

BULLETIN DE LA S. M. F.

J. A. DE SÉGUIER

Sur certains groupes d'ordre $p^m q^n$

Bulletin de la S. M. F., tome 33 (1905), p. 242-250

[<http://www.numdam.org/item?id=BSMF_1905__33__242_0>](http://www.numdam.org/item?id=BSMF_1905__33__242_0)

© Bulletin de la S. M. F., 1905, 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 D'ORDRE $p^m q^n$;

Par M. J. DE SÉGUIER.

Dans la recherche des groupes d'ordre $p^m q^n$ (p, q premiers) pour les premières valeurs de m et de n , un cas s'impose de suite à l'attention : c'est celui où le groupe considéré G contient normalement un g_{p^m} abélien principal ⁽¹⁾ A , aucun $e_{(q^n)}$ n'étant permutable à tout élément de A .

C'est ce cas et un autre cas voisin que je vais considérer.

1. B étant un g_{q^n} quelconque de G , on a $G = AB$, et comme B divise ici le groupe $L(m, p)$ des isomorphismes de A ⁽²⁾, G divise l'holomorphe K de A . Je supposerai K, L , et B pris sous la forme de groupes concrets de substitutions linéaires, en sorte que G est complètement déterminé par B (tout système de générateurs réels de B joint à une base de A forme un système de générateurs de G sur lequel on lit les équations du groupe). Soient $\mathfrak{B}$ un système de générateurs de B , $(\mathfrak{B})$ l'ensemble des conjugués de $\mathfrak{B}$ dans L ; $\mathfrak{B}, \mathfrak{B}', \dots$, des systèmes de générateurs de B non conjugués dans L . J'appellerai l'ensemble $(\mathfrak{B}) + (\mathfrak{B}') + \dots$ la *catégorie* des systèmes des générateurs de B . Si $\mathfrak{B}$ parcourt un système de *représentants* des catégories des divers g_{q^n} de L , $\{A, \mathfrak{B}\}$ fournira tous les types cherchés chacun une fois, car deux g_{q^n} distincts de L ne peuvent être formés des mêmes isomorphismes de A avec lui-même.

On remarquera que, l'ordre de B étant premier à p , la forme canonique d'un élément quelconque de B est complètement déterminée par la fonction caractéristique de cet élément.

⁽¹⁾ Je me servirai de la même terminologie et des mêmes notations que dans mes *Éléments de la théorie des groupes abstraits* (Paris, Gauthier-Villars, 1904), auxquels je renverrai par la lettre E .

⁽²⁾ Cf. HÖLDER, *M. A.*, t. XLVI, 1895, p. 325. Le groupe $L(m, p)$ est le groupe des substitutions linéaires (mod p) à m variables. Sur ce point et sur la définition de l'holomorphe, voir MOORE, *S. M. A.*, t. II, 1895, p. 33; HÖLDER, *loc. cit.*, ou BURNSIDE, *Theory of groups*, p. 243, 228.

