BULLETIN DE LA S. M. F.

ED. MAILLET

Sur les groupes de substitutions deux fois transitifs à trois degrés

Bulletin de la S. M. F., tome 25 (1897), p. 189-208
<http://www.numdam.org/item?id=BSMF_1897__25__189_0>

© Bulletin de la S. M. F., 1897, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (http://smf.emath.fr/Publications/Bulletin/Presentation.html) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

SUR LES GROUPES DE SUBSTITUTIONS DEUX FOIS TRANSITIFS A TROIS DEGRÉS;

Par M. Ed. Maillet.

1.

Définition. — Si dans un groupe quelconque G de substitutions de degré N on peut trouver (en laissant de côté le groupe formé de la substitution 1) des groupes déplaçant N, $N-u_1$, $N-u_2, \ldots, N-u_{\lambda-1}$ lettres, avec $0<u_1<u_2<\ldots<u_{\lambda-1}$, et non $N-u_\lambda$ lettres, avec u_λ différent de $0, u_1, u_2, \ldots, u_{\lambda-1}$, G est dit *un groupe à λ degrés*. Ainsi, un groupe régulier de degré N est à un degré; un groupe de classe $N-1$ et de degré N est à deux degrés, etc. D'après un théorème connu [1], l'ordre $\mathcal{G}$ de C divise

$$N(N-u_1)(N-u_2)\ldots(N-u_{\lambda-1}).$$

Nous nous proposons d'étudier ici les groupes deux fois transitifs de degré N et de classe $N-u$ à trois degrés, et d'établir en particulier à leur sujet les propriétés suivantes :

1. $u-1$ divise $N-1$, et $u(u-1)$ divise $N(N-1)$; par suite, si u est impair, N est impair; si N est pair, u est pair. On a

$$N \geqq 1+\frac{u-1}{2}\left(1+\sqrt{1+4u}\right).$$

Si $u=3$, N est d'une des formes $6h+1$ ou $6h+3$; si $u=4$, N est d'une des formes $12h+1$ ou $12h+4$.

2. Si $\mathcal{G}=N(N-1)\mathcal{H}$, G renferme un nombre de substitutions de classe N égal à

$$\mathcal{G}\left[\frac{1}{u-1}-\frac{\mathcal{H}-1}{\mathcal{H}(u-1)u}-\frac{N-u}{\mathcal{H}(u-1)(N-1)}\right]-1$$
$$=\mathcal{G}\left[\frac{1}{u}+\frac{1}{\mathcal{H}(u-1)u}-\frac{N-u}{\mathcal{H}(u-1)(N-1)}\right]-1<\frac{\mathcal{G}}{u}-1.$$

---

[1] *Ann. Fac. Sc. Toulouse*, 1895, D.8.

3. Si $\mathcal{G} = N(N-1)\mathcal{K}$, on a pour $N = 4h + 2$, $N - u = 4h_1$ et $\mathcal{K}$ pair.

4. Si $N = \rho f$ (f premier impair et premier à ρ) et si l'ordre $\mathcal{G}$ d'un groupe G deux fois transitif à trois degrés de degré N et de classe $N - u$, ou *a fortiori* le nombre $N(N-1)(N-u)$ est $\not\equiv 0 \pmod{f^2}$, on a $u < \frac{fd}{f-1} \leqq f$, d étant le plus grand commun diviseur de $\mathcal{G}$ et $f - 1$, ou *a fortiori* de $N(N-1)(N-u)$ et $f - 1$.

Si $u > 2$, on a $d > \frac{f-1}{f} u \geqq 2$, et en particulier l'on ne peut avoir $f = 3$ que si $\mathcal{G} \equiv 0 \pmod 9$.

Pour $u \geqq 2$, G ne peut exister que pour des valeurs de f et u limitées en fonction de ρ, à moins que $\mathcal{G}$ ne soit multiple de $\rho f(\rho f - 1)\frac{\rho f - u}{\delta}$, δ étant le plus grand commun diviseur de ρu et $\rho f - u$; $\rho(\rho f - 1)$ est divisible par $u(u-1)$, et u est pair si ρ est pair.

5. Si $N = f$ (f premier impair) il faut $\mathcal{G} = f(f-1)(f-u)$, $f - 1 \equiv 0 \bmod u(u-1)$. De plus, si $f = 4h + 3$, il faut $u = 4h' + 3$. Enfin, quel que soit f, on n'a pas $\frac{f-1}{u}$ impair, ni $f - u = 4l + 2$.

6. Si $N - u = fp$ ($u \geqq 3$, f et p premiers différents), le degré N est $fp + p + 1$ ou $fp + f + 1$.

Soit $2 < f < p$; si $u = p + 1$, on a

$$f + 1 = 2^m, \qquad \mathcal{G} = (fp + p + 1)(fp + p)f,$$

$p + 1$ diviseur de $f(f+1)$ et divisible par f; si $u = f + 1$, on a $f + 1$ diviseur de $p + 1$ et $\mathcal{G} \equiv 0 \pmod p$ exige $p + 1 = 2^m$, ou f diviseur de $p - 1$.

Si $N - u = 2p$ ($u \geqq 3$, p premier impair) on a $u = 3$, $N = 2p + 3$ et $p = 36k + 17$.

7. Si $N - u = p^2$ (p premier impair) on a $u = p + 1 = 2^m$, $N = p^2 + p + 1$.

8. Si $u = 3$, on n'a $N - 3 = 4p$ (p et N premiers impairs) que si $N = 48h + 7$.

9. Si $u = 3$, $N \leqq 103$, N est égal à 33, $2^m - 1$ ou 3^μ.

Nous croyons devoir signaler que l'étude du cas où $N \leqq 103$, avec $u > 3$, pourrait de même être faite à l'aide des propriétés qui précèdent : nous laissons ce soin à d'autres.

II.

Soit G un groupe transitif à λ degrés, H le groupe des substitutions de G qui laissent une même lettre de G immobile : H est à $\lambda - 1$ degrés.

Si $\lambda = 2$, et si G est de classe $N - u$ et de degré N, $\mathcal{G} = N\mathcal{H}$; H est à un degré et $\mathcal{H}$ divise $N - u$. G admet [1] une répartition de ses lettres en systèmes de non-primitivité u à u, et u divise N et $N - u$, les u lettres de G que H laisse immobiles formant un système : le groupe des substitutions opérées par G entre les systèmes est de degré $\frac{N}{u}$; G ne peut être primitif que si $u = 1$: c'est alors un groupe de classe $N - 1$ et de degré N.

