nu_1''$ substitutions distinctes d'ordre $\equiv 0 \pmod{p}$ et $\not\equiv 0 \pmod{p^2}$. Les substitutions de Θ_1 diffèrent de celles de Θ; et ainsi de suite.

Quand on aura $h = 0$, à l'ensemble des $p-1$ substitutions de (S), nous ferons correspondre l'ensemble θ des

$$\lambda'(p-1) \geqq (p-1)\nu'''$$

substitutions échangeables à S, d'ordre $\equiv 0 \pmod{p}$ et $\not\equiv 0 \pmod{p^2}$, appartenant au groupe d'ordre $p^2\nu'''$ des substitutions échangeables à S.

Enfin, soit T une substitution d'ordre p^2 de G. On a dans (T) $p(p-1)$ substitutions d'ordre p^2, et, puisque $p^2\nu_1$ est l'ordre du groupe K des substitutions de G échangeables à celles de (T), et que K contient au moins ν_1 substitutions distinctes d'ordre premier à p, (T) contient $\lambda''(p^2-p) \geqq \nu_1(p^2-p)$ substitutions d'ordre $\equiv 0 \pmod{p^2}$ et non contenues dans un autre groupe de G semblable à (K). A l'ensemble de ces $p(p-1)$ substitutions d'ordre p^2 de G, nous faisons correspondre l'ensemble Θ' de ces $\lambda''(p^2-p)$ substitutions.

Nous formerons encore les ensembles A, B, C, l'ensemble C comprenant tous les ensembles Θ, θ, Θ' ci-dessus obtenus. C contient

$$D \geqq \Sigma(p-1)\nu''(1+hp) + (1+np)\nu_1(p^2-p)\eta$$

substitutions distinctes d'ordre $\equiv 0 \pmod{p}$, où η est 1 ou 0 suivant que G contient ou non des substitutions d'ordre p^2.

Si les quantités ν'' qui sont toutes multiples de ν_1 sont de la forme $\nu'' = \nu_1 l\mu''$, $\nu_1 l$ étant leur plus grand commun diviseur, on aura

$$\Sigma(p-1)\nu''(1+hp) = (p-1)\nu_1 l \Sigma\mu''(1+hp) \geqq (p-1)\nu_1 l(1+np)(\varepsilon p+1)$$

et

$$(5)\quad D \geqq (p-1)\nu_1(1+np)[l(\varepsilon p+1)+\eta p] = \mathcal{G}\frac{p-1}{p^2\nu'}[l(\varepsilon p+1)+\eta p],$$

avec $l \geqq 1$ et $\varepsilon + \eta = 1$.

Le lemme I résulte de là immédiatement comme nous allons le voir. Mais la formule (5) pourra donner parfois une limite plus avantageuse.

En effet, si $p^2\nu_1''$ est l'ordre du groupe des substitutions de H' échangeables à une substitution d'ordre p de H', on aura $l\nu_1$ multiple de ν_1' et $l\nu_1 \geqq \nu_1'$.

Enfin, on remarquera que (1) ν' doit diviser $(p^2-1)(p-1)$ si G ne contient pas de substitution d'ordre p^2, et $p-1$ si G en contient. Dans le premier cas,

$$(6) \qquad D \geqq \mathcal{G}\frac{p-1}{p^2\nu'}\, l(p+1) \geqq \mathcal{G}\frac{p^2-1}{p^2}\,\frac{l\nu_1}{\nu_1\nu'} \geqq \mathcal{G}\frac{p^2-1}{p^2\nu_2},$$

puisque

$$\frac{\nu_1\nu'}{l\nu_1} \leqq \frac{\nu_1\nu'}{\nu_1'} = \nu_2;$$

d'ailleurs ν_1 divise ν_1', en sorte que ν_2 divise ν', par suite δ; dans le second cas,

$$(7) \qquad D \geqq \mathcal{G}\frac{p^2-1}{p^2\nu'};$$

en sorte que, dans les deux cas,

$$(8) \qquad D \geqq \mathcal{G}\frac{p^2-1}{p^2\delta}.$$

C. Q. F. D.

Ce lemme nous permet de formuler pour les groupes de degré $p^m r^2$ (p et r premiers différents) ou de degré ρp des théorèmes analogues aux théorèmes I et II.

Théorème III. — *Un groupe* G *transitif de classe* $N-1$ *et de degré* $N = p^m r^2$ (p *et* r *premiers différents*), *d'ordre* $\mathcal{G} = N\mathcal{K}$, *ne peut exister que si* $\mathcal{K} < \frac{2r^2-p-1}{2r^2-2}\zeta < \zeta$, *avec* $r^2-1 \equiv 0 \pmod p$, *ou s'il est non primitif et renferme un sous-groupe invariant d'ordre* p^m, ζ *ayant même signification qu'au lemme I.*

D'après le lemme I, on aura, en raisonnant comme au théorème I,

$$(9) \qquad \mathcal{K} < \frac{2r^2-p-1}{2r^2-2}\zeta < \zeta < \delta,$$

(1) *Bull. Soc. Math.*, t. XXV, p. 204; 1897.

où δ a même signification qu'au lemme I. On retrouve la condition connue (¹) $r^2 > \frac{p+1}{2}$. De plus ζ n'est pas premier à p, puisque $\mathfrak{K} < \zeta$, et $r^2 - 1 \equiv 0 \pmod{p}$.