2. Soit désormais $B = \{b\}$ cyclique. On sait construire *a priori* toutes les formes canoniques de b . Cherchons les b^β ayant même forme canonique que b . Si $(b) = (b^\beta)$ (β est alors premier à q), on a évidemment $(b^x) = (b^{\beta x})$. Si donc $(b) = (b^\beta) = (b^{\beta'})$, on a $(b) = (b^{\beta\beta'})$. Donc $\beta, \beta', \dots$ forment un groupe B_0 qui divise le $g_{\varphi(q^n)}$ engendré par une racine primitive α de q^n . B_0 est donc cyclique; soit $B_0 = \{\beta\}$. $(B_0, 1) = \delta$ est l'ordre de $\beta \bmod q^n$. $(b^x), (b^{\beta x}), \dots, (b^{\beta^{\delta-1}x})$ coïncidant quel que soit x , les $\varphi(q^n)$ classes (b^x) où x est premier à q coïncident δ à δ et les $\frac{\varphi(q^n)}{\delta}$ classes distinctes se réunissent en une catégorie. Supposons que q^{n-i} soit diviseur propre de $p^{r_i} - 1$ ($i = 0, \dots, n; r_0 = r$). Les facteurs irréductibles de la fonction caractéristique Δ_b de b appartiendront chacun à un des q^{n-i} . Soit ρ_i le nombre des facteurs irréductibles appartenant à l'exposant q^{n-i} (ils sont tous de degré r_i), ρ_{is} le nombre de ceux qui sont de multiplicité s que je désignerai par $P_{is1}, \dots, P_{is\rho_i}$. $\rho_0 = \rho$ sera ≥ 1 et $\rho_n = m - \sum_{i=0}^{n-1} \rho_i r_i$ est le nombre des facteurs linéaires de racine 1. Si ξ est une racine de P_{ist} et ξ' de $P_{ist'}$ ($t' \neq t$), ξ^x sera, pour x premier à q , de même ordre que ξ et distinct de ξ'^x , car, si $xx' \equiv 1 \bmod q^n$, l'égalité $\xi^x \equiv \xi'^x$ (je sous-entendrai toujours le module p) élevée à la puissance x' donnera $\xi \equiv \xi'$. Les nombres r_i, ρ_{is} sont donc les mêmes pour b^x que pour b , et l'on pourra dire que $G, b, (b), \Delta_b, B$ appartiennent à la répartition $(\rho_{01}, \rho_{02}, \dots; \rho_{11}, \rho_{12}, \dots)$ (lorsque les ρ_{is} seront donnés, je supprimerai dans la parenthèse ceux qui sont tous nuls à partir d'un certain rang).

B_0 étant formé de tous les $x \bmod q^n$ tels que $(b^x) = (b)$ ou $\Delta_{b^x} = \Delta_b$, à chaque x de B_0 répondra une substitution (z, z^x) des racines z de Δ_b . Donc B_0 est isomorphe au groupe $B_1 = \{(z, z^\beta)\}$ et l'on peut définir β et δ par la condition que (z, z^β) soit une substitution d'ordre maximum δ conservant Δ_b . Je dirai que δ est l'indice de Δ_b . Si z appartient à l'exposant q^{n-i} , le cycle de (z, z^β) où il figure est $(z, z^\beta, \dots, z^{\beta^{\delta_i-1}})$, δ_i étant l'exposant auquel appartient $\beta \bmod q^{n-i}$ [δ_i divise δ_{i-1} et $\delta_0 = \delta$ divise $\varphi(q^n)$]. Si β^{ω_i} est la première puissance de β qui soit congrue $\bmod q^{n-i}$ à une puissance de p , (z, z^β) permute $P_{is1}, \dots, P_{is\rho_i}$ par cycles de ω_i ; donc ω_i divise ρ_{is} , ρ_{is} divise δ_i , et le plus petit commun multiple π des ω_i divise celui des ρ_{is} et celui δ des δ_i . β^π est la première puissance

de β congrue mod q^n à une puissance de p , et $(z, z^\beta)^\varpi$ est la première puissance de (z, z^β) qui ne permute pas les P_{it} . Donc $(z, z^\beta)^\varpi r = 1$ et δ divise ϖr . On remarquera que B_1 devant contenir $\{(z, z^p)\}$, δ est multiple de r . Si $\delta = kr$, $(z, z^\beta)^k$ est d'ordre r ; donc β^k est d'ordre $r \bmod q^n$ et est par suite une puissance de p (B_1 n'a qu'un diviseur d'ordre r qui est $\{(z, z^p)\}$). Donc k est multiple de ϖ et $\delta = \varpi r$.

Soit n_δ le nombre des fonctions caractéristiques d'indice δ répondant à une répartition $(\rho_{01}, \dots)$. Le nombre $N_{\rho_{01}, \dots}$ des types de G répondant à la répartition sera $\sum_\delta \frac{\delta n_\delta}{\varphi(q^n)}$.

