BULLETIN DE LA S. M. F.

J. A. 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>

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* $1, \ldots, n, \sigma_1, \ldots, \sigma_t$, *où* A *est le groupe fixant* $\sigma_1, \ldots, \sigma_t$, F *le groupe fixant* $1 = \sigma_0, \sigma_1, \ldots, \sigma_t$, *sont qu'il existe des substitutions d'ordre* 2, $s_h = (\sigma_0)\ldots(\sigma_{h-2})(\sigma_{h-1}, \sigma_h)(\sigma_{h+1})\ldots(\sigma_t)\ldots$, telles que

$$\left\{\begin{array}{l} s_h^2 = 1, \qquad s_h f s_h = f_h, \qquad s_1 r s_1 = a' s_1 a'', \\ s_l a s_l = a_l, \qquad (s_i s_{i+1})^3 = f_{i1}, \qquad (s_j s_{j+k})^2 = f_{jk} \\ (h = 1, \ldots, t;\ i = 1, \ldots, t-1;\ j = 1, \ldots, t-2;\ k = 2, \ldots, t-j; \\ l = 2, \ldots, t;\ f \text{ parcourt les générateurs de F, } a \text{ ceux de A qui sont} \\ \text{hors de F; } r \text{ un système de restes} \not\equiv 1 \text{ de A mod F; } a', a'', a_l \text{ sont} \\ \text{dans A hors de F; } f_h, f_{i1}, f_{jk} \text{ dans F}), \end{array}\right.$$

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) $c = (0\infty)\ldots$ telle que A soit le diviseur fixant un symbole dans $\{A, c\} = G$. On devra avoir $cac = a^\alpha$, $\alpha^2 = 1$. Si $\alpha = 1$, comme $a = (i^0, i^1, i^2, \ldots)$, il faut que $c = (0\infty)(i^2, i^{x+\rho})$ 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* $g_{\pi(\pi^2-1)}\mathfrak{L} = \sum\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)$, *les paramètres* $\alpha, \beta, \gamma, \delta$ *parcourant* $C(\alpha\delta - \beta\gamma \not\equiv 0)$, z *parcourant* C *et* ∞ (2). On voit immédiatement par le même procédé que $\mathfrak{L}$ *ne peut être le diviseur fixant un symbole dans un* $g^{\pi+2}$. Les équations de $\mathfrak{L}$ s'obtiennent en adjoignant à celles de $\{a, b\}$ $c^2 = (cb)^3 = (ca)^2 = 1$.

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

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 $a=(i^2z)=(i^0, i^2, \ldots, i^{\pi-3})(i, i^3, \ldots, i^{\pi-2})$ et le $g_\pi^{\frac{\pi-1}{2}}$ 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 $a^{\frac{\pi-1}{2}}=b_h^p=1$, $b_hb_k=b_kb_h$, $a^{-1}b_ha=b_{i^2h}$, h, k parcourant 1, i, ..., i^{m-1} (si $i^\rho=\Sigma_0^{m-1}\alpha_{\rho s}i^s$, $b_{i^\rho}=\Pi_0^{m-1}b_{i^s}^{\alpha_{\rho s}}$). Cherchons à adjoindre à A une s_2 $c=(0\infty)\ldots$ telle que, dans $\mathcal{G}=\{A, c\}$, 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 $\equiv 3 \bmod 4$, c'est-à-dire que $\mathcal{G}=\mathfrak{V}(2,\pi)$, *sauf que, si* $\pi=7$, $\mathcal{G}$ *peut encore être le* g_{168}^8 *composé; et l'on obtient ainsi les équations de* $\mathfrak{V}$.

$\mathfrak{V}(2,\pi)$ *ne peut être le diviseur fixant un symbole* σ *dans un* $g^{\pi+2}$. Soit en effet d la s_2 à adjoindre à $\mathfrak{V}$ pour engendrer ce $g^{\pi+2}$ et supposons d'abord $\pi\equiv 1 \bmod 4$. On voit, comme dans la recherche précédente, que $d=(\sigma\infty)(z, \xi'_z z^{-1})$ $(z\not\equiv 0)$, $\xi'_z=r'^{i}=i^{2\rho'}$ ou $\xi'_z=s'=i^{2\sigma'}$ selon que z est carré ou non. On a $c=(rz^{-1})$, $dc=(\sigma 0\infty)(z, r\xi'^{-1}_z z)$ $(z\not\equiv 0)$, et $(dc)^3$, qui fixe o, doit être dans $\{a\}$, ce qui exige $r'=s'$. De plus d doit être permutable à A, donc à B, seul g_π de A; or $cb_hc=\left(\frac{r'z}{hz+r'}\right)$ n'est pas de la forme $(z+k)$. Si $\pi\equiv 3 \bmod 4$, 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 $g_{\frac{1}{2}p(p^2-1)}X$ qui a plus d'un g_p en a $p+1$. Si donc X est simple, il est représentable en $g^{p+1}=\mathfrak{V}(2,p)$.