Si $\lambda = 3$, et si G est deux fois transitif, $\mathcal{G} = N(N-1)\mathcal{K}$, $\mathcal{K}$ étant l'ordre du groupe K des substitutions de G qui laissent 2, par suite u lettres de G immobiles, G étant de classe $N - u$: $\mathcal{K}$ divise $N - u$. H étant transitif et à deux degrés, $N - 1 - (N - u) = u - 1$ divise $N - 1$ et $N - u$, et K possède $\frac{N-1}{u-1}$ transformés distincts par les substitutions de H et appartenant à H. Or H possède N transformés distincts par les substitutions de G, lesquels renferment chacun $\frac{N-1}{u-1}$ transformés distincts de K. En considérant les N transformés de H on voit que G contient $N\frac{N-1}{u-1}$ transformés de K qui sont identiques u à u, puisque chacun laisse exactement u lettres de G immobiles, et, par suite, appartient à u transformés de H exactement. On en conclut que $u(u-1)$ divise $N(N-1)$.

Alors si u est impair, $u - 1$, $N - 1$ et $N - u$ sont pairs; si N est pair, $N - 1$ et $u - 1$ sont impairs et u est pair. Donc :

Théorème I. — *Soit* G *un groupe deux fois transitif à trois*

---

[1] *Voir*, par exemple, *Ann. Fac. Sc. Toulouse*, 1895, D.18.

degrés de classe $N-u$ *et de degré* N; $u-1$ *divise* $N-1$, *et* $u(u-1)$ *divise* $N(N-1)$. *Par suite, si* u *est impair,* N *est impair et* $N-u$ *pair; si* N *est pair,* u *et* $N-u$ *sont pairs.*

Exemples : Si $u=3$, N est d'une des formes $6h+1$ ou $6h+3$; si $u=4$, N est d'une des formes $12h+1$ ou $12h+4$.

Corollaire I. — Si $N-u=f_1f_2\ldots f_\lambda$, où $f_1, f_2, \ldots, f_\lambda$ sont des nombres premiers, différents ou non, et si $f'_1, f'_2, \ldots, f'_\mu, f'_{\mu+1}, \ldots, f'_\lambda$ désignent ces λ facteurs dans un ordre différent ou non, on a $u=f'_1f'_2\ldots f'_\mu+1$ diviseur de $f'_{\mu+1}\ldots f'_\lambda(f'_{\mu+1}\ldots f'_\lambda+1)$, μ étant un des nombres $1, 2, \ldots, \lambda-1$ si $u>2$.

Corollaire II. — Le degré N de G est limité inférieurement en fonction de u par les inégalités $N \geqq 1+\frac{u-1}{2}\left(1+\sqrt{1+4u}\right)$ et $N-1 \geqq 3(u-1) \geqq 2u$, dès que $u \geqq 3$.

Il suffit de remarquer que $u-1$ est premier à u qui divise $N(N-1)$ et $(N-u)(N-1)$, en sorte que $(u-1)^2u$ divise $(N-u)(N-1)$ et $(u-1)^2u \leqq (N-u)(N-1)$.

De plus on a $N>u$ et $N-1 \geqq 2(u-1)$; on n'aurait $(N-1)=2(u-1)$ que si $u(u-1)$ divisait $(2u-2)(2u-1)$, ce qui donne $u=2$. Donc $N-1 \geqq 3(u-1) \geqq 2u$ dès que $u \geqq 3$.

Théorème II. — *Soit* G *un groupe deux fois transitif à trois degrés, d'ordre* $\mathcal{G}=N(N-1)\mathcal{K}$, *de classe* $N-u$; G *renferme un nombre de substitutions de classe* N *égal à*

$$\mathcal{G}\left[\frac{1}{u-1}-\frac{\mathcal{K}-1}{\mathcal{K}(u-1)u}-\frac{N-u}{\mathcal{K}(u-1)(N-1)}\right]-1$$
$$=\mathcal{G}\left[\frac{1}{u}+\frac{1}{\mathcal{K}(u-1)u}-\frac{N-u}{\mathcal{K}(u-1)(N-1)}\right]-1<\frac{\mathcal{G}}{u}-1.$$

En effet, H renferme $\frac{\mathcal{K}-1}{u-1}(N-1)=\frac{\mathcal{K}-1}{\mathcal{K}(u-1)}\mathcal{K}$ substitutions de classe $N-u$, et, par suite,

$$\mathcal{K}-1-\mathcal{K}\frac{\mathcal{K}-1}{\mathcal{K}(u-1)}=\mathcal{K}\frac{\mathcal{K}(u-2)+1}{\mathcal{K}(u-1)}-1$$

substitutions de classe $N-1$. G contiendra

$$(1) \qquad (\mathcal{K}-1)\frac{N(N-1)}{u(u-1)}$$

substitutions distinctes de classe $N - u$, et

$$(2) \qquad \mathcal{G}\frac{\mathcal{K}(u-2)+1}{\mathcal{K}(u-1)} - N = \mathcal{G}\frac{u-2}{u-1} + \frac{N(N-u)}{u-1}$$

substitutions de classe $N - 1$, soit en tout

$$\Sigma = \mathcal{G}\left[\frac{1}{u-1} - \frac{\mathcal{K}-1}{\mathcal{K}u(u-1)} - \frac{N-u}{\mathcal{K}(u-1)(N-1)}\right] - 1$$

substitutions de classe N.

Or

$$\frac{1}{u-1} - \frac{\mathcal{K}-1}{\mathcal{K}u(u-1)} = \frac{1}{u-1} - \frac{1}{u(u-1)} + \frac{1}{\mathcal{K}u(u-1)} = \frac{1}{u} + \frac{1}{\mathcal{K}u(u-1)}$$

et

$$\frac{1}{\mathcal{K}u(u-1)} - \frac{N-u}{\mathcal{K}(u-1)(N-1)}$$
$$= \frac{1}{\mathcal{K}(u-1)}\left(\frac{1}{u} - \frac{N-u}{N-1}\right) = \frac{N-1-u(N-u)}{\mathcal{K}u(u-1)(N-1)}.$$

D'après le corollaire II du théorème I, on a, puisque $u \geqq 2$ et $N > 3$, $u(N-u) \geqq 2(N-2) > N-1$, et

$$(3) \qquad \Sigma + 1 = \mathcal{G}\left[\frac{1}{u} + \frac{N-1-u(N-u)}{\mathcal{K}u(u-1)(N-1)}\right] < \frac{\mathcal{G}}{u}.$$

C. Q. F. D.

Lemme I. — Soit G un groupe d'ordre $\mathcal{G}$ divisible par le nombre premier f sans l'être par f^2, f^{ν_1} l'ordre du groupe M des substitutions de G échangeables à toutes les puissances d'une substitution d'ordre f formant un groupe F, $f^{\nu_1 \nu'}$ l'ordre du groupe L des substitutions de G permutables à F; G contient

$$\mathcal{G}\frac{f-1}{f^{\nu'}} \geqq \mathcal{G}\frac{f-1}{f^{\delta}}$$

substitutions d'ordre $\equiv 0 \pmod{f}$, où ν' divise le plus grand commun diviseur δ de $\mathcal{G}$ et $f-1$.

