

BULLETIN DE LA S. M. F.

DE SÉGUIER

Sur certains groupes de Mathieu

Bulletin de la S. M. F., tome 32 (1904), p. 116-124

<http://www.numdam.org/item?id=BSMF_1904_32_116_1>

© Bulletin de la S. M. F., 1904, 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 CERTAINS GROUPES DE MATHIEU;

Par M. DE SÉGUIER.

1. On trouvera dans le *Journal de M. Jordan* (1902, p. 159) la démonstration du théorème suivant :

Les conditions nécessaires et suffisantes pour l'existence

d'un groupe G_t $t+1$ fois transitif entre les symboles $1, \dots, n, \sigma_1, \dots, \sigma_t$, où A est le groupe fixant $\sigma_1, \dots, \sigma_t$, F le groupe fixant $1 = \sigma_0, \sigma_1, \dots, \sigma_t$, sont qu'il existe des substitutions d'ordre 2, $s_h = (\sigma_0) \dots (\sigma_{h-2})(\sigma_{h-1}, \sigma_h)(\sigma_{h+1}) \dots (\sigma_t) \dots$, telles que

$$\left\{ \begin{array}{l} s_h^2 = 1, \quad s_h f s_h = f_h, \quad s_1 r s_1 = a' s_1 a'', \\ s_l a s_l = a_l, \quad (s_i s_{i+1})^2 = f_{ii}, \quad (s_j s_{j+k})^2 = f_{jk} \\ (h = 1, \dots, t; i = 1, \dots, t-1; j = 1, \dots, t-2; k = 2, \dots, t-j; \\ l = 2, \dots, t; f \text{ parcourt les générateurs de } F, a \text{ ceux de } A \text{ qui sont hors de } F; r \text{ un système de restes } \not\equiv 1 \text{ de } A \bmod F; a', a'', a_l \text{ sont dans } A \text{ hors de } F; f_h, f_{ii}, f_{jk} \text{ dans } F), \end{array} \right.$$

et ces équations jointes à celles de A définissent G_t .

2. Prenons pour A le groupe $\{(z, iz), (z, 1-z)\}$, z parcourant un corps de Galois $C_\pi = C$ d'ordre $p^m = \pi$ (p premier, $\pi > 2$) dont i est racine primitive. Posons $(z, iz) = a, (z, 1-z) = b$ et cherchons à adjoindre à A une s_2 (¹) $c = (0\infty) \dots$ telle que A soit le diviseur fixant un symbole dans $\{A, c\} = G$. On devra avoir $cac = a^\alpha, a^2 = 1$. Si $\alpha = 1$, comme $a = (i^0, i^1, i^2, \dots)$, il faut que $c = (0\infty)(i^2, i^{x+2\rho})$ avec $i^{x+2\rho} = i^x, 2\rho = \pi - 1$, ou $c = (0\infty)a^{\frac{\pi-1}{2}}$, et G contiendrait (0∞) , ce qui ne se peut, la classe étant $\pi - 1$. Soit donc $\alpha = -1$. Alors $c = (0\infty)(i^x, i^{\rho-x})$ est de la forme (rz^{-1}) et la condition $(cb)^3 = 1$ donne $r = 1$. Donc G coïncide avec le $\mathcal{L}_{\pi(\pi-1)} = \sum \left(\frac{\alpha z + \beta}{\gamma z + \delta} \right)$, les paramètres $\alpha, \beta, \gamma, \delta$ parcourant $C(z\delta - \beta\gamma \not\equiv 0)$, z parcourant C et ∞ (²). On voit immédiatement par le même procédé que \mathcal{L} ne peut être le diviseur fixant un symbole dans un $g^{\pi+2}$. Les équations de \mathcal{L} s'obtiennent en adjoignant à celles de $\{a, b\}$ $c^2 = (cb)^3 = (ca)^2 = 1$.

