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>

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 $\mathfrak{V}$ un système de générateurs de B, $(\mathfrak{V})$ l'ensemble des conjugués de $\mathfrak{V}$ dans L; $\mathfrak{V}$, $\mathfrak{V}'$, ..., des systèmes de générateurs de B non conjugués dans L. J'appellerai l'ensemble $(\mathfrak{V}) + (\mathfrak{V}') + \ldots$ la *catégorie* des systèmes des générateurs de B. Si $\mathfrak{V}$ parcourt un système de *représentants* des catégories des divers g_{q^n} de L, $\{A, \mathfrak{V}\}$ 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 $\beta, \beta', \ldots$ 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), $(b^{\beta x}), \ldots, (b^{\beta^{\delta-1}x})$ 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 $p^{r_i} - 1$ ($i = 0, \ldots, n$; $r_0 = r$). 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 $P_{is1}, \ldots, P_{is\rho_{is}}$. $\rho_0 = \rho$ sera ≥ 1 et $\rho_n = m - \Sigma_0^{n-1} \rho_i r_i$ 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), Δ_b, B *appartiennent* à la *répartition* $(\rho_{01}, \rho_{02}, \ldots; \rho_{11}, \rho_{12}, \ldots)$ (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 $(z, z^\beta, \ldots, z^{\beta^{\delta_i - 1}})$, 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 $P_{is1}, \ldots, P_{is\rho_{is}}$ 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_{ist}. 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 mod 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 $(\rho_{01}, \ldots)$. *Le nombre* $N_{\rho_{01}, \ldots}$ *des types de* G *répondant* à la répartition sera $\Sigma_\delta \frac{\delta n_\delta}{\varphi(q^n)}$.

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 mod q^n, on a $\delta = r$, d'où $N_1 = 1$. Soit donc θ d'ordre q^n dans C_{p^r} et $\theta^r = \Sigma_0^{r-1} \alpha_i \theta^i$. Si $n = 1$,

$$\alpha_0 = (-1)^{r-1} \theta^{\Sigma_0^{r-1} p^i} = (-1)^{r-1}$$

(q, diviseur propre de $p^r - 1$, divise $\Sigma_0^{r-1} p_i$). La forme canonique générale de b répondant à la répartition (1) est

$$| y_i' = \theta^{p^i} y_i ; y_j' = y_j | \qquad (i = 0, \ldots, r-1; j = r, \ldots, m-1);$$

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 $y_i = \Sigma_0^{r-1} \theta^{kp^i} x_k$, $y_j = x_j$, la forme canonique réelle qui s'obtient en prenant les x pour variables est

$$b = | x_0' = \alpha_0 x_{r-1}, \; x_i' = x_{i-1} + \alpha_i x_{r-1}, \; x_j' = x_j | \\ (i = 1, \ldots, r-1; j = r, \ldots, m-1).$$

Les substitutions

$$a_k = | x_k' = x_k + 1, \; x_i' = x_i | \qquad (i, k = 0, \ldots, m-1; i \neq k)$$

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

$$b^q = 1, \qquad b^{-1} a_h b = a_{h+1} \qquad (h = 0, \ldots, r-2),$$
$$b^{-1} a_{r-1} b = \Pi_0^{r-1} a_i^{\alpha_i}, \qquad b^{-1} a_k b = a_k \qquad (k = r, \ldots, m-1).$$

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 $p \equiv g^\pi \bmod q$, 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 $p\left(-1 \equiv p^{\frac{r}{2}} \bmod q\right)$. Soit donc $\pi = 2\pi'$ et d'abord r pair $= 2r'$. Alors $-1 \equiv p^{r'} \bmod q$ et les racines de tout polynome 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} ($\tau\tau_1 \equiv 1 \bmod r$) 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

$$b_\lambda = | x'_0 = \alpha x_0,\ x'_1 = \alpha^\lambda x_1,\ x'_i = x_i | \qquad (i = 2, \ldots, m-1;\ \lambda \not\equiv 1 \bmod q),$$

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 $\not\equiv 1$ mod 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^u soit conjuguée de $b_{\lambda'}$ dans $L(m, p)$, il faut et suffit (si $\lambda \not\equiv \lambda'$ mod q) que $\alpha^u \equiv \alpha^{\lambda'}$, $\alpha^{u\lambda} \equiv \alpha$ ou que $\lambda\lambda' \equiv 1$ mod q. De là les types

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

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

5. Considérons pour $r = 1$ la répartition $(\rho_{01}, \ldots, \rho_{0\nu})$. n_δ ne sera $\not= 0$ que si : 1° δ divise $\rho_{01} = h_1\delta, \ldots, \rho_{0\nu} = h_\nu\delta$ et $\varphi(q^n) = Q = K\delta$; 2° on peut ranger $\Sigma\rho_{0s} = \rho_0 = \rho$ des Q nombres z appartenant à l'exposant q^n en séries de δ termes, la $i^{\text{ième}}$ étant $z_i, z_i^\beta, \ldots, z_i^{\beta^{\delta-1}}$. 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