3. En particulier la répartition (1) donne lieu à $\frac{\varphi(q^n)}{r}$ fonctions caractéristiques. Si $r > 1$, on peut supposer β est, pour chacune d'elles, $\equiv p \bmod q^n$, et comme p est d'ordre $r \bmod q^n$, on a $\delta = r$, d'où $N_1 = 1$. Soit donc θ d'ordre q^n dans C_{p^r} et $\theta^r = \sum_0^{r-1} \alpha_i \theta^i$. Si $n = 1$,

$$\alpha_0 = (-1)^{r-1} \theta^{\sum_0^{r-1} p^i} = (-1)^{r-1}$$

(q , diviseur propre de $p^r - 1$, divise $\sum_0^{r-1} p^i$). La forme canonique générale de b répondant à la répartition (1) est

$$|y'_i = \theta^{p^i} y_i; y'_j = y_j| \quad (i = 0, \dots, r-1; j = r, \dots, m-1);$$

y_i est une fonction des variables réelles à coefficients dans C_{p^r} , y_j une fonction des variables réelles à coefficients dans C_p . Si $y'_i = \sum_0^{r-1} \theta^{k p^i} x_k$, $y'_j = x_j$, la forme canonique réelle qui s'obtient en prenant les x pour variables est

$$b = |x'_0 = \alpha_0 x_{r-1}, x'_i = x_{i-1} + \alpha_i x_{r-1}, x'_j = x_j| \\ (i = 1, \dots, r-1; j = r, \dots, m-1).$$

Les substitutions

$$a_k = |x'_k = x_k + 1, x'_i = x_i| \quad (i, k = 0, \dots, m-1; i \neq k)$$

engendrent A , et les équations de G s'obtiennent en adjoignant à celles de A

$$b q^n = 1, \quad b^{-1} a_k b = a_{k+1} \quad (k = 0, \dots, r-2), \\ b^{-1} a_{r-1} b = \Pi_0^{r-1} a_i^{q^i}, \quad b^{-1} a_k b = a_k \quad (k = r, \dots, m-1).$$

Comme ces équations sont vérifiées par des substitutions engendrant effectivement un $g_{p^m q^n}$, on est assuré *a priori* qu'elles définissent bien un $g_{p^m q^n}$ (E., 18). Il est clair que $\{b\}$ n'est primaire⁽¹⁾ que si $r = m$, et le groupe G correspondant divise le $g_{p^m(p^m-1)}$ de Mathieu. On voit d'ailleurs que, pour la répartition (1) ($r < m$), G est le produit direct d'un diviseur du $g_{p^r(p^r-1)}$ de Mathieu par un groupe abélien principal. Ces résultats complètent ceux obtenus par MM. Miller et Moreno sur les groupes dont tous les diviseurs sont abéliens (*Transact. of the Am. math. Soc.*, t. IV, 1903, p. 398).

4. Soit $n = 1$ et $\rho = 2$. Considérons d'abord la répartition (2). Elle donne lieu à $\frac{1}{2} \frac{q-1}{r} \left(\frac{q-1}{r} - 1 \right)$ fonctions caractéristiques de la forme $\Delta_\delta = PP'$, P et P' étant distincts, irréductibles, de degré r . Si $r > 1$, q est ici > 2 . Si $r = 1$ et $q = 2$, le nombre des fonctions caractéristiques est 1 et il n'y a qu'un type dont on trouvera les équations au n° 5. Soit donc $q > 2$ et $p \equiv g^\pi \pmod{q}$, g étant une racine primitive de $q \left(\pi = \frac{q-1}{r} \right)$. On sait *a priori* que $\delta = r$ ou $2r$. Cherchons dans quel cas $\delta = 2r$. Alors β^2 est de la forme $g^{\pi\tau}$, τ étant premier à r et pris mod r . π ne peut pas être impair, car r et τ seraient pairs et $\beta \equiv \pm p^{\frac{\tau}{2}}$ serait une puissance de $p \left(-1 \equiv p^{\frac{r}{2}} \pmod{q} \right)$. Soit donc $\pi = 2\pi'$ et d'abord r pair $= 2r'$. Alors $-1 \equiv p^{\pi'} \pmod{q}$ et les racines de tout polynôme P ou P' sont deux à deux inverses l'une de l'autre. De plus τ est impair, sans quoi $\beta = p^{\frac{\tau}{2}}$ serait une puissance de p . En remplaçant au besoin β par β^{τ_1} ($\tau_1 \equiv 1 \pmod{r}$) on peut supposer que $\beta^2 \equiv g^\pi$ et que $\beta \equiv g^{\pi'}$. Alors (z, z^β) est bien d'ordre $2r$ et pour chaque P il y a un seul P' ayant les racines z^β , c'est-à-dire que PP' a $\frac{q-1}{2r} = \frac{\pi}{2}$ déterminations pour lesquelles $\delta = 2r$. Soit maintenant r impair. En changeant au besoin τ en $\tau + r$, on peut supposer τ pair $= 2\tau'$. Alors $\beta \equiv -p^{\tau'}$, P' est déterminé par la condition que ses racines

