

JOURNAL  
DE  
MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

---

J.-A. DE SÉGUIER

**Sur les diviseurs de certains groupes galoisiens**

*Journal de mathématiques pures et appliquées* 9<sup>e</sup> série, tome 5 (1926), p. 67-124.

[http://www.numdam.org/item?id=JMPA\\_1926\\_9\\_5\\_67\\_0](http://www.numdam.org/item?id=JMPA_1926_9_5_67_0)

 gallica

NUMDAM

Article numérisé dans le cadre du programme  
Gallica de la Bibliothèque nationale de France  
<http://gallica.bnf.fr/>

et catalogué par Mathdoc  
dans le cadre du pôle associé BnF/Mathdoc  
<http://www.numdam.org/journals/JMPA>

*Sur les diviseurs de certains groupes galoisiens;*

PAR J.-A. DE SÉQUIER.

Lorsqu'on cherche les diviseurs d'un groupe linéaire dans un champ galoisien  $\mathfrak{G}$  d'ordre  $\pi = p^k$  ( $p$  premier), un des premiers problèmes qui se posent est de déterminer les diviseurs isomorphes au groupe  $\mathfrak{L}(2, p^m)$  formé des substitutions  $\frac{\alpha z + \beta}{\gamma z + \delta}$  dans le champ  $\mathfrak{C}_m$  d'ordre  $p^m$ , ou à son diviseur  $\mathfrak{D}(2, p^m)$  d'indice 2. C'est à ce problème qu'est consacré le présent travail, dans le cas où le groupe linéaire a un invariant hermitien, gauche ou quadratique, où  $p$  est  $> 2$ , et où les substitutions d'ordre  $p$  du diviseur cherché n'ont qu'une suite canonique <sup>(1)</sup>.

Je me servirai des mêmes notations que dans mon Mémoire *Sur les groupes à invariant bilinéaire ou quadratique dans un champ de Galois* (*J. M.*, 1916) <sup>(2)</sup> dont je rappellerai seulement quelques-unes.

Soit  $A(n, \pi)$  un groupe linéaire à  $n$  variables conservant un invariant  $\alpha$  hermitien, bilinéaire gauche ou quadratique, les substitutions de  $A$  étant dans  $\mathfrak{G}$  si  $\alpha$  est gauche ou quadratique, dans le champ  $\mathfrak{G}'$

<sup>(1)</sup> On trouvera un résumé des résultats obtenus ici dans une Note présentée à l'Académie des Sciences le 30 octobre 1922.

<sup>(2)</sup> Au n° 44 de ce Mémoire, au lieu de « car les normalisants... », il faut lire « car, pour  $\nu > 2$ ,  $C_{\nu+1} | C_1$  est abélien dans  $B(n, \pi)$ , mais ne l'est pas dans  $\mathfrak{G}(2\nu, \pi)$ . Je renverrai à ce Mémoire par la lettre  $G$ . Je renverrai aussi à mes *Éléments de la Théorie des groupes abstraits* par la lettre  $E$ , et à mes *Éléments de la Théorie des groupes de substitutions* par la lettre  $S$ .

d'ordre  $p^{2k}$  si  $\alpha$  est hermitien. Je désigne par  $A^0(n, \pi)$  le diviseur de  $A$  formé de ses substitutions unimodulaires, par  $D = \{d\}$  le groupe engendré par la similitude (à  $n$  variables) d'ordre 2, par  $A'(n, \pi)$  le groupe conservant  $\alpha$  à un facteur près, par  $\mathfrak{A}(n, \pi)$  ce que devient  $A$  quand on regarde les variables comme homogènes.

Je supposerai  $\alpha$  de l'une des formes suivantes :

$$1^\circ \quad \begin{cases} \Sigma_1^{\gamma}(x_i \bar{y}_i - y_i \bar{x}_i) + \eta \omega x \bar{x} \quad (1), & \eta = 0 \text{ ou } 1, \\ \omega = \nu - \bar{\nu}, & \nu \text{ étant un élément définissant de } \mathfrak{E}' \end{cases}$$

(je remplacerai alors les lettres  $A, \mathfrak{A}$  par  $H, \mathfrak{H}$ );

$$2^\circ \quad \omega \left[ \frac{1}{2} \Sigma_1^{\gamma}(x_i \bar{y}_i + y_i \bar{x}_i) + \eta c x \bar{x} \right]$$

(je remplacerai alors les lettres  $A, \mathfrak{A}$  par  $\bar{H}, \bar{\mathfrak{H}}$ );

$$3^\circ \quad \begin{cases} \Sigma_1^{\gamma}(x_i y'_i - y_i x'_i), \\ \text{les } x'_i, y'_i \text{ étant cogrédients aux } x_i, y_i \end{cases}$$

(je remplacerai alors les lettres  $A, \mathfrak{A}$  par  $G, \mathfrak{G}$ );

$$4^\circ \quad \begin{cases} \Sigma_1^{\gamma} x_i y_i + \psi(x, y), & \psi(x, y) = c x^2 + b x y + c' y^2, \\ \psi \text{ pouvant être réductible dans } \mathfrak{E} \end{cases}$$

(je remplacerai alors les lettres  $A, \mathfrak{A}$  par  $Q, \mathfrak{Q}$ ).

Le cas  $n = 2$  étant connu, je supposerai encore  $n > 2$ .

## I.

1. Rangeons les variables dans l'ordre  $y_1, \dots, y_n, y, x, x_n, x_{n-1}, \dots, x_1$ , en supprimant celles des variables  $x, y$  qui ne se présenteraient pas, et convenons d'écrire aussi  $y_1, \dots, y_n$  pour les variables prises dans cet ordre.

Appelons *transversale* d'une matrice  $\varphi = (\varphi_{ik})$  d'ordre  $n$  la diagonale autre que la diagonale principale que j'appellerai simplement *diagonale*;  $r^{\text{ième}}$  *sous-diagonale* la rangée (parallèle à la diagonale) formée des  $\varphi_{ik}$  où  $i - k = r$ , c'est-à-dire la suite d'éléments  $\varphi_{r+1,1},$

---

(1) Je désigne généralement par  $\bar{u}$  le conjugué d'un élément  $u$  de  $\mathfrak{E}'$ .

$\varphi_{r+2,2}, \dots, \varphi_{n,n-r}$ ;  $r^{\text{ième}}$  sous-transversale la rangée (parallèle à la transversale) formée des  $\varphi_{ik}$  où  $i + k = n + r + 1$ , c'est-à-dire la suite d'éléments  $\varphi_{n,r+1}, \varphi_{n-1,r+2}, \dots, \varphi_{r+1,n}$ . Supposons maintenant  $\varphi$  dans le groupe sylowien  $\mathbf{P}$  défini précédemment (*G.*, 13, 25, 42). Alors les  $\varphi_{ik}$  situés *au-dessus* de la diagonale sont nuls, et ceux de la diagonale égaux à 1. Les  $\varphi_{ik}$  situés à la fois *au-dessous* de la diagonale et *au-dessus* de la transversale sont ceux qui, dans l'ordre ancien des variables, étaient *au-dessous* de la diagonale sans être nécessairement égaux à 0 ou à 1, et l'on a vu (*loc. cit.*) qu'on peut les choisir arbitrairement, dans  $\varrho'$  si  $A = H$  ou  $\bar{H}$ , dans  $\varrho$  si  $A = G$  ou  $Q$ ; les  $\varphi_{ik}$  de la transversale situés *au-dessous* de la diagonale sont les  $\alpha'_{ii}$  de *G.*, 13, 25, 42, et l'on a vu qu'on peut les choisir arbitrairement dans  $\varrho$  si  $A = H, \bar{H}$  ou  $G$ , mais qu'ils sont déterminés si  $A = Q$ . Une fois déterminés les  $\varphi_{ik}$  situés à la fois au-dessous de la diagonale et au-dessus de la transversale ou sur cette transversale, tous les autres le sont également (1).

Considérons d'abord les diviseurs de  $\mathbf{P}$  dont les substitutions  $\neq 1$  n'ont qu'une suite canonique. Je dirai qu'une telle substitution est *irréductible*, et je supposerai  $p \geq n$ , en sorte que toute substitution irréductible de  $\mathbf{P}$  soit d'ordre  $p$  (*S.*, 10). Soit  $\sigma = |y_i, \sum_i^i \sigma_{ik} y_k|$  ( $\sigma_{ii} = 1$ ) une  $s_p$  irréductible de  $\mathbf{P}$ . Pour que le premier diviseur élémentaire  $\neq 1$  de  $\sigma - s\varepsilon$  ( $\varepsilon$  étant la matrice unité d'ordre  $n$ ) soit  $(s - 1)^n$  (*cf.* *S.*, 3), il faut et suffit que les mineurs d'ordre  $n - 1$  de  $\sigma - \varepsilon$  ne soient pas tous nuls, c'est-à-dire que les  $\sigma_{i,i-1}$  ( $i = 2, \dots, n$ ) soient  $\neq 0$ . Si donc  $A = Q$ ,  $n$  doit être impair, sans quoi  $\sigma_{\nu+1,\nu}$  si  $\psi = 0$  ou  $\sigma_{\nu+2,\nu+1}$  si  $\psi \neq 0$  est nul.

Soit  $\varpi = \sum_1^m \sigma^{(2)}$  un diviseur de  $\mathbf{P}$  formé de  $s_p$  irréductibles et de

(1) Avec l'ordre actuel des variables, c'est en combinant la  $i^{\text{ième}}$  colonne avec les  $(i - r)^{\text{ième}}$  pour  $i = r + 1, r + 2, \dots$  qu'on détermine les éléments de la  $r^{\text{ième}}$  sous-transversale ( $r > 0$ ) situés au-dessous de la diagonale : ce sont les  $\varphi_{n-i+r+1,i}$  (la valeur maxima de  $i$  est le plus grand entier tel que  $n - i + r + 1$ , soit  $\geq i + 1$ , c'est-à-dire le plus grand entier  $\leq \frac{n+r}{2}$ ). La combinaison de chaque colonne avec elle-même détermine les éléments de la transversale dans la mesure où ils sont déterminés.

l'unité, et  $\sigma^{(x)} = (\sigma_{ik}^{(x)})$ . Si  $\sigma^{(x)}\sigma^{(\beta)} = \sigma^{(\gamma)}$ ,  $\sigma_{ik}^{(\gamma)}$  est nul pour  $i < k$ , égal à 1 pour  $i = k$ , et à  $\sum_k \sigma_{ip}^{(\beta)}\sigma_{pk}^{(\alpha)}$  pour  $k < i$ . En particulier, pour  $k = i - 1$ ,  $\sigma_{i,i-1}^{(\gamma)} = \sigma_{i,i-1}^{(\alpha)} + \sigma_{i,i-1}^{(\beta)}$ . Si donc  $\sigma^{(x)}\sigma^{(\beta)} = \mathbf{1}$ ,  $\sigma_{i,i-1}^{(\beta)} = -\sigma_{i,i-1}^{(x)}$ .

Donc 1°  $\varpi$  est abélien, car, la première sous-diagonale de

$$(\sigma^{(\beta)}\sigma^{(x)})^{-1}\sigma^{(x)}\sigma^{(\beta)} = \sigma^{(\gamma)}$$

étant formée d'éléments nuls, on a  $\sigma^{(\gamma)} = \mathbf{1}$ .

2°  $\sigma^{(x)}$  est complètement déterminé dans  $\varpi$  par  $\sigma_{21}^{(x)}$ , car si l'on avait  $\sigma^{(\alpha)} \neq \sigma^{(\beta)}$  avec  $\sigma_{21}^{(\beta)} = \sigma_{21}^{(x)}$ ,  $\sigma^{(\beta)-1}\sigma^{(x)} = \sigma^{(\gamma)}$  serait  $\neq \mathbf{1}$  avec  $\sigma_{21}^{(\gamma)} = 0$ , ce qui est impossible si  $\sigma^{(\gamma)}$  est dans  $\varpi$ .

3° En désignant désormais par  $\sigma_x = (\sigma_{xik})$  la substitution de  $\varpi$  où  $\sigma_{\alpha 21} = \alpha$ ,  $\alpha$  parcourt un groupe additif de  $\mathcal{E}'(E., 34)$  quand  $\sigma_x$  parcourt  $\varpi = \Sigma \sigma_x (\sigma_0 = \mathbf{1})$ . Or l'action du p. p. c. m. des  $V_{1,2}, V_{2,1}$  sur  $y_1$  et  $y_2$ , est semblable à  $L(2, \pi^2)$  si  $A = H$  ou  $\bar{H}$ , et à  $L(2, \pi)$  si  $A = G$  ou  $Q$  ( $G., 11, 40$ ). En transformant donc au besoin  $\varpi$  par ce p. p. c. m., on peut supposer que  $x$  parcourt le champ  $\mathcal{E}_m$  d'ordre  $p^m$ ,  $m$  divisant  $K = mx$  si  $A = G$  ou  $Q$ , et  $2K = mx'$  si  $A = H$  ou  $\bar{H}$ .

Je poserai alors  $\sigma_x = \sigma = (\sigma_{ik})$ . Comme  $\sigma_x\sigma_\beta = \sigma_{x+\beta}$  (donc  $\sigma_x^{-1} = \sigma_{-x}$ ), on voit que, dans l'isomorphisme de  $\varpi$  avec le groupe des substitutions  $(z + \alpha)$  où  $\alpha$  parcourt  $\mathcal{E}_m$ ,  $\sigma_x$  correspond à  $z + \alpha$ .

2. Soit  $\lambda = (\lambda_{ik})$  une substitution de  $A$ , telle que  $\sigma_x\lambda = \lambda\sigma_\beta$ . Le développement de cette condition donne

$$(1) \quad \sum_l \lambda_{kl} \sigma_{xpl} = \sum_l \sigma_{\beta kl} \lambda_{pl}$$

En faisant  $l = n$  et, successivement,  $k = 2, \dots, n$ , on en tire  $\lambda_{1n} = \lambda_{2n} = \dots = \lambda_{n-1,n} = 0$ . Admettons que  $\lambda_{ik} = 0$  pour  $k > l$  si  $i < k$ , et faisons dans (1)  $k = 2, \dots, l$ . On aura successivement  $\lambda_{1l} = 0, \lambda_{2l} = 0, \dots, \lambda_{l-1,l} = 0$ . Donc  $\lambda_{ik} = 0$  pour  $i < k$ . Il résulte alors de (1), pour  $l = k - 1$ , en écrivant  $\lambda_i$  pour  $\lambda_{il}$ , que l'on a

$$\lambda_k \sigma_{\alpha, k, k-1} = \sigma_{\beta, k, k-1} \lambda_{k-1} \quad (k = 2, \dots, n).$$

Or la condition  $\sigma_x\sigma_\beta = \sigma_\beta\sigma_x$  donne

$$\sigma_{\alpha, k, k-1} \sigma_{\beta, k-1, k-2} = \sigma_{\beta, k, k-1} \sigma_{\alpha, k-1, k-2} \quad (k = 3, \dots, n).$$

Donc  $\frac{\lambda_1}{\lambda_2} = \frac{\lambda_2}{\lambda_3} = \dots = \frac{\lambda_{n-1}}{\lambda_n}$ , soit  $= \varphi$ , ou  $\lambda_k = \lambda_n \varphi^{n-k}$ .

D'autre part, la condition que  $\lambda$  conserve  $a$  donne (quelle que soit la détermination de  $A$ )

$$(2) \quad \lambda_i \lambda_{n+1-i} = 1 \quad (i=1, \dots, n).$$

Donc la multiplication  $\lambda_0$  dont les multiplicateurs sont  $\lambda_1, \dots, \lambda_n$ , est dans le p. p. c. m.  $\mathbf{M}$  des  $m_i$ , et  $\lambda_0^{-1}\lambda$ , qui est dans  $A$  et a la forme des substitutions de  $\mathbf{P}$ , est aussi dans  $\mathbf{P}$ . Donc  $\lambda$  est dans  $\lambda_0\mathbf{P} = \mathbf{P}\lambda_0$ .

De plus (2) montre, en faisant le quotient des équations correspondant à  $i=1, 2$ , et en tenant compte de  $\lambda_k = \lambda_n \rho^{n-k}$ , que  $\rho^{\pi-1} = 1$ , et alors (2) donne  $\lambda_n^{\pi+1} = \rho^{1-n}$ . Si donc  $A$  est dans  $\mathfrak{Q}$ , et  $n$  pair, c'est-à-dire si  $A = G$ ,  $\rho$  est carré.

Ainsi, en posant  $\mu_0 = |y_k, {}^t y_k|$ ,  $\lambda$  est, quel que soit  $A$ , dans  $|\mu_0| \mathbf{I}'$ , et, si  $A = G$ , dans  $|\mu_0^2| \mathbf{I}'$ .

Quel que soit  $A$ ,  $\mu_0$  multiplie  $a$  par  $\iota^{n+1}$  et est donc dans  $A'$ . Cherchons une similitude de multiplicateur  $\xi_\lambda = \xi$  telle que  $[\xi^{-1}] \mu_0 = \mu_\lambda = \mu$  ou, si  $A = G$ ,  $\mu^2$  conserve  $a$ .  $\xi$  est évidemment dans  $\mathfrak{Q}'$ . Posons  $\xi = \iota^w$ , faisons  $\iota = \iota^{\pi+1}$ , et désignons par  $\omega_0$  le p. g. c. d. de  $\omega$ ,  $\pi^2 - 1$ ; l'ordre  $f$  de  $\xi$  sera  $\frac{\pi^2 - 1}{\omega_0}$ . Je désignerai encore par  $\pi'$  le p. g. c. d. de  $n+1$ ,  $\pi-1$ , et par  $2^t$  la plus haute puissance de 2 divisant  $\pi+1$ .

Pour  $n = 2\nu + 1$ , on peut faire  $\xi = \iota^{\nu+1}$ . Alors  $\mu = \Pi_1^\nu m_{i, \xi^{-1}, \iota^{\nu+1}}$  est d'ordre  $\pi - 1$ .

Soit  $n = 2\nu$ . Alors  $\mu = \Pi_1^\nu m_{i, \xi^{-1}, \iota^{\nu+1}}$ , et  $\pi'$  est impair. Si  $r$  est l'ordre de  $\mu = [\xi^{-1}] \mu_0$ , on a  $\xi^r = \iota^{kr}$  quel que soit  $k$ , d'où  $\iota^r = 1$ . Donc  $r$  a la forme  $s(\pi - 1)$ , et  $s$  est l'ordre de  $\xi^{\pi-1}$ .

Soit d'abord  $A = H$  ou  $\bar{H}$ . La condition  $\xi^{\pi+1} = \iota^{n+1}$  donne  $\omega = n+1 + l(\pi-1)$ . Déterminons  $l$  par la condition  $n+1 - 2l = \frac{\pi+1}{2^t}$ .

On aura

$$\omega = \frac{\pi+1}{2^t} (2^t l + 1) = \frac{\pi+1}{2^t} \left[ 2^{t-1} (n+1) - \frac{\pi-1}{2} \right],$$

$$\omega_0 = \frac{\pi+1}{2^t} \pi', \quad f = 2^t \frac{\pi-1}{\pi'}.$$

Donc  $s = 2^t$ , et  $\mu$  est, comme  $\xi$ , d'ordre  $2^t(\pi-1)$ .

Soit  $A = G$ . La condition que  $\mu^2$  conserve  $a$  donne  $\xi^s = \iota^{2(n+1)}$

ou  $\omega = \frac{\pi+1}{2} \omega'$ ,  $\omega' = n+1 + l \frac{\pi-1}{2}$ . Faisons  $l=0$ . Alors

$$\omega_0 = \frac{\pi+1}{2} \omega', \quad f = 2 \frac{\pi-1}{\pi'}, \quad s=2, \quad \mu^{\pi-1} = d \quad (1).$$

Quel que soit  $A$ ,  $\mu$  est, comme  $\mu_0$ , permutable à  $\mathbf{P} (G., 13)$ , et  $\mu$  transforme  $\mathbf{P}$  comme  $\mu_0$ . Le p. g. c. d. de  $\{\mu_A\} = \mathbf{M}_A = \mathbf{M}$ ,  $I'$  est toujours  $\{\mu^{\pi-1}\}$ ; car pour que  $\mu^h$  soit dans  $I'$ , il faut et suffit que  $\mu_0^h$  y soit, donc que  $t^h = t^{2h} = \dots = t^{nh}$ , d'où  $h \equiv 0 \pmod{\pi-1}$ .

Ainsi, en désignant par  $\Omega (\geq D)$  le groupe des similitudes de  $A$ , par  $\Omega_0$  son groupe sylozien d'ordre pair, par  $\Delta$  un groupe égal à  $\mathbf{1}$  si  $n=2\nu+1$ , et à  $\Omega_0$  si  $n=2\nu$ ,  $\lambda$  est dans  $\mathbf{PM}\Omega$  (dans  $\mathbf{P}\{\mu^2\}$  si  $A=G$ ), et le p. g. c. d. de  $\mathbf{M}, \Omega$  (qui est le groupe des similitudes de  $\mathbf{PM}$ ) est  $\Delta$  (2).

5. En exceptant le cas  $n=p=\pi$ ,  $\mathbf{M}$  est son propre normalisant dans  $\mathbf{PM}$ . En effet, soit  $\varphi = (\varphi_{ik})$  une substitution de  $\mathbf{P}$ . Si  $\varphi^{-1} \mathbf{M} \varphi = \mathbf{M}$ , on a, pour chaque valeur de  $r$ ,  $\varphi \mu^r = \mu^s \varphi$ , ou  $\varphi \mu_0^r = \mu_0^s \varphi [\zeta^{r-s}]$ , ou

(1) Pour  $\pi \equiv 3 \pmod{4}$ , on pourrait déterminer  $l$  de manière que  $\omega' \equiv 0 \pmod{4}$ . Alors  $\omega_0 = 2\pi'(\pi+1)$ ,  $f = \frac{\pi-1}{2\pi'}$ ,  $s=1$ ,  $\mu^{\pi-1} = 1$ . Mais, quel que soit le choix de  $l$ ,  $\frac{\pi-1}{2}$  étant ici impair, le groupe  $\{\mu^2\} D = \{d\mu^2\}$ , qui seul importe, reste le même.