En effet, d'après M. Sylow [1],

$$\mathcal{G} = f^{\nu_1 \nu'}(1 + nf),$$

[1] *Math. Ann.*, t. V, p. 584.

où $1 + nf$ est le nombre des sous-groupes d'ordre f de G, tous transformés de F par les substitutions de G. Le groupe des substitutions échangeables à celles d'un groupe d'ordre f et le groupe des substitutions permutables à ce groupe sont respectivement transformés de M et L par une substitution de G.

M et ses $1 + nf$ transformés contiennent chacun $(f - 1)\nu_1$ substitutions d'ordre $\equiv 0 \pmod{f}$, soit en tout $(1 + nf)(f - 1)\nu_1$ substitutions, toutes distinctes; toute substitution de G d'ordre $\equiv 0 \pmod{f}$ fait partie de ces substitutions, dont le nombre est bien $\mathcal{G}\frac{f-1}{f\nu'}$.

Enfin toute substitution de F autre que l'unité ayant exactement ν' transformées distinctes par les substitutions de L, ν' divise $f - 1$ et $\mathcal{G}$, par suite leur plus grand commun diviseur δ.

Nous croyons d'ailleurs ce lemme connu.

Lemme II. — Dans un groupe G de degrés $N, N_1, N_2, \ldots, N_\mu$, avec $N > N_1 > N_2 > \ldots > N_\mu$, si $N_\lambda > N_\mu$ est le plus petit degré de G qui soit divisible par 4, tout sous-groupe de G de degré $< N_\lambda$ est d'ordre $\not\equiv 0 \pmod{4}$. Si aucun des degrés de G n'est divisible par 4, G et ses sous-groupes ont leur ordre $\not\equiv 0 \pmod{4}$.

Car un groupe dont aucun degré n'est divisible par 4 ne contient pas de substitution paire d'ordre 2 : si son ordre est pair, il contient une substitution d'ordre 2 impaire, par suite un sous-groupe invariant d'ordre moitié moindre et impair, ce sous-groupe ne contenant que des substitutions paires. C. Q. F. D.

Corollaire I. — Parmi les degrés d'un groupe primitif G, de degré N pair, il y en a un divisible par 4.

Car l'ordre d'un groupe primitif de degré pair est divisible par 4.

Corollaire II. — Dans un groupe G deux fois transitif à trois degrés d'ordre $\mathcal{G} = N(N - 1)\mathfrak{X}$, de classe $N - u$ et de degré N, si $N = 4h + 2$, on a $N - u = 4h_1$, et $\mathfrak{X}$ pair.

Théorème III. — *Un groupe* G *deux fois transitif à trois degrés, de degré* $N = f\varphi$ (f *et* φ *premiers impairs et différents*), *ne peut renfermer de substitution d'ordre* $f\varphi$, *quand sa classe*

$N - u (u \geqq 2)$ *est première à* N, *que si son ordre*

$$\mathcal{G} = f\varphi(f\varphi - 1)(f\varphi - u),$$

si $f\varphi - 1$ *est divisible par* $u(u-1)$, *et si* u *est un diviseur commun à* $f - 1$ *et* $\varphi - 1$; *en particulier, si* $u = 2$, G *doit être trois fois transitif avec* $f\varphi - 1 = 2^m$ (¹).

La démonstration repose sur la considération des égalités

$$\mathcal{G} = N(N-1)\mathcal{H} = f\nu(af+1) = \varphi n(\alpha\varphi + 1)$$

avec $a > 0$, $\alpha > 0$, déduite de la formule de MM. Mathieu et Sylow, et si l'on pose $k\mathcal{H} = N - u$, sur la considération des égalités

$$k\mathcal{G} = f\varphi(f\varphi - 1)(f\varphi - u), \qquad k\nu = u\varphi + lf, \qquad kn = uf + \lambda\varphi.$$

Théorème IV. — *Il n'existe aucun groupe* G *d'ordre* $\mathcal{G}$ *et de degré* $f\varphi$ (f *et* φ *premiers impairs et différents*) *et de classe* $f\varphi - u$, *avec* $f\varphi - u$ *premier à* $f\varphi$, *deux fois transitif à trois degrés qui ne renferme une substitution d'ordre* $f\varphi$: 1° *quand* $u \geqq 3$, *si* $f - 1$ *ou* $\varphi - 1$ *n'a avec* $\mathcal{G}$, *par suite* a fortiori *avec* $\varphi(N-1)(N-u)$ *ou* $f(N-1)(N-u)$ *respectivement que le plus grand commun diviseur* 2; 2° *quand* $u = 2$, *si* $f - 1$ *n'a avec* $\mathcal{G}$ *ou,* a fortiori, *avec* $\varphi(N-1)(N-u)$ *que le plus grand commun diviseur* 2, *et si en même temps :* 1° *ou bien* $\varphi < 2f + 1$; 2° *ou bien le plus grand commun diviseur de* $\varphi - 1$ *et* $\mathcal{G}$, *ou* a fortiori *de* $\varphi - 1$ *et* $f(N-1)(N-u)$ *est* $\leqq 4$.

Il suffit, en effet, de remarquer que si, d'après la formule de MM. Mathieu et Sylow,

$$\mathcal{G} = f\nu(af+1) = \varphi n(\alpha\varphi + 1),$$

G renferme, d'après le lemme I, $\mathcal{G}\frac{f-1}{f\nu}$ substitutions d'ordre f et $\mathcal{G}\frac{\varphi - 1}{\varphi n}$ substitutions d'ordre φ : si d est le plus grand commun

---

(¹) Le théorème est encore vrai quand $u \leqq 4$ et qu'on suppose seulement G transitif à trois degrés N, $N - 1$, $N - u$, à moins que G ne contienne un sous-groupe invariant d'ordre f ou φ : la démonstration est presque identique.

Voir aussi notre Thèse de doctorat, p. 78-80.

diviseur de $\mathcal{G}$ et $f-1$, δ celui de $\mathcal{G}$ et $\varphi-1$, on aura, d'après le théorème II,

$$(4)\qquad \left\{\begin{aligned} \frac{1}{u} &> \frac{1}{u} + \frac{1}{\mathcal{H}u(u-1)} - \frac{N-u}{\mathcal{H}(u-1)(N-1)} \\ &> \frac{f-1}{\nu f} + \frac{\varphi-1}{n\varphi} \geqq \frac{f-1}{df} + \frac{\varphi-1}{\delta\varphi}. \end{aligned}\right.$$

Le théorème résulte immédiatement de ces inégalités.