(1) JORDAN, *Traité des substitutions*. p. 110.

soient les inverses de celles de P et il y a encore $\frac{\pi}{2}$ fonctions PP' telles que $\delta = 2r$. Donc si p est non carré mod q (alors π est impair donc r pair), $\delta = r$; $n_r = \frac{1}{2}\pi(\pi - 1)$; $N_2 = \frac{q-r-1}{2r}$.

Si p est carré mod q (alors π est pair), $\delta = r$ ou $2r$; $n_{2r} = \frac{\pi}{2}$, $n_r = \frac{1}{2}\pi(\pi - 1) - \frac{\pi}{2} = \frac{\pi^2}{2} - \pi$; $N_2 = \frac{q-1}{2r}$.

Soit par exemple $r = 1$. En remplaçant au besoin b par une de ses puissances, on peut toujours représenter la catégorie de b par

$$b_\lambda = |x'_0 = \alpha x_0, x'_1 = \alpha^\lambda x_1, x'_i = x_i| \quad (i = 2, \dots, m-1; \lambda \not\equiv 1 \pmod{q}),$$

α étant une racine primitive arbitraire de $\alpha^q \equiv 1$. Les $\frac{q-1}{2}$ types s'obtiennent alors en faisant parcourir à λ un système de valeurs $\not\equiv 1 \pmod{q}$ dont aucune ne soit inverse d'une autre mod q ; car, pour que b_λ et $b_{\lambda'}$ appartiennent à la même catégorie, c'est-à-dire pour que b_λ'' soit conjuguée de $b_{\lambda'}$ dans $L(m, p)$, il faut et suffit (si $\lambda \not\equiv \lambda' \pmod{q}$) que $\alpha^\mu \equiv \alpha^{\lambda'}$, $\alpha^{\mu\lambda} \equiv \alpha$ ou que $\lambda\lambda' \equiv 1 \pmod{q}$. De là les types

$$\alpha_i^p = b^q = 1, \quad a_i a_j = a_j a_i, \quad b^{-1} a_0 b = a_0^\alpha, \quad b^{-1} a_1 b = a_1^{\alpha^\lambda}, \quad b^{-1} a_h b = a_h; \\ (i, j = 0, \dots, m-1; h = 2, \dots, m-1).$$

La répartition $(0, 1)$ donne de suite $N_{0,1} = 1$. Les équations du type correspondant se déduisent des précédentes en y faisant $\lambda = 1$.

§. Considérons pour $r = 1$ la répartition $(\rho_{01}, \dots, \rho_{0v})$. n_δ ne sera $\neq 0$ que si : 1° δ divise $\rho_{01} = h_1 \delta, \dots, \rho_{0v} = h_v \delta$ et $\varphi(q^n) = Q = \mathbb{N} \delta$; 2° on peut ranger $\Sigma \rho_{0s} = \rho_0 = \rho$ des Q nombres x appartenant à l'exposant q^n en séries de δ termes, la $i^{\text{ième}}$ étant $x_i, x_i^\beta, \dots, x_i^{\beta^{\delta-1}}$. Alors on pourra prendre pour les ρ_{01}, P_{01t} les racines de h_1 quelconques de ces séries, puis pour les ρ_{02}, P_{02t} celles de h_2 quelconques des séries restantes, etc. Le nombre

$$\binom{K}{h_1} \binom{K-h_1}{h_2} \dots = \frac{K!}{h_1! h_2! \dots}$$

des déterminations de Δ_b ainsi obtenues, est $\geq n_\delta$ (car on peut seulement affirmer que ces Δ_b ont pour indice un multiple de δ); il est égal à δ si δ est le plus grand commun diviseur des ρ_{0s} et

de Q ; si ce plus grand commun diviseur d est premier, δ prend les seules valeurs 1, d , et $n_1 = \frac{Q!}{\rho_{01}! \rho_{02}! \dots} - n_d$.