Si $p=2q+1$ (q premier), X est encore représentable en g^{p+1} [donc isomorphe à $\mathfrak{V}(2,p)$ 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 $\pi\equiv 3 \bmod 4$), $c=(0\infty)$ $(i^{2x}, i^{2\rho+1-2x})=(z, rz^{-1})$ $(r=i^{2\rho+1})$. Or $cbc=\left(\infty, r, \frac{r}{2}, \frac{r}{3}, \ldots, -r\right)$, et $cb_\beta c$ devant être de la forme $b_x cb_{x'}b_{-t}a^\gamma b_t$, où t est arbitraire, il faut, pour $t=r$, que l'on ait $x=x'=r$, $cbc=b_r ca^\gamma b_r$: le second membre devant fixer o, $i^{2\gamma}$ doit être égal à $-r$, ce qui exige que l'on ait $\pi\equiv 3 \bmod 4$; alors γ 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_{56} de Mathieu. Si Y a $3\,g_8$, 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 $Q=\{a\}$. Y est défini par les équations de Δ, Q jointes à $d^2=1$, $db=bd$, $dc=cd$, $dad=a^2$. D'ailleurs X | ΔQ, 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 $\mathfrak{V}(2, 3^2)$ *est le seul* g_{360} *simple*, le théorème précédent fournissant une démonstration plus simple que celle donnée par M. Cole (1). Un g_{360} simple G a 10 ou 40 g_9. Supposons-en 40. Comme 40 est $\not\equiv 1 \bmod 9$, les g_9 ne sont pas premiers entre eux deux à deux. Soit $\{a\}$ un g_3 divisant deux g_9. Il en divisera $\nu\equiv 1 \bmod 3$ et le groupe A des éléments permutables à $\{a\}$ est d'ordre $k\nu 9$. G_7 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. a, 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 | $\{a\}$ est un g_{12} ayant 4 g_3 (il est donc tétraédral) et un g_4 non cyclique. Donc A a un g^9_{12} B $>\{a\}$ 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_{36} A formé des éléments permutables au g_9 B. 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 $\mathfrak{V}(2, 3^2)$.

5. Cherchons à construire un $g_{\pi(\pi^2-1)}$ (π impair > 3) G dont un groupe facteur soit $\mathfrak{V}(2, \pi)$. Le groupe des isomorphismes I de $\mathfrak{V}$ est $\{\mathfrak{V}, (iz), (z^p)\}$ en sorte que I | $\mathfrak{V}$ est un groupe abélien engendré par deux générateurs indépendants d'ordres respectifs 2 et m. $\mathfrak{V}$ est donc unique de son type dans I, car si I contenait un groupe $\mathfrak{V}' \neq \mathfrak{V}$ et isomorphe à $\mathfrak{V}$, il contiendrait $\mathfrak{V}\mathfrak{V}'$ et I | $\mathfrak{V}$ 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 $\mathfrak{L}(2, \pi)$, $\left\{\mathfrak{V}, \left(z^{p^{\frac{n}{2}}}\right)\right\} = \mathfrak{L}'$, $\left\{\mathfrak{V}, \left(iz^{p^{\frac{n}{2}}}\right)\right\} = \mathfrak{L}''$. Si m est impair, I n'a qu'un $g_{\pi(\pi^2-1)}$ qui est $\mathfrak{L}(2, \pi)$. G n'a pas d'autre type si sa seule suite de composition est G, $\mathfrak{V}$, 1.