Le diviseur fixant un symbole dans un $g_{p(p^2-1)}^{\pi+1}$ transitif étant métacyclique, il résulte de ce qui précède que le seul $g_{p(p^2-1)}^{\pi+1}$ transitif est $\mathcal{L}(2, p)$.

3. Prenons maintenant pour A le $g_{\frac{\pi(\pi-1)}{2}}$ (π impair) engendré

(¹) Je me servirai des mêmes notations que dans le Mémoire cité.

(²) Cf. MILLER, *Comptes rendus de l'Académie des Sciences*, t. CXXXVI, 1903, p. 294.

par $a = (i^2 z) = (i^0, i^2, \dots, i^{\pi-3}) (i, i^3, \dots, i^{\pi-2})$ et le g_π^π abélien principal B formé des substitutions $b_\beta = (z + \beta)$, β parcourant C (je poserai $b_1 = b$; si $\pi = p$, $b_\beta = b^\beta$). A est défini (¹) par $a^{\frac{\pi-1}{2}} = b_h^p = 1$, $b_h b_k = b_k b_h$, $a^{-1} b_h a = b_{i^h}$, h, k parcourant $1, i, \dots, i^{m-1}$ (si $i^p = \sum_0^{m-1} x_p i^p$, $b_{i^p} = \prod_0^{m-1} b_i^{x_p}$). Cherchons à adjoindre à A une s_2 $c = (\infty) \dots$ telle que, dans $\mathcal{G} = \langle A, c \rangle$, A soit le groupe fixant ∞ .

Par les mêmes raisonnements que dans le Mémoire cité (²) où l'on changera en indices les exposants de b , on trouve que $c = (rz^{-1})$, r étant un carré ou un non-carré suivant que $\pi \equiv 1$ ou $\equiv 3 \pmod{4}$, c'est-à-dire que $\mathcal{G} = \mathcal{O}(2, \pi)$, sauf que, si $\pi = 7$, \mathcal{G} peut encore être le g_{168}^8 composé; et l'on obtient ainsi les équations de \mathcal{O} .

$\mathcal{O}(2, \pi)$ ne peut être le diviseur fixant un symbole σ dans un $g^{\pi+2}$. Soit en effet d la s_2 à adjoindre à \mathcal{O} pour engendrer ce $g^{\pi+2}$ et supposons d'abord $\pi \equiv 1 \pmod{4}$. On voit, comme dans la recherche précédente, que $d = (\infty)(z, \xi'_z z^{-1})(z \neq 0)$, $\xi'_z = r'^i = i^{2\sigma'}$ où $\xi'_z = s' = i^{2\sigma'}$ selon que z est carré ou non. On a $c = (rz^{-1})$, $dc = (\infty)(z, r\xi'^{-1} z)(z \neq 0)$, et $(dc)^3$, qui fixe 0 , doit être dans $\langle a \rangle$, ce qui exige $r' = s'$. De plus d doit être permutable à A , donc à B , seul g_π de A ; or $cb_h c = \left(\frac{r'z}{hz+r'} \right)$ n'est pas de la forme $(z+k)$. Si $\pi \equiv 3 \pmod{4}$, on a de suite $r' = s'$.

Au contraire, le g_{168}^8 composé est le diviseur fixant un symbole dans un g_{1512}^9 trois fois transitif; on le verra bientôt dans un théorème plus général.

4. Tout $g_{2p(p^2-1)} X$ qui a plus d'un g_p en a $p+1$. Si donc X est simple, il est représentable en $g^{p+1} = \mathcal{O}(2, p)$.

Si $p = 2q + 1$ (q premier), X est encore représentable en g^{p+1} [donc isomorphe à $\mathcal{O}(2, p)$ ou au g_{168}^8 composé] sauf s'il a un g_q

(¹) Cf., loc. cit., p. 264.