A chaque choix des z_i répondent une forme canonique de b et des équations de G qui s'écrivent immédiatement. Mais il est plus simple encore de former à la fois tous les types répondant à une valeur de ρ . La forme canonique générale correspondante de b est $|x'_i = \theta_i x_i, x'_j = x_j|$ ($i = 0, \dots, \rho - 1; j = \rho, \dots, m - 1; \theta_i \neq 1$). Les types de G qu'elle détermine sont

$$a_h^p = b^p = 1, \quad a_h a_k = a_k a_h, \quad b^{-1} a_i b = a_i^{\theta_i}, \quad b^{-1} a_j b = a_j \\ (h, k = 0, \dots, m - 1; i = 0, \dots, \rho - 1; j = \rho, \dots, m - 1).$$

On peut prendre $\theta_i = \alpha^{\lambda_i} (\neq 1)$, α étant une racine primitive arbitraire de $\alpha^n \equiv 1$, $\lambda_0 = 1$ et $\lambda_1, \dots, \lambda_{\rho-1}$ parcourant des valeurs telles que, dans deux des systèmes $\alpha, \alpha^{\lambda_1}, \dots, \alpha^{\lambda_{\rho-1}}$, les exposants n'aient jamais de valeurs proportionnelles mod q^n , quel que soit l'ordre où l'on prend les α^{λ_i} .

6. Cherchons enfin les $g_{p^m q^n}$ G ayant un g_{p^m} normal A de figure (1) (11...1) et un g_{q^n} cyclique, lorsque G/D (D étant le central de A) répond à la répartition (1) pour $r = m - 1$.

m étant impair ($E.$, 143), soit $m = 2v + 1$. G aura des équations de la forme ($E.$, 144, 145)

$$a^p = j^q = 1, \quad c_1^p = a^\varepsilon, \quad d_1^p = a^\eta, \quad c_h^p = d_h^p = 1 \quad (h = 2, \dots, v), \\ c_i c_k = c_k c_i, \quad d_i d_k = d_k d_i, \quad c_i d_k = d_k c_i, \quad c_i^{-1} d_i c_i = d_i a \\ (i, k = 1, \dots, v; i \neq k),$$

$$j^{-1} a j = a^\varepsilon, \quad j^{-1} c_i j = a^{\lambda_i} \Pi_l c_l^{\alpha_l} d_l^{\beta_l}, \quad j^{-1} d_i j = a^{\mu_i} \Pi_l c_l^{\gamma_l} d_l^{\delta_l}; \\ \text{si } p > 2, \quad \varepsilon = 0, 1, \quad \eta = 0; \quad \text{si } p = 2, \quad \varepsilon = \eta = 0, 1,$$

les $\alpha, \beta, \gamma, \delta$ satisfaisant aux conditions suivantes :

ξ et le déterminant Δ des $\alpha, \beta, \gamma, \delta$ sont $\neq 0$,

$$(1) \quad \begin{cases} \Sigma_j (\alpha_{ji} \delta_{jk} - \beta_{ji} \gamma_{jk}) \equiv 0 \text{ si } i \neq k, & \equiv \xi \text{ si } i = k, \\ \Sigma_j (\alpha_{ji} \beta_{jk} - \beta_{ji} \alpha_{jk}) \equiv \Sigma_j (\gamma_{ji} \delta_{jk} - \delta_{ji} \gamma_{jk}) \equiv 0, \end{cases} \quad i, j, k = 1, \dots, v,$$

et, en observant que $\Pi_l c_l^{\alpha_l} d_l^{\beta_l}$ par exemple est égal à

$$a^{\frac{n(n-1)}{2} \sum_k \alpha_{ki} \beta_{ki}} \Pi_k c_k^{\alpha_{ki}} d_k^{\beta_{ki}}$$

et que, si $p = 2$, tout nombre x est $\equiv x^2$,

$$(2) \quad \text{si } p > 2 \text{ et } \varepsilon = 1, \quad \alpha_{11} \equiv \xi, \quad \alpha_{1h} \equiv 0, \quad \gamma_{1i} \equiv 0, \quad h > 1, \quad i \geq 1,$$

$$(3) \quad \text{si } p = 2, \quad \sum_k \alpha_{ki} \beta_{ki} + \varepsilon(\alpha_{1i}^2 + \beta_{1i}^2) \equiv \sum_k \gamma_{ki} \delta_{ki} + \varepsilon(\gamma_{1i}^2 + \delta_{1i}^2) \equiv \begin{cases} \varepsilon & \text{si } i = 1, \\ 0 & \text{si } i > 1. \end{cases}$$

