BULLETIN DE LA S. M. F.

J. A. DE SÉGUIER

Sur une proposition de Mathieu

Bulletin de la S. M. F., tome 31 (1903), p. 65-66
<http://www.numdam.org/item?id=BSMF_1903__31__65_0>

SUR UNE PROPOSITION DE MATHIEU;

Par M. DE SÉGUIER.

Mathieu a énoncé ce principe que *dans un groupe* $\mathcal{G}$ *transitif de degré* $q = 2p + 1$ (*p et q étant premiers*) *d'ordre* $< \frac{1}{2}(q!)$ *et* $> q(q-1)$, *les diviseurs d'ordre p sont permutables à des substitutions de degré* $2(p-1) = q - 3$ (*J. M.*, 1873, p. 26).

La démonstration que j'en ai donnée récemment (*J. M.*, 1902, p. 281) [1] peut être remplacée par la suivante, qui est beaucoup plus simple.

On verra toujours de la même manière que $\mathcal{G}$ n'a pas de diviseur d'ordre p^2 et que ses substitutions d'ordre p ont deux cycles. Soient N l'ordre du diviseur G de $\mathcal{G}$ qui fixe un symbole et dp l'ordre du groupe des substitutions permutables à un diviseur d'ordre p. On peut supposer que G n'a pas de substitutions paires, sans quoi on considérerait le plus petit multiple commun des substitutions paires. Alors le groupe des éléments de $\mathcal{G}$ permutables à un de ses diviseurs d'ordre q est d'ordre pq et $\mathcal{G}$ contient

$$\frac{\mathrm{N}q}{pq}(q-1) = 2\mathrm{N}$$

substitutions d'ordre q.

Si $d = 1$, G contient $\mathrm{N}\frac{p-1}{p}$ substitutions d'ordre p et $\mathcal{G}$ contient $2\mathrm{N} + \mathrm{N}q\frac{p-1}{p}$ substitutions ($\neq 1$) d'ordre p ou q.

Il reste donc dans $\mathcal{G}$, et de même dans G, $\frac{\mathrm{N}}{p}$ substitutions. Mais cela est impossible, les conjugués de G étant premiers entre eux.

On obtient une autre démonstration simple en s'appuyant sur ce théorème de M. Frobenius que les diverses substitutions de $\mathcal{G}$ fixent en tout qN symboles.

---

(1) Les inégalités hors texte de la page 281 doivent être remplacées par

$$\tfrac{1}{2}q\mathrm{N} + e_3 \geqq q\mathrm{N}\frac{p-1}{dp}, \qquad d > \frac{3}{2}\,\frac{p-1}{p},$$

et ne donnent $d \geqq 2$ que pour $p > 2$. Mais le cas $p = 2$ est obvie. On remarquera que, pour un groupe quelconque G d'ordre N, $e_1 + e_2 = \Sigma_1^n i g_i = \tau \mathrm{N}$, τ étant le nombre des systèmes d'intransitivité de G.

Je profiterai de l'occasion pour réparer une omission. Dans le Mémoire cité j'ai développé la démonstration (¹) de ce théorème qu'*un groupe de degré* $p+1$ *et d'ordre* $\frac{p(p^2-1)}{2}$ *deux fois transitif* (il est clair qu'il le sera deux fois, s'il l'est seulement une) *est nécessairement le groupe des substitutions* $\left(z, \frac{\alpha z+\beta}{\gamma z+\delta}\right)$ *où* $\alpha\delta-\beta\gamma\equiv 1 \pmod{p}$ *sauf si* $p=7$ *auquel cas il y a un autre type* (*C. R.*, avril 1901). M. Frobenius en a publié une nouvelle démonstration (*S. A. B.*, avril 1902) dont je n'ai eu connaissance que tout récemment.

(¹) Au dernier alinéa de la page 274 il faut faire $s=r$; mais le raisonnement n'en est que simplifié.