Théorème V. — *Si* $N = \rho f$ *(f premier impair et premier à* ρ*) et si l'ordre* $\mathcal{G}$ *d'un groupe* G *deux fois transitif à trois degrés de degré* N *et de classe* $N-u$, *ou,* a fortiori, *le nombre* $N(N-1)(N-u)$ *est* $\not\equiv 0 \pmod{f^2}$, *on a* $u < \frac{fd}{f-1} \leqq f$, *d étant le plus grand commun diviseur de* $\mathcal{G}$ *et* $f-1$, *ou,* a fortiori *de* $N(N-1)(N-u)$ *et* $f-1$. *De plus, si* $u > 2$, *on a* $d > \frac{f-1}{f}u \geqq 2$, *et, en particulier, l'on ne peut avoir* $f = 3$ *que si* $\mathcal{G}$ *est* $\equiv 0 \pmod 9$.

En effet, si, d'après la formule de MM. Mathieu et Sylow et le lemme I,

$$\mathcal{G} = f\nu_1\nu'(af+1)$$

où $f\nu_1$ est l'ordre du groupe des substitutions de G échangeables à une d'ordre f, et où ν' divise $f-1$, par suite le plus grand diviseur d de $\mathcal{G}$ et $f-1$, G renferme $\frac{f-1}{f\nu'}$ substitutions d'ordre divisible par f, et, d'après le théorème II,

$$\frac{1}{u} > \frac{1}{u} + \frac{1}{\mathcal{H}u(u-1)} - \frac{N-u}{\mathcal{H}(u-1)(N-1)} > \frac{f-1}{f\nu'} \geqq \frac{f-1}{fd};$$

d'où

$$(5)\qquad u < \frac{f\nu'}{f-1} \leqq \frac{fd}{f-1}.$$

Le théorème en résulte de suite [1].

---

[1] Pour un groupe quelconque transitif à trois degrés de classe $N-2$ et de degré $N = f\varphi$ ou ρf, on obtient les théorèmes analogues aux théorèmes IV et V en remarquant que, si $\mathcal{H}$ est l'ordre du groupe H des substitutions de G laissant une même lettre immobile, $\mathcal{K}$ l'ordre d'un sous-groupe de G laissant deux lettres immobiles, $\mathcal{G} = N\mathcal{H}$, $\mathcal{H} = (p\mathcal{K}+1)\mathcal{K}$, $N = (p\mathcal{K}+1)(q\mathcal{K}+1)+1$, avec

Théorème VI. — *Un groupe* G *deux fois transitif à trois degrés, de degré* $N = \rho f$ *(f premier impair et premier à* ρ*), de classe* $N - u$, *d'ordre* $\not\equiv 0 \pmod{f^2}$, *ne peut exister que pour des valeurs de f et u limitées en fonction de* ρ, *à moins que* G *ne soit d'ordre* $\mathcal{G}$ *multiple de* $\frac{1}{\delta}\rho f(\rho f - 1)(\rho f - u)$, δ *étant le plus grand commun diviseur de* ρu *et* $\rho f - u$, $\rho(\rho f - 1)$ *étant divisible par* $u(u-1)$, *et u étant pair si* ρ *est pair.*

En effet, considérons les valeurs de f telles que $\rho < f \leqq \rho u$. D'après le théorème I, $u - 1$ divise $\rho f - 1$ et est premier à f. u ne peut être divisible par f que si $u = \theta f$, avec $1 \leqq \theta < \rho$. Mais $\theta f - 1$ diviserait $\rho f - 1$, et l'on en conclurait

$$\rho f - 1 = \mu(\theta f - 1) = \mu\theta f - \mu < f(f-1)$$

et

$$\mu - 1 = (\mu\theta - \rho)f \quad \text{avec} \quad \mu < f,$$

ce qui exige $\mu = 1$, $\theta = \rho$, alors que $\theta < \rho$: donc u est premier à f et $u(u-1)$ divise $\rho(\rho f - 1)$. Ceci a lieu encore *a fortiori* si $f > \rho u$.

On en conclut $f \geqq \dfrac{\rho + u^2 - u}{\rho^2}$.

Si $f \leqq \rho u$, cette inégalité donne

$$\rho^3 u \geqq \rho + u^2 - u$$

$p > 0$ (*voir* notre Thèse de doctorat, p. 68-70). G renferme

$$\mathcal{G}\left[\frac{1}{2} - \frac{p\mathcal{K} - 1}{2\mathcal{K}(p\mathcal{K} + 1)}\right] - 1$$

substitutions de classe N, et l'on a les formules

$$(4\,bis) \qquad \frac{1}{2} > \frac{f-1}{\nu f} + \frac{\varphi - 1}{n\varphi} \geqq \frac{f-1}{df} + \frac{\varphi - 1}{\delta\varphi};$$

$$(5\,bis) \qquad 2 < \frac{f\nu'}{f-1} \leqq \frac{fd}{f-1},$$

analogues à (4) et (5) et qui donnent mêmes résultats qu'aux théorèmes IV et V. Notons encore que si $N = \rho f$, comme au théorème V, et si ν' ou d est $\lesseqgtr 2$, on a

$$(5\,ter) \qquad f < \mathcal{K}\frac{p\mathcal{K} + 1}{p\mathcal{K} - 1}.$$

et u est limité supérieurement en fonction de ρ. De même pour f, d'après $f \leqq \rho u$.

Soit $f > \rho u$: d'après MM. Mathieu et Sylow

$$\mathcal{G} = f\nu(af+1) = \rho f(\rho f - 1)\mathcal{H},$$

où $\mathcal{H}$ divise $\rho f - u$. Posant

$$k\mathcal{H} = N - u, \qquad k\mathcal{G} = kf\nu(af+1) = \rho f(\rho f - 1)(\rho f - u),$$

on a

$$k\nu \equiv \rho u \pmod{f}, \qquad \text{d'où} \qquad k\nu = \rho u + lf \qquad \text{et} \qquad l \geqq 0.$$

On en tire

$$\begin{aligned}(\rho u + lf)(af+1) &= \rho(\rho f - 1)(\rho f - u) = alf^2 + (l + a\rho u)f + \rho u \\ &= \rho^3 f^2 - \rho^2(u+1)f + \rho u\end{aligned}$$

et

$$(6) \qquad (\rho^3 - al)f = \rho^2(u+1) + l + a\rho u.$$

Tous les termes du deuxième membre étant positifs, il faut $al < \rho^3$, et, si $l > 0$,

$$(7) \qquad f \leqq \rho^2(u+1) + \rho u(\rho^3 - 1) + 1,$$

ce qui, joint à l'inégalité $f \geqq \frac{\rho + u^2 - u}{\rho^2}$, donne une limite supérieure de u et de f en fonction de ρ, quand $l > 0$.