(2) Pour  $n=2\nu$ ,  $G$  divise  $H$ . On a alors  $\xi_{\mathbf{H}}^{\pi+1} = \iota^{n+1} = \zeta_6^2$ , d'où  $\mu_6^2 = \mu_{\mathbf{H}}^{\pi+1}$ . On remarquera que  $\mu_6$ , qui multiplie l'invariant  $\alpha$  de  $H$  par  $-1$ , n'est pas dans  $H$ . Mais, quelle que soit la racine  $j = \iota^{\frac{h\pi-1}{2}}$  ( $h$  impair) de  $j^{\pi+1} = -1$ ,  $[j] \mu_6 = \mu'$  est dans  $H$ , et  $(j \zeta_6)^{\pi+1} = \iota^{n+1} = \xi_{\mathbf{H}}^{\pi+1}$ .

Je dis de plus que  $\{\mu'\}$  contient  $\{\mu_{\mathbf{H}}\}$ . Il suffit de montrer que  $\mu_{\mathbf{H}}$  est une puissance de  $\mu'$ , c'est-à-dire qu'il y a un nombre  $\alpha$  tel que

$$\xi_{\mathbf{H}}^{-1} \iota^k = (j \zeta_6^{-1} \iota^k)^\alpha \quad (k=1, \dots, n).$$

Il faut et suffit pour cela que  $\alpha \equiv 1 + \beta(\pi-1)$ ,  $\beta$  vérifiant la congruence

$$\beta [h(\pi-1) - (n+1)(\pi+1)] + h + \frac{\pi+1}{2\pi'} \equiv 0 \pmod{2(\pi+1)}.$$

Or soient  $\beta_0$  et  $\gamma_0$  deux entiers vérifiant  $\beta_0(\pi-1) + 1 = \gamma_0 \frac{\pi+1}{2}$ ;  $\gamma_0$  est néces-

$v^r \varphi_{ik} = \varphi_{ik} v^{sk} \xi^{r-s}$ . De là, pour  $i = k$ ,  $v^{i(r-s)} = \xi^{r-s}$ . En faisant  $i = 1, 2$ , on voit que  $v^{r-s} = 1$ , d'où  $r \equiv s \pmod{\pi - 1}$ , et  $\xi^{r-s} = 1$ . Si donc  $\varphi_{ik} \neq 0$  (alors  $k$  est  $\leq i \leq n$ ),  $i - k$  a la forme  $f(\pi - 1)$ ,  $f$  étant entier. Mais  $i - k$  est  $\leq n - 1 \leq p - 1$ . Donc, en dehors du cas excepté, on a  $\varphi = 1$ , et  $M$  est son propre normalisant.

Si  $n = p = \pi$ , on a  $f = 1$ ,  $i = n = p$ ,  $k = 1$ , et  $\varphi$  est une  $u_1$  ou une  $\bar{u}_1$  ( $G.$ , 9). Donc,  $n$  étant ici impair,  $A = H$  ou  $\bar{H}$ . Alors, en négligeant le cas  $A = \bar{H}$ , et en désignant par  $|u_1|$  le p.p.c.m. des  $u_1$ , qui est le central de  $\mathbf{P}$ , le normalisant de  $M$  dans  $\mathbf{PM}$  est  $M |u_1|$ ,  $\mu$  étant permutable à chaque  $u_1$ .

Soit plus généralement  $|\mu^s|$  un diviseur de  $M$  d'ordre  $q \pmod{\Delta}$  : alors  $gq$  est le p.p.c.m. de  $g$ ,  $\pi - 1$ ; donc  $gq = g \frac{\pi - 1}{e}$ ,  $e$  étant le p.g.c.d. de  $g = eg'$  et de  $\pi - 1 = eq$ . Comme il y a toujours des entiers  $u, v$  tels que  $ug' + vq = 1$ , on peut supposer, en prenant au besoin  $\mu^{us}$  pour  $\mu^s$ , ce qui n'altère pas  $q$ , que  $g = \frac{\pi - 1}{q}$ . Pour que  $|\mu^s|$  soit permutable à  $\varphi$ , il faut que  $\varphi \mu^s$  ait la forme  $\mu^s \varphi$ . Comme tout à l'heure, cela exige que  $\xi^{s-s} = 1$ , et,  $\mu$  ayant l'ordre de  $\xi$ ,  $\mu^s = \mu^s$ . Donc  $\mu^{-s} \varphi \mu^s = \varphi$  ou  $\varphi_{ik} v^{s(i-k)} = \varphi_{ik}$ . Si donc  $\varphi_{ik} \neq 0$ , on a  $i - k \equiv 0 \pmod{q}$ . Donc les  $\varphi$  permutable à  $|\mu^s|$  sont celles où les  $\varphi_{ik}$  situés hors des sous-diagonales de rang  $\equiv 0 \pmod{q}$  sont tous nuls, et elles sont permutable à  $\mu^s$ . Elles forment a priori un groupe  $\Gamma^s$ . Soient  $l$  et  $l'$  les nombres de  $\varphi_{ik}$  où  $i - k = fq > 0$  ( $f$  entier) qui, dans une

sairement impair, et l'on peut supposer  $\beta_0$  pair. En posant alors  $\beta = \beta_0 + u \frac{\pi + 1}{2^t}$ , la congruence précédente revient à

$$u \left( h \frac{\pi - 1}{2} - \frac{\pi + 1}{2} \right) + \frac{h \gamma_0 + 1}{2} \equiv 0 \pmod{2^t},$$

toujours résoluble en  $u$ .

Pour que  $|\mu'| = |\mu_{h_1}|$ , il faut et suffit que  $\mu'$  soit d'ordre  $2^t(\pi - 1)$ . Or, la première puissance de  $\mu'$  qui soit dans  $\Gamma'$  est  $\mu'^{\pi-1} = [j^{-2}]$ , et l'ordre de  $j^2$  est  $\frac{\pi + 1}{h_1}$ ,  $h_1$  étant le p. g. c. d. de  $h$ ,  $\pi + 1$ . Donc il faut et suffit que

$$h = \frac{\pi + 1}{2^t} h', \quad h' \text{ étant impair.}$$



$\varphi$  quelconque, sont respectivement au-dessus de la transversale et dans la transversale. L'ordre de  $\Gamma^s$  est  $\pi^{2+l}$  si  $A = H$ ,  $\pi^{l+l'}$  si  $A = G$ ,  $\pi^l$  si  $A = Q$  (cela résulte des relations fondamentales). Si donc  $q \geq p - 1$ ,  $\Gamma^s = 1$  ou  $\{u_i\}$  (en négligeant le cas  $A = \bar{H}$ ) selon que  $n$  est  $> p$  ou  $= p$ .  $\mu$  est évidemment permutable à  $\Gamma^s$ . Donc le normalisant de  $\{\mu^s\}$  dans  $\mathbf{PM}$  est  $\Gamma^s \mathbf{M}$ .

Il est clair que  $\{\mu^s\}$  divise tous les transformés de  $\mathbf{M}$  par  $\Gamma^s$ . Soit  $Z$ , d'ordre  $r \bmod \Delta$ , le p. g. c. d. de ces transformés. Comme  $Z$  contient  $\mu^s$ ,  $r$  est  $\geq q$ . Toute substitution  $\varphi = (\varphi_{ik})$  de  $\Gamma^s$  est permutable à  $Z$ . Or cela exige, comme tout à l'heure, que tous les  $\varphi_{ik}$  où  $i - k \not\equiv 0 \bmod r$  soient nuls. Donc  $r = q$ , et  $Z = \{\mu^s\}$ .

4. Soit  $\mu^s \varphi$ ,  $\varphi = (\varphi_{ik})$  étant dans  $\mathbf{P}$ , une substitution de  $\mathbf{PM}$  permutable à  $\mu$ , et soit  $q$  (premier à  $p$ ) son ordre mod  $\mathbf{P}\Delta$ . On voit par récurrence que  $(\mu^s \varphi)^s = \mu^{s^2}$  mod  $\mathbf{P}$ . Donc  $\mu^s$  est d'ordre  $q \bmod \mathbf{P}\Delta$ . Mais  $\mu^{s^q}$  est d'ordre premier à  $p$ . Donc  $\mu^{s^q}$  est dans  $\Delta$ , et  $gq$  est le p. p. c. m. de  $g$  et de  $\pi - 1$ . Donc  $gq = g \frac{\pi - 1}{e}$ ,  $e$  étant le p. g. c. d. de  $\pi - 1 = eq$  et de  $g = eg'$ . Comme d'ailleurs il y a des entiers  $u, v$  tels que  $ug' + eq = 1$ , on peut supposer, en prenant au besoin  $(\mu^s \varphi)^u$  pour  $\mu^s \varphi$ , que  $g' = \frac{\pi - 1}{q}$ . C'est ce que je ferai désormais.

Je dis maintenant que  $\mu^s \varphi$  a une transformée  $\mu^s \varphi'$  par  $\mathbf{P}$  où  $\varphi'$  est une substitution de  $\mathbf{P}$  permutable à  $\mu^s$ .

Tout d'abord, si l'on désigne généralement par  $[z]$  la substitution déduite d'une substitution  $z$  de  $A$  en supprimant les deux lignes et colonnes de rangs 1 et  $n$ ,  $[\mu^s \varphi]$  est dans  $A(n - 2, \pi)$ . Car on voit de suite (et mieux encore avec l'ordre ancien des variables) que  $[\mu^s \varphi]$  vérifie les relations fondamentales exprimant qu'elle conserve  $a - x, y$ . Si d'ailleurs  $z = (z_{ik})$  et  $z' = (z'_{ik})$  sont dans  $\mathbf{P}$ , et si  $zz' = z'' = (z''_{ik})$ , on a  $z''_{ik} = 0$  pour  $i < k$  et  $z''_{ik} = \sum_k z'_{i\ell} z_{\ell k}$  pour  $k \leq i$ , d'où  $[z''] = [z][z']$ .

On peut donc admettre que  $[\varphi]$  est permutable à  $[\mu^s]$  (Cela est évident pour  $n = 2, 3$ ). Soit maintenant  $\zeta = (\zeta_{ik})$  une substitution indéterminée de  $\mathbf{P}$  telle que  $[\zeta] = 1$ , et soit  $\zeta^{-1} \mu^s \varphi \zeta = \mu^s \varphi'$ , d'où  $\varphi \zeta = \mu^{-s} \zeta \mu^s \varphi'$  (donc  $\varphi'$ , comme  $\mu^{-s} \zeta \mu^s$ , est dans  $\mathbf{P}$ , et  $[\varphi'] = [\varphi]$ ), ou, en posant  $\varphi' = (\varphi'_{ik})$ ,

$$(3) \quad \sum_{s=k}^i \zeta_{is} \varphi_{sk} = \sum_{s=k}^i \varphi'_{is} \mu^{s(s-k)} \zeta_{sk} \quad (k = 1 \text{ ou } i = n).$$

Pour que  $\varphi'_{2i} = 0$ , il faut et suffit, d'après (3), que  $\zeta_{2i} + \varphi_{2i} = \iota^s \zeta_{2i}$ , ce qui détermine  $\zeta_{2i}$ . Supposons donc dès l'abord que, pour  $i = 2, \dots, r$ , on ait  $\varphi'_{i1} = 0$  quand  $i \not\equiv 1 \pmod{q}$ , et cherchons à déterminer  $\zeta$  de manière que l'on ait  $\varphi'_{i1} = \varphi_{i1}$  pour  $i = 2, \dots, r$ , et  $\varphi'_{r+1,i} = 0$  ou  $\varphi_{r+1,i}$  selon que  $r \not\equiv 0$  ou  $\equiv 0 \pmod{q}$ . Il suffit pour cela de faire  $\zeta_{21} = \zeta_{31} = \dots = \zeta_{r1} = 0$  et  $\zeta_{r+1,1} = \frac{\varphi_{r+1,i}}{\iota^{s^r} - 1}$  ou 0 selon que  $r \not\equiv 0$  ou  $\equiv 0 \pmod{q}$ .

Il suffit donc de prendre pour  $\zeta$  celle des substitutions V, U,  $u$  qui remplace  $y_{r+1}$  par  $y_{r+1} + \zeta_{r+1,1} y_1$  (alors  $\zeta = 1$  si  $r \equiv 0 \pmod{q}$ ).

En faisant successivement  $r = 2, \dots, n - 1$ , on établira finalement la proposition (quand  $\varphi_{21} = \dots = \varphi_{n1} = 0$ , il résulte des relations fondamentales que  $\varphi_{n2} = \dots = \varphi_{n,n-1} = 0$ ).

Il reste pourtant à lever une objection dans le cas où  $\Lambda = Q$  (alors  $n = 2\nu + 1$ ) et où  $r = n - 1 \not\equiv 0 \pmod{q}$ , car alors la détermination choisie de  $\zeta$  est  $u_{1, \zeta_{n1}}$ , qui n'existe dans  $\mathbf{P}$  qu'à la condition de se réduire à 1. Mais précisément la combinaison de la première colonne de  $\varphi$  avec elle-même donne ici

$$\varphi_{n1} + \sum_{i=2}^{\nu} \varphi_{i1} \varphi_{n+1-i,1} + c \varphi_{\nu+1,1}^2 = 0.$$

Or on ne peut avoir à la fois  $i \equiv 1 \pmod{q}$  et  $n + 1 - i \equiv 1 \pmod{q}$ , ni  $\nu + 1 \equiv 1 \pmod{q}$ . Donc  $\varphi_{n1} = 0$  et  $\zeta_{n1} = 0$ .

Comme toute substitution de  $\mathbf{P}$  transforme  $\sigma_x$  en une substitution  $\sigma'_x = (\sigma'_{xik})$  où  $\sigma'_{x,k+1,k} = \sigma_{x,k+1,k}$ , et par suite  $\omega$  en un groupe ayant les mêmes propriétés, on voit qu'en transformant au besoin  $\omega$  par une substitution de  $\mathbf{P}$ , on peut supposer que son normalisant dans  $\mathbf{PM}$  contient une substitution de la forme  $\mu^s \varphi$  ( $g\varphi = \pi - 1$ ,  $q$  étant donné) où  $\varphi$  est dans  $\mathbf{P}$  et permutable à  $\mu^s$ . Alors,  $(\mu^s \varphi)^q = \mu^{s^q} \varphi^q$  étant permutable à  $\varphi$ , et  $\mu^{s^q}$  dans  $\Delta$ ,  $\varphi^q$  est permutable à  $\omega$ . Donc  $\varphi$  et  $\mu^s$  sont permutables à  $\omega$ .

Supposons désormais  $q$  maximum, et  $\omega$  déterminé comme il vient d'être dit. Soient  $\mu^{s_i} \varphi_i$  ( $i = 1, 2, \dots$ ;  $g_1 = g$ ;  $\varphi_1 = \varphi$ ) les substitutions de  $\mathbf{A}$  permutables à  $\omega$ ,  $\mu^{s_i} \varphi_i$  étant d'ordre  $q_i \pmod{\mathbf{P}\Delta}$ . Alors  $(\mu^s \varphi)^q (\mu^{s_i} \varphi_i)^r$  sera l'une d'elles, telle que  $\mu^{s^k} \varphi_k$ , et  $g_k = ug + v g_i$ . Or on peut choisir  $u$  et  $v$  de manière que  $g_k$  soit le p. g. c. d. de  $g$ ,  $g_i$ . Soit  $g = l g_k$ , et  $g'_k = \frac{\pi - 1}{q_k} g'_k$ ,  $g'_k$  étant premier à  $q_k$ . On aura  $l q g'_k = g_k$ . Mais  $g'_k$  est

premier à  $q_k$ . Donc  $g'_k = 1$ , et  $lq = q_k$ . Or  $q$  est maximum. Donc  $l = 1$ , et  $g_k = g$ . Donc  $g$  divise  $g_i$ . Donc  $\mu^{g_i}$  est permutable à  $\varpi$ . Donc  $\varphi_i$  est aussi permutable à  $\varpi$ . Si donc  $\varpi'$  est le normalisant de  $\varpi$  dans  $\mathbf{P}$ , le normalisant de  $\varpi$  dans  $\mathbf{PM}$ , et par suite dans  $\mathbf{A}(\mathbf{2})$ , est  $\{\mu^s\}\varpi'$ .

Comme les  $\sigma_{\alpha, i, i-1}$  sont tous  $\neq 0(\mathbf{1})$ , aucune puissance de  $\mu^s$  autre que  $\mu^{sq}$  n'est permutable à une  $\sigma_x(\mathbf{5})$ . Donc la substitution opérée sur les  $p^m - 1$   $\sigma_x$  quand on transforme  $\varpi$  par  $\mu^s$ , est formée de cycles d'ordre  $q$ . Donc  $q$  divise  $p^m - 1$ . Donc  $q$  divise le p. g. c. d.  $\Theta$  de  $\pi - 1$ ,  $p^m - 1$ . Or  $m$  divise  $K = mx$  si  $A = G$  ou  $Q$ , et  $2K = mx'$  si  $A = H$  ou  $\bar{H}(\mathbf{1})$ . Si  $m$  divise  $K$ ,  $\Theta = p^m - 1$ . Si  $m$  divise  $2K$  sans diviser  $K$ , c'est-à-dire si  $x'$  est impair et  $m = 2m'$ ,  $\Theta = 2(p^{m'} - 1)(\mathbf{1})$ .

On verra que  $q$  est toujours égal à  $\Theta$ .

3. Supposons que  $m$  divise  $K$  et admettons que  $q = p^m - 1$ . — Écrivons alors  $\iota_m, \mu_{0m}, \xi_{m\lambda} = \xi_m, \mu_{m\lambda} = \mu_m, M_{m\lambda} = M_m$  pour  $\iota^s, \mu_0^s, \xi_{\lambda}^s, \mu_{\lambda}^s, \{\mu_{\lambda}^s\}$ , désignons par  $\varpi_m$  le champ d'ordre  $p^m$ , et posons

$$\{\varpi, \mu_{m\lambda}\} = \Phi_A = \Phi, \quad \{\varpi, \mu_{m\lambda}^2\} = \Phi_A^u = \Phi^0.$$

Remarquons de suite que, si  $A = Q$ ,  $\mu_m = \prod_i m_i (\nu+1-i)^{s_i}$ , qui est toujours dans  $A^0$ , n'est pas toujours dans  $B$  (cf. *G.*, 59). Il y est évidemment si  $g$  ou  $x$  ( $\equiv g \pmod{2}$ ) est pair. Supposons donc  $x$  impair, et soit  $l$  un des nombres  $1, \dots, \nu$ . Si  $\nu$  est pair  $= 2\rho$ ,  $\nu+1-i$  prend des valeurs de parité différente pour  $i=l$  et  $i=\nu+1-l$ . Donc  $\mu_m$  est alors dans  $B$  toujours et seulement quand  $\rho$  est pair. Si  $\nu$  est impair  $= 2\rho+1$ ,  $\nu+1-i$  prend des valeurs de même parité pour  $i=l$  et  $i=\nu+1-l$ . Donc  $\mu_m$  est alors dans  $B$  toujours et seulement quand  $\rho$  est impair. Ainsi, pour  $A = Q$ ,  $\mu_m$  est dans  $B$  toujours et seulement si  $x$  est pair ou si  $\nu \equiv 0, 3 \pmod{4}$ .

On a maintenant  $\mu_m^{-r} \sigma_{\mu_m}^r = \sigma_{\mu_m}^r$ , et  $\mu_m^{-s} \sigma_{\mu_m}^s \mu_m^s = \mu_m^{-r-s} \sigma_{\mu_m}^{r+s} = \sigma_{\mu_m}^{r+s}$ . Donc  $\sigma_{\alpha\beta, i, k} = \beta^{i-k} \sigma_{\alpha ik}$ .

Donc  $\Phi | \Delta \equiv \{\varepsilon+1, \iota_m \varepsilon\}$ ,  $\Delta \sigma$  correspondant à  $\varepsilon+1$ , et  $\Delta \mu_m$  à  $\iota_m \varepsilon$ .

(1) Ici  $K = m'x'$ , et  $\frac{1}{2}(p^{m'}+1)$  est premier à  $\frac{1}{2}(p^k-1)$ . Car tout facteur  $\theta$  commun à  $\frac{1}{2}(p^m+1)$  et  $\frac{1}{2}(p^k-1)$  divise leur somme  $\frac{1}{2}(p^k+p^m)$ , donc  $\frac{1}{2}(p^{k-m}+1)$ , donc aussi  $\frac{1}{2}[p^{k-m}+1-(p^k-1)]$ , donc  $\frac{1}{2}(p^{k-2m}-1)$  et, en continuant ainsi, on voit que  $\theta = 1$ .

Si donc  $\beta$  est un des nombres  $1, \dots, p-1 \pmod p$ , l'élément de  $\Delta\omega$  qui répond à  $z + \alpha\beta = (z + \alpha)^\beta$  est  $\Delta\sigma_{z\beta} = \Delta\sigma_\alpha^\beta$ .

$\Phi$  est défini par les équations de  $\omega$  et de  $M_m$  jointes à  $\mu_m^{-1}\sigma_x\mu_m = \sigma_{x:m}$ ,  $\sigma_x$  parcourant les générateurs de  $\omega$  qu'on peut supposer être  $\sigma = \sigma_{:m}$ ,  $\sigma_{:1:m}, \dots, \sigma_{:m-1:m}$ . D'une part, en effet, il résulte de ces équations que  $\mu_m^{-1}$  est permutable aux  $\sigma_x$  (S., 73). D'autre part,  $\Phi$  vérifie ces équations et contient  $\Delta$  (cf. E., 18, 19).