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

des déterminations de Δ_b ainsi obtenues, est $\geqq n_\delta$ (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 $|x'_i = \theta_i x_i,\ x'_j = x_j|$ $(i = 0, \dots, \rho-1;\ j = \rho, \dots, m-1;\ \theta_i \not\equiv 1)$. Les types de G qu'elle détermine sont

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

On peut prendre $\theta_i = \alpha^{\lambda_i} (\not\equiv 1)$, α étant une racine primitive arbitraire de $\alpha^{q^n} \equiv 1$, $\lambda_0 = 1$ 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 $m = 2\nu + 1$. G aura des équations de la forme (*E.*, **144**, **145**)

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

$$j^{-1} a j = a^\xi, \qquad j^{-1} c_i j = a^{\lambda_i} \Pi_l c_l^{\alpha_{li}} d_l^{\beta_{li}}, \qquad j^{-1} d_i j = a^{\mu_i} \Pi_l c_l^{\gamma_{li}} d_l^{\delta_{li}};$$
$$\text{si } p > 2, \ \varepsilon = 0, 1, \ \eta = 0; \qquad \text{si } p = 2, \ \varepsilon = \eta = 0, 1,$$

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

$$(1) \quad \begin{cases} \xi \text{ et le déterminant } \Delta \text{ des } \alpha, \beta, \gamma, \delta \text{ sont } \not\equiv 0, \\ \Sigma_j(\alpha_{ji}\delta_{jk} - \beta_{ji}\gamma_{jk}) \equiv 0 \text{ si } i \neq k, \quad \equiv \xi \text{ si } i = k, \\ \Sigma_j(\alpha_{ji}\beta_{jk} - \beta_{ji}\alpha_{jk}) \equiv \Sigma_j(\gamma_{ji}\delta_{jk} - \delta_{ji}\gamma_{jk}) \equiv 0, \end{cases} \qquad i, j, k = 1, \dots, \nu,$$

et, en observant que $\Pi_l c_l^{\alpha_{li}} d_l^{\beta_{li}}$ par exemple est égal à

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

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

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

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

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

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 $j^{q^n} = 1$ par $j^M = 1$ et considérons j comme un isomorphisme de A avec lui-même, remplaçant

$$a \text{ par } a^{\xi} = a', \qquad c_i \text{ par } a^{\lambda_i} \Pi_l c_l^{\alpha_{li}} d_l^{\beta_{li}} = a^{\lambda_i} c_i',$$
$$d_i \text{ par } a^{\mu_i} \Pi_l c_l^{\gamma_{li}} d_l^{\delta_{li}} = a^{\mu_i} d_i'.$$

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 $L(2\nu, p)$ des isomorphismes de G|D. G|D est isomorphe au groupe $\mathfrak{S}$ des substitutions $|x_i, y_k; x_i + g_i, y_k + h_k|$ et H à celui $\mathfrak{H}$ des substitutions

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

Un calcul direct montre d'après (1) que

$$s' = |x_i, y_i; \Sigma_k(\alpha_{ik}'x_k + \gamma_{ik}'y_k), \Sigma_k(\beta_{ik}'x_k + \delta_{ik}'y_k)|$$

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) :

(1') $$\begin{cases} \Sigma_j(\alpha_{ij}\delta_{kj} - \beta_{ij}\gamma_{kj}) \equiv 0 \text{ si } i \neq k, \quad \equiv \xi \text{ si } i = k, \\ \Sigma_j(\alpha_{ij}\beta_{kj} - \beta_{ij}\alpha_{kj}) \equiv \Sigma_j(\delta_{ij}\delta_{kj} - \delta_{ij}\gamma_{kj}) \equiv 0, \end{cases} \quad i, j, k = 1, \ldots, \nu,$$

(2') si $p > 2$ et $\varepsilon = 1$, $\delta_{11} \equiv \xi^2$, $\delta_{h1} \equiv 0$, $\gamma_{i1} \equiv 0$, $h > 1$, $i \geqq 1$,

(3') si $p = 2$, $\Sigma_k \gamma_{ik}\delta_{ik} + \varepsilon(\beta_{i1}^2 + \delta_{i1}^2) \equiv \Sigma_k \alpha_{ik}\gamma_{ik} + \varepsilon(\alpha_{i1}^2 + \gamma_{i1}^2) \equiv \begin{cases} \varepsilon & \text{si } i = 1, \\ 0 & \text{si } i > 1. \end{cases}$