(²) Je reprendrai seulement ici un point de détail. Si $\alpha = -1$ et si c échange les cycles de a (dont $\pi \equiv 3 \pmod{4}$), $c = (\infty)(i^x, i^{x+1-2x}) = (z, rz^{-1})$ ($r = i^{2x+1}$).

Or $cbc = (\infty, r, \frac{r}{2}, \frac{r}{3}, \dots, -r)$, et $cb_\beta c$ devant être de la forme $b_x cb_{x'} b_{-t} \alpha x b_t$, où t est arbitraire, il faut, pour $t = r$, que l'on ait $x = x' = r$, $cbc = b_r c a x b_r$: le second membre devant fixer 0 , i^y doit être égal à $-r$, ce qui exige que l'on ait $\pi \equiv 3 \pmod{4}$; alors y se trouve déterminé.

normal Q dont chaque élément est permutable à chaque c_p . Dans ce cas d'exception, $X|Q$ est représentable en g^{p+1} 2 fois transitif de classe p , et $p+1=2^\omega$. Or, pour que $2^\omega-1=p$ et $2^{\omega-1}-1=q$ soient premiers, il faut que ω et $\omega-1$ le soient; donc $q=3$. Mais alors, $X|Q$ ayant un g_8 abélien normal, X a un $g_{3,8}$ abélien Y . Si Y n'a qu'un $g_8 A$, il est le produit direct de Q par A , et X est le produit direct de Q par un $g_{5,6}$ de Mathieu. Si Y a $3g_8$, ils ont un g_4 non cyclique commun Δ , caractéristique dans Y , donc normal dans X , et ΔQ est le produit direct de $\Delta=\{b, c\}$ par $Q=\{\alpha\}$. Y est défini par les équations de Δ , Q jointes à $d^2=1$, $db=bd$, $dc=cd$, $dad=a^2$. D'ailleurs $X|\Delta Q$, d'ordre 14, n'a qu'un g_7 auquel répond dans X un $g_{7,12}$ contenant un seul g_7 $S=\{s\}$. Ainsi $sa=as$, $dsd=s^{-1}$, et (en prenant au besoin bd pour b , cd pour c) $sb=bs$, $sc=cs$.

Pour le cas $\pi \neq p$, je prouverai seulement que $\nu(2, 3^2)$ est le seul $g_{3,60}$ simple, le théorème précédent fournissant une démonstration plus simple que celle donnée par M. Cole (¹). Un $g_{3,60}$ simple G a 10 ou 40 g_9 . Supposons-en 40. Comme 40 est $\not\equiv 1 \pmod{9}$, les g_9 ne sont pas premiers entre eux deux à deux. Soit $\{\alpha\}$ un g_3 divisant deux g_9 . Il en divisera $\nu \equiv 1 \pmod{3}$ et le groupe A des éléments permutables à $\{\alpha\}$ est d'ordre $k\nu g$. G , n'étant pas représentable en moins de six symboles, n'a aucun diviseur d'indice < 6 . Donc $\nu=4$, $k=1$. Considérons G comme représenté en g^{10} relativement à A . α , n'entrant que dans 4 g_9 qui sont ceux de A , ne divise aucun conjugué de A et est par suite de degré 9. $A|\{\alpha\}$ est un $g_{1,2}$ ayant 4 g_3 (il est donc tétraédral) et un g_4 non cyclique. Donc A a un $g_{1,2}^0$, $B>\{\alpha\}$ qui est abélien ou contient 3 g_4 non cycliques ayant un e_2 normal dans B . Cela étant, B ne peut avoir 3 systèmes d'intransitivité de degré 3; il devrait donc en avoir 1 de degré 6 et 1 de degré 3 et serait impair, ce qui ne se peut, G étant simple. Donc G a 10 g_9 . Considérons G comme représenté en g^{10} relativement au $g_{3,60}A$ formé des éléments permutables au g_9B . B , étant premier à tous ses conjugués (le raisonnement fait dans le cas précédent le montre), est de classe 9 et, par suite, transitif. B n'est pas cyclique, car le groupe des substitutions permutables à B dans le champ

(¹) *A. J.*, t. XV, 1893, p. 307.

de B serait d'ordre 54 non divisible par 36. Donc $A = BC$, C étant un g_4 du groupe linéaire à 2 variables mod p , et, comme G est simple, donc pair, C est cyclique. Dès lors le g^{10} deux fois transitif où A est le g^9 fixant un symbole est $\mathcal{O}(2, 3^2)$.