$\Phi^0$  est défini par les équations de  $\omega$  et de  $\{\mu_m^2\}$  jointes à  $\mu_m^{-2}\sigma_x\mu_m^2 = \sigma_{x:m^2}$  (S., 73).

La condition  $\sigma_x\sigma_\beta = \sigma_{x+\beta}$  (qui entraîne  $\sigma_\alpha\sigma_\beta = \sigma_\beta\sigma_\alpha$ ) équivaut à

$$(4) \quad (\alpha + \beta)^{i-k}\sigma_{ik} = \sum_{\rho=i}^{\rho=k} \alpha^{\rho-k}\beta^{i-\rho}\sigma_{i\rho}\sigma_{\rho k} \quad (i \geq k),$$

d'où, en comparant les coefficients de  $\beta\alpha^{i-k}$ ,

$$(i-k)\sigma_{ik} = \sigma_{i,i-1}\sigma_{i-1,k}.$$

En remplaçant  $i$  par  $i-1, i-2, \dots, k+1$ , en multipliant les égalités ainsi obtenues, et en posant  $\sigma_{2,1}\sigma_{3,2} \dots \sigma_{l,l-1} = s_l$  si  $l > 1$ ,  $s_1 = 1$ , on obtient

$$(5) \quad \dots \quad (i-k)!\sigma_{ik} = \frac{s_i}{s_k} \quad (i \geq k \geq 1; 0! = 1).$$

Donc les  $\sigma_{ik}$  sont complètement déterminés par les  $\sigma_{j,j-1}$ , et  $\neq 0$  pour  $i \geq k$ . On voit d'ailleurs de suite que l'expression (5) de  $\sigma_{ik}$  vérifie (4) quels que soient les  $\sigma_{j,j-1}$ . Or, en transformant au besoin  $\omega$  par des  $m_i$ , on peut donner à  $\sigma_{2,1}, \sigma_{3,2}, \dots, \sigma_{\nu,\nu-1}$  si  $n = 2\nu$ , et à  $\sigma_{2,1}, \sigma_{3,2}, \dots, \sigma_{\nu+1,\nu}$  si  $n = 2\nu + 1$ , des valeurs arbitraires  $\neq 0$ . On va voir qu'alors les  $\sigma_{j,j-1}$  sont déterminés par les relations fondamentales.

6. Supposons d'abord que A soit le groupe  $H(n, \pi)$ . — Les relations fondamentales donnent

$$\sigma_{n-i+1,n-i} + \sigma_{i+1,i} = 0 \quad (i = 1, \dots, \nu-1, \text{ si } \nu > 1)$$

et

$$\sigma_{\nu+1,\nu} = \sigma_{\nu+1,\nu} \text{ si } n = 2\nu; \quad \sigma_{\nu+2,\nu+1} + \omega\sigma_{\nu+1,\nu} = 0 \text{ si } n = 2\nu + 1.$$

Si donc  $n = 2\nu$ , on peut, en transformant au besoin  $\omega$  par une  $\Pi'_{i=1} m_i$ ,

(ce qui multiplie  $\sigma_{\nu+1,\nu}$  par  $\rho\delta$  sans altérer  $\sigma_{21}, \sigma_{32}, \dots, \sigma_{\nu,\nu-1}$ ), donner à  $\sigma_{\nu+1,\nu}$  une valeur arbitraire dans  $\mathfrak{O}$ .

Supposons que  $\sigma_{21} = \sigma_{32} = \dots = \sigma_{\nu+1,\nu} = 1$ . On aura

$$s_l = \begin{cases} 1 & \text{pour } l = 1, \dots, \nu + 1, \\ (-1)^{l-\nu+1} \omega^\eta & \text{pour } l \geq \nu + 2, \end{cases}$$

et par suite

$$(6) \quad \left\{ \begin{array}{l} (i-k)! \sigma_{ik} = \begin{cases} 1 & \text{pour } i \geq \nu + 1 \\ (-1)^{i+\nu+1} \omega^\eta & \text{pour } i \geq \nu + 2 \text{ et } k \geq \nu + 1 \\ (-1)^{i+k} & \text{pour } i \geq \nu + 2 \text{ et } k \geq \nu + 2 \end{cases} \quad k < i. \\ \sigma_{ik} = 0 & \text{pour } i < k; \quad \sigma_{ii} = 1. \end{array} \right.$$

Ainsi, quand  $n$  divise  $\mathbf{K}$ ,  $\varpi$  est complètement déterminé. Mais on ne sait pas encore si  $\varpi$  divise  $\mathbf{A}$ , c'est-à-dire s'il conserve  $\alpha$ . Or, en posant

$$\begin{aligned} S_{\alpha\beta} &= \sum_1^\nu \sigma_{n+1-i,\alpha} \dot{\sigma}_{i\beta}, & S'_{\alpha\beta} &= \sum_1^\nu \sigma_{i\alpha} \dot{\sigma}_{n+1-i,\beta}; \\ T_{\alpha\beta} &= S_{\alpha\beta} - S'_{\alpha\beta}, & \tau_{\alpha\beta} &= \omega \sigma_{\nu+1,\alpha} \dot{\sigma}_{\nu+1,\beta}, \end{aligned}$$

cette condition, formulée dans  $G, \mathbf{1}$ , s'écrit

$$(7) \quad \left\{ \begin{array}{l} T_{\alpha\beta} + \tau_{\alpha\beta} = \begin{cases} 0 & \text{si } \alpha + \beta \neq n + 1, \\ 0 & \text{si } \alpha + \beta = n + 1 \text{ et } \alpha \neq \beta, \\ \omega & \text{si } \alpha + \beta = n + 1 \text{ et } \alpha = \beta \text{ (alors } n = 2\nu + 1); \end{cases} \\ \theta = 1 & \text{si } \alpha \geq \beta; \quad \theta = -1 & \text{si } \alpha < \beta. \end{array} \right.$$

Il s'agit de montrer que les valeurs (6) des  $\sigma_{ik}$  vérifient (7).

Soit d'abord  $n = 2\nu$ . Les seuls termes  $\neq 0$  de  $S_{\alpha\beta}$  sont ceux où  $i \geq \beta$  et  $n + 1 - i \geq \alpha$ . Si donc  $\beta > n + 1 - \alpha$  ou  $\alpha + \beta > n + 1$ ,  $S_{\alpha\beta} = 0$ , et de même  $S'_{\alpha\beta} = 0$ . Si  $\alpha + \beta = n + 1$ , ou bien  $\beta$  est  $\leq \nu$  (donc  $\alpha > \nu$ ), et  $S_{\alpha\beta}$  se réduit à un terme égal à 1, tandis que  $S'_{\alpha\beta} = 0$ , d'où  $T_{\alpha\beta} = 1$ , ou bien  $\alpha$  est  $\leq \nu$  (donc  $\beta > \nu$ ), et  $S_{\alpha\beta} = 0$ ,  $S'_{\alpha\beta} = 1$ , d'où  $T_{\alpha\beta} = -1$ . Soit  $\alpha + \beta < n + 1$  et  $n + 1 - \alpha - \beta = f$ . Il suffit de faire croître  $i$ , dans  $S_{\alpha\beta}$ , de  $\beta$  (si  $\beta \leq \nu$ ) jusqu'au plus petit  $\mu$  des deux nombres  $\nu, n + 1 - \alpha$ , et dans  $S'_{\alpha\beta}$ , de  $\alpha$  (si  $\alpha \leq \nu$ ) jusqu'au plus petit  $\mu'$  des deux nombres  $\nu, n + 1 - \beta$ . Si alors  $B \leq \nu$  et  $\alpha > \nu$ , on

a  $S'_{\alpha\beta} = 0$ ,  $\mu = n + 1 - \alpha$ , et, en posant  $i = \beta + h$ ,

$$S_{\alpha\beta} = (-1)^{\nu-\beta} \sum_0^f \frac{(-1)^h}{h!(f-h)!} = \frac{(-1)^{\nu-\beta}}{f!} (1-1)^\nu = 0.$$

Si  $\alpha \leq \nu$  et  $\beta > \nu$ , on a de même  $S_{\alpha\beta} = S'_{\alpha\beta} = 0$ .

Si  $\alpha$  et  $\beta$  sont  $\leq \nu$ , on a  $\mu = \mu' = \nu$ . En posant dans  $S_{\alpha\beta}$   $i = \beta + h$ , et dans  $S'_{\alpha\beta}$   $n + 1 - i = \beta + h$ , on a  $T_{\alpha\beta} = (-1)^{\nu-\beta} \sum_0^f \frac{(-1)^h}{h!(f-h)!} = 0$ .

Soit  $n = 2\nu + 1$ . Si  $\alpha + \beta > n + 1$ , on a  $S_{\alpha\beta} = S'_{\alpha\beta} = \tau_{\alpha\beta} = 0$ . Si  $\alpha + \beta = n + 1$ , ou bien  $\alpha \neq \beta$  (donc  $\alpha$  ou  $\beta$  est  $> \nu$ ) et l'on a  $T_{\alpha\beta} = 0$ ,  $\tau_{\alpha\beta} = \omega$ , ou bien  $\alpha = \beta = \nu + 1$ , et l'on a  $T_{\alpha\beta} = 0$ ,  $\tau_{\alpha\beta} = \omega$ .

Soit  $\alpha + \beta < n + 1$  et  $n + 1 - \alpha - \beta = f$ . On définit  $\mu$  et  $\mu'$  comme précédemment. Si alors  $\beta$  est  $\leq \nu$  et  $\alpha > \nu + 1$ , ou si  $\alpha \leq \nu$  et  $\beta > \nu + 1$ , on a encore  $T_{\alpha\beta} = \tau_{\alpha\beta} = 0$ . Si  $\beta \leq \nu$  et  $\alpha \leq \nu + 1$ , ou si  $\alpha \leq \nu$  et  $\beta \leq \nu + 1$ , on a  $\mu' = \mu = \nu$ . En posant dans  $S_{\alpha\beta}$   $i = \beta + h$ , et dans  $S'_{\alpha\beta}$   $n + 1 - i = \beta + h$  ( $S'_{\alpha\beta} = 0$  pour  $\alpha = \nu + 1$ , et  $S_{\alpha\beta} = 0$  pour  $\beta = \nu + 1$ ), on a  $T_{\alpha\beta} + \tau_{\alpha\beta} = (-1)^{\nu+1-\beta} \omega (1-1)^f = 0$ .

Ainsi  $\varpi$  divise  $\Lambda$ , et  $q$  est effectivement égal à  $p^m - 1$ .

7. *Supposons maintenant que  $\Lambda = G(n, \pi)$ . En transformant  $\varpi$  par une  $\Pi'_{i=1} m_i \rho$ ,  $\rho$  étant dans  $\mathcal{E}'$ , on peut ramener  $\sigma_{\nu+1, \nu}$  à 1,  $\sigma_{2,1}, \dots, \sigma_{\nu, \nu-1}$  restant égaux à 1. On reconnaît alors, comme dans le cas  $\Lambda = H$ , l'existence, dans  $\Lambda(n, \pi^2)$  du diviseur  $\Phi = \{\varpi, \mu_m\}$  qui est contenu dans  $\mathbf{PM}$  ( $\mathbf{P}$  ayant toujours le même sens). Donc  $q$  est encore effectivement égal à  $p^m - 1$ . Si  $x$  est pair,  $\mu^x$  est dans  $\{\mu^2\}$  ( $g \equiv x \pmod{2}$ ), et  $\Phi$  divise  $\Lambda$ . Si  $x$  est impair, le p. g. c. d. de  $\Phi$ ,  $\Lambda$  est  $\Phi^0$ .*

Mais ici se pose une question nouvelle. En transformant le groupe initial  $\varpi$  où  $\sigma_{\nu+1, \nu}$  était encore indéterminé par les  $m_i$  de  $\Lambda$ , on peut ramener  $\sigma_{\nu+1, \nu}$  soit à 1, soit à un non carré de  $\mathcal{E}$  arbitraire  $N$ . Appelons encore  $\varpi$  le groupe où  $\sigma_{\nu+1, \nu} = 1$ , et  $\varpi_N$  celui où  $\sigma_{\nu+1, \nu} = N$ . Nous savons que  $\varpi$  divise  $\Lambda$ . Mais  $\varpi_N$  divise-t-il aussi  $\Lambda$ ? Et si  $\varpi_N$  divise  $\Lambda$ , y est-il conjugué de  $\varpi$ ? Tout d'abord  $\varpi_N$  est premier à  $\varpi$ , car  $\mu_m$ , qui est permutable à  $\varpi_N$  comme à  $\varpi$  (toute  $m_i$  est permutable à  $\mu_m$ ), transforme chaque  $s_p$  de l'un quelconque de ces groupes en toutes les autres. De plus  $\varpi$  et  $\varpi_N$  sont conjugués dans  $\Lambda'$ , car la substitution  $s$  de  $\Lambda'$  qui multiplie  $y_1, \dots, y_\nu$  par  $N^{-1}$  sans altérer  $x_1, \dots, x_\nu$  transforme  $\varpi$

en  $\varpi_N$ . Donc  $\varpi_N$  divise A. En posant alors  $s^{-1}\sigma_\alpha s = \sigma_\alpha^{(N)} = (\sigma_{\alpha ik}^{(N)})$  et  $\sigma_i^{(N)} = \sigma^{(N)}$ ,  $\sigma_{ik}^{(N)} = \sigma_{ik}^{(N)}$ , on aura  $\sigma_{\alpha ik}^{(N)} = \sigma_{\alpha ik} = \alpha^{i-k} \sigma_{ik}$  si  $i$  et  $k$  sont tous deux  $> \nu$  ( $i > k$ ) ou tous deux  $\leq \nu$ , et  $\sigma_{\alpha ik}^{(N)} = N \sigma_{\alpha ik} = N \alpha^{i-k} \sigma_{ik}$  si  $i > \nu$  et  $k \leq \nu$ . Comme d'ailleurs  $s$  est permutable à  $\mu$ , on voit que, si  $\nu'_m = \alpha$ ,  $\mu_m^{-r} \sigma_\beta^{(N)} \mu_m^r = s^{-1} \mu_m^{-r} \sigma_\beta \mu_m^r s = s^{-1} \sigma_{\alpha\beta} s = \sigma_{\alpha\beta}^{(N)}$ .

Supposons qu'il y ait dans A une substitution  $\lambda = (\lambda_{ik})$  transformant  $\varpi$  en  $\varpi_N$ . Il y aura dans  $\lambda\varpi_N$  une substitution transformant  $M_m$  en lui-même (et toujours  $\varpi$  en  $\varpi_N$ ). Prenons-la pour  $\lambda$ . On voit comme au n° 2 que  $\lambda$  est dans  $\lambda_0 \mathbf{P} = \mathbf{P} \lambda_0$ ,  $\lambda_0$  étant un produit de  $m_i$ , donc permutable à  $\mu_m$ . Or,  $n$  étant ici pair, donc  $> p$ , toute substitution de  $\mathbf{P}$  permutable à  $M_m$  se réduit à 1 (5). Donc  $\lambda$  coïncide avec  $\lambda_0$ . Supposons que  $\lambda^{-1} \sigma \lambda = \sigma_\alpha^{(N)}$  (en prenant pour  $\lambda$  une substitution de  $\lambda \mid \mu_m^2 \mid$ , on peut remplacer  $\alpha$  par un élément quelconque de  $\varepsilon_m$  ayant le même caractère quadratique dans  $\varepsilon_m$ ). On aura, comme au n° 2, en posant  $\lambda_{ii} = \lambda_i$ ,  $\lambda_i \lambda_{n+1-i} = 1$  et  $\lambda_k \sigma_{k,k-1} = \alpha \sigma_{k,k-1}^{(N)} \lambda_{k-1}$ , d'où  $\lambda_k = \alpha \lambda_{k-1}$  pour  $k = 2, \dots, \nu$  ou  $k = \nu + 2, \dots, n$ , et  $\lambda_{\nu+1} = N \alpha \lambda_\nu$ . Comme  $\lambda_{\nu+1} \lambda_\nu = 1$ , on a  $N \alpha = \lambda_\nu^{-1}$ , et  $\alpha$  est non carré dans  $\varepsilon$ . Or  $\alpha$  a la forme  $\nu'_m = \nu^{gr}$ , et  $g$  a la parité de  $z$ .

Donc, si  $z$  est pair,  $\varpi$  et  $\varpi_N$  ne sont pas conjugués dans A.

Supposons donc  $z$  impair,  $\alpha$  non carré et  $\lambda = \sqrt[n]{N\alpha}$ . On aura  $\lambda_i = \alpha^{i-\nu} \lambda_\nu$  pour  $i = 1, \dots, \nu - 1$ , et la condition  $\lambda_k = \alpha \lambda_{k-1}$  ( $\nu + 2 \leq k \leq n$ ) qui, en posant  $k = n + 1 - i$  ( $1 \leq i \leq \nu - 1$ ), s'écrit  $\lambda_{i+1} = \alpha \lambda_i$ , est vérifiée d'elle-même. On a alors effectivement  $\lambda^{-1} \sigma \lambda = \sigma_\alpha^{(N)}$  (on peut supposer que  $N = \alpha^{1-2\nu}$ , et prendre alors  $\lambda_\nu = \alpha^{\nu-1}$ , d'où  $\lambda_i = \alpha^{i-1}$  pour  $i \leq \nu$ ) et,  $\lambda$  étant permutable à  $\mu$ ,  $\lambda^{-1} \sigma_\beta \lambda = \sigma_{\alpha\beta}^{(N)}$ .

Ainsi les diviseurs de A semblables à  $\varpi$  forment dans A deux systèmes conjugués (représentés par  $\varpi$  et  $\varpi_N$  conjugués dans A') ou un seul selon que  $z$  est pair ou impair.

8. Supposons que A soit le groupe  $\bar{H}(n, \pi)$ . Les relations fondamentales donnent ici

$$\sigma_{n+1-i, n-i} + \dot{\sigma}_{i+1, i} = 0 \quad (i = 1, \dots, \nu - 1, \text{ si } \nu > 1)$$

et

$$\sigma_{\nu+1, \nu} + \dot{\sigma}_{\nu+1, \nu} = 0 \quad \text{si } n = 2\nu; \quad \sigma_{\nu+2, \nu+1} + 2c \dot{\sigma}_{\nu+1, \nu} = 0 \quad \text{si } n = 2\nu + 1.$$

Si  $n = 2\nu$ ,  $\sigma_{\nu+1, \nu}$  est de la forme  $\omega e$ ,  $e$  étant dans  $\mathfrak{S}$ . Prenons  $\sigma_{21} = \sigma_{32} = \dots = \sigma_{\nu, \nu-1} = 1$  et (en transformant au besoin par une  $\Pi'_{i=1} m_{i2}$ , ce qui laisse  $\sigma_{11}, \dots, \sigma_{\nu, \nu-1}$  inaltérés)  $\sigma_{\nu+1, \nu} = \omega$ . On aura

$$s_l = \begin{cases} 1 & \text{pour } l = 1, \dots, \nu, \\ (-1)^{l-\nu+1} \omega & \text{si } l \geq \nu + 1. \end{cases}$$

Le groupe ainsi obtenu se déduit de celui obtenu pour  $A = \Pi(n, \pi)$  par le changement de variables qui consiste à remplacer  $y_i$  par  $\omega y_i$  pour  $i = 1, \dots, \nu$  sans altérer les  $x_i$  (ce qui change  $\Pi$  en  $\bar{\Pi}$ ). Je le négligerai désormais.

Si  $n = 2\nu + 1$ , je prendrai  $c = \frac{1}{2}$  (en changeant au besoin la variable  $x$ ). Alors  $\sigma_{n+1-i, n-i} = -\dot{\sigma}_{i+1, i}$  quel que soit  $i$ . Je prendrai en outre  $\sigma_{i+1, i} = (-1)^i$  pour  $i = 1, \dots, \nu$ . Alors  $\sigma_{i, i-1} = (-1)^i$  pour  $i = 1, \dots, n$ , et  $s_l = (-1)^{2+3+\dots+l} = (-1)^{\frac{(l-1)(l-2)}{2}}$ .

Pour que  $\varpi$  conserve  $a$ , qui peut s'écrire  $\frac{\omega}{2} \sum_1^n (y_k \dot{y}_{n+1-k} + \dot{y}_k y_{n+1-k})$ , il faut et suffit que la somme  $S_{\alpha\beta} = \sum_{k=1}^n \sigma_{k\alpha} \dot{\sigma}_{n+1-k, \beta}$  soit égale à 0 pour  $\alpha + \beta \neq n + 1$ , et à 1 pour  $\alpha + \beta = n + 1$ . Or, ici encore, si  $\alpha + \beta > n + 1$ ,  $S_{\alpha\beta} = 0$ . Si  $\alpha + \beta = n + 1$ ,  $S_{\alpha\beta}$  se réduit à 1. Si  $\alpha + \beta < n + 1$ , il suffit de faire varier  $k$  de  $\alpha$  à  $n + 1 - \beta$  ou, en posant  $k = \alpha + h$ , de faire varier  $h$  de 0 à  $f = n + 1 - \alpha - \beta$ . On a alors

$$S_{\alpha\beta} = \sum_0^f \frac{1}{h! (f-h)!} \frac{s_{\alpha+h}}{s_\alpha} \frac{\dot{s}_{n+1-\alpha-h}}{\dot{s}_{n+1-\alpha-f}}$$

Or

$$\frac{s_{\alpha+h}}{s_\alpha} \frac{\dot{s}_{n+1-\alpha-h}}{\dot{s}_{n+1-\alpha-f}} = (-1)^{h\alpha + \frac{h(h+1)}{2} + (f-h)(n+1-\alpha-f) + \frac{(f-h)(f-h+1)}{2}}$$

se réduit, à un facteur près indépendant de  $h$ , à  $(-1)^h$ . Donc  $S_{\alpha\beta} = 0$ .