Ce sont les conditions d'automorphisme, etc. (*E.*, 19). Un calcul direct montre que, d'après (1), $\Delta^2 \equiv \xi^2 v$.

7. Pour l'intelligence de ce qui va suivre je présenterai d'abord sous une forme particulière des résultats dus à M. Jordan (*Traité des substitutions*).

Remplaçons un instant l'équation $j^{\eta} = 1$ par $j^{\mu} = 1$ et considérons j comme un isomorphisme de A avec lui-même, remplaçant

$$\begin{aligned} a & \text{ par } a\xi = a', & c_i & \text{ par } a^{\lambda_i} \Pi_l c_l^{\alpha_{li}} d_l^{\beta_{li}} = a^{\lambda_i} c'_i, \\ d_i & \text{ par } a^{\mu_i} \Pi_l c_l^{\gamma_{li}} d_l^{\delta_{li}} = a^{\mu_i} d'_i. \end{aligned}$$

On aura les équations de $\{A, j\}$. Or le groupe des substitutions $|Dc_i, Dd_i; Dc'_i, Dd'_i|$ ($D = \{a\}$) qui représente l'action du groupe J des isomorphismes de G sur $G|D$ est le groupe H des isomorphismes contragrédients de G (HÖLDER, BURNSIDE, *loc. cit.*) et divise le groupe $L(2v, p)$ des isomorphismes de $G|D$. $G|D$ est isomorphe au groupe $\odot$ des substitutions $|x_i, y_k; x_i + g_i, y_k + h_k|$ et H à celui $\S$ des substitutions

$$(4) \quad s = |x_i, y_i; \sum_k (\alpha_{ik} x_k + \gamma_{ik} y_k), \sum_k (\beta_{ik} x_k + \delta_{ik} y_k)|.$$

Un calcul direct montre d'après (1) que

$$s' = |x_i, y_i; \sum_k (\alpha'_{ik} x_k + \gamma'_{ik} y_k), \sum_k (\beta'_{ik} x_k + \delta'_{ik} y_k)|$$

vérifie $ss' = 1$ toujours et seulement si $\xi \alpha'_{ik} = \delta_{ki}$, $\xi \gamma'_{ik} = -\gamma_{ki}$, $\xi \beta'_{ik} = -\beta_{ki}$, $\xi \delta'_{ik} = \alpha_{ki}$. Les conditions (1), (2), (3) écrites pour s^{-1} donnent donc les conditions suivantes respectivement équivalentes en vertu de (1) :

$$\begin{aligned} (1') \quad & \begin{cases} \sum_j (\alpha_{ij} \delta_{kj} - \beta_{ij} \gamma_{kj}) \equiv 0 & \text{si } i \neq k, & \equiv \xi & \text{si } i = k, \\ \sum_j (\alpha_{ij} \beta_{kj} - \beta_{ij} \alpha_{kj}) \equiv \sum_j (\delta_{ij} \delta_{kj} - \delta_{ij} \gamma_{kj}) \equiv 0, & i, j, k = 1, \dots, v, \end{cases} \\ (2') \quad & \text{si } p > 2 \text{ et } \varepsilon = 1, \quad \delta_{11} \equiv \xi^2, \quad \delta_{h1} \equiv 0, \quad \gamma_{11} \equiv 0, \quad h > 1, \quad i \geq 1, \\ (3') \quad & \text{si } p = 2, \quad \sum_k \gamma_{ik} \delta_{ik} + \varepsilon(\beta_{i1}^2 + \delta_{i1}^2) \equiv \sum_k \alpha_{ik} \gamma_{ik} + \varepsilon(\alpha_{i1}^2 + \gamma_{i1}^2) \equiv \begin{cases} \varepsilon & \text{si } i = 1, \\ 0 & \text{si } i > 1. \end{cases} \end{aligned}$$

