BULLETIN DE LA S. M. F.

ED. MAILLET

Des groupes primitifs de classe $N-1$ et de degré N

Bulletin de la S. M. F., tome 25 (1897), p. 16-32

<http://www.numdam.org/item?id=BSMF_1897__25__16_0>

DES GROUPES PRIMITIFS DE CLASSE N − 1 ET DE DEGRÉ N;

Par M. Ed. Maillet.

I.

Dans notre Thèse de Doctorat (p. 49-68) nous avons établi le théorème suivant :

Théorème. — *Les seuls groupes primitifs de classe* $N-1$ *et de degré* $N \leqq 101$ *sont ceux de degré* $N = p^m$ *(p étant premier) et sont linéaires à indices réels.*

Pour y arriver, nous avons établi un certain nombre de conditions auxquelles doit satisfaire N pour un groupe primitif G de degré N et de classe N − 1. Ainsi, on ne peut avoir N égal à $4h+2$, à pp_1, p^2p_1, $p^2p_1^2$, $p_1p_2p_3$, p_1p^3, les nombres premiers p, p_1, p_2, p_3 étant différents.

De même, soit (1) H le sous-groupe des substitutions de G qui laissent une même lettre de G immobile : on a $\mathcal{G} = N\mathcal{H}$, $\mathcal{H}$ divisant $N-1$, $N = n\mathcal{H}+1$, et G ne peut être primitif, si $\mathcal{H}$ est égal à 2 ou 3, ou si $n < 11$, que quand $N = p^m$. Ainsi, si $N-1$ est égal à q, $2q$ ou $3q$, q étant premier impair, G ne peut être primitif que si $N = 2^m$.

Enfin, les $N-1$ substitutions de G, qui sont de classe N, ne peuvent former avec l'unité un groupe de degré et d'ordre N que si ce groupe est régulier, $N = p^m$, et G linéaire à indices réels.

En nous appuyant sur ce qui précède, et aussi principalement sur ce lemme :

Lemme. — *Si* p^2 *est la plus haute puissance du nombre premier p qui divise l'ordre* $\mathcal{G}$ *d'un groupe quelconque* G, *on sait que* (2)

$$\mathcal{G} = p^{2\nu}(1+hp),$$

où $1+hp$ *est le nombre des groupes d'ordre* p^2 *contenu dans* G.

---

(1) Les ordres des groupes A, B, ..., G, H, ... seront désignés par $\mathfrak{A}, \mathfrak{B}, \ldots, \mathcal{G}, \mathcal{H}, \ldots$; de même (S), (T), ... seront les groupes des puissances de la substitution S, T, ...

(2) Sylow, *Math. Ann.*, t. V.

Alors G *contient au moins* $\frac{\mathcal{G}}{p^{2\nu}}(p^2-1)$ *substitutions d'ordre* $\equiv 0 \pmod p$;

et sur les théorèmes suivants :

THÉORÈME I. — *Un groupe primitif* G *de degré* $N = \rho p$ (p *premier impair,* $\rho > 1$ *et premier à* p) *et de classe* $N-1$ *ne peut exister si* $\rho < p+1$;

THÉORÈME II. — *Un groupe primitif* G *de degré* $N = \rho p^2$ (p *premier impair,* $\rho > 1$ *et premier à* p) *et de classe* $N-1$ *ne peut exister si* $\rho < p^2+1$;

THÉORÈME III. — *Un groupe primitif* G *de degré* $N = \rho p^m$ (p *premier impair,* $\rho > 1$ *et premier à* p) *et de classe* $N-1$ *ne peut exister que si* $\rho > \frac{p+1}{2}$;

nous conclurons (théorème IV) que le théorème énoncé au début a lieu pour toutes les valeurs de $N \leqq 201$.

II.

LEMME I. — *Soit* $\mathcal{G}'$ *l'ordre d'un groupe* L' *de substitutions tel que* $\mathcal{G}'$ *soit* $\equiv 0 \pmod p$ *et* $\not\equiv 0 \pmod{p^2}$, p *étant premier. On sait que* $\mathcal{G}' = p\nu_1(1+hp)$, *où* $1+hp$ *est le nombre des groupes d'ordre* p *contenus dans* L' : L' *contient au moins* $1+hp$ *substitutions d'ordre premier à* p (*y compris l'unité*).

En effet, $p\nu_1$ est l'ordre du groupe des substitutions de L' permutables au sous-groupe (T') des puissances d'une substitution T' d'ordre p de L'; si donc il y a, dans L', θ substitutions $\neq 1$ échangeables à T', ces substitutions sont permutables à (T'), en sorte que $\theta \leqq p\nu_1 - 1$. Le nombre des substitutions T'' différentes de 1 de L' telles qu'on puisse trouver une substitution d'ordre p de L' échangeable à T'' est donc au plus égal à $(1+hp)(p\nu_1-1)$, puisque $1+hp$ est le nombre des sous-groupes d'ordre p de L'. Or, toute substitution U_1 de L' d'ordre kp multiple de p (k premier à p) est de la forme UV (¹), où U est d'ordre k, V d'ordre p

(¹) En effet, on peut trouver φ et ψ premiers à kp et tels que $k\varphi + p\psi = 1$,

et U et V sont échangeables. Dès lors, UV étant échangeable à V, c'est-à-dire à une substitution d'ordre p, le nombre des substitutions de la forme UV, c'est-à-dire d'ordre $\equiv 0 \pmod p$, est au plus égal à $(p\nu_1 - 1)(1 + hp)$. Il en résulte de suite que le nombre des substitutions de L' (y compris la substitution 1) d'ordre $\not\equiv 0 \pmod p$ est au moins égal à

$$(1 + hp)p\nu_1 - (1 + hp)(p\nu_1 - 1) = 1 + hp.$$

En remarquant que le nombre des substitutions échangeables à (T') et d'ordre $\equiv 0 \pmod p$ est $\leqq (p - 1)\nu_1$, on voit même que L' renferme au moins $(1 + hp)\nu_1$ substitutions d'ordre premier à p.