9. *Supposons enfin que  $A = Q(n, \pi)$ . On a vu (1) que, si  $n = 2\nu$ ,  $\varpi$  n'existe pas.*

*Soit  $n = 2\nu + 1$ . En prenant  $c = \frac{1}{2}$ , on obtient évidemment le même groupe que dans le cas  $A = \bar{H}$ .*



Ainsi, quand  $m$  divise  $K = mx$ ,  $q$  est effectivement égal à  $p^m - 1$ .

**10.** Supposons maintenant que  $m$  ne divise pas  $K$ . Alors  $A = H$  ou  $\bar{H}$ ,  $m$  divise  $K = mx'$ ,  $m = 2m'$ , et  $q$  divise  $2(p^{m'} - 1)$ . Or le groupe  $\omega$  construit précédemment est évidemment dans  $A$ , et  $A$  contient toujours  $\mu$ . Donc  $A$  contient le  $g_{2p^m, p^{m'-1}}$  de  $\Phi$ . Donc  $q = 2(p^{m'} - 1)$ .

**11.** Il est maintenant facile de déterminer le normalisant  $\omega'$  de  $\omega$  dans  $\mathbf{P}$ . Pour qu'une substitution  $\varphi = (\varphi_{kl})$  de  $\mathbf{P}$  transforme  $\sigma_\alpha$  en  $\sigma_\beta$ , il faut et suffit qu'on ait

$$\sum_{\rho=1}^n \varphi_{k\rho} \sigma_{\rho l} \alpha^{\rho-l} = \sum_{\rho=1}^n \sigma_{\rho k} \beta^{\rho-l} \varphi_{\rho l}$$

ou

$$\sum_{\rho=1}^n \varphi_{k\rho} \sigma_{\rho l} \alpha^{\rho-l} = \sum_{\rho=1}^n \sigma_{\rho k} \beta^{\rho-l} \varphi_{\rho l}$$

$\alpha$  et  $\beta$  étant dans  $\mathfrak{E}_m$ . Comme  $\varphi_{kl} = \sigma_{kl} = 0$  pour  $k < l$ , et que  $\varphi_{kk} = \sigma_{kk} = 1$ , l'équation est identique pour  $k \leq l$ . Soit  $k = l + h > l$ . Pour  $h = 1$ , elle donne  $\alpha = \beta$  (donc  $\varphi$  est permutable à  $\sigma_\alpha$ ), et l'on a, en supprimant les termes qui se détruisent,

$$\sum_{i=1}^{h-1} \varphi_{l+h, l+i} \sigma_{l+i, l} \alpha^{i-l} = \sum_{i=1}^{h-1} \sigma_{l+h, l+i} \alpha^{h-i} \varphi_{l+i, l}$$

On voit que, pour  $h = 2$ ,  $\frac{\varphi_{l+2, l+1}}{\sigma_{l+2, l+1}} = \frac{\varphi_{l+1, l}}{\sigma_{l+1, l}}$  est indépendant de  $l$ . Soit donc  $\varphi_{l+1, l} = \theta_1 \sigma_{l+1, l}$  et admettons que l'on ait, pour  $\rho = 1, \dots, h-2$ ,  $\varphi_{l+\rho, l} = \theta_\rho \sigma_{l+\rho, l}$ ,  $\theta_\rho$  ne dépendant pas de  $l$  ( $\theta_0 = 1$ ). L'équation précédente donne alors, en remplaçant généralement  $\sigma_{uv}$  par  $\frac{s_u}{s_v} \frac{1}{(u+v)!}$ ,

$$\varphi_{l+h, l+1} \frac{s_{l+1}}{s_l} = \varphi_{l+h-1, l} \frac{s_{l+h}}{s_{l+h-1}},$$

ou, en multipliant par  $(h-1)! \frac{s_l}{s_{l+h}}$ ,

$$\frac{\varphi_{l+h, l+1}}{\sigma_{l+h, l+1}} = \frac{\varphi_{l+h-1, l}}{\sigma_{l+h-1, l}},$$

c'est-à-dire que  $\varphi_{l+h-1, l} = \theta_{h-1} \sigma_{l+h-1, l}$ ,  $\theta_{h-1}$  étant indépendant de  $l$ . Mais les  $\theta_i$  (qui sont dans  $\mathfrak{E}$  si  $A = \bar{G}$  ou  $Q$ ) doivent satisfaire à la

condition que  $\varphi$  conserve la même forme  $a$  que  $\tau$ . D'après la vérification faite au n° 3, cette condition équivaut, quel que soit  $A$ , à

$$(1) \quad \sum_{h=0}^f (-1)^h \binom{f}{h} \theta_h \hat{\theta}_{f-h} = 0 \quad (\theta_0 = 1 \text{ pour } f = 1, \dots, n-1),$$

qui s'écrit encore :

$$\text{si } f \text{ est impair} = 2\mu + 1,$$

$$(2) \quad \theta_f - \hat{\theta}_f - f(\theta_1 \hat{\theta}_{f-1} - \theta_{f-1} \hat{\theta}_1) + \dots + (-1)^\mu \binom{f}{\mu} (\theta_\mu \hat{\theta}_{\mu+1} - \theta_{\mu+1} \hat{\theta}_\mu) = 0;$$

$$\text{si } f \text{ est pair} = 2\mu,$$

$$(3) \quad \theta_f + \hat{\theta}_f - f(\theta_1 \hat{\theta}_{f-1} - \theta_{f-1} \hat{\theta}_1) + \dots + (-1)^{\mu-1} \binom{f}{\mu-1} (\theta_{\mu-1} \hat{\theta}_{\mu+1} - \theta_{\mu+1} \hat{\theta}_{\mu-1}) + (-1)^\mu \binom{f}{\mu} \theta_\mu \hat{\theta}_\mu = 0.$$

Soit  $A = H$ ,  $\nu = \nu$ , et  $\theta_f = \theta'_f + \nu \theta''_f$ ,  $\theta'_f$  et  $\theta''_f$  étant dans  $\mathfrak{O}$ . En choisissant arbitrairement les  $\theta'_{2\mu+1}$  et les  $\theta''_{2\mu}$ , on détermine successivement les  $\theta'_{2\mu+1}$  par (2) ( $\theta'_1 = 0$ ), et les  $\theta'_{2\mu}$  par (3). Donc  $\mathfrak{O}'$  est d'ordre  $\pi^{n-1}$ .

Si  $\theta_1 = \theta_2 = \dots = \theta_{n-2} = 0$ , on a  $\theta_{n-1} = (-1) \hat{\theta}_{n-1}$ . Or, on vérifie de suite que  $s_n = (-1)^n s_n$ . Donc  $\varphi_{n1} = \frac{s_n \hat{\theta}_{n-1}}{(n-1)!} = \hat{\varphi}_{n1}$ . Donc  $\varphi$  est une  $u_1$  (si  $A = \bar{H}$  on trouverait une  $\bar{u}_1$ ) arbitraire. Donc  $\mathfrak{O}'$  contient  $\{u_1\}$ , ce qui devrait être, *a priori*, puisque  $\{u_1\}$  est le central de  $\mathbf{P}(G., 13)$ .

Soit  $A = G$  ou  $Q$ . Alors (2) s'évanouit, et, en prenant arbitrairement les  $\theta_{2\mu+1}$ , on détermine successivement les  $\theta_{2\mu}$  par (3). Donc  $\mathfrak{O}'$  est d'ordre  $\pi^\nu$ .

Supposons  $\theta_1, \theta_3, \dots, \theta_{2\nu-3}$  nuls. Si alors  $n = 2\nu$  ( $A = G$ ),  $\varphi$  est une  $u_1$  arbitraire [ici encore le central de  $\mathbf{P}$  est  $\{u_1\}$  ( $G., 23$ )]. Si  $n = 2\nu + 1$  ( $A = Q$ ),  $\theta_{2\nu-2}$  et  $\theta_{2\nu}$  sont nuls, et  $\varphi$  est une  $U_{1,2}$  arbitraire, c'est-à-dire que  $\varphi$  parcourt le central de  $\mathbf{P}(G., 42)$ .

Plus généralement, d'après (3), si  $\theta_1, \dots, \theta_\mu$  sont nuls,  $\theta_{2\mu} = 0$ . Donc, si tous les  $\theta_f$  d'indice impair  $\leq \mu$  sont nuls,  $\theta_{2\mu} = 0$ . Pour que  $\theta_1, \dots, \theta_f$  soient nuls, il faut donc et il suffit que tous les  $\theta_f$  d'indice impair  $\geq f$  soient nuls.

**12.** Déterminons encore le normalisant  $\Phi'$  et  $\Phi$  dans  $A$ . Soit  $s$

une substitution de  $A$  permutable à  $\Phi$ .  $s$ , étant évidemment permutable à  $\varpi$ , est dans  $\{\mu_m\} \varpi'$  (5), et, en prenant pour  $s$  une substitution convenable de  $\Phi s$ , on peut supposer  $s$  dans  $\varpi'$ .  $s$  transforme  $\mu_m$  en une substitution de la forme  $\sigma_x^{-1} \mu_m^h \sigma_x$ . Donc  $s \sigma_x^{-1} = \varphi = (\varphi_{ik})$  est dans  $\varpi'$  et permutable à  $\{\mu_m\}$ . Or, on a vu (5) qu'une telle substitution n'existe hors de  $\Phi$  que si  $n = p$  avec  $m = 1$  et  $A = H$  ou  $\bar{H}$ , et qu'alors elle peut être quelconque dans  $\{u_{1,1,m}\}$  si  $A = H$  ou dans  $\{\bar{u}_{1,\omega,m}\}$  si  $A = \bar{H}$ .

Donc, en exceptant le cas où  $n = p$  avec  $m = 1$  et  $A = H$  ou  $\bar{H}$ ,  $\Phi' = \Phi$ . Si  $n = p$  avec  $m = 1$ ,  $\Phi' = \{\Phi, u_{1,1,m}\}$  pour  $A = H$ , et  $\Phi' = \{\Phi, \bar{u}_{1,\omega,m}\}$  pour  $A = \bar{H}$ .

**15.** Pour que  $A(n, p^h)$  divise  $A(n, \pi)$ , il faut que  $n$  divise  $K$ . Si  $A = G$  ou  $Q$ , cela suffit. Si  $A = H$  ou  $\bar{H}$ , il faut en outre et il suffit que  $\frac{K}{n}$  soit impair (1).

Supposons que  $mk$  divise  $K$ , le quotient étant impair pour  $A = H$  ou  $\bar{H}$ , et cherchons si  $\Phi$  ou, pour  $A = G$  avec  $x \equiv 1 \pmod{2}$ ,  $\Phi^v$  divise  $A(n, p^{mk})$ . Par construction  $\varpi$  divise  $A(n, p^{mk})$ , sauf peut-être si  $A = H$  avec  $n = 2v + 1$  ou si  $A = \bar{H}$  avec  $n = 2v$ , à cause de la présence de  $\omega$ . On pourrait négliger ces deux cas comme sans intérêt. Mais, comme  $\frac{K}{mk}$  est impair, le champ  $\mathfrak{E}_{mk}$  d'ordre  $p^{mk}$  contient un non carré  $N$  de  $\mathfrak{C}$ . En supposant donc que  $v^2 = N$ ,  $v$  délimite à la fois  $\mathfrak{C}'$  relativement à  $\mathfrak{C}$  et le champ  $\mathfrak{E}'_{mk}$  d'ordre  $p^{2mk}$  relativement à  $\mathfrak{E}_{mk}$ . Alors  $\omega$  est dans  $\mathfrak{E}'_{mk}$ , et  $\varpi$  divise toujours  $A(n, p^{mk})$ .

Il suffit donc de considérer  $\mu_m$  ou, si  $A = G$  avec  $x \equiv 1 \pmod{2}$ ,  $\mu_m^z$ . On voit de suite que  $A(2v + 1, p^{mk})$  contient toujours  $\Phi$ , et que  $G(2v, p^{mk})$ , qui contient toujours  $\Phi^v$ , contient  $\Phi$  toujours et seulement si  $k$  est pair (pour qu'il contienne  $\Phi$ , il faut et suffit que  $\xi_m^{p^{mk}-1} = 1$ , d'où  $\frac{p^{mk}-1}{p^m-1} \equiv 0 \pmod{2}$ ).

Soit donc  $A = H$  avec  $n = 2v$ . Comme  $\mu_{0,m}$  multiplie l'invariant de

(1) Si  $A = G$  ou  $Q$ , les générateurs de  $A(n, \pi)$  appartiennent évidemment à  $A(n, \pi')$  quel que soit  $l$ . Si  $A = H(n, \pi)$ , les générateurs de  $A(n, \pi)$  ne conservent l'invariant de  $H(n, \pi')$  que si  $l$  est impair.

$H(n, p^{mk})$  par  $\iota_m^{n+1}$ , la condition que  $\mu_m$  soit dans  $H(n, p^{mk})$  revient à  $\xi_m^{p^{mk}+1} = \iota_m^{n+1}(\xi_m$  est alors dans  $\mathcal{D}'_{mk}$ ).

Soit d'abord  $\pi \equiv 1 \pmod 4$  (donc  $t = 1$ ). Comme  $\frac{K}{mk}$  est impair, on a  $k \equiv \alpha \pmod 2$ , donc, même si  $p \equiv 3 \pmod 4$ ,  $p^{mk} \equiv 1 \pmod 4$ . La condition précédente revient alors à  $\frac{p^{mk}-1}{p^m-1} \equiv \frac{\pi-1}{p^m-1} \pmod 2$ , qui est vérifiée.

Soit  $\pi \equiv 3 \pmod 4$  (donc  $mk \equiv K \equiv 1 \pmod 2$ ) et  $p = -1 + 2^\rho h$  ( $h$  impair). On voit par récurrence que  $p^\alpha = -1 + 2^\rho h_\alpha$  ( $\alpha, h_\alpha$  impairs). Donc  $\rho = t$ , et  $\frac{p^{mk}+1}{2^t}$  est impair. On trouve alors, comme précédemment,  $\frac{p^{mk}-1}{p^m-1} \equiv \frac{\pi-1}{p^m-1} \pmod 2$ .

Donc tout diviseur  $H(n, p^{mk})$  de  $H$  contient  $\Phi^{(1)}$ .

(1) En partant du diviseur  $A(n, p^{mk})$  de  $A$  comme on est parti de  $A$ , on obtient la même détermination de  $M_m$ . Désignons, en effet, par  $\iota_{km}, \iota'_{km}, \mu_{0,km}, \mu_{km}, \xi_{km}$  les éléments qui remplacent alors  $\iota, \iota', \mu_{0m}, \mu_m, \xi_m$ , en faisant  $\iota_{km} = \iota \frac{\pi-1}{p^{km}-1}$ ,  $\iota'_{km} = \iota' \frac{\pi^2-1}{p^{2km}-1}$ .

Si  $n = 2\gamma + 1$ , on a évidemment  $\mu_{0,km} = \mu_{km}$  et  $\xi_{km} = \xi_m$ .

Soit donc  $n = 2\gamma$ . La condition  $\mu_m = \mu_{km}^u$  s'écrit  $[\xi_{km}^u \xi_m^{-1}] = \mu_{0,km}^u \mu_{0m}^{-1}$ . Or, pour que le second membre soit dans  $I'$ , il faut et suffit que

$$\mu_m^{-1} = \iota_m^{2u} \mu_m^{-1} = \dots = \iota_m^{u(u-1)},$$

d'où  $u = 1 + h(p^m - 1)$ , et  $\xi_m = \xi_{km}^u$ .

Soit d'abord  $A = H$ . Alors  $\frac{\alpha}{k}$  est impair, donc aussi  $\frac{\pi+1}{p^{mk}+1}$ ; donc la plus haute puissance de 2 divisant  $p^{mk} + 1$  est  $2^t$ . La condition  $\xi_m = \xi_{km}^u$  revient alors à la congruence

$$h \left[ 2^t \left( n + 1 - \frac{p^{mk} + 1}{2^t} \right) + 2 \right] \equiv \frac{\pi - 1}{p^m - 1} - \frac{p^{mk} - 1}{p^m - 1} \pmod{2^{t+1}},$$

qui est toujours résoluble en  $h$  (le premier membre est  $\equiv 2h \pmod{2^{t+1}}$ , et le second est  $\equiv \alpha - k \pmod 2$ ).

Soit  $A = G$ , et  $k$  pair. La condition  $\xi_m = \xi_{km}^u$  revient à  $h \equiv 0 \pmod 2$ .

Pour  $A = G$  et  $k$  impair, la question qui se pose est celle de l'égalité  $\mu_m^2 = \mu_{km}^2$ . Elle exige d'abord que  $2u = 2 + h(p^m - 1)$ , puis que  $\xi_m^2 = \xi_{km}^{2u}$ , d'où encore  $h \equiv 0 \pmod 2$ .

14. Cherchons maintenant dans  $\mathfrak{A}$  un diviseur  $\mathfrak{X}$  isomorphe à  $\mathfrak{L}(2, p^m)$ , dont les  $s_p$  soient irréductibles, en entendant par là qu'elles sont irréductibles quand on regarde les variables comme non homogènes.

Soit  $\bar{X}$  un diviseur de  $A$  contenant  $\Omega(2)$  et tel que  $\bar{X} \mid \Omega \equiv \mathfrak{X}$ . De la structure des  $\mathfrak{g}_{p^m, p^{m-1}}$  de  $\mathfrak{X}$  et de l'analyse précédente il résulte : 1° que  $m$  divise  $K = mz$ , et si  $A = G$ , que  $z$  est pair (7); 2° qu'en transformant au besoin  $\bar{X}$  par  $A$  ou, si  $A = G$  par  $A'$ , on peut supposer  $\Phi = [\varpi, \mu_m]$  contenu dans  $\bar{X}$ .

Soit  $\gamma = (\gamma_{ik})$  une substitution de  $X$  telle que  $\Omega\gamma$  corresponde à  $(-z^{-1})$  de  $\mathfrak{L}(2, p^m)$ . Pour l'existence de  $\bar{X}$ , il faut que l'on ait mod  $\Omega$  (S., 85).

$$\gamma^2 = 1, \quad (\gamma\sigma)^2 = 1, \quad \gamma^{-1}\mu_m\gamma \equiv \mu_m^{-1}$$

et ces conditions, jointes à celles déjà indiquées, sont suffisantes (*loc. cit.*).

Je poserai  $\gamma^2 = [\zeta]$ ,  $[\zeta]$  étant dans  $\Omega$ , et, si  $\Omega = D$ ,  $[\zeta] = d^h$ .

L'équation  $[\gamma\sigma]^2 \equiv 1 \pmod{\Omega}$  s'écrit  $\sigma\gamma\sigma = \gamma\sigma^{-1}\gamma[\varrho]$ ,  $[\varrho]$  étant dans  $\Omega$ . En prenant  $[\varrho]\gamma$  pour  $\gamma$  (c'est-à-dire en posant  $\gamma = [\varrho^{-1}]\gamma'$ , et en effaçant l'accent), on peut supposer que  $\varrho = 1$ . Je poserai alors  $[\Phi, \gamma] = X_1 = X, [\Phi, \gamma'] = X_1' = X^0$ , et je désignerai par

$$X^0 = X^0 \equiv \mathfrak{U}(2, p^m)$$

ce que devient  $X^0$  quand on y regarde les variables comme homogènes. L'équation précédente s'écrit encore  $(\sigma\gamma)^2 = [\zeta^2]$ , ou, en désignant par  $Y_i = \sum_l c_{il} y_l$ ,  $Y_i' = \sum_l c'_{il} y_l$  les fonctions substituées à  $y_i$  par  $\gamma\sigma^{-1}\gamma$  et  $\sigma\gamma\sigma$  respectivement,  $Y_i' = Y_i$ , ou  $c'_{il} = c_{il}$ .

L'équation  $\gamma^{-1}\mu_m\gamma \equiv \mu_m^{-1} \pmod{\Omega}$  s'écrit, en introduisant

$$[\xi_m^{-2}\mu_m^{-1}] = \delta, \quad \gamma^{-1}\mu_m\gamma = [s]\delta\mu_m^{-1}$$

Si  $A = H$  avec  $n = 2v$  et  $z \equiv 1 \pmod{2}$ ,  $\delta$  est d'ordre  $2^v$  et engendre  $\Delta$ . Dans tous les autres cas  $\delta = 1$ . On voit que  $[s]$  est dans  $\Omega$ . L'équation précédente s'écrit  $\mu_{0m}\gamma = [s^v\mu_m^{-1}]\mu_{0m}^{-1}$ , ou, en développant,  $\gamma_{ik}^k = s^v\mu_m^{-1-i}\gamma_{ik}$ .

Or, si  $\gamma$  existe, il y a, pour chaque valeur de  $i$ , au moins un  $\gamma_{ik} \neq 0$ , et.

pour  $\gamma_{ik} \neq 0$ ,  $t^{i+k-n-1} = s$ . Donc  $s$  a la forme  $t_m^c$  ( $0 \leq c \leq p^m - 2$ ). Supposons que  $t = t^{\pi+1}$ , ce qui est toujours permis. On aura  $s = t^{c\pi(\pi+1)}$ . Mais,  $[s]$  étant dans  $\Omega$ ,  $s$  a la forme  $t^{(\pi-1)\varepsilon}$ . Donc

$$(\pi - 1)\varepsilon = (\pi + 1)c\pi + l(\pi^2 - 1),$$

d'où  $c\pi = f \frac{\pi-1}{2}$  ou  $c = f \frac{p^m-1}{2}$  ( $f = 0$  ou  $1$ ). Ainsi, pour chaque valeur de  $i$ , les  $\gamma_{ik} \neq 0$  vérifient la condition

$$(1) \quad i + k = n + 1 + f \frac{p^m-1}{2} + f'(p^m - 1),$$

$f$  ( $= 0$  ou  $1$ ) étant indépendant de  $i$ ,  $k$  ( $f \frac{p^m-1}{2} = c$  et  $t_m^c = s$ ), et  $f'$  entier.