On en conclut que, sauf pour des valeurs de f et u limitées supérieurement en fonction de ρ, il faut $l = 0$, $k\nu = \rho u$, et k diviseur commun à ρu et $\rho f - u$. C. Q. F. D.

Corollaire. — Si $N = f$, il faut [1] $\mathcal{G} = f(f-1)(f-u)$, $f - 1 \equiv 0 \,[\bmod u(u-1)]$. De plus, si $f = 4h + 3$, il faut $u = 4h' + 3$; enfin, quel que soit f, on n'a pas $\frac{f-1}{u}$ impair, ni $f - u = 4l + 2$.

En effet, on a $f > u$ et, d'après (6), $l = 0$, $k\nu = u$, $\delta = 1$, $\nu = u$, $\mathcal{G} = f(f-1)(f-u)$: $u(u-1)$ divise $f - 1$, d'après le

---

[1] Un raisonnement presque identique à celui du théorème VI montrera qu'un groupe G transitif à trois degrés, de degré premier f et de classe $f - u$, avec $u \leqq 4$, est deux fois transitif, c'est-à-dire que le corollaire du théorème VI lui est applicable.

théorème I. Si $f - u = 4l + 2$, G contiendrait un sous-groupe invariant d'ordre moitié moindre deux fois transitif à trois degrés, lequel ne peut exister d'après ce qui précède.

Enfin, soit $\frac{f-1}{u}$ impair, et, par suite, u pair. On a

$$\mathcal{G} = fu(af + 1),$$

avec $af + 1$ impair. G renferme un sous-groupe d'ordre fu renfermant un sous-groupe invariant d'ordre f, et une substitution d'ordre u à $\frac{f-1}{u}$ cycles, qui est impaire. G renfermerait donc un sous-groupe invariant G′ transitif et d'ordre moitié moindre $f\frac{f-1}{2}(f-u)$. Le groupe H′ des substitutions de G′ qui laissent une même lettre de G′ immobile permute une quelconque de ses $f-1$ lettres, α, transitivement avec au moins $\frac{f-1}{2}$ lettres, car le groupe K′ des substitutions de H′ laissant α immobile est d'ordre diviseur de $f - u$. H′ ne pouvant être transitif entre $f - 1$ lettres, puisque $\mathcal{H}'$ n'est pas divisible par $f - 1$, α est permutée transitivement par H′ avec $\frac{f-1}{2}$ lettres; K′ permutant transitivement les $f - u$ lettres qu'il déplace, il faut $\frac{f-1}{2} \geqq f - u + 1$, ce qui est impossible d'après le corollaire II du théorème I (la propriété subsiste si $u = 2$).

Remarque. — Nous nous contenterons de signaler qu'on peut obtenir des théorèmes analogues au théorème VI quand $N = \rho f^2$ ou $N = f^3$ (f premier impair, premier à ρ et $> u$) en s'appuyant sur des théorèmes connus [1].

III.

Nous signalerons l'application du théorème I au cas où $N = \varphi f + 1$ (φ et f premiers) avec $u > 2$. En particulier :

Si $\varphi = 2$, on a $u = 3$, $f = 6h + 1$, et G est de classe $N - 3$ et de degré N.

---

[1] *Ann. Fac. Sc. Toulouse*, 1896, A.17.

Si $\varphi = 3$, on a $u = 4$, $f = 4h + 1$, et G est de classe $N - 4$ et de degré N.

Dans ce dernier cas, le cas exceptionnel où $N = 16$ avec $u = 6$, que le corollaire I du théorème I ne permet pas d'écarter, s'élimine directement.

On peut encore faire application du théorème I au cas où $N = \rho f + 1$ (f premier impair, ρ quelconque), avec $u > 2$. En particulier :

Si $\rho = 4$, et $N = 4f + 1$, on a $u = 3$ avec $f = 6h - 1$, ou $u = 5$ avec $f = 10h + 1$.

Les cas particuliers où $N = 13$ avec $u = 3$, $N = 21$ avec $u = 5$, $N = 13$ avec $u = 4$, $N = 21$ avec $u = 6$, $N = 45$ avec $u = 12$ s'éliminent directement.

Si $\rho = 6$, et $N = 6f + 1$, on a ou $u = 3$, ou $f = 14h + 1$ avec $u = 7$.

Les cas particuliers où $N = 43$ avec $u = 7$, $N = 31$ avec $u = 6$, $N = 175$ avec $u = 30$ s'éliminent directement.

Théorème VII. — *Un groupe* G *deux fois transitif à trois degrés de degré* $N = f^\lambda + 1$ (f *premier*) *et de classe* $N - u$ ($u > 2$) *est tel que* $u = f^\mu + 1$, *où* $\lambda = (2h + 1)\mu$ ($h > 0$), *c'est-à-dire que* μ *est divisible par la plus haute puissance de* 2 *qui divise* λ *et est* $< \lambda$. *Donc* G *ne peut exister si* λ *est puissance exacte de* 2.

Théorème VIII. — *Un groupe* G *deux fois transitif à trois degrés, de degré* $N = 2f^2 + 1$ (f *premier impair*) *et de classe* $N - u$ ($u > 2$), *ne peut exister que si* $u = 3$.

Théorème IX. — *Un groupe* G *deux fois transitif à trois degrés, de classe* $N - u = f^\lambda$ (f *premier*, $u > 2$) *ne peut exister que si* λ *est pair et* $= 2h\mu$, *et si* $N = f^\lambda + f^\mu + 1$.

Théorème X. — *Dans un groupe* G *deux fois transitif à trois degrés de classe* $N - u = fp$ ($u > 3$, f *et* p *premiers différents*), *le degré* N *est* $fp + p + 1$, *ou* $fp + f + 1$. *Soit* $2 < f < p$. *Si* $u = p + 1$, *on a* $f + 1 = 2^m$, $\mathcal{G} = (fp + p + 1)(fp + p)f$, $p + 1$ *diviseur de* $f(f + 1)$ *et divisible par* f; *si* $u = f + 1$, *on a* $f + 1$ *diviseur de* $p + 1$, *et* $\mathcal{G} \equiv 0$ (*mod* p) *exige* $p + 1 = 2^m$ *ou* f *diviseur de* $p - 1 = 4h + 2$.

Le corollaire I du théorème I nous donne de suite $u = p + 1$ diviseur de $f(f+1)$ avec $p + 1 \equiv 0 \pmod{f}$ ou $u = f + 1$ diviseur de $p + 1$.