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 $F = \Sigma_i(X_i y_i - Y_i x_i)$ de a dans l'un des commutateurs de $\Pi_i c_i^{x_i} d_i^{y_i}$, $\Pi_i c_i^{X_i} d_i^{Y_i}$ 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 $(\Pi_i c_i^{x_i} d_i^{y_i})^p$ garde sa forme (mod p) : si $p = 2$, (3) ou (3′) est nécessaire et suffisante pour que l'exposant $\Sigma_i x_i y_i + \varepsilon(x_i^2 + y_i^2)$ de a dans $(\Pi c_i^{x_i} d_i^{y_i})^2$ 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 $\mathfrak{A}_0(2\nu, \pi)$. 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 $\frac{2\Pi_1^\nu(\pi^{2i}-1)\pi^{2i}}{\pi^{2\nu}(\pi^\nu+1)}$ (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 $\frac{2\Pi_1^\nu(\pi^{2i}-1)\pi^{2i}}{\pi^{2\nu}(\pi^\nu-1)}$ (*Ibid.*). Pour $p > 2$, le diviseur de $\mathfrak{A}$ qui vérifie (2) ou (2′) sera désigné par $\mathfrak{K}(2\nu, \pi)$.

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 $\mathfrak{A}_0(2\nu, p)$ ou à $\mathfrak{K}(2\nu, p)$, 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 $\varepsilon = \tau_1 = 1$.

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

$$a^p = j^{q^n} = 1, \quad c_i^p = a^{\gamma_i}, \quad d_i^p = a^{\delta_i}, \quad c_i^{-1} a c_i = d_i^{-1} a d_i = a,$$
$$c_i c_h = c_h c_i, \quad d_i d_h = d_h d_i, \quad c_i d_h = d_h c_i, \quad c_i^{-1} d_i c_i = d_i a, \quad j^{-1} a j = a^{\xi}$$
$$(i, h = 1, \ldots, \nu).$$

$$(5) \quad \begin{cases} j^{-1} c_\sigma j = a^{\lambda_\sigma} c_{\sigma+1}, \quad j^{-1} d_\sigma j = a^{\lambda_{\nu+\sigma}} d_{\sigma+1}, \\ j^{-1} c_\nu j = a^{\lambda_\nu} d_1, \quad j^{-1} d_\nu j = a^{\lambda_{2\nu}} c_1^{\alpha_0} \ldots c_\nu^{\alpha_{\nu-1}} d_1^{\alpha_\nu} \ldots d_\nu^{\alpha_{2\nu-1}} \end{cases} \quad (\sigma = 1, \ldots, \nu - 1),$$

$\theta^{2\nu} - \Sigma_0^{2\nu-1} \alpha_i \theta^i = f(\theta)$ étant irréductible dans C_p et appartenant à l'exposant q^n. Les conditions (1) donnent $\xi = 1$, $\alpha_0 = 1$ (si $\nu = 1$, elles donnent seulement $\xi = -\alpha_0$; mais alors $-\alpha_0 = \theta^{1+p}$ et q^n divise $1+p$) et, si $\nu > 1$, $\alpha_{\nu+1} = \ldots = \alpha_{2\nu-1} = 0$. Si $p > 1$, ou si $p = 2$ avec $\nu > 1$, les conditions (2) et (3) donnent $\varepsilon = 0$ et, sauf si $\nu = 1$ avec $p > 1$, $\alpha_1 = \ldots = \alpha_{\nu-1} = 0$. Donc s est dans $\mathfrak{A}_1$ si $p > 2$ et dans $\mathfrak{H}_0$ si $p = 2$ avec $\nu > 1$. Si $p = 2$ avec $\nu = 1$, on a vu que $\varepsilon = 1$ et que s est dans $\mathfrak{H}_1$. En prenant $c_i a^{x_i}$ pour c_i et $d_i a^{x_{\nu+i}}$ pour d_i, λ_k est remplacé par $\lambda_k + \xi x_k - x_{k+1}$ ($k = 1, \ldots, 2\nu - 1$) et $\lambda_{2\nu}$ par $\lambda_{2\nu} + \xi x_{2\nu} - \Sigma_0^{2\nu-1} \alpha_i x_{i+1}$. Les équations obtenues en annulant ces quantités mod p déterminent $x_2, \ldots, x_{2\nu}$ 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 $\lambda_1, \ldots, \lambda_{2\nu}$. Si $p > 2$, ou si $p = 2$ avec $\nu > 1$, 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 $\nu = 1$, A a des e_{p^2} en sorte que les γ_i, δ_i ne peuvent pas être tous nuls. D'ailleurs (5) montre que $c_1, \ldots, c_\nu$, $d_1, \ldots, d_\nu$ 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 polynome irréductible de la forme $\theta^{2\nu} - \alpha\theta^\nu - 1$ appartenant à l'exposant q^n mod p (il faut d'abord pour cela que q^n soit diviseur propre de $p^{2\nu} - 1$).*