5. Cherchons à construire un $g_{\pi(\pi^2-1)}$ (π impair > 3) G dont un groupe facteur soit $\mathcal{O}(2, \pi)$. Le groupe des isomorphismes I de \mathcal{O} est $\{\mathcal{O}, (iz), (z^p)\}$ en sorte que $I|\mathcal{O}$ est un groupe abélien engendré par deux générateurs indépendants d'ordres respectifs 2 et m . \mathcal{O} est donc unique de son type dans I , car si I contenait un groupe $\mathcal{O}' \neq \mathcal{O}$ et isomorphe à \mathcal{O} , il contiendrait $\mathcal{O}\mathcal{O}'$ et $I|\mathcal{O}$ n'aurait pas le type indiqué. Il résulte dès lors d'un théorème de M. Hölder (*M. A.*, t. XLVI, p. 331) que, si m est pair, I a exactement trois $g_{\pi(\pi^2-1)}$ distincts non isomorphes qui sont $\mathcal{L}(2, \pi)$, $\{\mathcal{O}, (z^{p^2})\} = \mathcal{L}'$, $\{\mathcal{O}, (iz^{p^2})\} = \mathcal{L}''$. Si m est impair, I n'a qu'un $g_{\pi(\pi^2-1)}$ qui est $\mathcal{L}(2, \pi)$. G n'a pas d'autre type si sa seule suite de composition est G, \mathcal{O}, I .

Supposons que G admette la suite G, D, I ($D = \{d\}$, $d^2 = 1$; je supposerai les exposants de d réduits à 0 ou à 1). h, k, β parcourant les mêmes valeurs que précédemment et $y_\beta = y$ étant défini par $\beta \circ r \equiv x$, G aura pour équations

$$\begin{aligned} a^{\frac{\pi-1}{2}} &= d^\alpha, & b_h^k &= d^{\delta_h}, & c^2 &= d^\gamma, & d^2 &= 1, & b_k^{-1} b_h b_k &= b_k d^{\mu_{hk}}, \\ a^{-1} b_h a &= b_{ph} d^{\varphi_h}, & c^{-1} ac &= a^{-1} d^\delta, & c^{-1} b_\beta d^{\theta_\beta} c &= b_{-\frac{x}{\beta}} c a r_\beta b_{-\frac{x}{\beta}}, \\ da &= ad, & db_h &= b_h d, & dc &= cd. \end{aligned}$$

En prenant $b_h d^{\delta_h}$ pour b_h , on peut supposer ($b_k^{-1} b_h b_k$ et $a^{-1} b_h a$ étant alors, comme b_h , d'ordre p) que $\delta_h = \mu_{hk} = \varphi_h = 0$.

Si $\gamma = 0$, on a nécessairement $\delta = 0$. Cela est clair si $\pi \equiv 3 \pmod{4}$, car, a et $a^{-1} d$ n'étant pas alors du même ordre, on ne peut avoir $c^{-1} ac = a^{-1} d$. Soit donc $\pi \equiv 1 \pmod{4}$: Dc , dans la représentation de $G|D$ donnée au n°3, sera représenté par (rz^{-1}) , r étant un carré. La transformée de (rz^{-1}) par $w = \left(ir \frac{\xi z + \eta}{\eta z + \xi r}\right)$ où $\xi^2 r - \eta^2 \equiv -ir$ est $(rz^{-1})(i^2 z)$ qui correspond ici à Dca de $G|D$. w étant dans $\mathcal{O}(2, \pi)$, on voit que Dc et Dca sont conjugués dans $G|D$. Donc c est conjugué de ca ou de cad dans G , et, dans les deux cas, $(ca)^2 = 1$.