Premier cas : $u = p + 1$. On a $\mathcal{H} = (fp + p)\mathcal{K}$, avec $\mathcal{K}$ égal à f, p ou fp, et H admet une répartition de ses lettres en $f + 1$ systèmes de non-primitivité de p lettres, les p lettres de H que K laisse immobiles formant un système. Si alors $\mathcal{K} \equiv 0 \pmod{f}$, K contient une substitution d'ordre f, en sorte que K est transitif entre les f systèmes qu'il déplace. H opère entre les $f + 1$ systèmes les substitutions d'un groupe deux fois transitif d'ordre $(f+1)f\eta$, avec η diviseur de p^2, et de degré $f + 1$. On a $p > f + 1$ et $\eta = 1$, en sorte que [1] $f + 1 = 2^m$. Si $\mathcal{K} \equiv 0 \pmod{p}$, H contient un sous-groupe invariant d'ordre p^2, car il opère entre les $f + 1$ systèmes les substitutions d'un groupe transitif de degré $f + 1$ et d'ordre premier à p. Dès lors, G contiendrait au plus autant de sous-groupes d'ordre p^2 que H a de transformés par les substitutions de G, c'est-à-dire au plus $fp + p + 1 < p^2 + 1$: G contiendrait [2] un sous-groupe invariant d'ordre p ou p^2 et ne pourrait être primitif. On n'a donc pas $\mathcal{K} \equiv 0 \pmod{p}$.

Deuxième cas : $u = f + 1$. On a $\mathcal{H} = (fp + f)\mathcal{K}$, avec $\mathcal{K}$ égal à f, p ou fp, et H admet une répartition de ses lettres en $p + 1$ systèmes de non-primitivité de f lettres, les f lettres de H que K laisse immobiles formant un système. Si alors $\mathcal{K} \equiv 0 \pmod{p}$, K est transitif entre p systèmes, et H opère entre les $p + 1$ systèmes un groupe de substitutions deux fois transitif d'ordre $(p + 1)p\theta$, avec θ égal à $1, f$ ou f^2, ce qui exige θ diviseur de $p - 1$, $p + 1 = 2^m$ si $\theta = 1$, $p = 4h + 3$ avec f diviseur de $p - 1$ si $\theta > 1$. C. Q. F. D.

Théorème XI. — *Un groupe* G *deux fois transitif, de classe* $2p$ (p *premier impair* > 3) *à trois degrés est de degré* $2p + 3$, *avec* $p = 36k + 17$.

D'après le corollaire I du théorème I, on a $u = 3$ diviseur de $p(p + 1)$, ou $u = p + 1$ diviseur de 6. Dans ce dernier cas, $p = 5$

(1) Jordan, *J. de Math.*, 1872.
(2) *Ann. Fac. Sc. Toulouse*, 1896, A.6, corollaire II.

et G serait de classe $10 = 2.5$ et de degré $16 = 1 + 3.5$: on sait que G ne peut exister. Dans le premier cas, si $p = 3$, G est de classe 6 et de degré 9 : on sait qu'il existe des groupes linéaires deux fois transitifs à trois degrés de degré 9 et de classe 6. Soit donc $p > 3$; on a $p + 1 \equiv 0 \pmod 3$, c'est-à-dire $p = 6h - 1$: étudions spécialement ce cas.

On a $\mathcal{G} = (2p + 3)\mathcal{H}$, $\mathcal{H} = (2p + 2)\mathcal{K}$, et $\mathcal{K}$ divise $2p$.

Si $\mathcal{K}$ est pair, G contient un sous-groupe invariant G′ deux fois transitif, d'ordre moitié moindre, qu'il nous suffit d'étudier. Ou bien $\mathcal{K} = 2$, et G est linéaire (¹) avec $2p + 3 = r^m$ (r premier); G′ contient un sous-groupe invariant M régulier, d'ordre r^m, formé de substitutions d'ordre r échangeables; M est invariant dans G, qui est linéaire, et, par suite, G étant de classe $r^m - 3$, on a $r^m - 3$ égal à $r^m - r^{m'}$, avec $m' < m$, c'est-à-dire $r = 3$, $2p + 3 = 3^m$, ce qui est absurde, puisque p est premier à 3. Ou bien $\mathcal{K} = 2p$, et G′ est lui-même un groupe deux fois transitif à trois degrés de degré $2p + 3$, de classe $2p$, d'ordre $\mathcal{G} = (2p + 3)(2p + 2)p$ qu'il nous suffira de considérer.

Nous n'avons donc plus à examiner que le cas où $\mathcal{K}$ est impair et égal à p.

On voit, comme au théorème précédent, que H opère entre les systèmes de la répartition de ses lettres deux à deux qu'il admet, les deux lettres de H laissées immobiles par K formant un système, les substitutions d'un groupe H_1 deux fois transitif de degré $p + 1$ et d'ordre $\mathcal{H}_1$ égal à $(p + 1)p$ ou $(p + 1).p.2$. Si $\mathcal{H}_1 = (p + 1)p$, il faut $p + 1 = 2^m$, ce qui est absurde, puisque $p + 1 = 6h$. Si $\mathcal{H}_1 = (p + 1).p.2$, on ne peut avoir $p = 4h' + 3$, sans quoi H_1 contiendrait un sous-groupe invariant d'ordre moitié moindre deux fois transitif pour lequel on devrait encore avoir $p + 1 = 6h = 2^m$. On en conclut $p = 6h - 1 = 4h' + 1 = 12l + 5$.

Ce n'est pas tout : H_1 est un groupe deux fois transitif de classe $p - 1$ et de degré $p + 1$, et ne peut exister (²) pour une foule de valeurs de $p + 1$. Ainsi, si $p + 1$ est divisible par 3, mais non par 9, d'après (5 *ter*) où l'on prend $f = 3$ il faut $p = 5$,

---

(¹) JORDAN, *J. de Math.*, 1872.

(²) *Voir* notre Thèse de doctorat, p. 68-98, et quelques-unes des propriétés précédentes.

$\mathcal{G} = 13.12.10$, ce qui est impossible d'après le corollaire du théorème VI. Donc $p + 1 \equiv 0 \pmod 9$, et $p = 36k + 17$.

C. Q. F. D.

Théorème XII. — *Un groupe* G *deux fois transitif, à trois degrés de classe* $N - u = p^2$ *(p premier impair) est de degré* $N = p^2 + p + 1$, *et* $p + 1 = 2^m$.

La démonstration se fait en établissant que H doit être isomorphe à un groupe deux fois transitif de degré $p + 1$ et d'ordre $(p + 1)p$.

IV.

Application de ce qui précède au cas ou $u = 3$.