Comme (1') donne, d'après (2), $\delta_{11} \equiv 1$, (2') montre que $\xi^2 \equiv 1$ (lorsque p est $> r$ et $\varepsilon = 1$). La condition (1) ou (1') qui dérive des équations de A est nécessaire et suffisante pour que l'exposant $F = \sum_i (X_i y_i - Y_i x_i)$ de a dans l'un des commutateurs de $\Pi_i c_i^{\gamma_i} d_i^{\gamma_i}$, $\Pi_i c_i^{\gamma_i} d_i^{\gamma_i}$ garde sa forme (mod p) au facteur ξ près lorsqu'on lui applique la substitution s (opérant sur les X_i , Y_i comme sur les x_i , y_i). Si s multiplie F par ξ , s^{-1} multiplie F par ξ^{-1} . Si $p > 2$, (2) ou (2') qui dérive des équations de A est la condition nécessaire et suffisante pour que le carré x_i^2 de l'exposant de a dans $(\Pi_i c_i^{\gamma_i} d_i^{\gamma_i})^p$ garde sa forme (mod p): si $p = 2$, (3) ou (3') est nécessaire et suffisante pour que l'exposant $\sum_i x_i y_i + \varepsilon(x_i^2 + y_i^2)$ de a dans $(\Pi_i c_i^{\gamma_i} d_i^{\gamma_i})^2$ garde sa forme (mod 2).

On voit donc que les substitutions s vérifient (1) ou (1') quand $\xi (\not\equiv 0)$ et les coefficients sont dans un C_π ($\pi = p^m$) formant un groupe $\mathfrak{A}(2\nu, \pi)$. C'est le *groupe linéaire abélien général* quand ξ reste indéterminé. Son diviseur relatif à $\xi = 1$ est le *groupe linéaire abélien spécial* $\mathfrak{A}_1(2\nu, \pi)$. Lorsque $p = 2$, le diviseur $\mathfrak{H}_0(2\nu, \pi)$ de $\mathfrak{A}$ vérifiant (3) ou (3') pour $\varepsilon = 0$ est le *premier groupe hypoabélien* d'ordre $\frac{2 \prod_1^{\nu} (\pi^{2i} - 1) \pi^{2i}}{\pi^{2\nu} (\pi^{\nu} + 1)}$ (JORDAN, *loc. cit.*; DICKSON, *Linear groups*). Le diviseur $\mathfrak{H}_d(2\nu, \pi)$ de $\mathfrak{A}$ vérifiant (3) ou (3') pour $\varepsilon = d$, d rendant $z^2 + z + d$ irréductible dans C_π (E., 45) est le *second groupe hypoabélien* d'ordre $\frac{2 \prod_1^{\nu} (\pi^{2i} - 1) \pi^{2i}}{\pi^{2\nu} (\pi^{\nu} - 1)}$ (*Ibid.*). Pour $p > 2$, le diviseur de $\mathfrak{A}$ qui vérifie (2) ou (2') sera désigné par $\mathfrak{X}(2\nu, \pi)$.

8. Revenons maintenant au groupe G du n° 6. On voit comme au n° 1 que G divise l'holomorphe K de A. Supposons que la substitution (4) corresponde à l'élément j du n° 6. Cette substitution appartient alors, pour $p > 2$, à $\mathfrak{A}(2\nu, p)$ ou à $\mathfrak{X}(2\nu, p)$, pour $p = 2$, à $\mathfrak{H}_0(2\nu, p)$ ou à $\mathfrak{H}_1(2\nu, p)$. Par hypothèse la fonction caractéristique $\varphi(z)$ de s est irréductible. Donc, si $p > 2$, il faut $\varepsilon = 0$, sans quoi, d'après (2), $\varphi(z)$ aurait le facteur $1 - z$; nous retrouverons d'ailleurs ce résultat tout à l'heure. Il faudra en outre que q^n soit diviseur propre de $p^{2\nu} - 1$, en sorte que q^n divise $p^\nu + 1$. Donc, si $p = 2$ et $\nu = 1$, $q^n = 3$ divise l'ordre de $\mathfrak{H}_1$ et non celui de $\mathfrak{H}_0$, c'est-à-dire que s est dans $\mathfrak{H}_1$ et que $\varepsilon = \eta = 1$.