THÉORÈME I. — *Un groupe primitif* G *de degré* $N = \rho p$ *(p premier impair, $\rho > 1$ et premier à p) et de classe* $N - 1$ *ne peut exister que si* $\rho < p + 1$.

En effet, l'ordre $\mathcal{G} = N\mathfrak{H}$ de G divise $N(N - 1)$, l'ordre $\mathfrak{H}$ du groupe H des substitutions de G laissant une lettre donnée de G immobile divisant $N - 1$, en sorte que $\mathcal{G}$ est $\equiv 0 \pmod p$ et $\not\equiv 0 \pmod{p^2}$. D'après un théorème de MM. Mathieu (1) et Sylow (2),

$$\mathcal{G} = p\nu(hp + 1),$$

où $hp + 1$ est le nombre des sous-groupes distincts d'ordre p de G. On ne peut avoir $h = 0$, sans quoi G contiendrait un sous-groupe invariant d'ordre $p \not\equiv 0 \pmod N$, ce qui est impossible, puisque G est primitif : donc $h \geqq 1$. G contient $hp + 1 \geqq p + 1$ sous-groupes distincts d'ordre p, par suite

$$(hp + 1)(p - 1) \geqq (p + 1)(p - 1) = p^2 - 1$$

substitutions d'ordre p, puisque deux sous-groupes distincts d'ordre p de G n'ont deux à deux d'autre substitution commune que l'unité. Ces substitutions sont d'ailleurs de classe $N = \rho p$, et puisque G renferme exactement $N - 1$ substitutions de classe N,

---

puisque k et p sont premiers entre eux, et l'on a $U_1^{k\gamma} U_1^{p\gamma'} = U_1$, et il suffit de prendre $U = U_1^{p\gamma'}$, $V = U_1^{k\gamma}$.

(1) *J. de Math.*, 1861.

(2) SYLOW, *loc. citat.*

dont quelques-unes d'ordre diviseur de ρ, il faut

$$N - 1 = \rho p - 1 > (hp + 1)(p - 1) \geq p^2 - 1,$$

et $\rho > p$ (1). C. Q. F. D.

Remarque. — Cette limite inférieure peut être améliorée dans une foule de cas : en effet, $hp + 1$ doit diviser $\rho(\rho p - 1)$, et est au moins égal au plus petit diviseur de $\rho(\rho p - 1)$ qui soit $\equiv 1 \pmod{p}$. On en conclut :

Théorème I *bis.* — *Soit* G *un groupe primitif de degré* $N = \rho p$ (p *premier impair,* $\rho > 1$ *et premier à* p) *et de classe* $N - 1$; *si* $lp + 1$ *est le plus petit diviseur de* $\mathcal{G}$, *et* a fortiori *de* $\rho(\rho p - 1)$ *qui soit* $\equiv 1 \pmod{p}$, *on a* : $\rho > l(p - 1) + 1$.

Supposons que $r = \lambda p + 1$ divise $\rho(\rho p - 1)$, d'où

$$\rho^2 \frac{r - 1}{\lambda} - \rho \equiv 0 \pmod{r} \quad \text{et} \quad -\rho^2 - \lambda\rho = -\rho(\rho + \lambda) \equiv 0 \pmod{r},$$

en sorte que r divise $\rho(\rho + \lambda)$. On en conclut :

Corollaire I. — *Si le nombre* $ip + 1$ *ne divise pas le nombre* $\rho(\rho + i)$, *pour une au moins des valeurs de* i *égales à* $1, 2, \ldots, \lambda$, *on en conclut que* $l \geq \lambda + 1$, *d'où*

$$\rho > (\lambda + 1)(p - 1) + 1.$$

En particulier quand $\lambda = 1$, il faut $\rho > 2p - 1$, et, puisque ρ est premier à p, $\rho \geq 2p + 1$; d'où :

Corollaire II. — *Si* $\rho(\rho + 1)$ *n'est pas divisible par* $p + 1$, *on a* $\rho \geq 2p + 1$.

Corollaire III. — *Soit* q *un nombre premier impair, et* $p = kq - 1$; *si* ρ *n'est pas de la forme* $k'q$ *ou* $k'q - 1$, *on a*

$$\rho \geq 2p + 1.$$

Car $\rho(\rho + 1) \not\equiv 0 \pmod{q}$, et $p + 1 \equiv 0 \pmod{q}$, en sorte que $p + 1$ ne divise pas $\rho(\rho + 1)$.

---

(1) Les limites inférieures trouvées ici sont plus avantageuses que celles indiquées dans notre Thèse de Doctorat, p. 67.

COROLLAIRE IV. — *Si p est de la forme $15k+2$, et ρ d'une des deux formes $15k'+1$ ou $15k'+7$, on a $\rho \geqq 3p-1$.*

Car $p+1 \equiv 0 \pmod 3$, en sorte que $p+1$ ne divise pas $\rho(\rho+1)$, et $2p+1 \equiv 0 \pmod 5$, en sorte que $2p+1$ ne divise pas $\rho(\rho+2)$.

Et ainsi de suite.