Supposons que G admette la suite G, D, 1 (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 $\beta i^\gamma \equiv \varkappa$, G aura pour équations

$$a^{\frac{\pi-1}{2}} = d^\alpha, \quad b_k^h = d^{\delta_h}, \quad c^2 = d^\gamma, \quad d^2 = 1, \quad b_k^{-1} b_h b_k = b_k d^{\mu_{hk}},$$
$$a^{-1} b_h a = b_{i^{\varphi_h}} d^{\varphi_h}, \quad c^{-1} a c = a^{-1} d^\delta, \quad c^{-1} b_\beta d^{\theta_\beta} c = b_{\frac{-\varkappa^1}{\beta}} c a^{y_\beta} b_{\frac{-\varkappa^2}{\beta}},$$
$$da = ad, \quad db_h = b_h d, \quad dc = cd.$$

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 $\pi \equiv 3 \bmod 4$, car, a et $a^{-1} d$ n'étant pas alors du même ordre, on ne peut avoir $c^{-1} a c = a^{-1} d$. Soit donc $\pi \equiv 1 \bmod 4$: 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 $\mathfrak{V}(2, \pi)$, 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 $c'^2 = 1$, $c'^{-1} a c' = a^{-1} d$, $c'^{-1} b_\beta d^{\theta_\beta} c' = b_{\underline{-i^\varepsilon \chi^\beta}} c' a^{\gamma+1} b_{\underline{i^\varepsilon \chi^\beta}}$, et l'on a bien $\beta i^{\gamma+1} = i\chi$, de sorte qu'en changeant χ en $i\chi$ on est ramené au cas impossible $\gamma = 0$, $\delta = 1$. *Donc* $\delta = 0$. On aura

$$a^{-1} c^{-1} b_\beta d^{\theta_\beta} ca = b_{\underline{-\chi^\varepsilon i^\varepsilon}} ca^{\gamma+2} b_{\underline{-\chi^\varepsilon i^\varepsilon}} = c^{-1} b_{\beta i^{-\varepsilon}} d^{\theta_{\beta i^{-\varepsilon}}} c,$$

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

Soit d'abord $\pi \equiv 3 \bmod 4$. On peut toujours, en prenant au besoin ad pour a, supposer $\alpha = 0$. La formule précédente donne alors $c^{-1} b_{\underline{-\chi^\varepsilon}} c = d^\gamma b_\beta c a^{-\gamma_\beta} b_\beta$. Donc on n'aura que deux types : l'un répondant à $\gamma = 0$ est le produit direct de $\mathfrak{V}(2, \pi)$ 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 $\pi \equiv 3 \bmod 4$.

Soit $\pi \equiv 1 \bmod 4$. Prenons χ carré; y sera pair pour β carré et impair pour β non carré. En prenant donc ad^{θ_i} pour α, on aura, quel que soit β, $c^{-1} b_\beta c = b_{\underline{-\chi^\varepsilon}} ca^\beta b_{\underline{-\chi^\varepsilon}}$. 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 $\mathfrak{V}(2, \pi)$ par D; l'autre, répondant à $\gamma = \alpha = 1$, est $U(2, \pi)$ dont on a ainsi les équations pour $\pi \equiv 1 \bmod 4$.

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

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 o 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 $(o\infty)$; cc' sera dans $\{a\}$, soit $c' = ca^x$; et inversement ca^x a le cycle $(o\infty)$. 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* $\pi \equiv 3 \bmod 4$. Ici encore toute substitution de $\mathcal{G}$ ayant le cycle $(o\infty)$ 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^{π} 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 a^x ($a^x \neq 1$) 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 $g_{\pi+1}$ $\mathfrak{S} = \{c_0, \ldots, c_{n-1}\}$ ($c_0 = c$) 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 ν l'exposant auquel appartient $2 \bmod p$. On aura $n = k\nu$ et, $2^{k\nu} - 1$ étant divisible par $2^{\nu} - 1$, $2^{\nu} - 1$ a la forme p^{μ} et $p^m = \Sigma_1^k \binom{k}{r} p^{r\mu}$. Soit $k = p^{\varkappa} l$, $r = p^{\rho} s$ (l, s premiers à p) : pour $r < p^{\varkappa}$, $\binom{k}{r} p^{r\mu}$ est divisible par $p^{r\mu+\varkappa-\rho}$ (*voir* Jordan, *Traité*, p. 127) qui est $> p^{\mu+\varkappa}$ si r