15. Soit d'abord  $f = 1$ , donc  $s = -1$ . L'équation (1) s'écrira

$$i + k = n + 1 + h \frac{p^m-1}{2} \quad (h \text{ impair}).$$

Or,  $i + k$  est  $\geq 2$  ou  $\leq 2n$ . On a donc

$$1 - n \leq h \frac{p^m-1}{2} \leq n - 1,$$

ou

$$h \geq 2 \frac{n-1}{p^m-1} \geq 2 \frac{p-1}{p^m-1}.$$

Donc,  $h$  étant impair,  $m = 1$ ,  $|h| = 1$  (quels que soient  $i$  et  $k$ ), et  $n \geq \frac{p+1}{2}$ .

Soit  $p = 2p' + 1$  et  $i = n - p' + 1$ . Alors  $k = (h+1)p'$ . Donc  $h = 1$  et  $k = 2p' \leq n$ . Donc  $p' \leq \nu$ . Mais  $p$  est  $\geq n$ , d'où  $p' \geq \nu$ . Donc  $p' = \nu$  et  $p = 2\nu + 1$ .

L'équation (1) devient donc  $k = n + 1 + h\nu - i$ . D'où

$$i \leq n + 1 + h\nu - i \leq n,$$

ou

$$\frac{i-n}{\nu} \leq h \leq \frac{i-1}{\nu}.$$

Donc, si  $i \leq \nu$ ,  $h$  est  $\leq \frac{\nu-1}{\nu}$ , d'où  $h = -1$ ; et si  $i > n - \nu$ ,  $h$  est  $> -1$ , d'où  $h = 1$ . Donc, sauf si  $i = \nu + 1$  avec  $n = 2\nu + 1$ ,  $\gamma_{ik}$  ne peut être  $\neq 0$  que pour une valeur de  $k$ . Mais si  $n = 2\nu + 1$ ,  $|\gamma|$  est nul, car les seuls éléments non nécessairement nuls de la première et de la dernière colonne, sont  $\gamma_{\nu+1,1}$  et  $\gamma_{\nu+1,n}$ ; en sorte que le coefficient de chacun d'eux dans  $|\gamma|$  est nul.

Soit donc  $n = 2\nu$ . Alors, pour  $i \leq \nu$ ,  $k = \nu + 1 - i$ ; pour  $i > \nu$ ,  $k = 3\nu + 1 - i$ . Donc  $\gamma$  remplace  $y_i$  ( $i \leq \nu$ ) par  $\gamma_{i,\nu+1-i} y_{\nu+1-i}$  et  $y_j$  ( $j > \nu$ ) par  $x_{n+1-j} = x_l$  ( $l = n + 1 - j \leq \nu$ ) par  $\gamma_{j,3\nu+1-j} y_{3\nu+1-j}$ .

La condition  $\gamma^2 = [\zeta]$  donne

$$(2) \quad \gamma_{i,\nu+1-i} \gamma_{\nu+1-i,i} = \gamma_{j,3\nu+1-j} \gamma_{3\nu+1-j,j} = \zeta.$$

Employons la condition  $Y'_1 = Y_1$ . On a ici

$$Y_1 = \gamma_{1\nu} \sum_1^\nu (-1)^{l+1} \sigma_{\nu,\nu+1-l} \gamma_{\nu+1-l,l} y_l, \quad Y'_1 = \gamma_{1\nu} \sum_1^\nu \sigma_{\nu l} y_l.$$

Donc

$$(3) \quad \sigma_{\nu l} = (-1)^{l+1} \sigma_{\nu,\nu+1-l} \gamma_{\nu+1-l,l} \quad (l \leq \nu).$$

Cette relation détermine les  $\gamma_{ik}$  où  $i \leq \nu$ . Les autres sont alors déterminés par la condition que  $\gamma$  conserve  $a$ , qui s'écrit

$$(4) \quad \gamma_{j,3\nu+1-j} \gamma_{l,\nu+1-l} = 1 \quad (l = n + 1 - j).$$

Enfin le produit de (3) par l'équation qu'on en déduit en changeant  $l$  en  $\nu + 1 - l$  donne, d'après (2),  $\zeta = (-1)^{\nu+1} = (-1)^{\frac{\nu+1}{2}}$ .

Il reste à voir si  $Y'_k = Y_k$  quel que soit  $k$ .

Dans ce qui suit, toute somme  $\sum_i f(i)$  dont les limites ne sont pas indiquées, s'étend à toutes les valeurs de  $i$  pour lesquelles  $f(i)$  est défini. En particulier  $\binom{u}{v} = \frac{u(u-1)\dots(u-v+1)}{v!}$ , défini pour  $v$  entier  $> 0$ , sera regardé comme égal à 1 (ainsi que  $v!$ ) pour  $v = 0$  et comme nul pour  $u < v$  (1).

(1) Quel que soit  $u$ , on a, pour  $v$  entier  $\geq 0$ ,  $\binom{-u}{v} = (-1)^v \binom{u+v-1}{v}$ , et, en vertu même de cette relation, le second membre se réduit à  $\binom{u}{v}$  quand on change  $u$  en  $-u$ .

On observera aussi les relations suivantes :

$$(5) \quad s_{n-k} = \begin{cases} (-1)^k \frac{s_n}{s_{k+1}} & \text{si } k \leq \nu - 1 \\ (-1)^{k+1} \frac{s_n}{s_{k+1}} & \text{si } k \geq \nu \end{cases} \quad (\dot{s}_n = s_n).$$

Remarquons maintenant que les formules (2)-(5) donnent

$$(6) \quad \begin{cases} \gamma_{i, \nu+1-i} = (-1)^{\nu+i} \frac{s_i}{s_{\nu+1-i}} \frac{(\nu-i)!}{(i-1)!} \\ \gamma_{\nu+1-i, i} = (-1)^{i+1} \frac{s_{\nu+1-i}}{s_i} \frac{(i-1)!}{(\nu-1)!} \end{cases} \quad (i \leq \nu),$$

$$(7) \quad \begin{cases} \gamma_{j, 3\nu+1-j} = (-1)^j \frac{s_j s_{j-\nu}}{s_n} \frac{(n-j)!}{(j-\nu-1)!} \\ \gamma_{3\nu+1-j, j} = - \frac{\dot{s}_n}{s_j s_{j-\nu}} \frac{(j-\nu-1)!}{(n-j)!} \end{cases} \quad (j > \nu).$$

On a donc, pour  $i \leq \nu$ ,

$$Y_i = \gamma_{i, \nu+1-i} \sum_{k=1}^{\nu+1-i} (-1)^{i+k+\nu+1} \sigma_{\nu+1-i, k} \gamma_{k, \nu+1-k} \mathcal{J}^{\nu+1-k},$$

d'où, en posant  $\nu + 1 - k = l$ ,

$$c_{il} = \frac{s_i}{s_l} (-1)^{\nu+1} \frac{(\nu-i)! (l-1)!}{(l-1)! (l-i)! (\nu-l)!} = \frac{s_i}{s_l} (-1)^{\nu+1} \frac{(l-1)!}{(i-1)!} \binom{\nu-i}{\nu-l}.$$

Pour  $j > \nu$ , on a

$$Y_j = \gamma_{j, 3\nu+1-j} \left[ \sum_{k=1}^{\nu} (-1)^{j+k+\nu+1} \sigma_{3\nu+1-j, k} \gamma_{k, \nu+1-k} \mathcal{J}^{\nu+1-k} + \sum_{k=\nu+1}^{3\nu+1-j} (-1)^{j+k} \sigma_{3\nu+1-j, k} \gamma_{k, 3\nu+1-k} \mathcal{J}^{3\nu+1-k} \right],$$

d'où, en posant dans la première somme  $\nu + 1 - k = l$ , et dans la seconde  $3\nu + 1 - k = r$ ,

$$c_{jl} = \frac{s_j}{s_l} (-1)^{\nu} \frac{(n-j)!}{(j-\nu-1)!} \frac{(l-1)!}{(n-j+l)! (\nu-l)!} \quad (l \leq \nu),$$

$$c_{jr} = - \frac{s_j}{s_r} \frac{(r-\nu-1)!}{(j-\nu-1)!} \binom{n-j}{n-r} \quad (r < \nu).$$



D'autre part, pour  $i \leq \nu$ ,

$$Y_i = \sum_{k=1}^{\nu} \sigma_{ik} \gamma_{k, \nu+1-k} \sum_{l=1}^{\nu} \sigma_{\nu+1-k, l} \mathcal{Y}_l$$

ou, en échangeant les deux sommations, et en observant qu'il suffit de faire varier  $k$  de 1 au plus petit  $l$  des deux nombres  $i, \nu+1-l$ ,

$$Y_i = \sum_{l=1}^{\nu} \sum_{k=1}^l \frac{s_i}{s_l} (-1)^{\nu+k} \frac{(\nu-k)!}{(i-k)! (k-1)! (\nu+1-k-l)!} \mathcal{Y}_l,$$

d'où pour  $l \geq \nu$ ,

$$c'_{il} = \frac{s_i}{s_l} \frac{(l-1)!}{(i-1)!} \sum_{k=1}^l (-1)^{\nu+k} \binom{\nu-k}{l-1} \binom{l-1}{k-1},$$

ou (1)

$$c'_{il} = \frac{s_i}{s_l} (-1)^{\nu+1} \frac{(l-1)!}{(i-1)!} \binom{\nu-1}{\nu-l} = c_{il}.$$

Pour  $j > \nu$ , on a

$$\begin{aligned} Y_j &= \sum_{k=1}^{\nu} \sigma_{jk} \gamma_{k, \nu+1-k} \sum_{l=1}^{\nu} \sigma_{\nu+1-k, l} \mathcal{Y}_l \\ &\quad + \sum_{k=\nu+1}^n \sigma_{jk} \gamma_{k, \nu+1-k} \sum_{r=1}^n \sigma_{\nu+1-k, r} \mathcal{Y}_r. \end{aligned}$$

(1) Considérons en effet l'identité  $(1-x)^{-m} (1-x)^{-n} = (1-x)^{-m-n}$ . La comparaison des coefficients de  $x^q$  ( $q$  entier  $\geq 0$ ) dans les deux membres donne, en supposant  $n$  entier  $\geq 1$ ,

$$\sum_s \binom{m+s-1}{s} \binom{n+q-s-1}{n-1} = \binom{m+n+q-1}{q},$$

d'où, en posant  $m = -k$ ,  $n-1 = l$ ,  $q = r-l$  (donc  $r$  est entier  $\geq l$ ),

$$\sum_s (-1)^s \binom{k}{s} \binom{r-s}{l} = \binom{r-k}{r-l},$$

et, en posant  $s = l + a$  ( $a$  entier quelconque  $\geq 0$  ou  $< 0$ ),

$$\sum_l (-1)^{l+a} \binom{k}{l+a} \binom{r-l-a}{l} = \binom{r-k}{r-l} \quad (r, l \text{ entiers, et } r \geq l).$$

C'est la formule employée au texte, et qui servira encore plusieurs fois.

ou, en échangeant dans chaque somme double les deux sommations, et en observant qu'il suffit de faire varier  $k$ , dans la première somme double, de 1 à  $\nu + 1 - l$ , et dans la seconde, de  $\nu + 1$  au plus petit  $u$  des deux nombres  $j, 3\nu + 1 - r$  (pour  $r < \nu, u = j$ ),

$$V_j = \sum_{l=1}^{\nu} \left[ \sum_{k=1}^{\nu+1-l} \sigma_{jk} \gamma_{k, \nu+1-k} \sigma_{\nu+1-k, l} + \sum_{k=\nu+1}^j \sigma_{jk} \gamma_{k, 3\nu+1-k} \sigma_{3\nu+1-k, l} \right] \gamma^l + \sum_{r=\nu+1}^n \sum_{k=\nu+1}^u \sigma_{jk} \gamma_{k, 3\nu+1-k} \sigma_{3\nu+1-k, r} \gamma^r.$$

On a donc, pour  $l \leq \nu$ ,

$$c_{jl} = \frac{s_j}{s_l} \left[ \sum_{k=1}^{\nu+1-l} (-1)^{\nu+k} \frac{(\nu-k)!}{(j-k)!(k-1)!(\nu+1-k-l)!} + \sum_{k=\nu+1}^j (-1)^k \frac{(n+k)!}{(j-k)!(k-\nu-1)!(3\nu+1-k-l)!} \right].$$

ou, en posant, dans la première somme,  $k = 1 + k', j = 1 + j'$ , et dans la seconde  $k = \nu + 1 + k', n - l = n'$ ,

$$c_{jl} = \frac{s_j}{s_l} (-1)^{\nu+1} \left[ \frac{(l-1)!}{(j-1)!} \sum_{k'} (-1)^{k'} \binom{j'}{k'} \binom{\nu-1-k'}{l-1} + \frac{(n-l)!}{(n-l)!} \sum_{k'} (-1)^{k'} \binom{n'}{k'} \binom{n'+l-\nu-1-k'}{n'+l-j} \right] = \frac{s_j}{s_l} (-1)^{\nu+1} \left[ \frac{(l-1)!}{(j-1)!} \binom{\nu-j}{\nu-l} + \frac{(n-l)!}{(n-l)!} \binom{l-\nu-1}{j-\nu-1} \right],$$

ou, en observant que

$$\binom{\nu-j}{\nu-l} = (-1)^{\nu+l} \binom{j-l-1}{\nu-l},$$

et que

$$\binom{l-\nu-1}{j-\nu-1} = (-1)^{j-\nu-1} \binom{j-l-1}{j-\nu-1} = (-1)^{j-\nu-1} \binom{j-l-1}{\nu-l},$$

$$c_{jl} = \frac{s_j}{s_l} \binom{j-l-1}{\nu-l} \frac{(l-1)!}{(j-1)!} \left[ (-1)^{\nu+l} + (-1)^j \frac{\binom{n-l}{l-1}}{\binom{n-l}{j-1}} \right],$$

ou, puisque

$$\binom{n-1}{t-1} = \frac{(p-2)(p-3)\dots(p-t)}{1.2.\dots(t-1)} = (-1)^{t-1} t \quad (t \text{ entier } \geq 1 \text{ et } \leq n),$$

$$c'_{jt} = \frac{s_j}{s_l} (-1)^{t+1} \binom{j-t-1}{\nu-t} \frac{(t-1)!}{(j-1)!} \left(1 - \frac{t}{j}\right) = \frac{s_j}{s_l} (-1)^{t+1} \frac{(j-t)!(t-1)!}{(\nu-t)!(j-\nu-1)!j!},$$

et la condition  $c'_{jt} = c_{jt}$  revient à

$$(-1)^t \frac{(j-t)!}{j!} = \frac{(n-j)!}{(n-j+t)!}, \quad \text{c'est-à-dire à} \quad (-1)^t = \frac{\binom{n}{j-t}}{\binom{n}{j}},$$

qui est vérifiée, puisque, d'après ce qu'on vient de voir,  $\binom{n}{t} = (-1)^t \binom{n}{n-t}$ .

On a enfin, pour  $r > \nu$ ,

$$c'_{jr} = \frac{s_j}{s_r} \sum_{k=\nu+1}^n (-1)^k \frac{(n-k)!}{(j-k)!(k-\nu-1)!(3\nu+1-k-r)!},$$

ou, en posant  $k = \nu + 1 + k'$ ,  $j = \nu + 1 + j'$ ,

$$c'_{jr} = \frac{s_j}{s_r} (-1)^{\nu+1} \frac{(r-\nu-1)!}{(j-\nu-1)!} \sum_{k'} \binom{j'}{k'} \binom{\nu-1-k'}{r-\nu-1}$$

$$= \frac{s_j}{s_r} (-1)^{\nu+1} \frac{(r-\nu-1)!}{(j-\nu-1)!} \binom{n-j}{n-r},$$

et la condition  $c'_{jr} = c_{jr}$  exige que  $\nu$  soit pair.

Ainsi, pour  $f=1$ ,  $X$  n'existe que si  $p \equiv 1 \pmod{4}$  avec  $m=1$ ,  $n=p-1$ . Ces conditions sont d'ailleurs suffisantes, et l'on a alors  $(\mathbf{2}) \quad \varrho_m^{-1} = \gamma^2 = d$ ,  $(\gamma\sigma)^3 = 1$ ,  $\gamma^{-1}\varrho_m\gamma = \varrho_m^{-1}d^{k-1}$  (cf. 19).

Ces équations, jointes à celles de  $\Phi(\mathcal{A})$  et à  $\gamma d = d\gamma$ , définissent le groupe abstrait isomorphe à  $X$ , puisqu'elles sont satisfaites par  $X$ , qui contient effectivement  $d$  (E., 18, 19). Elles montrent aussi que  $X^0 \equiv U(2, p)$  (S., 92).

(1) On remarquera le cas  $t=\nu$ , qui donne, en observant que

$$n! = (p-1)! = -1,$$

$$(\nu!)^2 = (-1)^{\nu+1} \quad \text{ou} \quad \left[ \binom{p-1}{2} \right]^2 = (-1)^{\frac{n+1}{2}},$$

quel que soit le nombre premier  $p > 2$ .

Je désignerai par  $\gamma_i, \zeta_i, X_i, X_i^0, \mathcal{X}_i, \mathcal{X}_i^0, \bar{X}_i$  les déterminations exceptionnelles de  $\gamma, \zeta, X, X^0, \mathcal{X}, \mathcal{X}^0, X$  qui viennent d'être obtenues.

16. Soit maintenant  $f = 0$ , donc  $s = 1$ . — Alors, pour chaque valeur de  $i$  (ou de  $k$ ), les seuls  $\gamma_{ik} \neq 0$  sont déterminés par

$$i + k = n - 1 + f'(p^m - 1) \quad (f' \text{ entier}).$$

Or  $i$  et  $k$  sont  $\geq 1$  et  $\leq n$ . On a donc :

$$1 - n \leq f'(p^m - 1) \leq n - 1, \quad \text{ou} \quad |f'| \leq \frac{n - 1}{p^m - 1} \leq \frac{p - 1}{p^m - 1}.$$

Donc, si  $m > 1$ , ou si  $p > n$ ,  $f' = 0$ .

Étudions d'abord le cas exceptionnel où  $f'$  prend des valeurs  $\neq 0$  (c'est-à-dire où il y a des  $\gamma_{ik} \neq 0$  correspondant à des valeurs  $f' \neq 0$ ). Alors  $n = p$ ,  $m = 1$ , et les valeurs  $\neq 0$  de  $f'$  sont  $\pm 1$ .

Si  $f' = -1$ , on a  $i + k = 2$ , donc  $i = k = 1$ . Si  $f' = 1$ , on a  $i + k = 2n$ , donc  $i = k = n$ . Et, par hypothèse,  $\gamma_{11}$  et  $\gamma_{nn}$  ne sont pas tous deux nuls.

On a ici

$$Y_1 = (\gamma_{11}^2 + \sigma_{n1}\gamma_{1n}\gamma_{11} + \gamma_{1n}\gamma_{n1})Y_1 + \gamma_{1n} \sum_{i=2}^{n-1} \sigma_{ni}(-1)^{n-i}\gamma_{i,n+1-i}Y_{n+1-i} + \gamma_{1n}(\gamma_{11} + \sigma_{n1}\gamma_{1n} + \gamma_{nn})Y_n,$$

$$Y_i = \gamma_{1i}Y_1 + \gamma_{1n} \sum_{i=1}^n \sigma_{ni}Y_i.$$

$n$  étant impair,  $A = H, \bar{H}$  ou  $Q$ . Je négligerai le cas  $A = H$  ( $H$  se déduit de  $\bar{H}$  par un changement de variables).

Soit  $A = \bar{H}$ , et d'abord  $\gamma_{1n} \neq 0$ . La condition  $\gamma^2 = [\zeta]$  donne ici  $\gamma_{11} + \gamma_{nn} = 0$ .

La condition que  $\gamma$  conserve  $a$  donne, en posant  $\dot{\gamma}_{1n} = \theta\gamma_{1n}$ ,  $\dot{\gamma}_{nn} = \theta\gamma_{nn}$  (donc  $\dot{\gamma}_{11} = \theta\gamma_{11}$ ),  $\dot{\gamma}_{ni} = \theta\gamma_{ni}$ ,  $\theta(-\gamma_{11}^2 + \gamma_{1n}\gamma_{n1}) = 1$ .

La condition  $c_{1n} = c'_{1n}$  donne  $\sigma_{n1}\gamma_{1n} = 1$ , donc  $\gamma_{1n} = \frac{(n-1)!}{s_n}$ .

Or, pour  $n$  impair,  $s_n = -s_n$ . Donc  $\dot{\gamma}_{1n} = -\gamma_{1n}$ . Donc  $\theta = -1$ , et  $\gamma_{11}^2 - \gamma_{1n}\gamma_{n1} = 1$ .

La condition  $c_{11} = c'_{11}$  donne  $\gamma_{11}^2 - \gamma_{1n}\gamma_{n1} = 1$ .

Mais alors  $\gamma_{11}^2 = 1$  et  $\theta$  devrait être égal à 1.

Donc  $\gamma_{in} = 0$ . La condition que  $\gamma$  conserve  $a$  donne alors  $\gamma_{ii} \gamma_{nn} = 1$ . La condition  $c'_{ii} = c_{ii}$  donne  $\gamma_{ii}^2 = \gamma_{ii}$ . Donc  $\gamma_{ii} = \gamma_{nn} = 1$ , et la condition  $\gamma^2 = [\zeta]$  exige que  $\gamma_{ni} = 0$ .

Soit  $\Lambda = Q$ . Si  $\gamma_{in}$  ou  $\gamma_{ni}$  est  $\neq 0$ , la condition  $\gamma^2 = [\zeta]$  donne  $\gamma_{ii} + \gamma_{nn} = 0$ , et la condition que  $\gamma$  conserve  $a$  donne  $\gamma_{ii} = \gamma_{nn} = 0$  contre l'hypothèse.