D'après le théorème I, N est impair et $N(N - 1) \equiv 0 \pmod 6$, c'est-à-dire que N est de la forme $6h + 1$ ou $6h + 3$.

D'après le corollaire du théorème VI, si N est premier et impair, il faut $N = 12h + 7$ et $\mathcal{G} = f(f - 1)(f - 3)$.

La classe $N - 3$ ne peut être de la forme fp, avec $f < p$, et f et p premiers, que si $f = 2$, en sorte que, d'après le théorème XI, $p = 36k + 17$, $N = 72k + 37$.

Nous allons encore établir cette propriété.

Théorème XIII. — *La classe d'un groupe* G *deux fois transitif à trois degrés, de degré* N *premier, ne peut être de la forme* $4p = N - 3$ *(p premier impair) que si l'on a* $N = 48h + 7$.

En effet, on peut supposer $p > 3$. L'ordre $\mathcal{G}$ de G est $\mathcal{G} = (4p + 3)(4p + 2)4p$, $4p + 2$ est divisible par 3, et $p = 6h + 1$.

H est isomorphe à un groupe deux fois transitif H′ d'ordre $\mathcal{H}' = (2p + 1)2p.\theta$, de degré $2p + 1$, formé par les substitutions que H opère entre les systèmes de la répartition de ses lettres deux à deux qu'il admet, θ divisant 4.

Si $\theta < 4$, H contiendrait un sous-groupe invariant d'ordre $\frac{4}{\theta} = 2^\varphi$, où φ est égal à 1 ou 2; d'après le lemme suivant, que nous

nous contenterons d'énoncer [1], et qui permet de généraliser le lemme I :

Lemme III. — Si un groupe M contient un sous-groupe invariant P d'ordre p^2 (p premier), auquel cas l'ordre $\mathfrak{M}$ de M est divisible par p^2, l'ordre $\mathfrak{L}$ du sous-groupe L des substitutions de M échangeables à toutes celles de P est $\mathfrak{L} = \frac{\mathfrak{M}}{\mu}$, où μ divise la quantité $p^2 - p$ ou la quantité $(p^2 - 1)(p^2 - p)$, suivant que P est formé ou non des puissances d'une substitution d'ordre p^2, H contient un sous-groupe invariant d'ordre 2^φ formé de substitutions échangeables à une d'ordre p, puisque $p > 3$, par suite une substitution impaire et de classe $4p + 2$. G contiendrait ainsi un groupe d'ordre moitié moindre transitif, qui ne peut exister (corollaire du théorème VI). Donc $\theta = 4$.

Le sous-groupe K_1 des substitutions de H′ laissant une même lettre de H′ immobile est d'ordre $8p$ et contient un sous-groupe invariant d'ordre p, à moins que $p = 7$ et que K_1 contienne un sous-groupe invariant d'ordre 8 formé de substitutions échangeables. Dans ce dernier cas, on démontrera directement l'impossibilité de l'existence de H′; dans le premier, l'ordre du groupe des substitutions de H′ échangeables à une d'ordre p n'étant pas divisible par 4, d'après le lemme I, on a $p = 4h' + 1$, par suite $p = 12l + 1$ et $4p + 3 = 48l + 7$. C. Q. F. D.

Enfin, nous allons déduire de ce qui précède le théorème suivant :

Théorème XIV. — *Les groupes deux fois transitifs, à trois degrés, de classe* $N - 3 \leqq 100$ *et de degré* N, *sont tous de degrés* 3^μ, $2^m - 1$ *ou* 33.

Ce qui précède permet, en effet, de montrer que ce théorème ne pourrait être en défaut que pour les valeurs de N égales à 19,

---

[1] Si $1 = h_1, h_2, \ldots, h_{p^2}$ sont les substitutions de P, T une substitution quelconque de M, on peut faire correspondre à T la substitution

$$T' = \begin{pmatrix} h_1, & h_2, & \ldots \\ T^{-1}h_1T, & T^{-1}h_2T, & \ldots \end{pmatrix}$$

entre les symboles h_i. Le lemme résulte de suite de la considération des substitutions T′ : on peut l'étendre au cas où P est d'ordre p^i (i quelconque).

21, 39, 43, 45, 51, 55, 57, 67, 69, 75, 87, 91, 93, 99, 103.

Cas où $N = 3f$ (*f premier impair*) : N est un des nombres 21, 39, 51, 57, 69, 87, 93.

On appliquera un raisonnement analogue à celui que nous allons faire pour $N = 21 = 3.7$. On a alors $\mathcal{G} = 21.20.\mathcal{K}$, où $\mathcal{K}$ divise 18. Si $\mathcal{K}$ est pair, G renferme un sous-groupe invariant d'ordre moitié moindre qui ne peut exister que s'il est de classe 18 : il suffira de considérer ce dernier, c'est-à-dire le cas où $\mathcal{K}$ est impair et égal à 3 ou 9.

Si $\mathcal{G} = (7h + 1)\nu.7$ d'après la formule de MM. Mathieu et Sylow, le nombre $(7h + 1)6$ des substitutions d'ordre 7 est multiple de $20\mathcal{K}$.

Si $\mathcal{K} = 3$, $7h + 1 = 10\lambda$, où λ divise 18; on voit de suite qu'il n'y a aucun diviseur de 180 qui soit à la fois des formes 10λ et $7h + 1$.

Si $\mathcal{K} = 9$, $7h + 1 = 30\lambda$, où λ divise 18; on voit de suite qu'il n'y a aucun diviseur de 540 qui soit à la fois des formes 30λ et $7h + 1$, sauf le nombre 540 lui-même : on aurait $\nu = \frac{540}{30\lambda} = 1$, ce qui est impossible, d'après le théorème V.

Cas où N *premier impair :* N est un des nombres 19, 43, 67, 103. On a $\mathcal{G} = N(N - 1)(N - 3)$.

On démontre l'impossibilité de l'existence du groupe H de degré $N - 1$ et d'ordre $(N - 1)(N - 3)$, lequel ne peut contenir de substitution impaire.

Si $N = 19$, H ne peut contenir de sous-groupe invariant d'ordre 9 sans contenir (lemme III) une substitution d'ordre 2 échangeable à toutes celles de ce sous-groupe, c'est-à-dire de classe 18, par suite impaire, ce qui est impossible. Alors $\frac{\mathcal{H}}{9}$ ne possédant pas de diviseur $9h + 1$, on peut trouver dans H deux sous-groupes d'ordre 9 ayant deux à deux une substitution d'ordre 3 commune. Le groupe dérivé de ces deux sous-groupes contiendrait une substitution d'ordre 2 impaire, ce qui est impossible. On n'a donc pas $N = 19$.