LEMME II. — *Soit p^2 la plus haute puissance du nombre premier p qui divise l'ordre $\mathcal{G}$ d'un groupe quelconque* G; *on sait que*

$$\mathcal{G} = p^2\nu(1+np),$$

où $p^2\nu$ est l'ordre du groupe des substitutions de G *permutables à un sous-groupe* H *d'ordre p^2 de* G. *Alors* G *contient au moins $\frac{\mathcal{G}}{p^2\nu}(p^2-1)$ substitutions d'ordre $\equiv 0 \pmod p$.*

En effet, on sait(1) que les sous-groupes d'ordre p^2 de G sont les transformés d'un quelconque d'entre eux par les substitutions de G, en nombre $1+np$, et que (2) $1+np = 1+n_1p+n_2p^2$, où n_1p est le nombre des transformés de H ayant en commun avec H une substitution d'ordre p, n_2p^2 le nombre des transformés de H n'ayant en commun avec H d'autre substitution que l'unité. De plus les substitutions de H sont échangeables.

Soit S une substitution de H d'ordre p; elle est échangeable à toutes les substitutions de H, et à toutes celles des transformés de H par G dont elle fait partie; le groupe L des substitutions échangeables à S contient H et ces transformés. Si

$$\mathcal{L} = p^2\nu'(1+hp),$$

$p^2\nu'$ étant l'ordre du sous-groupe des substitutions de L permutables à H, et $1+hp$ le nombre des sous-groupes d'ordre p^2 de L, lesquels sont les transformés de H par L, chacun de ces transformés contient S, puisque toute substitution g de L est échangeable à S et que $g^{-1}Hg$ contient dès lors S. On a $h \leqq n_1$.

---

(1) SYLOW, *loc. citat.*

(2) *Voir* notre Mémoire des *Ann. Fac. Sc. de Toulouse,* 1895, D. 7, et 1896, A. 17.

Soit $h > 0$ (ce qui n'a lieu que si $n_1 \not\equiv 0$) : L contient le sous-groupe H d'ordre p^2 qui n'y est pas invariant, tandis que (S) y est invariant. Dès lors (¹), L est isomorphe à un groupe L′ transitif, de degré $\frac{f}{p^2} = (1+hp)\nu'$, et d'ordre $\frac{f}{p} = (1+hp)p\nu'$, le groupe H′, qui correspond à H dans L′, étant formé des puissances d'une substitution S′ d'ordre p, et $p\nu'$ étant l'ordre du groupe des substitutions de L′ permutables à H′. Au groupe (S) de L correspond dans L′ la substitution 1, et réciproquement.

D'après le lemme I, L′ contient au moins $1 + hp$ substitutions d'ordre premier à p. Soit donc :

$$\tau_1 = 1, \quad \tau_2, \quad \ldots, \quad \tau_\lambda, \quad \text{avec } \lambda \geqq 1 + hp, \tag{1}$$

les λ substitutions de L′ d'ordre premier à p,

$$\sigma_1 = 1, \quad \sigma_2, \quad \ldots, \quad \sigma_\lambda \tag{2}$$

λ substitutions de L telles que σ_i soit une des substitutions correspondant à τ_i ($i = 1, 2, \ldots, \lambda$). A la substitution τ_i de L′ correspondent dans L les p substitutions

$$\sigma_i, \quad S\sigma_i, \quad S^2\sigma_i, \quad \ldots, \quad S^{p-1}\sigma_i \tag{3}$$

de L, par suite aux λ substitutions (1) les $p\lambda$ substitutions distinctes de L

$$\left\{\begin{array}{l} \sigma_1 = 1, \quad S, \quad S^2, \quad \ldots, \quad S^{p-1}, \\ \sigma_2, \quad S\sigma_2, \quad S^2\sigma_2, \quad \ldots, \quad S^{p-1}\sigma_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \sigma_\lambda, \quad S\sigma_\lambda, \quad S^2\sigma_\lambda, \quad \ldots, \quad S^{p-1}\sigma_\lambda. \end{array}\right. \tag{4}$$

Si φ_k est l'ordre de σ_k, $\sigma_k^{\varphi_k} = 1$ correspond à $\tau_k^{\varphi_k}$, en sorte que $\tau_k^{\varphi_k} = 1$, et que l'ordre ψ_k, premier à p, de τ_k, divise celui de σ_k, *a fortiori* celui de $\sigma_k S^j$, σ_k et S^j étant échangeables : donc les $p\lambda$ substitutions (4) sont contenues dans L, et, puisque $\varphi_k > 1$, pour $k > 1$, sont d'ordre $\not\equiv p^\alpha (\alpha = 1 \text{ ou } 2)$, sauf celles de la première ligne. De plus $\tau_k^{\psi_k} = 1$ correspond aux p substitutions

$$\sigma_k^{\psi_k} = S^{u_k}, \qquad (S\sigma_k)^{\psi_k} = S^{\psi_k + u_k}, \qquad (S^2\sigma_k)^{\psi_k} = S^{2\psi_k + u_k}, \quad \ldots,$$
$$(S^{p-1}\sigma_k)^{\psi_k} = S^{u_k + (p-1)\psi_k},$$

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

formant la première ligne de (4). Parmi ces p substitutions on en a une $(S^l\sigma_k)^{\psi_k} = S^{u_k+l\psi_k} = 1$, à savoir celle pour laquelle l est tel que $u_k + l\psi_k \equiv 0 \pmod p$. Son ordre ψ_k, le même que celui de τ_k, est premier à p; les $p-1$ autres ont pour ordre $p\psi_k$, en sorte que, dans chaque ligne de (4), il y a une et une seule substitution d'ordre premier à p : nous pourrons évidemment supposer que ce soit celle de la première colonne, puisque nous avons seulement supposé que $\sigma_i (i = 1, 2, \ldots, \lambda)$ était une des substitutions de L correspondant à τ_i dans L', sans rien spécifier de plus. Les substitutions de la $k^{\text{ième}}$ ligne, sauf $\sigma_k (k = 1, 2, \ldots, \lambda)$, étant d'ordre p ou $p\psi_k$, sont toutes d'ordre $\not\equiv 0 \pmod{p^2}$ et $\equiv 0 \pmod p$. Nous pourrons faire correspondre au sous-groupe (S) de G le Tableau Θ formé des $(p-1)\lambda$ substitutions des $p-1$ dernières colonnes de (4).