Corollaire I. — Si $p = 2$, G ne peut être primitif que si le plus grand commun diviseur de $(r-1)(r^2-1)$ et $2^m(2^m r^2 - 1)$ est 8 ou $\geqq 10$.

En effet, si $\mathfrak{K}$ est premier, $\nu_1 \nu' = \nu'_1 \nu_2$ n'est pas $\equiv 0 \pmod{\mathfrak{K}}$; donc $\zeta = 2^\alpha$, en sorte que $\mathfrak{K} \geqq 5$, $2^\alpha > 5\frac{2r^2-2}{2r^2-3}$, c'est-à-dire $\zeta \geqq 8$. Si $\mathfrak{K}$ n'est pas premier, on a

$$\zeta > \frac{2r^2-2}{2r^2-3}\mathfrak{K} > 9.$$

On a ici, quand $p \geqq 3$, une remarque analogue à celle du théorème I.

Théorème IV. — *Soit* $N = \rho p^2$ (p *premier et premier à* $\rho < 1$): *un groupe* G *transitif de degré* N, *de classe* $N - 1$, *d'ordre* $\mathcal{G} = N\mathfrak{K}$, *ne peut exister que si* $\mathfrak{K} < \frac{p^2\delta}{p^2-1} \leqq p^2(p-1)$, δ *ayant même signification qu'au lemme* I. *De plus, si* G *est primitif, on a* $p \geqq 3$, $p^2 - 1$ *non premier à* ρ, $\rho \geqq p^2 + 1$.

On raisonnera comme au théorème II : on remarquera que si G contient des substitutions d'ordre p^2, δ doit diviser $p-1$, et $\mathfrak{K} < p$, en sorte que $p \geqq 3$; quand G est primitif, il faut dans ce cas $p - 1$ non premier à ρ et $p > 5$.

Corollaire I. — Un groupe G transitif de degré $N = 4\rho$ (ρ impair) et de classe $N - 1$ est imprimitif et d'ordre 12ρ, avec

$$\rho = 3l + 1.$$

En effet, on a $\mathfrak{K} < 4$, c'est-à-dire $\mathfrak{K} = 3$, $\mathcal{G} = 12\rho$, $\rho = 3l + 1$. G n'est pas primitif, puisque $\mathfrak{K} = 3$ et $\rho > 1$.

Exemple : G ne peut être primitif quand $N = 324 = 2^2.3^4$ ou $N = 364 = 2^2.7.13$ ou $N = 396 = 2^2.3^2.11$.

(¹) *Bull. Soc. Math.*, t. XXV, p. 27-29; 1897.

Corollaire II. — Un groupe G primitif de degré $N = 9\rho$ et de classe $N - 1$ est de degré pair.

En effet, d'après le théorème IV, $9 - 1 = 8$ ne peut être premier à ρ.

Exemple : G ne peut être primitif si $N = 225 = 3^2.5^2$.

On pourrait encore obtenir ici des corollaires analogues aux corollaires I, II et III du théorème II. Nous croyons inutile de les énoncer.

IV.

En appliquant ce qui précède et les résultats déjà obtenus par nous antérieurement (1), on établit de suite le théorème suivant :

THÉORÈME V. — *Les seuls groupes primitifs de classe* $N - 1$ *et de degré* $N \leqq 401$ *sont ceux de degré égal à* p^m (*p étant premier*), *et sont linéaires à indices réels.*

En effet, les seules valeurs de N qui puissent faire exception (2) seraient $N = 216 = 2^3 3^3$ et $N = 288 = 3^2 2^5$.

1° $N = 216 = 2^3 3^3$.

On a $N - 1 = 5.43 = 215$, en sorte que $\mathcal{G} = N\mathfrak{K} = 216.5$ quand G est primitif (3).

On a alors (4)

$$\mathcal{G} = 3^3\nu(1 + 3n_1 + 3^2 n_2 + 3^3 n_3) = 3^3\nu(1 + 3n),$$

où $3^3\nu$ est l'ordre du groupe des substitutions de G permutables à un groupe P d'ordre 3^3 de G. On a, puisque G est primitif, ν premier à 5 et $n > 0$, en sorte que $1 + 3n$ est égal à 10 ou 40.