Si $\gamma = \delta = 1$, en posant $ca = c'$, on obtient $c'^2 = 1$, $c'^{-1}ac' = a^{-1}d$, $c'^{-1}b_\beta d^{\theta_\beta} c' = b_{\frac{-x}{\beta}} c' \alpha^{x+1} b_{\frac{-x}{\beta}}$, et l'on a bien $\beta i^{x+1} = ix$, de sorte qu'en changeant x en ix on est ramené au cas impossible $\gamma = 0$, $\delta = 1$. Donc $\delta = 0$. On aura

$$a^{-1}c^{-1}b_\beta d^{\theta_\beta} ca = b_{\frac{-x^2}{\beta}} ca x^{+2} b_{\frac{-x^2}{\beta}} = c^{-1}b_{\beta i^{-2}} d^{\theta_{\beta i^{-2}}} c,$$

et, puisque $b_\beta d^{\theta_\beta}$ et $b_{\beta i^{-2}} d^{\theta_{\beta i^{-2}}}$ sont du même ordre, il faut que $\theta_\beta = \theta_{\beta i^{-2}}$. Mais alors, changeant c en cd^{θ_1} , on aura, pour β carré, $c^{-1}b_\beta c = b_{\frac{-x}{\beta}} carb_{\frac{-x}{\beta}}$.

Soit d'abord $\pi \equiv 3 \pmod{4}$. On peut toujours, en prenant au besoin ad pour a , supposer $\alpha = 0$. La formule précédente donne alors $c^{-1}b_{\frac{-x}{\beta}} c = d^r b_\beta ca^{-r} b_\beta$. Donc on n'aura que deux types : l'un répondant à $\gamma = 0$ est le produit direct de $\mathcal{O}(2, \pi)$ par D , l'autre répondant à $\gamma = 1$ coïncide avec le groupe $U(2, \pi)$ des substitutions linéaires homogènes à deux variables de déterminant 1. Ce groupe U n'est pas un produit direct et l'on en a ainsi les équations $\pi \equiv 3 \pmod{4}$.

Soit $\pi \equiv 1 \pmod{4}$. Prenons x carré; γ sera pair pour β carré et impair pour β non carré. En prenant donc ad^{θ_1} pour a , on aura, quel que soit β , $c^{-1}b_\beta c = b_{\frac{-x}{\beta}} ca^\beta b_{\frac{-x}{\beta}}$. On peut donc supposer $\theta_\beta = 0$. Or, dans la représentation de $G|D$ en $g^{\pi+1}$ deux fois transitif du n° 3, $Dc = (rz^{-1})$, qui fixe les deux symboles $\pm r^{\frac{1}{2}}$, est une $s_2^{\pi-1}$. Comme $\{Da\}$ est le diviseur fixant 0, ∞ , toutes les $s_2^{\pi-1}$ sont conjuguées de $Da^{\frac{\pi-1}{4}}$.

Donc, dans G , c est conjuguée de $a^{\frac{\pi-1}{4}}$ ou de $a^{\frac{\pi-1}{4}}d$ et, ces deux éléments étant d'ordre $2^{\alpha+1}$, il faut que $\gamma = \delta = \alpha$. On a donc encore deux types : l'un, répondant à $\gamma = \alpha = 0$, est produit direct de $\mathcal{O}(2, \pi)$ par D ; l'autre, répondant à $\gamma = \alpha = 1$, est $U(2, \pi)$ dont on a ainsi les équations pour $\pi \equiv 1 \pmod{4}$.