Si alors S_1 est une substitution d'ordre p de G non contenue dans (S), L_1 le groupe correspondant analogue à L, formé des substitutions de G échangeables à S_1, on a

$$\mathfrak{L}_1 = (1 + h_1 p) p^2 \nu'_1, \tag{5}$$

$1 + h_1 p$ étant le nombre des groupes d'ordre p^2 contenus dans L_1; et l'on voit de même que L_1 contient les $p\lambda_1$ substitutions distinctes

$$\left\{\begin{array}{lllll} \sigma'_1 = 1, & S_1, & S_1^2, & \ldots, & S_1^{p-1}, \\ \sigma'_2, & S_1\sigma'_2, & S_1^2\sigma'_2, & \ldots, & S_1^{p-1}\sigma'_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & & & \\ \sigma'_{\lambda_1}, & S_1\sigma'_{\lambda_1}, & S_1^2\sigma'_{\lambda_1}, & \ldots, & S_1^{p-1}\sigma'_{\lambda_1}, \end{array}\right. \tag{6}$$

qui sont d'ordre $\equiv 0 \pmod p$, et $\not\equiv 0 \bmod p^2$, sauf celles de la première ligne qui sont d'ordre premier à p. On a

$$\lambda_1 \geq 1 + h_1 p,$$

d'après le lemme I, et l'on peut faire correspondre au sous-groupe (S_1) de G le Tableau Θ_1 formé des $(p-1)\lambda_1$ substitutions des $p-1$ dernières colonnes de (6). Les substitutions de Θ_1 diffèrent d'ailleurs de celles de Θ, car si

$$S^j\sigma_k = S_1^{j'}\sigma'_k \qquad [j \text{ et } j' \not\equiv 0 \pmod p],$$

et si ψ_k, ψ'_k sont les ordres respectifs, premiers à p, de σ_k, σ'_k, on

aura

$$(S^j\sigma_k)\psi_k = (S_1^{j'}\sigma_k')\psi_k = S^j\psi_k = S_1^{j'\psi_k}\sigma_k^{j'\psi_k}.$$

Or $S^j\psi_k$ est d'ordre p : donc $\sigma_k^{j'\psi_k p} = 1$, en sorte que ψ_k' divise $p\psi_k$, par suite ψ_k; de même ψ_k divise

$$\psi_k', \quad \text{et} \quad \psi_k = \psi_k',$$

d'où

$$S^j\psi_k = S_1^{j'\psi_k},$$

ce qui est impossible, puisque $(S) \not\equiv (S_1)$.

On peut continuer de la sorte : à chaque groupe (S_q) des puissances d'une substitution S_q d'ordre p de G nous ferons correspondre un Tableau ou ensemble Θ_q de substitutions analogue à Θ et Θ_1, et tel que les ensembles

$$(7) \qquad \Theta, \quad \Theta_1, \quad \Theta_2, \quad \ldots, \quad \Theta_q, \quad \ldots$$

correspondant à

$$(8) \qquad (S), \quad (S_1), \quad (S_2), \quad \ldots, \quad (S_q), \quad \ldots$$

respectivement, n'aient deux à deux aucune substitution commune, et contiennent respectivement au moins

$$(9) \quad (1+hp)(p-1), \quad (1+h_1p)(p-1), \quad \ldots, \quad (1+h_qp)(p-1), \quad \ldots$$

substitutions autres que l'unité, distinctes de celles des autres ensembles, et toutes d'ordre $\equiv 0 \pmod p$ et $\not\equiv 0 \bmod p^2$, $1+h_qp$ étant le nombre des transformés de H par les substitutions de G qui ont en commun (S_q).

Quand on aura $h = 0$, au groupe (S) d'ordre $\not\equiv 1$, nous ferons correspondre l'ensemble θ des $p-1$ substitutions de S d'ordre $\equiv 0 \pmod p$.

Enfin, si T est une substitution de G d'ordre p^2, elle ne peut être commune à deux groupes distincts d'ordre p^2: aux $p(p-1)$ substitutions de (T) d'ordre p^2, on fera correspondre l'ensemble Θ' de ces mêmes substitutions.

Les substitutions des ensembles Θ, θ, Θ' sont évidemment distinctes.

Ceci posé, considérons l'ensemble A obtenu en écrivant successivement les substitutions $\not\equiv 1$ des divers transformés H, H_1, H_2, ...

de H par les substitutions de G; l'ensemble B formé de celles de ces substitutions qui sont distinctes; l'ensemble C des ensembles Θ, θ, Θ' obtenus précédemment.