Donc  $\gamma_{in} = \gamma_{ni} = 0$ . La condition que  $\gamma$  conserve  $a$  donne alors  $\gamma_{ii} \gamma_{nn} = 1$ , et la condition  $c'_{ii} = c_{ii}$  donne  $\gamma_{ii}^2 = \gamma_{ii}$ . Donc  $\gamma_{ii} = \gamma_{nn} = 1$ .

Ainsi, pour  $\Lambda = \bar{I}$  ou  $Q$ , on a ici  $\gamma_{ii} = \gamma_{nn} = 1$ ,  $\gamma_{in} = \gamma_{ni} = 0$ , et  $\gamma$  remplace  $y_j$  ( $1 \leq j \leq n-1$ ) par  $\gamma_{i, n+1-j} y_{n+1-j}$ .

La condition  $\gamma^2 = [\zeta]$  donne

$$\zeta = \gamma_{ii}^2 = \gamma_{nn}^2 = 1 \quad \text{et} \quad \gamma_{i, n+1-j} \gamma_{n+1-j, i} = 1 \quad (2 \leq j \leq n-1).$$

La condition que  $\gamma$  conserve  $a$  donne alors  $\gamma_{j, n+1-j} \gamma_{n+1-j, j} = 1$ .

La condition  $c'_{2l} = c_{2l}$  donne

$$\gamma_{n+1-l, l} = (-1)^l \frac{s_{n+1-l}}{s_l} \frac{(l-2)!}{(n-l-1)!},$$

d'où

$$\gamma_{l, n+1-l} = (-1)^l \frac{s_l}{s_{n+1-l}} \frac{(n-l-1)!}{(l-2)!},$$

et la condition  $c'_{ll} = c_{ll}$  est alors satisfaite dans  $\mathcal{C}$ .

Ainsi  $\gamma$  est complètement déterminé, et il reste à voir si la condition  $Y'_k = Y_k$  est vérifiée pour  $k > 2$ .

On a d'abord

$$Y_n = \sigma_{n1} Y_1 + \sum_{l=2}^{n-1} (-1)^{l+1} \sigma_{n, n+1-l} \gamma_{n+1-l, l} Y_l + Y_n,$$

$$Y_n = \sigma_{n1} Y_1 + \sum_{k=2}^{n-1} \sigma_{nk} Y_{k, n+1-k} + \sum_{l=1}^{n-1} \sigma_{n+1-k, l} Y_l + \sum_{l=1}^n \sigma_{nl} Y_l,$$

ou, en changeant l'ordre des sommations dans la somme double, puis  $k$  en  $n+1-k$ , et en négligeant les termes nuls où  $k < l$ ,

$$Y_n = Y_1 \left( 2\sigma_{n1} + \sum_{k=2}^{n-1} \sigma_{n, n+1-k} \gamma_{n+1-k, k} \sigma_{k1} \right) + \sum_{l=2}^{n-1} Y_l \left( \sum_{k=l}^{n-1} \sigma_{n, n+1-k} \gamma_{n+1-k, k} \sigma_{kl} + \sigma_{nl} \right) + Y_n.$$

On voit que  $c'_{n,n-1} = c_{n,n-1} = 1$ . Considérons la condition  $c'_{nl} = c_{nl}$  pour  $l = 2, \dots, n-2$ . Elle s'écrit [en multipliant par  $(n-2)! \frac{s_l}{s_n}$ ]

$$\frac{l-n}{l-1} = \sum_{k=l}^{n-1} (-1)^k \frac{n-l}{k-1} \binom{n-l-1}{k-l} + 1$$

ou ( $n = 0$  dans  $\otimes$ ) (<sup>1</sup>)

$$\frac{1}{l-1} = (-1)^{l+1} l \frac{(l-2)! (n-l-1)!}{(n-2)!},$$

ou  $\frac{(p-1)(p-2)\dots(p-l)}{1 \cdot 2 \dots l} = (-1)^l$ , ce qui est évident.

(<sup>1</sup>) Considérons la somme  $S_{b,h} = \sum_{s=0}^h \frac{(-1)^s}{s+b} \binom{h}{s}$  ( $-b$  n'étant pas un des nombres  $0, \dots, h$ ). Je dis que  $S_{b,h} = \frac{\Gamma(b)\Gamma(h+1)}{\Gamma(b+h+1)}$ . On a d'abord évidemment  $S_{b,0} = \frac{1}{b} = \frac{\Gamma(b)\Gamma(1)}{\Gamma(b+1)}$ . Or, en admettant la formule pour une valeur entière quelconque de  $h$ , on a

$$S_{b,h+1} = \sum_{s=0}^{h+1} \frac{(-1)^s}{s+b} \left[ \binom{h}{s} + \binom{h}{s-1} \right] = \frac{\Gamma(b)\Gamma(h+1)}{\Gamma(b+h+1)} + \sum_{s=1}^{h+1} \frac{(-1)^s}{s+b} \binom{h}{s-1}.$$

Par hypothèse, la dernière somme est égale à  $-\frac{\Gamma(b+1)\Gamma(h+1)}{\Gamma(b+h+2)}$  (on le voit en posant  $s = t-1$ ). Donc  $S_{b,h+1} = \frac{\Gamma(b)\Gamma(h+2)}{\Gamma(b+h+2)}$ .

On peut d'ailleurs établir plus simplement la formule en question par la théorie des intégrales eulériennes, car on a

$$S_{b,h} = \left[ \sum_{s=0}^h (-1)^s \binom{h}{s} \frac{x^{s+b}}{s+b} \right]_0^1 = \int_0^1 x^{b-1} (1-x)^h dx = \frac{\Gamma(b)\Gamma(h+1)}{\Gamma(b+h+1)}.$$

La somme  $\sum_{s=0}^h \frac{(-1)^s}{as+b} \binom{h}{s}$  est évidemment égale à  $\frac{1}{a} S_{\frac{b}{a},h}$ .

La somme  $\sum_s \frac{(-1)^s}{s+b} \binom{h}{s+c}$  ( $c$  entier) est de même égale à

$$(-1)^c \frac{\Gamma(b)\Gamma(h+1)}{\Gamma(b-c+h+1)}.$$

Pour traiter le cas exclu où  $-b$  est un des nombres  $0, \dots, h$  tel que  $i$ , suppo-

La condition  $c_{n1} = c_{n1}$  s'écrit, en divisant par  $\sigma_{n1}$ ,

$$-1 = (n-1) \sum_{l=2}^{n-1} \frac{(-1)^l}{l-1} \binom{n-2}{l-1},$$

ou, en posant  $l = 1 + s$ , et en observant que

$$\binom{n-2}{s} = (-1)^s (s+1) \binom{n-1}{s}, \quad \sum_1^{n-1} \frac{1}{s} = 0,$$

ce qui est évident, puisque à chaque nombre  $s$  répond un nombre  $p - s = s'$  pour lequel  $\frac{1}{s'} = -\frac{1}{s}$ .

Il s'agit maintenant d'étudier la condition  $Y'_j = Y_j$  pour  $j = 2, \dots, n-1$ .

On a, pour  $2 \leq j \leq n-1$ ,

$$Y_j = \gamma_{j, n+1-j} \left[ (-1)^{j+1} \sigma_{n+1-j, 1} \gamma_1 + \sum_{k=2}^{n+1-j} (-1)^{j+k} \sigma_{n+1-j, k} \gamma_{k, n+1-k} \gamma_{n+1-k} \right],$$

d'où, en posant  $n+1-k = l$ ,

$$c_{jl} = \frac{s_j}{s_l} \frac{(l-2)!}{(j-2)!} \binom{n-j-1}{n-l-1} \quad (l = 2, \dots, n-1; \text{ donc } c_{jl} = 0 \text{ pour } 2 \leq l < j),$$

et, puisque  $n = p$ ,  $c_{j1} = \frac{s_j}{(j-2)! j}$ .

sous d'abord que  $b = -i + \varepsilon$ , pour faire ensuite tendre  $\varepsilon$  vers zéro. La somme  $S_{ih}^b$  déduite de  $S_{bh}$ , en retranchant le terme où  $s = i$  est égale à

$$\frac{\Gamma(b) \Gamma(h+1)}{\Gamma(b+h+1)} - \frac{(-1)^i}{i+b} \binom{h}{i},$$

ou, en posant  $b(b+1) \dots (b+h) = \varepsilon f(\varepsilon)$ , à

$$\frac{\Gamma(h+1)}{\varepsilon f(\varepsilon)} - \frac{(-1)^i}{\varepsilon} \binom{h}{i} = \frac{h! - (-1)^i \binom{h}{i} f(\varepsilon)}{\varepsilon f(\varepsilon)}.$$

Or  $f(0) = (-1)^i i! (h-i)!$ , et  $f'(0) = f(0) (S_{h-i} - S_i)$ , en posant  $S_n = \sum_1^n \frac{1}{s}$

et  $S_0 = 0$ . Donc  $S_{ih}^b = \lim_{\varepsilon=0} S_{bh}^b = (-1)^i \binom{h}{i} (S_i - S_{h-i})$ .

Les formules obtenues ici serviront dans la suite.

(<sup>1</sup>) On peut aussi se servir de la fin de la note précédente.

On a ensuite

$$Y_j = \sigma_{j1} Y_1 + \sum_{k=2}^{n-1} \sigma_{jk} \gamma_{k, n+1-k} \sum_{l=1}^{n-1} \sigma_{n+1-k, l} Y_l,$$

ou, en échangeant les deux sommations et en désignant par  $l$  le plus petit des deux nombres  $j, n+1-k$ ,

$$Y_j = \sigma_{j1} \left( \sigma_{j1} + \sum_{k=2}^l \sigma_{jk} \gamma_{k, n+1-k} \sigma_{n+1-k, 1} \right) + \sum_{l=2}^{n-1} \sum_{k=2}^l \sigma_{jk} \gamma_{k, n+1-k} \sigma_{n+1-k, l} Y_l.$$

Donc, pour  $l = 2, \dots, n-1$ ,

$$\begin{aligned} c'_{jl} &= \frac{s_j}{s_l} \frac{(l-2)!}{(j-2)!} \sum_{k=2}^l (-1)^k \binom{j-2}{k-2} \binom{n-k-1}{l-2} \\ &= \frac{s_j}{s_l} \frac{(l-2)!}{(j-2)!} \binom{n-j-1}{n-l-1} = c_{jl}. \end{aligned}$$

et

$$c'_{j1} = \frac{s_j}{s_1} \left[ \frac{1}{(j-1)!} + \sum_{k=2}^l \frac{(-1)^k}{(j-k)! (k-2)! (n-k)} \right],$$

ou, puisque  $n = p$ ,

$$\begin{aligned} c'_{j1} &= s_j \left[ \frac{1}{(j-1)!} - \frac{1}{(j-2)!} \sum_{k=2}^l \frac{(-1)^k}{k} \binom{j-2}{k-2} \right] \\ &= s_j \left[ \frac{1}{(j-1)!} - \frac{1}{j!} \right] = \frac{s_j}{(j-2)! j} = c_{j1}. \end{aligned}$$

Ainsi, pour  $f = 0$ ,  $X$  n'existe que si  $m = 1$  et  $n = p$ . Ces conditions sont d'ailleurs suffisantes, et l'on a alors  $\gamma^2 = 1$ ,  $(\gamma\sigma)^3 = 1$ ,  $\gamma^{-1} \alpha_m \gamma = \alpha_m^{-1}$ . Donc  $X \equiv \mathfrak{X} \equiv \mathfrak{X}(2, p)$ .

Je désignerai par  $\gamma_2, \zeta_2, X_2, X_2^0, \mathfrak{X}_2, \mathfrak{X}_2^0, \bar{X}_2$  les déterminations exceptionnelles de  $\gamma, \zeta, X, X^0, \mathfrak{X}, \mathfrak{X}^0, \bar{X}$  qui viennent d'être obtenues.

17. Il reste à étudier le cas où l'équation (1) se réduit à

$$i+k = n+1 \quad (s=1).$$

Soit d'abord  $A = H$  ou  $G$  (pour passer, dans ce qui suit, de  $H$  à  $G$ , il suffit de supposer tous les coefficients des substitutions dans  $\mathfrak{S}$ , et



de faire  $\gamma_i = 0$ ). En posant  $\Theta = \Pi_i \tau_i$ ,  $\Theta \gamma$  a la forme

$$[\gamma_j, \beta_j, \gamma_j] = \beta_j \quad (j = 1, \dots, n).$$

Pour que  $\beta$  conserve  $\alpha$ , il faut et suffit que  $\beta_{n+1-j} \beta_j = 1$ , et l'on a

$$\gamma = \Theta^{-1} \beta = \begin{bmatrix} \gamma_i (i \leq \nu) & \beta_i, \gamma_{n+1-i} \\ \gamma_{n+1-i} & -\beta_{n+1-i} \gamma_i \\ \gamma_{\nu+1} \text{ (si } n = 2\nu + 1) & \beta_{\nu+1} \gamma_{\nu+1} \end{bmatrix}.$$

La condition  $\gamma^2 = [\zeta]$  donne  $-\beta_i \beta_{n+1-i} = \zeta$ , ou  $\beta_i = -\zeta \beta_i (i \leq \nu)$ , donc  $\beta_{n+1-i} = -\zeta \beta_{n+1-i}$  et, si  $n = 2\nu + 1$ ,  $\beta_{\nu+1}^2 = \zeta$ .

On a, pour  $i \leq \nu$ ,

$$\begin{aligned} Y_i &= \beta_i \sum_{k=1}^{\nu-i} (-1)^{n-1-i+k} \beta_k \sigma_{n+1-i,k} \gamma_{n+1-k} \\ &\quad - \beta_i \sum_{k=n-\nu+1}^{n-i-1} (-1)^{n+1+i+k} \beta_k \sigma_{n+1-i,k} \gamma_{n+1-k} + \gamma_i (-1)^{n+\nu+i} \beta_i \beta_{\nu+1} \gamma_{\nu+1}, \\ Y_{n+1-i} &= -\beta_{n+1-i} \sum_{k=1}^i (-1)^{i+k} \beta_k \sigma_{ik} \gamma_{n+1-k}, \\ Y_{\nu+1} &= \beta_{\nu+1} \sum_{k=1}^{\nu-i} (-1)^{k-\nu+1} \beta_k \sigma_{\nu+1,k} \gamma_{n+1-k} \quad (\text{si } n = 2\nu + 1), \\ Y_i' &= \sum_{k=1}^i \sum_{l=1}^{n+1-k} \beta_k \sigma_{ik} \sigma_{n+1-k,l} \gamma_l, \\ Y_{n+1-i}' &= S + S' + S'', \\ S &= \sum_{k=1}^{\nu} \sum_{l=1}^{n+1-k} \beta_k \sigma_{n+1-i,k} \sigma_{n+1-k,l} \gamma_l, \\ S' &= - \sum_{k=n-\nu+1}^{n+1-i} \sum_{l=1}^{n+1-k} \beta_k \sigma_{n+1-i,k} \sigma_{n+1-k,l} \gamma_l, \\ S'' &= \gamma_i \beta_{\nu+1} \sigma_{n+1-i,\nu+1} \sum_{l=1}^{\nu+1} \sigma_{\nu+1,l} \gamma_l, \\ Y_{\nu+1}' &= \sum_{k=1}^{\nu-1} \sum_{l=1}^{n+1-k} \beta_k \sigma_{\nu+1,k} \sigma_{n+1-k,l} \gamma_l \quad (\text{si } n = 2\nu + 1). \end{aligned}$$

La condition  $c'_{in} = c_{in}$  donne  $\beta_i = (-1)^{i+n} \frac{\sigma_{i1}}{\sigma_{n+1-i,1}}$  ( $i \leq \nu$ ). La condition  $c'_{n+1-i,n} = c_{n+1-i,n}$  donne  $\beta_{n+1-i} = (-1)^i \frac{\sigma_{n+1-i,1}}{\sigma_{i1}}$ . La condition  $c'_{\nu+1,n} = c_{\nu+1,n}$  (pour  $n = 2\nu + 1$ ) donne  $(-1)^\nu \beta_{\nu+1} = 1$ . Donc

$$\zeta = -\beta_i \beta_{n+1-i} = (-1)^{n+1}.$$

On remarquera que, si  $n = 2\nu + 1$ , la valeur de  $\beta_i$  se réduit à  $\beta_{\nu+1}$ , et celle de  $\beta_{n+1-i}$  à  $-\beta_{\nu+1}$  quand on y remplace  $i$  par  $\nu + 1$ . On peut donc écrire, en remplaçant dans les  $Y$  la variable de sommation  $k$  par  $n + 1 - l$ , et en changeant dans les  $Y'$  l'ordre des sommations,

$$Y_i = (-1)^{i+n} \sum_{l=i}^n \frac{\sigma_{i1} \sigma_{n+1-l,1}}{\sigma_{n+1-i,1} \sigma_{l1}} \sigma_{n+1-i,n+1-l} Y_l \quad (i = 1, \dots, \nu),$$

$$Y_{n+1-j} = (-1)^{n+1-j} \sum_{l=n-\nu}^n \frac{\sigma_{n+1-j,1} \sigma_{n+1-l,1}}{\sigma_{j1} \sigma_{l1}} \sigma_{j,n+1-l} Y_l \quad (j = 1, \dots, \nu + \tau_1 = n - \nu),$$

$$Y_i = \sum_{l=1}^n \sum_{k=1}^l (-1)^{i+n} \frac{\sigma_{k1} \sigma_{ik}}{\sigma_{n+1-k,1}} \sigma_{n+1-k,l} Y_l \quad (i = 1, \dots, \nu),$$

$l$  étant le plus petit des nombres  $i, n + 1 - l$ ,

$$Y_{n+1-j} = \sum_{l=1}^n \sum_{k=1}^l f(j, k, l) + \sum_{l=1}^{n-\nu} \sum_{k=\nu+1}^{n'} f(j, k, l) \quad (j = 1, \dots, n - \nu),$$

$$f(j, k, l) = \frac{\sigma_{k1} \sigma_{n+1-j,k}}{\sigma_{n+1-j,1}} \sigma_{n+1-j,k} Y_l.$$

$u$  étant le plus petit des nombres  $\nu, n + 1 - l$ , et  $u'$  le plus petit des nombres  $n + 1 - j, n + 1 - l$  pour  $l \leq n - \nu$ .

On a donc

$$\begin{aligned} c_{ij} &= (-1)^n \frac{s_i}{s_j} \frac{(l-1)!}{(i-1)!} \sum_{k=1}^l (-1)^k \binom{n-k}{l-1} \binom{i-1}{k-1} \\ &= (-1)^{n+1} \frac{s_i}{s_j} \frac{(l-1)!}{(i-1)!} \binom{n-i}{n-l} = c_{ij}. \end{aligned}$$

et, pour  $l > n - \nu$  (alors  $u = n + 1 - l$ ),

$$\begin{aligned} c_{n+1-j,l} &= (-1)^n \frac{s_{n+1-j}}{s_l} \frac{(j-1)!}{(n-l)!} \sum_{k=1}^u (-1)^k \binom{n-k}{j-1} \binom{n-l}{k-1} \\ &= (-1)^{n+1} \frac{s_{n+1-j}}{s_l} \frac{(j-1)!}{(n-l)!} \binom{l-1}{n-j} = c_{n+1-l,l}, \end{aligned}$$

pour  $l = n - \nu$  (alors  $u = \nu$ )

$$\begin{aligned} c_{n+1-j,l} &= (-1)^n \frac{s_{n+1-j}}{s_l} \frac{(j-1)!}{(n-l)!} \sum_{k=1}^u (-1)^k \binom{n-k}{j-1} \binom{n-l}{k-1} \\ &= (-1)^{n+1} \frac{s_{n+1-j}}{s_l} \frac{(j-1)!}{(n-l)!} \binom{l-1}{n-j}. \end{aligned}$$

Or,  $\binom{l-1}{n-j}$  est nul pour  $j+l < n+1$ , ce qui a toujours lieu si  $l < n - \nu$ . Donc on a encore  $c_{n+1-l,l} = c_{n+1-j,l}$  pour  $l \geq n - \nu$ .

Le groupe  $X$  est ici défini abstraitement par les équations de  $\Phi$  (4) jointes à  $\gamma_i^2 = d^{n-i}$ ,  $\gamma_i^{-1} \alpha_m \gamma_i = \alpha_m^{-1} \delta_i$ ,  $\delta_i = 1$  si  $n = 2\nu + 1$ ,  $\delta_i^{2^{i-1}} = d^h$  si  $n = 2\nu$  (2),  $d^2 = 1$  et aux équations exprimant que  $\delta_i$  et  $d$  sont permutable aux autres générateurs.

Le seul cas où  $\langle \delta_i \rangle$  soit  $> D$  est celui où  $A = H(2\nu, \pi)$  avec  $\pi \equiv 3 \pmod{4}$ . Alors  $\frac{p^m-1}{3}$  est impair, et le diviseur  $\Gamma = \langle \omega, d, \alpha_m^{\frac{p^m-1}{3}}, \gamma_i \rangle$  de  $X$  est  $\cong U(2, p^m)(S, 92)$ . Le groupe  $Z = \langle \gamma_i, \delta_i \rangle (Z|D)$  est produit direct de  $\gamma_i | D$  par  $\Delta | D$  est d'indice 2 dans  $X = Z + \alpha_m^{\frac{p^m-1}{2}} Z$ . Dans tous les autres cas, le diviseur  $\langle \omega, \alpha_m^{\frac{p^m-1}{2}}, \gamma_i \rangle = \Lambda^0$ , d'indice 2 dans  $X$ , est isomorphe à  $\psi(2, p^m)$  si  $n = 2\nu + 1$ , et à  $U(2, p^m)$  si  $n = 2\nu$  (loc. cit.).