$G|D$ n'ayant qu'un type déjà trouvé (2), on pourra, par un changement de générateurs, ramener les équations de G à la forme

$$\begin{aligned} a^p = j^q = 1, \quad c_i^p = a\gamma_i, \quad d_i^p = a\delta_i, \quad c_i^{-1}ac_i = d_i^{-1}ad_i = a, \\ c_ic_h = c_hc_i, \quad d_id_h = d_hd_i, \quad c_id_h = d_hc_i, \quad c_i^{-1}d_ic_i = d_ia, \quad j^{-1}aj = a^\xi \\ (i, h = 1, \dots, v). \end{aligned}$$

$$(5) \quad \begin{cases} j^{-1}c_\sigma j = a^{\lambda_\sigma}c_{\sigma+1}, & j^{-1}d_\sigma j = a^{\lambda_\sigma+\varepsilon}d_{\sigma+1}, \\ j^{-1}c_v j = a^{\lambda_v}d_1, & j^{-1}d_v j = a^{\lambda_v}c_1^{\alpha_0} \dots c_v^{\alpha_{v-1}} d_1^{\alpha_1} \dots d_v^{\alpha_{v-1}} \end{cases} \quad (\sigma = 1, \dots, v-1),$$

$\theta^{2v} - \sum_0^{v-1} \alpha_i \theta^i = f(\theta)$ étant irréductible dans C_p et appartenant à l'exposant q^n . Les conditions (1) donnent $\xi = 1$, $\alpha_0 = 1$ (si $v = 1$, elles donnent seulement $\xi = -\alpha_0$; mais alors $-\alpha_0 = \theta^{1+p}$ et q^n divise $1+p$) et, si $v > 1$, $\alpha_{v+1} = \dots = \alpha_{2v-1} = 0$. Si $p > 1$, ou si $p = 2$ avec $v > 1$, les conditions (2) et (3) donnent $\varepsilon = 0$ et, sauf si $v = 1$ avec $p > 1$, $\alpha_1 = \dots = \alpha_{v-1} = 0$. Donc s est dans $\mathfrak{A}_1$ si $p > 2$ et dans $\mathfrak{J}_0$ si $p = 2$ avec $v > 1$. Si $p = 2$ avec $v = 1$, on a vu que $\varepsilon = 1$ et que s est dans $\mathfrak{J}_1$. En prenant $c_i a^{x_i}$ pour c_i et $d_i a^{x_{v+i}}$ pour d_i , λ_k est remplacé par $\lambda_k + \xi x_k - x_{k+1}$ ($k = 1, \dots, 2v-1$) et λ_{2v} par $\lambda_{2v} + \xi x_{2v} - \sum_0^{2v-1} \alpha_i x_{i+1}$. Les équations obtenues en annulant ces quantités mod p déterminent $x_2, \dots, x_{2v}$ en fonction de x_1 , puis x_1 par une équation linéaire où le coefficient de x_1 est $f(\xi) \not\equiv 0$ (f est irréductible). On pourra donc supposer nuls $\lambda_1, \dots, \lambda_{2v}$. Si $p > 2$, ou si $p = 2$ avec $v > 1$, on sait *a priori* (*E.*, 144, 145) que A n'a que des e_p ; donc $\gamma_i = \delta_i = 0$. Au contraire, si $p = 2$ avec $v = 1$, A a des e_p , en sorte que les γ_i, δ_i ne peuvent pas être tous nuls. D'ailleurs (5) montre que $c_1, \dots, c_v, d_1, \dots, d_v$ sont du même ordre; donc $\gamma_i = \delta_i = 1$. Ainsi on n'a qu'un type pour $p \geq 2$, et ce type n'existe que s'il y a un polynôme irréductible de la forme $\theta^{2v} - a\theta^v - 1$ appartenant à l'exposant q^n mod p (il faut d'abord pour cela que q^n soit diviseur propre de $p^{2v} - 1$).