est >1 ; pour $r \geq p^{\varkappa}$, $p^{r\mu}$ est $> p^{\mu+\varkappa}$ si $\varkappa > 0$. Donc $\Sigma_1^k \binom{k}{r} p^{r\mu}$ et, par suite, p^m est congru à $p^{\mu+\varkappa} l \bmod p^{\mu+\varkappa+1}$. Donc $k=1$, $\nu = n$, $\mu = m$. De plus, m est impair, sans quoi p^m+1 serait $\equiv 2 \bmod 8$. 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, $\mathfrak{S}$ étant normal dans $\mathcal{G} = A\mathfrak{S}$, 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 $A\mathfrak{S}$. Les équations de $\mathcal{G}$ s'obtiennent en adjoignant à celles de $\{\mathfrak{S}, b\} = \{b, c\}$ 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 $a^q = 1$, $a^{-1}ba = b^{i'}$, $ac = ca$ (d'où $a^{-1}c_x a = ca_{xi'}$ 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, $d = (t, \varphi t) = (1)(0\,\infty)\ldots$, telle que, dans $\{\mathcal{G}, d\} = \mathfrak{K}$, $\mathcal{G}$ soit le diviseur fixant ∞. Il faudra que $dbd = b^{-1}$, $da = ad$ (dad doit transformer dbd en $db^{i'}d$) et que $(cd)^3$ soit dans $\{a\}$. La première condition donne $\varphi t = j\varphi(jt)$ $(t \not\equiv 0)$, d'où, en multipliant les équations répondant à $t = 1, j, \ldots, j^z = \zeta$, $\varphi\zeta \equiv h\zeta^{-1} \bmod 2$ $(h \equiv i^{-1}\varphi 1)$. La troisième, en écrivant que $(cd)^3$ fixe 0 et 1, donne

(1) L a toujours 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 $\varphi(j^{i''z}) = \varphi(j^z)^{i''}$, d'où $h^{i''-1} \equiv 1$ 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 $\mathfrak{L}(2, 2^n) = \mathfrak{O}(2, 2^n)$ dont elles vérifient les équations, et, comme les équations de $\mathfrak{K}$ s'obtiennent en adjoignant à celles de $\{b, c, d\}$ $a^q = 1$, $a^{-1}ba = b^{i''}$, $ca = ac$, $da = ad$, $\mathfrak{K}$ contient normalement $\mathfrak{L}$. Or $\mathfrak{K}$ divise le groupe J des isomorphismes de $\mathfrak{L}$ qui est d'ordre $2^n(2^{2n}-1)n$ et n est premier. *Donc* $q = 1$ *ou* n *et* $\mathfrak{K} = \mathfrak{L}$ *ou* J.

Soit maintenant $\alpha = -1$. On a certainement une solution pour $\mathfrak{G}$ en prenant $c = (rz^{-1})$, car on obtient alors, comme au n° 3 (*voir* le Mémoire cité), $cb_\beta c = b_{\overline{\beta}}\, ca^\gamma b_{\overline{\beta}}$ $(i^{\gamma\gamma}\beta^2 = -r)$, et ces équations jointes à celles de A définissent $\mathfrak{G}$. $\mathfrak{G}$ est toujours d'indice γ dans $\mathfrak{L}(2, \pi)$. Si donc γ est impair, $\gamma = 1$, sans quoi le p. g. c. d. de $\mathfrak{G}$, $\mathfrak{O}(2, \pi)$ serait d'indice γ dans $\mathfrak{O}$, 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), $\mathfrak{G}$ est d'indice $\frac{\gamma}{2}$ dans $\mathfrak{O}(2, \pi)$ 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 $g^p_{pq(1+q)}$ G *ayant exactement* $1 + p$ g_p *est nécessairement un des groupes* $\mathfrak{L}(2, 5)$, $\mathfrak{O}(2, 5)$, $\mathfrak{O}(2, 7)$, $\mathfrak{O}(2, 11)$.

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 $\mathfrak{O}(2, p)$. Donc $q' = \frac{1}{2}(p - 1)$ ou $p - 1$ et de même q. Si donc G est $\neq \mathfrak{O}$ et n'est pas le produit direct de $\mathfrak{O}$ par un g_2, il coïncide avec $\mathfrak{L}(2, p)$. Mais $\mathfrak{O}(2, p)$ n'est représentable en g^p que pour $p = 5, 7, 11$ et $\mathfrak{L}(2, p)$ ne l'est que pour $p = 5$, ce qui démontre le théorème.

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