D'après ce qui précède, A contient

$$(1 + n_1 p + n_2 p^2)(p^2 - 1) = \frac{G}{p^{2\nu}}(p^2 - 1)$$

substitutions : une substitution S d'ordre p et ses puissances y sont répétées chacune $1 + hp$ fois, $1 + hp$ ayant même signification que précédemment; A contient ainsi exactement $(1 + hp)(p - 1)$ substitutions appartenant à (S) et $\not\equiv 1$. A ces substitutions correspondent dans B les $p - 1$ substitutions de (S) $\not\equiv 1$, et dans C les $\lambda(p - 1) \geqq (1 + hp)(p - 1)$ substitutions distinctes d'ordre $\equiv 0 \pmod p$, et $\not\equiv 0 \pmod{p^2}$, de l'ensemble Θ. Aux substitutions de A appartenant à (S_1), S_1 étant d'ordre p et non contenu dans (S), correspondent de même dans C les $\lambda_1 (p - 1) \geqq (1 + h_1 p)(p - 1)$ substitutions d'ordre $\equiv 0 \pmod p$ et $\not\equiv 0 \pmod{p^2}$ de l'ensemble Θ_1; et ainsi de suite.

De même pour les substitutions S d'ordre p pour lesquelles $h = 0$: aux $p - 1$ substitutions de (S) dans A correspondent dans B et C les $p - 1$ substitutions de l'ensemble θ.

Finalement, si Φ est le nombre des substitutions de A qui sont d'ordre p, à l'ensemble de ces Φ substitutions correspond dans C un ensemble de $\Lambda \geqq \Phi$ substitutions distinctes d'ordre $\equiv 0 \pmod p$ et $\not\equiv 0 \pmod{p^2}$.

D'autre part, d'après ce qui précède, une substitution d'ordre p^2 figurera une fois et une seule dans A et C; si Ψ est le nombre des substitutions de G d'ordre p^2, c'est aussi le nombre des substitutions distinctes de C d'ordre p^2.

La considération de A donnant $\Phi + \Psi = \frac{G}{p^{2\nu}}(p^2 - 1)$, on voit que C, par suite G, contient

$$\Lambda + \Psi \geqq \frac{G}{p^{2\nu}}(p^2 - 1)$$

substitutions distinctes d'ordre $\equiv 0 \pmod p$. C. Q. F. D.

Remarque. — Ce lemme n'est qu'une extension de cette pro-

priété due à Mathieu (¹) que si G est d'ordre $\equiv 0 \pmod{p}$ et $\not\equiv 0 \pmod{p^2}$, p étant premier, on a

$$\mathcal{G} = p^\nu (1 + np),$$

où $1 + np$ est le nombre des sous-groupes de G d'ordre p, et G contient au moins $(1 + np)(p - 1) = \frac{\mathcal{G}}{p^\nu}(p - 1)$ substitutions d'ordre $\equiv 0 \pmod{p}$.

Corollaire. — *Dans un groupe* G *de degré* p^2 *transitif, et d'ordre* $\not\equiv 0 \pmod{p^3}$, *mais* $> p^2$, *on a* $\nu > 1$.

En effet, si $\nu = 1$, et si H est l'ordre du groupe H des substitutions de G laissant une lettre donnée de G immobile, G contient $\frac{\mathcal{G}}{p^2}(p^2 - 1) = \mathcal{K}(p^2 - 1)$ substitutions d'ordre $\equiv 0 \pmod{p}$, c'est-à-dire de classe p^2, et seulement $\mathcal{K}$ autres substitutions, ce qui est absurde, puisque G est transitif et contient toujours, en dehors des $\mathcal{K}$ substitutions de H d'ordre premier à p, quelques substitutions laissant une lettre de G immobile, par suite d'ordre premier à p, et n'appartenant pas à H.

Théorème II. — *Un groupe primitif* G *de degré* $N = \rho p^2$ (p *premier impair*, ρ *premier à* p *et* > 1) *ne peut exister si* $\rho < p^2 + 1$.

La démonstration est analogue à celle du théorème I. L'ordre $\mathcal{G} = N\mathcal{K}$ de G divise $N(N - 1)$, l'ordre $\mathcal{K}$ du groupe H des substitutions de G laissant une lettre donnée immobile divisant $N - 1$, en sorte que $\mathcal{G}$ est $\equiv 0 \pmod{p^2}$ et $\not\equiv 0 \pmod{p^3}$. On a

$$\mathcal{G} = p^{2\nu}(1 + n_1 p + n_2 p^2).$$

On ne peut avoir $n_2 = 0$, sans quoi (²) G contiendrait un sous-groupe invariant d'ordre p^θ ($\theta = 1$ ou 2), et ne serait pas primitif. D'après le lemme précédent G contient au moins

$$(1 + n_1 p + n_2 p^2)(p^2 - 1)$$

(¹) *J. de Liouville*, 1861.
(²) *Ann. Fac. Sc. de Toulouse*, 1896, A. 17.

substitutions d'ordre $\equiv 0 \pmod{p}$, par suite de classe N, puisque une de leurs puissances est d'ordre p, par suite de classe N. Il y a d'ailleurs des substitutions d'ordre diviseur de ρ qui sont de classe N, et $N-1$ substitutions de classe N, puisque G est primitif et de classe $N-1$. Donc

$$N-1=\rho p^2-1>(1+n_1p+n_2p^2)(p^2-1)\geqq(p^2+1)(p^2-1)=p^4-1,$$

d'où

$$\rho>p^2,$$

c'est-à-dire

$$\rho\geqq p^2+1.$$

Remarque. — Cette limite inférieure peut être améliorée dans une foule de cas : en effet, $1+n_1p+n_2p^2$ doit diviser $\rho(\rho p^2-1)$, et est égal au moins au plus petit diviseur de $\rho(\rho p^2-1)$ qui soit $\equiv 1 \pmod{p}$ et $\geqq p^2+1$. On en conclut :