6. Prenons maintenant pour le groupe A du n° 1 le $g_{\pi q}$ engendré par $a = (iz)(\gamma q = \pi - 1)$ et par le même $g_\pi^q B$ que précédemment. A est défini par les équations de B jointes à $a^q = 1$, $a^{-1}b_h a = b_{ih}$. Cherchons à adjoindre à A une s_2 $c = (0\infty)\dots$

telle que, dans $\mathcal{G} = \{A, c\}$, A soit le diviseur fixant ∞ . On aura $cac = a^\alpha, \alpha^2 = 1$.

Soit d'abord $\alpha = 1$. Si alors q est pair, A contient une seule $s_2 a^{\frac{q}{2}}$ fixant 0 et ∞ , en sorte que \mathcal{G} a $\frac{1}{2}\pi(\pi+1) s_2^{\pi-1}$ contenant $\frac{1}{4}\pi(\pi^2-1)$ cycles binaires. Or soient c et c' deux substitutions ayant le cycle (0∞) ; cc' sera dans $\{a\}$, soit $c' = ca^x$; et inversement ca^x a le cycle (0∞) . Chaque cycle binaire figurant ainsi dans q substitutions de \mathcal{G} , les substitutions de \mathcal{G} présentent $\frac{1}{2}\pi(\pi+1)q$ cycles binaires. Donc $\frac{1}{2}\pi(\pi+1)q$ est $\geq \frac{1}{4}\pi(\pi^2-1)$ et $q = \pi - 1$ ou $\frac{1}{2}(\pi - 1)$, ce qu'on a reconnu impossible.

Soit donc q impair. Alors, c , ne pouvant transformer en lui-même aucun cycle de a (la classe est $\pi - 1$), les échange deux à deux et est de degré $\pi + 1$. D'ailleurs c doit être paire, sans quoi les substitutions paires de \mathcal{G} formeraient un diviseur \mathcal{G}' dont le p. g. c. d. avec A serait d'indice 2 dans A, tandis que A est pair et divise \mathcal{G}' . Donc $\frac{1}{2}(\pi+1)$ est pair et $\pi \equiv 3 \pmod{4}$. Ici encore toute substitution de \mathcal{G} ayant le cycle (0∞) est de la forme ca^x , et parmi elles c est la seule s_2 [$c = (ca^x)^q$ étant de degré $\pi + 1$, il en est de même de ca^x]. Donc, \mathcal{G} étant deux fois transitif, toutes ses s_2 sont conjuguées et au nombre de π [il y a $\frac{1}{2}\pi(\pi+1)$ cycles binaires possibles, et chaque s_2 en a $\frac{1}{2}(\pi+1)$]. Donc c , par exemple, est normale dans un $g_{(\pi+1)q} \mathfrak{S}'$. D'ailleurs, \mathcal{G} a $\pi^2 - 1 s_p^\pi$ du type de b fixant un seul symbole, $\frac{1}{2}\pi(\pi+1)(q-1) s_q^{\pi-1}$ (q ' divisant q) conjuguées de ca^x ($ca^x \neq 1$) fixant deux symboles, $\frac{1}{2}\pi(\pi+1)(q-1) s_{2q}^{\pi+1}$ conjuguées de ca^x . Les $\pi + 1$ substitutions restantes qui sont les s_2 doivent être contenues dans \mathfrak{S}' et de même dans chaque conjugué de \mathfrak{S}' . Donc les s_2 sont permutables entre elles et forment avec l'unité un $g_{\pi+1} \mathfrak{S} = \{c_0, \dots, c_{n-1}\}$ ($c_0 = c$) normal dans \mathcal{G} (c'est le p. p. c. m. de $e_{(\pi+1)}$). Donc $\pi + 1$ est de la forme 2^n . Le procédé de démonstration précédent est emprunté à Frobenius (*S. A. B.*, 1902, p. 364), qui s'en est servi pour le cas $\pi = p$.