18. Supposons maintenant que  $n$  soit impair et que  $A = \bar{H}$  ou  $Q$  (on passe de  $\bar{H}$  à  $Q$  en supposant tous les coefficients dans  $\mathbb{C}$ ). En posant  $\Theta = H^i t_i$ ,  $\Theta_\gamma$  a la forme  $|y_i, \beta_i y_i| = \beta_i (\beta_{\nu+1} = \gamma_{\nu+1, \nu+1})$ . Pour que  $\beta$  conserve  $\alpha$ , il faut et suffit que  $\beta_{n+1-i} \beta_i = 1$  ( $1 \leq i \leq n$ ). Alors  $\gamma = \Theta \beta = |y_i, \beta_i y_{n+1-i}|$ , et  $\zeta = 1$  [pour que  $\gamma$  soit dans  $A^0$ , il faut et suffit que  $\beta_{\nu+1} = (-1)^\nu$ ].

On a ici, après des transformations analogues à celles du n° 17,

$$Y_i = \sum_{l=1}^n (-1)^{l+i} \frac{\beta_l}{\beta_i} \sigma_{n+1-l, n+1-l} Q^l,$$

$$Y_i = \sum_{l=1}^n \sum_{k=1}^n \beta_k \sigma_{i, k} \sigma_{n+1-k, l} Y_l,$$

$n$  étant le plus petit des nombres  $i, n+1-i$ .

La condition  $c_{in} = c_{in}$  donne, en observant que  $\beta_1 \beta_n = 1$ ,

$$\beta_i = (-1)^{i+1} \frac{\sigma_{i, 1}}{\sigma_{n+1-i, 1}} = (-1)^{i+1} \frac{\sigma_i}{\sigma_{n+1-i}} \frac{(n-i)!}{(i-1)!},$$

et ces valeurs vérifient les relations  $\beta_{n+1-i} \beta_i = 1, \beta_{n+1-i} = (-1)^i$ . Donc  $\gamma$ , si elle existe, est dans  $A^0$  <sup>(1)</sup>.

Il reste à voir si la condition  $Y_i = Y_i$  est remplie. Or on a

$$c_{in} = \frac{(n-i)!}{(n-i)!} \sum_{k=1}^n (-1)^{k+i} \binom{n-k}{n-i} \binom{n-l}{k-i} = \frac{(n-i)!}{(n-l)!} \binom{l-1}{i-1} = c_{in}$$

Je désignerai désormais par  $\gamma_0, \zeta_0, X_0, X_0^0, X_0^0, X_0^0, X_0^0$ , les déterminations de  $\gamma, \zeta, X, X^0, X, X^0, X$  obtenues aux nos 17-18.

Supposons maintenant que  $A = Q$  (alors  $\Omega = D$ ). Comme  $\gamma, \sigma$  et  $\mu_m$  sont dans  $A^0$  qui est ici premier à  $D$  ( $n$  est impair),  $\bar{X}_0$ , qui, par hypothèse, contient  $D$ , est produit direct de  $X_0$  par  $D$ . Ainsi  $X_0$  divise  $A^0$ , et  $X_0 = \mathfrak{g}(2, p^m)$ . Dans cet isomorphisme  $\sigma, \mu_m, \gamma_0$  répondent respectivement à  $z+1, \mu_m z, -z^{-1}$ . Donc  $\{\Phi^0, \gamma_0\} = X_0^0$  répond à  $\mathfrak{v}(2, p^m)$ . Donc  $X_0^0$  est d'indice 2 dans  $X_0$ , et  $X_0^0 D$  d'indice 2 dans  $\bar{X}_0$ . D'autre part,  $\gamma_0$  est dans  $R$  [voir G., 29, formule (29), en observant que  $\beta_{n+1-i} = (-1)^i$ ]. Donc, comme  $\mu_m(4)$ ,  $X_0$  est dans  $R$  toujours et seulement si  $x$  est pair ou si  $\nu = 0, 3 \pmod{4}$ ;  $X_0^0$  divise toujours  $R$ .

<sup>(1)</sup> Cela devait être *a priori*, puisque  $\gamma$  correspond à  $\frac{-1}{2}$  qui est dans le groupe simple  $\mathfrak{v}(2, p)$ .

**19.** D'après le n° 13 et les déterminations obtenues de  $\gamma$ , on peut énoncer encore les propositions suivantes :

Si  $n = 2v + 1$ ,  $X$  divise tous les  $A(n, p^{mk})$  qui divisent  $A(n, \pi)$  [on passe de  $H(n, \pi)$  à  $\bar{H}(n, \pi)$  par un changement de variables].

Si  $n = 2v$ ,  $X_u$  (14) divise tous les  $H(n, p^{mk})$  qui divisent  $H(n, \pi)$ .  $X_c$  si  $x$  est pair, ou  $X_c^0$  si  $x$  est impair divise tous les  $G(n, p^{mk})$  qui divisent  $G(n, \pi)$ .

De plus, comme  $\mu_c^2 = \mu_c^{v-1}$  (2), on a toujours  $X_c^0 = X_u^0$ , et, si  $x$  est pair (alors  $\frac{\pi-1}{p^m-1}$  est pair et  $\mu_{mc} = \mu_{mu}^{\frac{\pi-1}{2}}$ ),  $X_c = X_u$ .

## II.

**20.** Cherchons maintenant dans  $\mathfrak{A}$  un diviseur  $\mathfrak{s}_x = \mathfrak{s}$  isomorphe à  $\mathfrak{v}(2, p^m)$ , dont les  $s_p$  soient irréductibles. Soit  $\bar{Z}_x = \bar{Z}$  un diviseur de  $\Lambda$  contenant  $\Omega$ , tel que  $\bar{Z} | \Omega \equiv \mathfrak{s}$ . Ici encore (cf. 14)  $m$  doit diviser  $K = mx$ , et l'on peut supposer que  $\bar{Z}$  contient  $\Phi^0$ .

Soit  $\gamma = (\gamma_{ik})$  une substitution de  $\bar{Z}$  telle que  $\gamma\Omega$  corresponde à  $\frac{\pi-1}{2}$  de  $\mathfrak{v}(2, p^m)$ . Pour l'existence de  $\bar{Z}$ , il faut et suffit que l'on ait (S., 88)

$$(1) \quad \gamma^2 = [\zeta], \quad \gamma^{-1} \rho_m^2 \gamma = \rho_m^2 [s],$$

$$(2) \quad \sigma_{\zeta}^{-1} \gamma \rho_m^{m-1-2x} \sigma_{\zeta} = \gamma \sigma_{\zeta} \gamma [\zeta],$$

$x$  parcourant toutes les valeurs entières mod  $p^m - 1$ , et  $[\zeta]$ ,  $[s]$ ,  $[\rho_x]$  étant dans  $\Omega$ . Posons  $\frac{p^m-1}{2} = q$  et  $\rho_q = \rho$ . En prenant au besoin  $[\rho^{-1} | \gamma$  pour  $\gamma$ , on peut supposer que  $\rho = 1$ . On a alors en particulier, pour  $x = q$ ,  $\sigma \gamma \sigma = \gamma \sigma^{-1} \gamma$  ou  $\sigma^{-1} \gamma \sigma^{-1} [\zeta] = \gamma \sigma \gamma$ , et je poserai  $\{\Phi^0, \gamma\} = Z$ .

Changeons dans (2)  $x$  en  $q - x$ . On aura

$$\sigma_{\zeta}^{-1} \gamma \rho_m^x = \gamma \sigma_{\zeta}^{-1} \gamma [\rho_{q-x}],$$

d'où, en multipliant à gauche par  $[\rho_x | \gamma$ , en tenant compte de (2), et en divisant à gauche par  $\sigma_{\zeta}^{-1} \gamma$ ,

$$\rho_m^{m-1-2x} \sigma_{\zeta}^{-1} \rho_m^x \sigma_{\zeta} = [\zeta \rho_{q-x} \rho_x].$$

ou

$$\mu_m^{p^m-1} = \mu^{\pi-1} = [\zeta^2 \rho_{q-2} \rho_x]$$

et en particulier  $[\zeta^2 \rho_0] = \mu^{\pi-1}$ .

L'équation déduite de (2) en changeant  $x$  en  $x+2$  s'écrit, à l'aide des relations  $\gamma^{-1} \mu_m^2 \gamma = \mu_m^2 [s]$  et  $\mu_m^2 \sigma_x(\mu_m^2) = \sigma_{x+2}$

$$(3) \quad \sigma_{x+2} \gamma \mu_m^{p^m-1} \sigma_{x+2}^{-1} \sigma_{x+2}^{-1} [s^{-1}] = \gamma \sigma_{x+2} \gamma [\rho_{x+2}].$$

La division de (2) par (3) donne  $s = \frac{\rho_x}{\rho_{x+2}}$ .

En remplaçant  $\mu_m^{p^m-1}$  par  $[\zeta^2 \rho_0]$ ,  $\mu_m^{-2x}$  par  $[\zeta^{2x} | \mu_{0m}^{-2x}]$ , et  $\zeta^2$  par  $e^{-1} \mu_m^{n+1}$  ( $e = \pm 1$ , sauf si  $n = 2v$  avec  $\Lambda = 11$  et  $\pi \equiv 3 \pmod{4}$  (2)), l'équation (2) s'écrit

$$(4) \quad \gamma \sigma_{x+2}^{-1} \gamma \mu_{0m}^{2x} = \left[ \frac{\rho_x}{\rho_{x+2}} e^{-1} \mu_m^{n+1} \rho_x \right] \sigma_{x+2} \gamma \sigma_{x+2}^{-1}.$$

Je désignerai par  $Y_{xi} = \sum_l c_{xil} y_l$  et  $Y'_{xi} = \sum_l c'_{xil} y_l$  les fonctions substituées à  $y_i$  par le premier et le second membre de (4) respectivement. L'équation (4) montre comment on peut former de suite la condition  $c_{xii} = c'_{xii}$  en partant de la condition  $c_{0ii} = c'_{0ii}$ .

L'équation  $\gamma^{-1} \mu_m^2 \gamma = \mu_m^2 [s]$  s'écrit  $\mu_{0m}^2 \gamma = [\zeta^2 | s | \mu_{0m}^2]$ , ou, en développant,

$$\gamma_{ik} \mu_m^{2k} = \mu_m^{2(n+1-k)} s^k \gamma_{ik} \quad (s' = s e^{-2}).$$

Or, si  $\gamma$  existe, il y a pour chaque  $i$ , au moins un  $\gamma_{ik} \neq 0$ , et, pour  $\gamma_{ik} \neq 0$ , on a  $s^k = \mu_m^{2(n+1-k)}$ . Donc  $s$  a la forme  $\mu_m^{2c} \left( 0 \leq c \leq \frac{p^m-3}{2} \right)$ . Supposons toujours que  $\mu = \mu^{\pi-1}$ . On aura  $s' = \mu^{2c(\pi-1)}$  (5). Mais  $[s']$  étant dans  $\Omega$ ,  $s'$  a la forme  $\mu^{\pi-1}$ . Donc

$$(\pi-1)c = 2cg(\pi-1) + l(\pi-1).$$

Donc  $\frac{\pi-1}{2}$  divise  $2cg = f \frac{\pi-1}{2}$ , et  $2c = f \frac{p^m-1}{2}$  ( $f = 0$  ou  $1$ ; et, si  $f = 1$ ,  $p^m \equiv 1 \pmod{4}$ ). Ainsi, pour chaque valeur de  $i$ , les  $\gamma_{ik} \neq 0$  vérifient la condition

$$(5) \quad \begin{cases} 2(i+k-n-1) = f \frac{p^m-1}{2} + f'(p^m-1), \\ (f=0 \text{ ou } 1; \text{ si } f=1, p^m \equiv 1 \pmod{4} (f' \text{ entier}), \end{cases}$$

$f$  étant indépendant de  $i, k$  ( $f \frac{p^m-1}{2} = 2c$ , et  $\mu_m^{2c} = s'$ ).

**21.** Supposons d'abord  $f = 1$ , donc  $p^m \equiv 1 \pmod{4}$ , et  $s' = -1$ .

L'équation (5) aura la forme  $i + k = n + 1 + h \frac{p^m - 1}{4}$ ,  $h$  étant impair. Or  $i + k$  est  $\geq 2$  et  $\leq 2n$ . Donc

$$1 - n - h \frac{p^m - 1}{4} = n - 1, \quad \text{ou} \quad |h| = 4 \frac{n - 1}{p^m - 1} = 4 \frac{p^m - 1}{p^m - 1}.$$

Donc,  $h$  étant impair, on a :

$$\begin{aligned} \text{si } p > 3, \quad m = 1 \text{ (donc } p \equiv 1 \pmod{4}), \quad |h| = 1 \text{ ou } 3, \quad n = |h| \frac{p^m - 1}{4} + 1; \\ \text{si } p = 3, \quad m = 2, \quad |h| = 1, \quad n \geq 3, \quad \text{donc } n \equiv 3. \end{aligned}$$

La seconde hypothèse est inadmissible, car, pour  $i = 2$ , on aurait  $k = 4$  ou 0.

Soit donc  $p = 4q' + 1$ ,  $m = 1$ ,  $n = |h|q' + r(r - 1)$ . Si  $h$  ne prend que les deux valeurs  $\pm 1$ , les seuls  $\gamma_{ik}$  pouvant être  $\neq 0$  sont ceux de deux parallèles à la transversale (correspondant aux valeurs  $-1$  et  $+1$  de  $h$ ), et  $|\gamma| = 0$  (une addition de colonnes fait apparaître une colonne nulle). Donc  $h$  prend aussi les valeurs  $\pm 3$ , et  $n = 3q' + r(r - 1) \leq r^2 q' + 1$ . Les seuls  $\gamma_{ik}$  pouvant être  $\neq 0$  sont ceux de quatre parallèles à la transversale passant par les éléments  $\gamma_{1r}, \gamma_{1,3q'+r}, \gamma_{3q'+1,r}, \gamma_{3q'+1,3q'+r}$ .

Soit d'abord  $r = q' + 1$ . Un des éléments  $\gamma_{q'-1,1}, \gamma_{q'-1,2q'+1}, \gamma_{q'-1,3q'+1}$  est  $\neq 0$ , sans quoi la ligne  $q' + 1$  serait nulle. Par des additions de colonnes, on peut donc annuler deux d'entre eux, tels que  $\gamma_{q'-1,2q'+1}, \gamma_{q'-1,3q'+1}$ . Alors  $\gamma_{3q'+1,2q'+1}$  et  $\gamma_{3q'+1,3q'+1}$  sont tous deux  $\neq 0$ , sans quoi il y aurait une colonne nulle. On peut donc, par une addition de colonnes, annuler  $\gamma_{3q'+1,2q'+1}$ , sans altérer  $\gamma_{q'-1,2q'+1}$ . Alors la  $(\lambda q' + 1)^{\text{ième}}$  colonne est nulle. Donc  $r$  est  $> q'$ .

Soit  $r < q'$ . Les seuls éléments des lignes  $r + 1$  et  $2q' + r + 1$  pouvant être  $\neq 0$  sont  $\gamma_{r+1,2q'}$  et  $\gamma_{2q'+r+1,2q'}$ . Donc ces deux lignes sont proportionnelles, et  $|\gamma| = 0$ .

Soit  $r = q'$ . On a, pour  $\alpha, \beta = 1, \dots, q'$ ,

$$\begin{aligned} c_{0,\alpha,\beta} &= (-1)^{\alpha+\beta+1} \sigma_{3q'+1-\alpha,q'+\beta} \gamma_{\alpha,3q'+1-\beta} \gamma_{q'+\beta,p-\beta}, \\ c'_{0,\alpha,\beta} &= 0. \end{aligned}$$

Donc  $\gamma_{\alpha,3q'+1-\alpha} \gamma_{q'+\beta,p-\beta} = 0$ . Si donc un seul des  $\gamma_{\alpha,3q'+1-\alpha}$  est  $\neq 0$ ,

tous les  $\gamma_{q'+3, p-3}$  sont nuls; mais alors les  $\gamma_{q'+3, p-3}$  sont tous  $\neq 0$  (sans quoi  $\gamma$  aurait une colonne nulle), et la relation fondamentale correspondant aux colonnes  $3q' + 1 - \alpha$ ,  $3q' + \alpha$  montre que  $\gamma_{\alpha, 3q'+1-\alpha} = 0$  pour  $\alpha = 1, \dots, q'$ , contre l'hypothèse. Donc tous les  $\gamma_{\alpha, 3q'+1-\alpha}$  sont nuls. Donc tous les  $\gamma_{\alpha, q'+1-\alpha}$  sont  $\neq 0$ . Mais alors la relation fondamentale correspondant aux lignes  $q' + 1 - \alpha$ ,  $q' + \alpha$  montre que les  $\gamma_{q'+3, p-3}$  sont nuls, et la relation fondamentale correspondant aux colonnes 1 et  $n$  donne  $\gamma_{q'+1} \gamma_{3q'+1, n} = 0$ . Donc la ligne  $q'$  ou la colonne  $n$  serait nulle.

22. Donc  $f = 0$  et  $s = 1$ . Alors  $i + k = n + 1 + f' \frac{p^m - 1}{2}$ , et comme  $i + k$  est  $\geq 2$  et  $\leq 2n$ , on a

$$1 - n \leq f' \frac{p^m - 1}{2} \leq n - 1, \quad \text{ou} \quad |f'| \geq 2 \frac{n - 1}{p^m - 1} \leq 2 \frac{p - 1}{p^m - 1}.$$

Si  $f' = 0$  pour chaque couple  $i, k$ , on est ramené au cas des nos 17-18 (ici encore  $\sigma\gamma\sigma = \gamma\sigma^{-1}\gamma$ ).

Supposons donc que  $f'$  soit  $\neq 0$  pour un au moins des couples  $i, k$ . On aura alors  $\frac{p^m - 1}{p - 1} \geq 2$ . Donc  $m = 1$ ,  $|f'| \leq 2$ ,  $n \geq |f'| \frac{p - 1}{2} + 1$ .

Supposons d'abord que  $|f'|$  reste  $< 2$ . Alors  $n$  est  $\geq \frac{p + 1}{2}$ . Posons  $n = q + r$  ( $p = 2q + 1$ ). Les seuls  $\gamma_{ik}$  pouvant être  $\neq 0$  sont ceux de trois parallèles à la transversale (correspondant aux valeurs  $-1, 0, 1$  de  $f'$ ) passant par les éléments  $\gamma_{1, r}, \gamma_{1, n}, \gamma_{n, q-1}$ .

Soit d'abord  $r < q$ . On a alors, pour  $r < j \leq q$ ,

$$c'_{0, j} = \sum_{i=1}^j \sigma_{ji} \gamma_{i, n+1-i} \sigma_{n+1-i, q},$$

$$c_{0, j} = (-1)^{q-j} \gamma_{j, n+1-j} \gamma_{n+1-q, q} \sigma_{n+1-j, n+1-q},$$

et l'équation  $c'_{1, j} = c_{1, j}$  s'écrit  $\frac{e_{01}}{\rho_0} c'_{0, j} = c_{0, j}$ , d'où, par comparaison avec  $c'_{0, j} = c_{0, j}$  ( $\gamma_{j, n+1-j}$  et  $\gamma_{n+1-q, q}$  sont  $\neq 0$ , sans quoi  $|\gamma|$  serait nul),  $\frac{e_{01}}{\rho_0} = 1$ .



On a d'ailleurs, pour  $\alpha, \beta \leq r$ ,

$$c'_{0\alpha\beta} = \sum_{h=1}^{\alpha} \sigma_{2h} (\gamma_{h,r+1-h} \sigma_{r+1-h,\beta} + \gamma_{h,n+1-h} \sigma_{n+1-h,\beta}),$$

$$c_{0\alpha\beta} = (-1)^{\alpha+\beta} (\gamma_{\alpha,r+1-\alpha} \sigma_{r+1-\alpha,r+1-\beta} \gamma_{r+1-\beta,\beta} + \gamma_{\alpha,n+1-\alpha} \sigma_{n+1-\alpha,n+1-\beta} \gamma_{n+1-\beta,\beta}).$$

La somme des deux conditions  $c'_{0\alpha\beta} = c_{0\alpha\beta}$ ,  $c'_{1\alpha\beta} = c_{1\alpha\beta}$  donne donc, en tenant compte de  $e\rho_1 = \rho_0$ ,

$$(6) \quad \sum_{h=1}^{\alpha} \sigma_{2h} \gamma_{h,r+1-h} \sigma_{r+1-h,\beta} = 0,$$

d'où, pour  $\beta = 1$ , en faisant  $\alpha = 1, \dots, r$ ,

$$\gamma_{1r} = \gamma_{2,r-1} = \dots = \gamma_{r1} = 0.$$

Or,  $\gamma^2$  remplace  $\gamma_x$  par  $\gamma_{x,n+1-x} (\gamma_{n+1-x,x} V_x + \gamma_{n+1-x,q+x} V_{q+x})$  et  $\gamma_{x,n+1-x}$  est  $\neq 0$  (sans quoi la ligne  $\alpha$  serait nulle). Donc  $\gamma_{n+1-x,q+x}$  est nul pour  $\alpha = 1, \dots, r$ , et l'on rentre dans le cas traité aux nos 17-18.