Soit $1 + 3n = 40$; on a $n_1 \neq 0$ et G contient un groupe P_1 semblable à P et ayant avec P un sous-groupe invariant P' d'ordre 3^2. Le groupe (P, P_1), dérivé de P et P_1 serait imprimitif, d'ordre $\varpi = 3^3\mu(1 + 3n') < \mathcal{G}$, et l'on aurait $n' > 0$, ce qui exigerait, puisque cet ordre est premier à 5 et que G ne peut contenir de

(1) *Loc. cit.*

(2) *Voir* notre Thèse de Doctorat, p. 55, et *Bull. Soc. math.*, t. XXV, p. 16 et suiv.; 1897.

(3) Thèse de Doctorat, p. 55.

(4) *Ann. Fac. Sc. Toulouse,* D.p. 7; 1895.

sous-groupe invariant d'ordre 216, $\mu(1+3n')=4$, $\varpi=3^3 2^3$. (P, P_1) ne contient aucun sous-groupe invariant dans G et est maximum dans G.

Soit $1+3n=10$: G contient encore un sous-groupe d'ordre $\varpi=3^3 2^2$ maximum dans G et ne contenant aucun sous-groupe invariant dans G.

Dans les deux cas, G sera donc (1) holoédriquement isomorphe à un groupe primitif de degré 10 et d'ordre $10.3^3.2^2$ que l'on sait ne pas exister (2).

2° $N=288=3^2.2^5$. — Conservons les notations du lemme I en prenant $p=3$. On a $N-1=287=7.41$. D'après (9),

$$\mathfrak{K}<\frac{15}{16}\zeta<\delta.$$

Puisque $\mathfrak{K}\geqq 7$, il faut $\delta>7$. On a $p-1=2$, et G ne contient pas de substitution d'ordre 9. Alors $(p-1)(p^2-1)=16$, ζ divise 16, $\mathfrak{K}=7$, $\mathcal{G}=3^2.2^5.7$; de plus $\zeta>\frac{16}{15}\cdot 7$, d'où $\zeta\geqq 8$.

On a

$$\mathcal{G}=3^2\nu'_1\nu_2(1+3n),$$

avec $n>0$ et $1+3n\equiv 0 \pmod 7$, puisque G est primitif. On n'a pas, pour la même raison, $\nu'_1\nu_2=2^5$, et $\nu'_1\nu_2$ divise 16, en sorte que $1+3n\geqq 28$, $\nu'_1\nu_2\leqq 8$; puisque $\nu_2=\zeta$, $\nu_2=8$, $\nu'_1=1$. D'après la signification de ν_2 et de ν'_1, le sous-groupe L des substitutions de G permutables à un sous-groupe M d'ordre $\mathfrak{M}=3^2$ de G est d'ordre $\mathfrak{L}=3^2.2^3$. Nous nous contenterons ici d'examiner le cas où L ne renferme pas d'autres substitutions échangeables à une d'ordre 3 de M que celles de M.

L ne renferme aucun sous-groupe invariant M_1 d'ordre 2^φ avec $\varphi\leqq 3$, sans quoi M_1 étant invariant par M, et M par M_1, avec $\mathfrak{M}$ premier à $\mathfrak{M}_1$, on sait (3) que les substitutions de M seraient échangeables à celles de M_1, ce qui est impossible, puisque $\nu'_1=1$. Donc (4) L est holoédriquement isomorphe à un groupe L′ tran-

(1) W. Dyck, *Math. Ann.*, t. XX et XXII, et notre Thèse de Doctorat, p. 12 et 15.

(2) Jordan, *Comptes rendus*, 1871 et 1872.

(3) *Voir* par ex. *Ann. Fac. Sc. Toul.*, 1895, D.17.

(4) *Voir* par ex. W. Dyck, *Math. Ann.*, t. XX et XXII, et notre Thèse de Doctorat, p. 12 et 15.

sitif, de degré 9 et d'ordre 9.8, dont les substitutions d'ordre 3 sont de classe 9, et contenues dans le groupe M′ d'ordre 9 correspondant à M dans L′. L′ ne contient pas de substitutions d'ordre $\equiv 0 \pmod 3$ et non contenues dans M′, en sorte que L′ et L contiennent au moins $9.8 - 9 = 63$ substitutions distinctes d'ordre diviseur de 2^3.

Or, un sous-groupe de G d'ordre 2^5 ne peut avoir en commun avec L plus de 2^3 substitutions. Il contiendra donc au moins $2^5 - 2^3 = 24$ substitutions d'ordre diviseur de 2^5 et > 1 non contenues dans L.

G renferme ainsi au moins $63 + 24 = 87$ substitutions distinctes d'ordre > 1 et diviseur de 2^5.

D'autre part, d'après la formule (6), G renferme au moins $7.2^5.3^2\frac{3^2-1}{3^2.2^3} = 7.2^5 = 224$ substitutions d'ordre non premier à 3, par suite de classe N. Donc G devrait renfermer au moins $87 + 224 = 311$ substitutions de classe N, alors qu'il n'en renferme pas plus de 287. Donc G ne peut exister. C. Q. F. D.