Je dis maintenant que $\pi = p$. Soit en effet v l'exposant auquel appartient $2 \pmod{p}$. On aura $n = kv$ et, $2^{kv} - 1$ étant divisible par $2^v - 1$, $2^v - 1$ a la forme p^μ et $p^m = \Sigma_i^k \binom{k}{r} p^{r\mu}$. Soit $k = p^x l$, $r = p^y s$ (l, s premiers à p): pour $r < p^x$, $\binom{k}{r} p^{r\mu}$ est divisible par $p^{r\mu+x-y}$ (*voir JORDAN, Traité*, p. 127) qui est $> p^{\mu+x}$ si r

est > 1 ; pour $r \geq p^x$, p^{rx} est $> p^{\mu+x}$ si $x > 0$. Donc $\Sigma_1^k \binom{k}{r} p^{rx}$ et, par suite, p^m est congru à $p^{\mu+x} l \pmod{p^{\mu+x+1}}$. Donc $k = 1$, $v = n$, $\mu = m$. De plus, m est impair, sans quoi $p^m + 1$ serait $\equiv 2 \pmod{8}$. Enfin $m = 1$, sans quoi $p + 1$, divisant $p^m + 1$, serait de la forme $2^n(n' < n)$ et 2 appartiendrait à l'exposant n' . Donc $\pi = p = 2^n - 1$. Donc n est premier et q divise $2^{n-1} - 1$.

Ces conditions sont suffisantes. En effet, \mathcal{S} étant normal dans $\mathcal{G} = A\mathcal{C}$, A divise le groupe linéaire $L(n, 2)$ à n variables mod 2 qui est d'ordre Kpq (K premier à p); donc, $B = \{b\}$ étant un g_p quelconque de L et a une s_q d'ordre impair permutable à $B^{(1)}$, on peut prendre $\{a, b\}$ pour A , et, une fois A choisi, \mathcal{G} n'a qu'une détermination qui est $A\mathcal{C}$. Les équations de \mathcal{G} s'obtiennent en adjoignant à celles de $\{\mathcal{S}, b\} = \{b, c\}$ sous la forme donnée (avec d'autres notations) au n° 3 ou sous la forme donnée dans le Mémoire déjà cité⁽²⁾ [j étant une racine primitive du corps galoisien C_{2^n} d'ordre 2^n et t parcourant C_{2^n} , on peut écrire $b = (jt) = (j^z, j^{z+1})$, $a = (j^z, j^{i^z})$, $c = (1-t)$] les équations $a^q = 1$, $a^{-1}ba = b^{i^z}$, $ac = ca$ (d'où $a^{-1}c_xa = ca_{xi^z}$ en posant $c_x = b^{-x}cb^x$).

On va voir que $q = 1$ ou n , en sorte que, si l'on fait abstraction du cas $q = 1$, \mathcal{G} est complètement déterminé pour tous les nombres premiers de la forme $2^n - 1$. Comme $q = n$ divise $2^{n-1} - 1$, on retrouve ce résultat que, si $q = \frac{1}{2}(p-1)$, on a $p = 7$.

Représentons désormais \mathcal{G} par les symboles de C_{2^n} , $A = \{a, b\}$ fixant 0, $\{a\}$ fixant 0, 1 et cherchons à adjoindre à \mathcal{G} une s_2 , $d = (t, \varphi t) = (1)(0\infty)\dots$, telle que, dans $\{\mathcal{G}, d\} = \mathcal{K}$, \mathcal{G} soit le diviseur fixant ∞ . Il faudra que $dbd = b^{-1}$, $da = ad$ (dad doit transformer dbd en $db^{i^z}d$) et que $(cd)^3$ soit dans $\{a\}$. La première condition donne $\varphi t = j\varphi(jt)(t \neq 0)$, d'où, en multipliant les équations répondant à $t = 1, j, \dots, j^z = \zeta$, $\varphi\zeta \equiv h\zeta^{-1} \pmod{2}$ ($h \equiv i^{-1}\varphi 1$). La troisième, en écrivant que $(cd)^3$ fixe 0 et 1, donne

(¹) La toujoures hors de B des éléments $\neq 1$ permutables à B , et il y en a d'ordre impair, sans quoi $\frac{1}{2}(p-1)$ étant impair, L serait impair et aurait un diviseur normal d'indice 2, tandis que ses facteurs de composition sont p et $(U, 1)$.