Théorème II *bis.* — *Soit* G *un groupe primitif de degré* $N=\rho p^2$ (*p premier impair et premier à* $\rho>1$) ; *de classe* $N-1$, *si* $1+np$ *est le plus petit diviseur de* ρ, *et* a fortiori *de* $\rho(\rho p^2-1)$ *qui soit* $\geqq p^2+1$ *et* $\equiv 1 \pmod{p}$, *on a*

$$\rho>\frac{1+(1+np)(p^2-1)}{p^2}.$$

On en déduit des corollaires analogues à ceux du théorème I *bis*. Si $r=\lambda p+1$, avec $\lambda\geqq p$, divise $\rho(\rho p^2-1)$, d'où

$$\rho^2\left(\frac{r-1}{\lambda}\right)^2-\rho\equiv 0 \pmod{r},$$
$$\rho^2(r-1)^2-\rho\lambda^2\equiv 0 \pmod{r},$$

r divise $\rho^2-\rho\lambda^2=\rho(\rho-\lambda^2)$, $(\rho>p^2)$.

Corollaire I. — *Si le nombre* $ip+1$ *ne divise pas le nombre* $\rho(\rho-i^2)$, *où* $\rho>p^2$, *pour une au moins des valeurs* $p, p+1, \ldots, \lambda$ *de* i, $(\lambda\geqq p)$, *on a* $n\geqq\lambda+1$;

$$\rho>\frac{1+[1+(\lambda+1)p](p^2-1)}{p^2}.$$

Corollaire II. — *Si* $\rho(\rho>p^2)$ *n'est pas égal à* p^2+1, *on a* $\rho\geqq p(p+1)$.

En effet, si $\rho(\rho - p^2)$ n'est pas divisible par p^2+1, d'après le corollaire précédent, on a $n \geqq p+1$,

$$\rho p^2 > 1 + (1 + p + p^2)(p^2 - 1) = p^4 + p^3 - p$$

et

$$\rho \geqq p(p+1).$$

Si $\rho(\rho - p^2) \equiv 0 \,[\mathrm{mod}(p^2+1)]$ et $\rho = p^2 + i$, on a

$$\rho(\rho - p^2) \equiv (p^2 + 1 + i - 1)i \equiv (i-1)i \qquad [\mathrm{mod}(p^2+1)],$$

et si $i > 1$, p^2+1 ne peut diviser $\rho(\rho - p^2)$ que si $i > p$.

Corollaire III. — *Soit q un nombre premier de la forme $4l+1$, a et b les deux racines de la congruence*

$$\xi^2 + 1 \equiv 0 \qquad (\mathrm{mod}\, q).$$

Sp est un nombre premier d'une des formes $kq + a$ ou $kq + b$, il faut $\rho \geqq p(p+1)$, quand ρ n'est pas de la forme

$$(4h+2)q = p^2 + 1.$$

Car on a $p^2 + 1 = (4h+2)q$, et il n'y a qu'à appliquer le corollaire II.

Et ainsi de suite.

Remarque. — Signalons encore que les théorèmes I et II permettent de démontrer très simplement qu'il n'existe aucun groupe primitif G de classe N — 1 et de degré N, quand N est d'une des formes pq, pq^2, p^2q^2, où p et q sont des nombres premiers différents (1). Ainsi pour $N = p^2q^2$, si par exemple $p > q$, G devrait contenir au moins $(p^2+1)(p^2-1) = p^4 - 1$ substitutions de classe N, ce qui exigerait $p^4 - 1 \leqq N - 1 = p^2q^2 - 1$ ou $p \leqq q$, contrairement à l'hypothèse.

Théorème III. — *Un groupe primitif* G *de degré* $N = \rho p^m$, *et de classe* N — 1 (p *premier impair*, $\rho > 1$ *et premier à* p) *ne peut exister que si* $\rho > \frac{p+1}{2}$.

En effet, on sait que, si G est primitif, il ne peut contenir un

(1) Thèse de Doctorat, p. 58 et suiv.

sous-groupe invariant d'ordre $\not\equiv 0 \pmod N$, puisqu'un sous-groupe invariant de G est transitif (¹). Par suite, si $\rho > 1$, G ne peut contenir un sous-groupe invariant d'ordre $p^\theta (1 \leqq \theta \leqq m)$. Dès lors, d'après la formule de M. Sylow (²),

$$\mathcal{G} = p^m \nu (1 + np),$$

où $n > 0$, $p^m \nu$ étant l'ordre du sous-groupe des substitutions de G permutables à un sous-groupe P d'ordre p^m de G : tous les sous-groupes d'ordre p^m de G sont les transformés de P par les substitutions de G, sont en nombre $1 + np$, et toute substitution d'ordre $p^\theta (1 \leqq \theta \leqq m)$ de G est contenue dans l'un d'eux ; leurs substitutions déplacent N lettres, et, à part l'unité, font partie des N — 1 substitutions de classe N de G.

Or, deux groupes P_1, P_2 transformés quelconques de P par G ont en commun au plus p^{m-1} substitutions dont l'unité. Considérons alors les divers transformés

$$P_1, P_2, \ldots, P_{1+np}$$

de P par G :

P_1 renferme $p^m - 1$ substitutions d'ordre diviseur de p^m et > 1 ;

P_2 renferme au moins $p^m - p^{m-1}$ substitutions d'ordre diviseur de p^m et > 1, et différentes de celles de P_1 ;

P_3 renferme au moins $p^m - p^{m-1} - (p^{m-1} - 1)$ substitutions d'ordre diviseur de p^m et > 1, et différentes de celles de P_1 et P_2 ;

. . . . . .