Si $N = 43$, H ne peut contenir un sous-groupe invariant d'ordre 7 sans contenir (lemme I) une substitution d'ordre 7 et de classe 42 échangeable à une d'ordre 5 et de classe 40, ce qui

est impossible. On en conclut, en raisonnant comme, par exemple, pour $N = 21$ et $\mathcal{H} = 3$, que si $\mathcal{H} = (7h + 1)\nu.7$, d'après la formule de MM. Mathieu et Sylow, H renferme $\frac{3}{7}\mathcal{H}$ substitutions d'ordre 7, et que $\nu = 2$. Une substitution d'ordre 3 ne pouvant être échangeable à une d'ordre 7, le nombre des substitutions d'ordre $\equiv 0 \pmod 3$ dans H est au moins [1] $\frac{1}{3}\mathcal{H}$. Enfin H contient $\frac{1}{2}\frac{39}{40}\mathcal{H}$ substitutions d'ordre diviseur de 40 et de classe 40 et il faudrait $\frac{3}{7} + \frac{1}{3} + \frac{1}{2}\frac{39}{40} < 1$, ce qui est absurde.

Si $N = 67$, le nombre des substitutions d'ordre 11 de H est multiple de 64; le nombre des sous-groupes d'ordre 11 de H est de la forme $11h + 1$, avec $h > 0$, et divise $\frac{\mathcal{H}}{11}$, ce qui est contradictoire, puisque $\frac{\mathcal{H}}{11}$ n'a pas de diviseur $11h + 1$ de la forme 32λ.

Si $N = 103$, un raisonnement semblable est applicable au nombre premier 17 diviseur de 102.

Cas où $N = 45$: $\mathcal{G} = 45.44.\mathcal{H}$, et l'on peut supposer $\mathcal{H}$ impair et égal à 3.7 ou 21. On voit que H ne pourrait exister que si $\mathcal{H} = 11.12$, et s'il renferme 12 sous-groupes d'ordre 11. H serait donc isomorphe [2] holoédriquement à un groupe deux fois transitif d'ordre 11.12 et de degré 12, lequel ne peut exister.

Cas où $N = 55$: $\mathcal{G} = 55.54.\mathcal{H}$. On a $\mathcal{G} = (11h + 1)\nu.11$, avec $\nu \equiv 0 \pmod 5$ (théorème V). D'autre part le nombre des sous-groupes d'ordre 11 de G est $27\mathcal{H}\lambda$, où $\mathcal{H}\lambda$ divise 2.52 et est > 1, alors qu'aucun des diviseurs de 54.52 de la forme 27μ n'est de la forme $11h + 1$. On est donc conduit à une impossibilité.

Cas où $N = 75$: $\mathcal{G} = 75.74.\mathcal{H}$; deux sous-groupes d'ordre 25 de G n'ont d'autre substitution commune que l'unité et, d'après ne formule connue, on a [3] $\mathcal{G} = 25\nu(1 + 25h)$, où $1 + 25h$ est le nombre des sous-groupes d'ordre 25 de G. On a $1 + 25h = 37\lambda$,

---

(1) Lemme I.
(2) W. Dyck, *Mat. Ann.*, t. XX et XXII et notre Thèse de doctorat.
(3) *Ann. Fac. Sc. Toulouse*, 1896, A.17.

où λ divise $6\mathcal{K}$, et $1 + 25h = 3.74.8$, d'où $\mathcal{K} \equiv 0 \pmod 8$. On a d'ailleurs [1] $\nu > 1$, d'où $\mathcal{K} \equiv 0 \pmod{24}$, et $\mathcal{K}$ égal à 24 ou 72. Alors H renfermerait un sous-groupe d'ordre 37, et d'après le lemme I le groupe des substitutions de H échangeable à une d'ordre 37 serait multiple de 74.2 : il y aurait ainsi une substitution d'ordre 2 et de classe 72 échangeable à une d'ordre 37 et de classe 74, ce qui est absurde.

Cas où $N = 91$: $\mathcal{G} = 91.90.\mathcal{K}$, où l'on peut supposer $\mathcal{K}$ pair, le cas où $\mathcal{K} = 11$ se traitant de la même manière : $\mathcal{K}$ divise $88 = 2^3.11$. On a $91 = 7.13$, $\mathcal{G} = (13h+1)\nu.13$ d'après la formule de MM. Mathieu et Sylow; le nombre des substitutions d'ordre 13 étant multiple de $(13h+1)12$ et $90\mathcal{K}$, on a $13h + 1 = 15\,\frac{\mathcal{K}}{2}\lambda$, où $\frac{\mathcal{K}}{2}\lambda$ est un diviseur de $7.88.6$; $13h+1$ est donc un des nombres 15.176 ou 15.33 qui sont premiers à 7, ou un des nombres 15.7 ou $15.14.33$.

Or ν doit diviser (lemme I) 12.7, puisqu'une substitution de classe < 91 ne peut être échangeable à une d'ordre 13.

Dès lors, si $13h + 1 = 15.7$, $\mathcal{K} = 2$, $\mathcal{G} = (7l+1)7.\nu'$ et $7l+1$ est multiple de 30.13 : on aurait $\nu' \leqq 2$, ce qui est impossible [théorème V, formule (5)].

Si $13h + 1 = 15.14.33$, ν divise 12 et $\mathcal{K}$ est égal à 22 ou 44. Quand $\mathcal{K} = 22$, on a $\nu = 2$, ce qui est impossible [théorème V, formule (5)]. Quand $\mathcal{K} = 44$, $7l+1$ est multiple de 15.44 : on aurait $\nu' = 2$, ce qui est impossible.

Si $13h + 1 = 15.33$, on a $\mathcal{K} = 22$: G ne peut exister (théorème III).

Si $13h + 1 = 15.176$, on a $\mathcal{G} = 91.90.88$: H ne peut exister. En effet, on sait [2] que $\mathcal{K} = 9\nu_1(1 + 9h_1)$. G ne renferme pas de substitution impaire et de classe 90, en sorte que le nombre $(1 + 9h_1)8$ de substitutions d'ordre diviseur de 9 est multiple de 88.2 et $1 + 9h_1 = 22\lambda$, où λ divise 5.8 : aucun des nombres 22λ n'étant de la forme $1 + 9h_1$, H ne peut exister.

---

[1] Sans quoi G renfermerait $\frac{24}{25}\mathcal{G}$ substitutions d'ordre diviseur de 25, de classe 75, ce qui est impossible (théorème II).

[2] *Ann. Fac. Sc. Toulouse*, 1895, D.17.

Cas où $N = 99$: $\mathcal{G} = 99 . 98 . \mathcal{X}$, et $99 = 9 . 11$. On applique à 11 le théorème V.

Le théorème XIV est ainsi complètement établi.