(²) *Journal de Mathématiques*, 1902, p. 263.

$h \equiv 1$ et devient $(cd)^3 = 1$. La deuxième donne $\varphi(j^{iz}) = \varphi(j^z)^i$, d'où $h^{i^n-1} \equiv 1$ qui est une identité si $q = 1$ et qui redonne $h \equiv 1$ (puisque $h^{2^n-1} \equiv h^p \equiv 1$) si $q > 1$. Les substitutions b, c, d sont les générateurs de $\mathcal{L}(2, 2^n) = \mathcal{O}(2, 2^n)$ dont elles vérifient les équations, et, comme les équations de \mathcal{K} s'obtiennent en adjointant à celles de $\{b, c, d\}$ $a^q = 1, a^{-1}ba = b^i, ca = ac, da = ad$, \mathcal{K} contient normalement \mathcal{L} . Or \mathcal{K} divise le groupe J des isomorphismes de \mathcal{L} qui est d'ordre $2^n(2^{2n}-1)n$ et n est premier. Donc $q = 1$ ou n et $\mathcal{K} = \mathcal{L}$ ou J .

Soit maintenant $\alpha = -1$. On a certainement une solution pour ζ en prenant $c = (rz^{-1})$, car on obtient alors, comme au n° 3 (voir le Mémoire cité), $cb_{\beta}c = b_{\bar{\beta}}ca^r b_r$ ($i\pi r\beta^2 = -r$), et ces équations jointes à celles de A définissent ζ . ζ est toujours d'indice γ dans $\mathcal{L}(2, \pi)$. Si donc γ est impair, $\gamma = 1$, sans quoi le p. g. c. d. de ζ , $\mathcal{O}(2, \pi)$ serait d'indice γ dans \mathcal{O} , et γ , qui divise $\pi - 1$, devrait être égal à $\pi + 1$ ou à π (ou à 6 si $\pi = 9$; mais 6 ne divise pas 8). Si γ est pair (donc π impair), ζ est d'indice $\frac{\gamma}{2}$ dans $\mathcal{O}(2, \pi)$ et l'on voit de même que $\gamma = 2$.

Les résultats précédents complètent et étendent au cas où m est > 1 les résultats partiels obtenus par M. Frobenius (*loc. cit.*) pour $m = 1$. On en déduit aisément aussi une nouvelle démonstration du théorème suivant, établi par le même géomètre à l'aide de la théorie des caractères :

Un $g_{pq(1+p)}^p$ G ayant exactement $1+p$ g_p est nécessairement un des groupes $\mathcal{L}(2, 5)$, $\mathcal{O}(2, 5)$, $\mathcal{O}(2, 7)$, $\mathcal{O}(2, 11)$.

En effet, le p. p. c. m. M d'ordre $pq'(1+p)$ des g_p de G est simple⁽¹⁾. Il est donc représentable en g^{p+1} et coïncide avec $\mathcal{O}(2, p)$. Donc $q' = \frac{1}{2}(p-1)$ ou $p-1$ et de même q . Si donc G est $\neq \mathcal{O}$ et n'est pas le produit direct de \mathcal{O} par un g_2 , il coïncide avec $\mathcal{L}(2, p)$. Mais $\mathcal{O}(2, p)$ n'est représentable en g^p que pour $p = 5, 7, 11$ et $\mathcal{L}(2, p)$ ne l'est que pour $p = 5$, ce qui démontre le théorème.

(1) MILLER, *P. L. M. S.*, t. XXXI, 1899, p. 148.