P_{p+1} renferme au moins $p^m - p(p^{m-1} - 1) - 1 = p - 1$ substitutions d'ordre diviseur de p^m et > 1, et différentes de celles de $P_1, \ldots, P_p$.

Donc, G renferme au moins

$$(p+1)p^m - (p^{m-1} - 1)p\frac{p+1}{2} - (p+1) = \frac{p+1}{2}[p^m + p - 2]$$

substitutions dont l'ordre est > 1 et divise p^m.

Or ρ est > 1 et premier à p ; il y a dans G des substitutions de

---

(¹) JORDAN, *Traité des Subst.*, p. 41

(²) *Loc. cit.*

classe N d'ordre premier à p, et il faut

$$N-1=\rho p^m-1>\frac{p+1}{2}(p^m+p-2),$$

d'où

$$\rho>\frac{p+1}{2}.$$

C. Q. F. D.

III.

Grâce aux théorèmes précédents et à ceux que nous avons rappelés dans le paragraphe I, nous pouvons établir le théorème suivant :

Théorème IV. — *Les seuls groupes primitifs de classe* $N-1$ *et de degré* $N\leqq 201$ *sont ceux de degré égal à* p^m (*p étant premier*) *et sont linéaires à indices réels.*

En effet, d'après un théorème connu (¹), il suffit d'établir que ces groupes ne peuvent exister que pour les valeurs de N égales à p^m, p étant premier. D'ailleurs nous savons déjà que ce théorème est vrai pour $N\leqq 101$.

La décomposition en facteurs premiers des nombres N compris entre 101 et 201 montre que les seuls de ces nombres qui ne pourraient satisfaire au théorème IV, en vertu des théorèmes rappelés dans le paragraphe I, sont les nombres $120=2^3.3.5$, $144=3^2.2^4$, $156=2^2.3.13=12.13$, $176=2^4.11$. Le théorème I permet d'écarter de suite la valeur $N=12.13=156$, et le corollaire III du théorème I *bis*, quand on y fait $q=3$,

$$p=11\equiv -1 \pmod 3,$$

donne, si $\rho\equiv 1\pmod 3$, $\rho\geqq 23$, ce qui permet d'écarter la valeur $N=2^4.11=176$, pour laquelle $\rho=16\equiv +1\pmod 3$.

Examinons spécialement les valeurs $N=120$ et $N=144$. Nous nous appuierons sur les lemmes suivants :

Lemme III. — *Dans un groupe transitif* G, *d'ordre* $\mathcal{G}=N\mathcal{H}$, *de classe* $N-1$ *et de degré* N, *le nombre des substitutions de*

(¹) Thèse de Doctorat, n. 54.

classe N *semblables à une substitution de classe* N *de* G *est un multiple de* $\mathfrak{K}$.

En effet, les substitutions de G sont toutes régulières (¹), puisque G est de classe N — 1 ; si g est une substitution de G de classe N, par suite régulière, φ l'ordre du groupe Φ des substitutions de G échangeables à g, ces substitutions sont toutes de classe N, et φ divise N, en sorte que $\frac{\mathcal{G}}{\varphi} \equiv 0 \pmod{\mathfrak{K}}$, g ayant d'ailleurs exactement $\frac{\mathcal{G}}{\varphi}$ transformées distinctes par G. Une substitution g', semblable à g, et distincte de ces $\frac{\mathcal{G}}{\varphi}$ transformées, aura de même par G $\frac{\mathcal{G}}{\varphi'}$ transformées distinctes et distinctes des $\frac{\mathcal{G}}{\varphi}$ précédentes, avec $\frac{\mathcal{G}}{\varphi'} \equiv 0 \pmod{\mathfrak{K}}$; et ainsi de suite. Donc le nombre des substitutions de G, semblables à g, est

$$\frac{\mathcal{G}}{\varphi} + \frac{\mathcal{G}}{\varphi'} + \ldots = \mathfrak{K}\left(\frac{N}{\varphi} + \frac{N}{\varphi'} + \ldots\right) \equiv 0 \pmod{\mathfrak{K}}.$$

Lemme IV. — *On sait que dans un groupe transitif* G *d'ordre* $\mathcal{G} = N\mathfrak{K}$, *de classe* N — 1 *et de degré* $N = \rho p$ (p *étant premier et* $\rho > 1$ *et premier à* p), *on a, d'après la formule de M. Sylow,* $\mathcal{G} = p^{\nu}(1 + hp)$, *et* G *renferme* $(1 + hp)(p - 1)$ *substitutions d'ordre* p, *toutes de classe* N.

Lemme V. — *Tout étant posé comme au lemme IV, si*

$$N = \rho_1 p_1 = \rho_2 p_2 = \ldots = \rho_k p_k,$$

où ρ_1 *est premier à* p_1, ρ_2 *premier à* p_2, ..., ρ_k *premier à* p_k, *et* $p_1, p_2, \ldots, p_k$ *premiers entre eux, on a*

$$\mathcal{G} = p_1^{\nu_1}(1 + h_1 p_1) = \ldots = p_k^{\nu_k}(1 + h_k p_k),$$

d'après la formule de M. Sylow, et G *renferme*

$$\sum_{1}^{k} i(h_i p_i + 1)(p_i - 1)$$

substitutions de classe N *et d'ordre* $p_1, p_2, \ldots, p_k$.

(¹) On remarquera, en effet, que, dans un groupe de classe u, les substitutions de classe u et $u + 1$ sont régulières; de même, les substitutions de classe $u + i$ et d'ordre premier $p > i$.

LEMME VI. — *Dans un groupe* G *d'ordre* $\mathcal{G} = N\mathcal{H}$, *où* $\mathcal{H}$ *est un nombre premier,* $N = \rho p^m$ (*p premier,* $\rho > 1$ *et premier à p*), *la formule de M. Sylow étant* $\mathcal{G} = p^m\nu(1 + hp)$, *où* $1 + hp$ *est le nombre des sous-groupes de* G *d'ordre* p^m, *on a*

$$1 + hp \equiv 0 \pmod{\mathcal{H}},$$

et $1 + hp \geqq 2\mathcal{H}$.

En effet, sinon on aurait $\nu \equiv 0 \pmod{\mathcal{H}}$, et G renfermerait un sous-groupe d'ordre $p^m\nu$ contenant H (puisque $\mathcal{H}$ est premier); H ne serait pas maximum dans G, qui ne serait pas primitif (1). Alors, si $1 + hp = \mathcal{H}$, G renfermerait un sous-groupe d'ordre $p^m\nu = N$, et serait (2) linéaire et de degré p^m et non ρp^m.

1° $N = 120 = 2^3.3.5$, $N - 1 = 119 = 7.17$. G étant supposé primitif, on a $N = n\mathcal{H} + 1$, avec $n \geqq 11$, et $\mathcal{H}$ diviseur de $N - 1$; il faut donc $\mathcal{H} = 7$ et $\mathcal{G} = 2^3.3.5.7$.

D'après le lemme IV, $\mathcal{G} = 5\nu(1 + 5h)$ et G renferme $5h + 1$ groupes d'ordre 5, $(5h + 1)4$ substitutions d'ordre 5, et, puisque $\mathcal{H} = 7$, d'après le lemme III, $5h + 1$ est $\equiv 0 \pmod 7$ et divise $\frac{\mathcal{G}}{5} = 2^3.3.7$.

Les diviseurs de ce nombre de la forme $5h + 1$ et divisibles par 7 sont $21 = 3.7$ et $56 = 7.2^3$. D'ailleurs

$$(5h + 1)4 < N - 1 = 119 \qquad \text{et} \qquad 5h + 1 < \frac{119}{4} < 30.$$

On ne pourrait donc avoir que $5h + 1 = 21$, $\nu = 2^3 = 8$, et G renfermerait $(5h + 1)4 = 84$ substitutions d'ordre 5.

On peut raisonner de même sur le diviseur premier 3 de $N = 120$: $\mathcal{G} = 3\nu'(1 + 3h')$ et G renferme $1 + 3h'$ groupes d'ordre 3, et $(3h' + 1)2$ substitutions d'ordre 3, avec

$$(3h' + 1)2 \equiv 0 \pmod 7,$$

d'après les lemmes IV et VI; $3h' + 1$ divise $\frac{\mathcal{G}}{3} = 2^3.5.7$. De plus,

---

(1) W. DYCK, *Math. Ann.*, t. XX et XXII, et notre Thèse de Doctorat, p. 18.
(2) Thèse de Doctorat, p. 53.

d'après le lemme V appliqué aux nombres premiers 3 et 5, on a

$$8\mathfrak{f} + 2(3h'+1) < 120,$$

d'où $3h'+1<18$. Il n'y a qu'un diviseur $3h'+1$ de $2^3.5.7$ qui soit $\equiv 0 \pmod 7$ et <18, c'est 7. Or, d'après le lemme VI, on ne peut avoir $3h'+1=\mathfrak{K}$, et l'on n'a pas de groupe primitif de classe 119 et de degré 120. C. Q. F. D.

2° $N=144=2^4.3^2$, $N-1=143=13.11$. G étant supposé primitif, $N=n\mathfrak{K}+1$, avec $n\geqq 11$, en sorte que $\mathfrak{K}$ est égal à 11 ou 13.

a. Soit $\mathfrak{G}=144.13$, $\mathfrak{G}=(3l+1)\nu.3^2$, et G renferme $3l+1$ groupes distincts d'ordre 3^2; d'après le lemme VI, $\mathfrak{K}$ étant premier, on a $3l+1\equiv 0 \pmod{13}$, c'est-à-dire que $3l+1$, divisant $2^4.13$, est un des nombres 13, $2^2.13$, $2^4.13$.

D'après le lemme II, G renferme au moins $(3l+1)(3^2-1)$ substitutions d'ordre $\equiv 0 \pmod 3$. Ces substitutions étant de classe $N=144$, on a

$$(3l+1)(3^2-1)=(3l+1)8<144,$$

d'où $3l+1<\frac{144}{8}=18$, ce qui exigerait $3l+1=13$, contrairement au lemme VI.

b. Soit $\mathfrak{G}=144.11$. $\mathfrak{G}=(3l+1)\nu.3^2$, et G renferme $3l+1$ groupes d'ordre 3^2; d'après le lemme VI, $\mathfrak{K}$ étant premier, on a $3l+1\equiv 0 \pmod{11}$, c'est-à-dire que $3l+1$ divisant $2^4.11$ est un des nombres 2.11 ou $2^3.11$.

D'après le lemme II, on a encore $3l+1<18$, en sorte que G ne peut exister.

On n'a donc pas de groupe primitif de classe 143 et de degré 144.

C. Q. F. D.

Le théorème IV se trouve ainsi complètement établi.