**25.** Soit  $r = q$ , donc  $n = p - 1 = 2\nu$ . La somme des équations  $c'_{0\alpha\beta} = c_{0\alpha\beta}$ ,  $c'_{1\alpha\beta} = c_{1\alpha\beta}$  pour  $\alpha \leq \nu$ ,  $\beta > \nu$  donne

$$(7) \quad \left(1 + \frac{e\rho_1}{\rho_0}\right) \sum_{h=1}^{\alpha} \sigma_{2h} \gamma_{h,n+1-h} \sigma_{n+1-h,\beta}$$

$$= (-1)^{\alpha+\beta} 2 \gamma_{\alpha,n+1-\alpha} \sigma_{n+1-\alpha,n+1-\beta} \gamma_{n+1-\beta,\beta}.$$

Supposons d'abord  $\gamma_{1n} \neq 0$ . Alors (7) donne, pour  $\beta = n$ ,

$$(8) \quad \gamma_{x,n+1-x} = \left(1 + \frac{e\rho_1}{\rho_0}\right) \frac{(-1)^x \sigma_{2x}}{2 \sigma_{n+1-x,1}}.$$

La différence des deux relations  $c'_{01\nu} = c_{01\nu}$ ,  $c'_{11\nu} = c_{11\nu}$  donne

$$\left(1 + \frac{e\rho_1}{\rho_0}\right) \gamma_{1\nu} + \left(1 - \frac{e\rho_1}{\rho_0}\right) \gamma_{1n} \sigma_{n\nu} = -2 \gamma_{1n} \gamma_{1\nu} \sigma_{n1}.$$

On a donc, d'après (8) (pour  $\alpha = 1$ ),  $\frac{e\rho_1}{\rho_0} = 1$ , puis  $\gamma_{x,n+1-x} = \frac{(-1)^x \sigma_{2x}}{\sigma_{n+1-x,1}}$ . En portant ces valeurs dans la somme des deux relations  $c'_{0\alpha\beta} = c_{0\alpha\beta}$ ,

$c_{ixx} = c_{ixx}$ , on obtient

$$\sum_{h=1}^x (-1)^h \frac{\sigma_{2h} \sigma_{n+1-2,x} \sigma_{h1}}{\sigma_{n+1-h,1}} = \gamma_{x, \nu+1-x}^2 + 1.$$

Le premier membre est égal à

$$\sum_{h=1}^x (-1)^h \binom{n-h}{n-x} \binom{n-x}{n-1},$$

qui se réduit à **1 (15)**. Donc  $\gamma_{x, \nu+1-x} = 0$ , et  $\gamma^2$  remplace  $\gamma_x$  par

$$\gamma_{x, n+1-x} (\gamma_{n-1-x, x}^2 x + \gamma_{n+1-x, x+\nu})^2 (x+\nu).$$

Donc  $\gamma_{n+1-x, x+\nu} = 0$ , et l'on rentre dans le cas traité au n° **17** ( $n$  est ici pair, donc  $A \neq Q$ ). On aura la même détermination de  $\gamma$ , et le groupe obtenu ici est  $X_0^0$  (**18**).

Supposons  $\gamma_{1n}, \gamma_{2, n-1}, \dots, \gamma_{x-1, n+2-x}$  nuls, et  $\gamma_{x, n-1-x} \neq 0$  ( $\alpha \geq 2$ ). La formule (7) donne alors

$$\left(1 + \frac{c_{\beta 1}}{\rho_0}\right) \sigma_{n-1-x, \beta} = (-1)^{x+\beta} \gamma_{n-1-\beta, \beta} \sigma_{n-1-x, n-1-\beta}.$$

Mais  $\gamma_{n-1-\beta, \beta}$  est nul pour  $\beta = n$ , et  $\neq 0$  pour  $\beta = n+1-x$ . Donc  $1 + \frac{c_{\beta 1}}{\rho_0}$  serait à la fois nul et non nul.

Donc tous les  $\gamma_{x, n-1-x}$  ( $\alpha \geq \nu$ ) sont nuls. Alors les  $\gamma_{x, \nu+1-x}$  et les  $\gamma_{x+\nu, n-1-x}$  sont  $\neq 0$  (sans quoi  $|\gamma| = 0$ ), et les équations  $c'_{0l} = c_{01l}, c'_{1l} = c_{11l}$  ( $l \geq \nu$ ) donnent

$$\gamma_{1\nu} \sigma_{\nu l} = \frac{c_{\beta 1}}{\rho_0} \gamma_{1\nu} \sigma_{\nu l} = (-1)^{l+1} \sigma_{\nu, \nu+1-l} \gamma_{\nu+1-l, l}.$$

Donc  $c_{\beta 1} = -\rho_0$ , et  $\gamma_{\nu+1-l, l} = \frac{(-1)^{l+1} \sigma_{\nu l}}{\sigma_{\nu, \nu+1-l}}$  ( $l \leq \nu$ ).

En retranchant l'équation  $c'_{nl} = c_{1nl}$  de  $c'_{0nl} = c_{0nl}$ , on a

$$\begin{aligned} & \sum_{h=\nu+1}^n \sigma_{nh} \gamma_{h, n+1-h} \sigma_{n+1-h, l} \\ & = (-1)^{l+\nu} (\gamma_{n1} \sigma_{1, \nu+1-l} \gamma_{\nu+1-l, l} + \gamma_{n, \nu+1} \sigma_{\nu+1, n+1-l} \gamma_{n-1-l, l}). \end{aligned}$$

Or, les  $\sigma$  du second membre sont nuls pour  $l < \nu$ , et, pour  $l = \nu$ , le

second membre est le coefficient de  $y_v$  dans la fonction que  $\gamma^2$  substitue à  $y_n$ . Donc le second membre est nul pour  $l \leq v$ . En faisant  $l = v, v-1, \dots, 1$ , on a donc, entre les  $\sigma_{nh} \gamma_{h, n+1-h}$ ,  $v$  équations homogènes de déterminant 1 (tous les éléments situés au-dessus de la diagonale, composée d'unités, sont nuls). Donc les  $\gamma_{h, n+1-h}$  ( $h > v$ ) sont nuls, et l'on rentre dans le cas traité au n° 13. On a la même détermination de  $\gamma$ , et le groupe obtenu ici est  $X_1^0$ .

24. Soit  $r = q + 1$ , donc  $n = p = 2q + 1$  et  $q = v$ . Les seuls  $\gamma_{ik}$  pouvant être  $\neq 0$  sont ceux de trois parallèles à la transversale, passant par les éléments  $\gamma_{1, v+1}, \gamma_{1n}, \gamma_{n, v+1}$ . La combinaison de la première ligne avec elle-même montre que  $\gamma_{1, v+1} = 0$ . Donc  $\gamma_{1n}$  est  $\neq 0$ , et le cas actuel sera traité dans la discussion du numéro suivant.

25. Supposons maintenant que  $|f'|$  prenne la valeur 2. Comme  $n$  est  $\geq |f'| \frac{p-1}{2} + 1$  et  $\geq p$ , on a  $n = p$ . Les seuls  $\gamma_{ik}$  pouvant être  $\neq 0$  sont ceux de cinq parallèles à la transversale (correspondant aux valeurs  $-2, -1, 0, 1, 2$  de  $f'$ ) passant par les éléments  $\gamma_{11}, \gamma_{1, v+1}, \gamma_{1n}, \gamma_{n, v+1}, \gamma_{nn}$  (la première et la cinquième ne contenant qu'un élément).

La somme et la différence des équations  $c'_{0n} = c_{01n}, c'_{1n} = c_{11n}$  donnent, en posant

$$\frac{1}{2} \left( 1 + \frac{c'_{01}}{c_n} \right) = u, \quad \frac{1}{2} \left( 1 - \frac{c'_{01}}{c_n} \right) = v,$$

$$(9) \quad u \gamma_{1n} = \gamma_{1n}^2 \sigma_{n1} + \gamma_{11} \gamma_{1n} + \gamma_{1, v+1} \gamma_{v+1, n} + \gamma_{1n} \gamma_{nn},$$

$$(10) \quad v \gamma_{1n} = (-1)^v \gamma_{1n} (\gamma_{1, v+1} \sigma_{v+1, 1} + \gamma_{v+1, n} \sigma_{n, v+1}).$$

La somme et la différence des équations

$$c'_{0, 1, v+1} = c_{0, 1, v+1}, \quad c'_{1, 1, v+1} = c_{1, 1, v+1}$$

donnent

$$(11) \quad u \gamma_{1, v+1} + v \gamma_{1n} \sigma_{n, v+1} = \gamma_{1n} \gamma_{1, v+1} \sigma_{n1} + \gamma_{11} \gamma_{1, v+1} + \gamma_{1, v+1} \gamma_{v+1, v+1} + \gamma_{1n} \gamma_{n, v+1}$$

$$(12) \quad u \gamma_{1n} \sigma_{n, v+1} + v \gamma_{1, v+1} = (-1)^v (\gamma_{1, v+1}^2 \sigma_{v+1, 1} + \gamma_{1n} \gamma_{v+1, v+1} \sigma_{n, v+1}).$$

La somme et la différence des équations  $c'_{011} = c_{011}, c'_{111} = c_{111}$

donnent

$$(13) \quad u(\gamma_{11} + \gamma_{1n}\sigma_{n1}) + v\gamma_{1,\nu+1}\sigma_{\nu+1,1} = \gamma_{11}\gamma_{1n} + \gamma_{11}^2 + \gamma_{1,\nu+1}\gamma_{\nu+1,1} + \gamma_{1n}\gamma_{n1}$$

$$(14) \quad u\gamma_{1,\nu+1}\sigma_{\nu+1,1} + v(\gamma_{11} + \gamma_{1n}\sigma_{n1}) = (-1)^\nu(\gamma_{11}\gamma_{1,\nu+1}\sigma_{\nu+1,1} + \gamma_{1n}\gamma_{\nu+1,1}\sigma_{n,\nu+1}).$$

En tenant compte de  $\gamma^2 = [\zeta]$ , les relations (9), (11), (13) s'écrivent

$$(15) \quad u\gamma_{1n} = \gamma_{1n}^2\sigma_{n1},$$

$$(16) \quad u\gamma_{1,\nu+1} + v\gamma_{1n}\sigma_{n,\nu+1} = \gamma_{1n}\gamma_{1,\nu+1}\sigma_{n1}$$

$$(17) \quad u(\gamma_{11} + \gamma_{1n}\sigma_{n1}) + v\gamma_{1,\nu+1}\sigma_{\nu+1,1} = \gamma_{11}\gamma_{1n} + \zeta.$$

Supposons d'abord  $\gamma_{1n} \neq 0$ . Alors, d'après (15) et (16),  $\nu = 0$ . Or on a ici (20)

$$e^{-\nu} s = 1, \quad \rho_{2\nu} = \rho_0, \quad \rho_{2\nu+1} = \rho_1, \quad [\zeta \rho_{q-\nu} \rho_\nu] = 1.$$

Donc, si  $q$  est pair,  $\rho_0^2 = \rho_0$ , et si  $q$  est impair,  $\rho_0 \rho_1 = \rho_0$ . Donc, comme  $\nu = 0$ , on a, quel que soit  $q$ ,  $\rho_0 = \rho_1 = 1$ ,  $\zeta = 1$ . Dès lors, la somme des équations  $c'_{0nn} = c_{0nn}$ ,  $c'_{1nn} = c_{1nn}$  donne

$$\gamma_{1n}\sigma_{n1} + \gamma_{nn} = 2\gamma_{1n}\gamma_{nn}\sigma_{n1} + \gamma_{n1}\gamma_{1n} + \gamma_{n,\nu+1}\gamma_{\nu+1,n} + \gamma_{nn}^2$$

ou, d'après la condition  $\gamma^2 = [\zeta]$ ,

$$\gamma_{1n}\sigma_{n1} + \gamma_{nn} = 2\gamma_{1n}\gamma_{nn}\sigma_{n1} + \zeta,$$

ou, puisque, d'après (15),  $\gamma_{1n}\sigma_{n1} = 1$ , et que  $\zeta = 1$ ,  $\gamma_{nn} = 0$ . La combinaison de la  $n^{\text{ième}}$  colonne avec elle-même donne donc  $\gamma_{\nu+1,\nu} = 0$ ; (10) donne alors  $\gamma_{1,\nu+1} = 0$ , la combinaison de la première ligne avec elle-même  $\gamma_{11} = 0$  (1), et la combinaison de la première colonne avec elle-même  $\gamma_{\nu+1,1} = 0$ .

La somme des équations  $c'_{0\alpha n} = c_{0\alpha n}$ ,  $c'_{1\alpha n} = c_{1\alpha n}$  ( $2 \leq \alpha \leq n$ ) donne maintenant

$$(18) \quad \gamma_{\alpha,n+1-\alpha} = \frac{(-1)^{\alpha+1}\sigma_{\alpha 1}}{\sigma_{n+1-\alpha,1}} \quad (\alpha = 2, \dots, \nu).$$

En portant cette valeur dans la somme des équations  $c'_{0\alpha\alpha} = c_{0\alpha\alpha}$

(1) C'est ici que l'on est ramené au cas non encore traité du numéro précédent.

$c'_{1\alpha\alpha} = c_{1\alpha\alpha}$ , on obtient

$$\sum_{h=1}^x (-1)^x \frac{\sigma_{2h} \sigma_{n+1-x, x} \sigma_{h1}}{\sigma_{n+1-h, 1}} = \gamma_{x, \nu+2-x}^2,$$

d'où, comme au n° 25,  $\gamma_{x, \nu+2-x} = 0$ . Mais alors  $\gamma^2$  remplace  $\gamma_x$  par

$$\gamma_{x, n+1-x} (\gamma_{n+1-x, x} \gamma_x + \gamma_{n+1-x, \nu} \gamma_{x, \nu}),$$

d'où  $\gamma_{n+1-x, x+\nu} = 0$ . On rentre donc dans le cas du n° 17.

Soit maintenant  $\gamma_m = 0$ . La combinaison de la première ligne avec elle-même et de la dernière colonne avec elle-même donnent  $\gamma_{1, \nu+1} = 0$ ,  $\gamma_{\nu+1, n} = 0$  (donc  $\gamma_{11} \gamma_{nn} \neq 0$ ). La condition  $\gamma^2 = |\zeta|$  donne alors  $\gamma_{\nu+1, 1} = 0$ ; la combinaison des colonnes 1,  $\nu+1$  donne  $\gamma_{n, \nu+1} = 0$ , et celle de la dernière ligne avec elle-même  $\gamma_{n1} = 0$ . Dès lors, l'équation (14) donne  $v = 0$ , d'où encore  $u = 1$ ,  $\rho_0 = \rho_1 = 1$ ,  $\zeta = 1$ .

La somme des équations  $c'_{0, x, n-1} = c_{0, x, n-1}$ ,  $c'_{1, x, n-1} = c_{1, x, n-1}$  ( $2^x \cdot 2^{\nu-n-1}$ ) donne maintenant

$$\gamma_{x, n+1-x} = \frac{(-1)^x \sigma_{2x}}{\sigma_{n+1-x, 2}}.$$

En portant cette valeur dans la somme des équations  $c'_{0, 2, 2} = c_{0, 2, 2}$ ,  $c'_{1, 2, 2} = c_{1, 2, 2}$ , on obtient

$$\sum_{h=2}^{\alpha} (-1)^h \frac{\sigma_{2h} \sigma_{n+1-x, x} \sigma_{h2}}{\sigma_{n+1-h, 2}} = \gamma_{x, \nu+2-x}^2 + 1,$$

d'où, par un calcul analogue à celui de tout à l'heure,  $\gamma_{x, \nu+2-x} = 0$ , et de même  $\gamma_{n+1-x, x+\nu} = 0$ . On rentre donc dans le cas du n° 16.

Il résulte finalement de cette analyse que *les seuls groupes  $\mathfrak{S}$  sont les groupes  $\mathfrak{S}_i^0$  obtenus précédemment.*

**26.** Quand  $m = 1$ ,  $\mathfrak{S}_0$  n'est pas conjugué dans  $\mathfrak{A}$  de  $\mathfrak{S}_1$  pour  $n = p - 1 \equiv 0 \pmod{4}$ , ni de  $\mathfrak{S}_2$  pour  $n = p$ .

En effet, si  $\mathfrak{S}_0$  est conjugué de  $\mathfrak{S}_i$  ( $i = 1, 2$ ) dans  $\mathfrak{A}$ , il y a dans  $\Lambda$  une substitution  $s$  telle que  $s^{-1} \bar{X}_i s = \bar{X}_0$  (et réciproquement). Donc  $s^{-1} X_i s = X_0 \Theta$ ,  $\Theta$  étant dans  $\Omega$ . Or, suivant que  $n = p - 1 \equiv 0 \pmod{4}$  ou que  $n = p$ , on a  $X_1 | D \equiv X_0 | D = \mathfrak{L}(2, p)$ , ou  $X_2 \equiv X_0 \equiv \mathfrak{L}(2, p)$ . Donc  $\Theta = 1$ . D'ailleurs, dans le groupe de degré  $p + 1$  deux fois tran-

sitif  $\mathcal{L}(2, p)$ , les diviseurs d'ordre  $p(p-1)$  qui fixent un symbole sont tous conjugués de  $\{z+1, \iota, z\}$ . On peut donc supposer  $s$  permutable à  $\Phi$ , donc à  $\varpi$ . De même les diviseurs d'ordre  $p-1$  de  $\{z+1, \iota, z\}$  y étant tous conjugués de  $\{\iota, z\}$ , on peut supposer  $s$  permutable à  $M_1$ . Mais alors  $s$  transforme  $\gamma_i$  en une  $s_2$  de  $X_0$  permutable à  $M_1$  et située hors de  $M_1$ . Or le normalisant de  $\{\iota, z\}$  dans  $\mathcal{L}(2, p)$  est  $\{\iota, z, z^{-1}\}^{(1)}$ , et ses  $s_2$  autres que  $z \rightarrow z^{-1}$  y forment deux classes représentées par  $z^{-1}$  et  $\iota, z$ . On peut donc supposer que  $s$  transforme  $\gamma_i$  en  $\mu_1^\alpha \gamma_0 d^\beta$  ( $\alpha, \beta = 0$  ou  $1$ )<sup>(2)</sup> ou que  $s\mu_1^\alpha \gamma_0 s^{-1} = \gamma_i d^\beta$ . Or  $s$ , étant permutable à  $\varpi$ , a la forme  $s = \mu_1^l \varphi$ ,  $\varphi$  étant dans  $\varpi'$  (4); et  $\varphi$ , étant donc permutable à  $M_1$ , a la forme  $u_{1l}$  ou  $\bar{u}_{1l}$  (5) ( $l = 0$  si  $n \neq p$ ). Donc  $s\mu_1^\alpha \gamma_0 s^{-1}$  remplace  $\gamma_i$  par une fonction où le coefficient de  $y_x$  est  $\neq 0$ , ce qui n'est pas le cas pour  $\gamma_i d^\beta$ .

**27. Remarque.** — Supposons encore  $m = 1$ ,  $n = p - 1$ , et soit  $A = G$ . Si  $x$  est pair, toute substitution de  $A'$  qui transforme  $\varpi$  en  $\varpi_x$  (7) transforme  $X_1$  et  $X_0$  en deux autres diviseurs de  $A$  qui contiennent  $\varpi_x$ , et ne sont par suite conjugués dans  $A$  ni de  $X_1$  ni de  $X_0$ . D'après ce qu'on vient de voir, ils ne sont pas conjugués entre eux.

Soit  $x$  impair. Considérons alors  $G(n, \pi^2)$ , et faisons jouer à  $\pi^2$  le rôle de  $\pi$ .  $X_1$  et  $X_0$  sont dans  $G(n, \pi)$ . Comme  $X_1^0$  et  $X_0^0$  déterminant complètement  $X_1$  et  $X_0$  (20-23) qui ne sont pas conjugués dans  $G(n, \pi^2)$ ,  $X_1^0$  et  $X_0^0$  ne sont pas conjugués dans  $G(n, \pi^2)$ .

**28. Cherchons maintenant le normalisant  $X_i^l$  dans  $A$  de  $X_i$  ( $i = 0, 1, 2$ ;  $A \neq G$  si  $x$  est impair).**

Soit  $s$  une substitution de  $A$  permutable à  $X_i$ , et  $s^{-1}\varpi s = \varpi_i$ .  $\Lambda_i$  contient une substitution  $s_1$  transformant  $\varpi$  en  $\varpi_i$ . Donc  $ss_1^{-1}$  est permutable à  $\varpi$  et a la forme  $\varphi\mu_1^l$ ,  $\varphi$  étant dans  $\varpi'$  (4). Donc  $s$  est

(1)  $\mathcal{L}(2, p)$  étant deux fois transitif, le diviseur fixant deux symboles a  $\frac{p(p+1)}{2}$  conjugués.

(2) Si  $n = p - 1$ , on voit de suite que cela est impossible, car  $\{M_1, \gamma_1\}$ , que  $s$  devrait transformer en  $\{M_1, \gamma_0\}$ , est  $\cong \{M_1, \gamma_0\} [\gamma_1^2 = \gamma_0^2 = d, \gamma_1^{-1}\mu_1\gamma_1 = \mu_1^{-1}d^{h+1}, \gamma_0^{-1}\mu_1\gamma_0 = \mu_1^{-1}d^h]$  (16, 17).

dans  $\varphi X_i$ , et  $\varphi$  est permutable à  $X_i$ . Donc  $\varphi$ , qui est permutable à  $\varpi$ , l'est au normalisant  $\Phi$  de  $\varpi$  dans  $X_i$ . Comme d'ailleurs  $\Phi$  détermine  $X_i$ , il suffit que  $\varphi$  soit dans  $\Phi'$  (12) pour qu'elle soit permutable à  $X_i$ . Donc en exceptant le cas où l'on a à la fois  $n = p$ ,  $m = 1$  et  $A = H$  ou  $\bar{H}$ ,  $X'_i$  coïncide avec  $X_i$ . Si l'on a à la fois  $n = p$ ,  $m = 1$  et  $A = H$  ou  $\bar{H}$ , on peut seulement affirmer que  $X'_i$  divise  $\{X_i, u_{1i}\}$  si  $A = H$ , ou  $\{X_i, \bar{u}_{1i}\}$  si  $A = \bar{H}$  (12). Mais  $u_{1i}$  et  $\bar{u}_{1i}$  sont ici permutables à  $\Phi$ , et quand  $\Phi$  est donné,  $X$  n'a qu'une des deux déterminations  $X_2$  et  $X_0$ . Donc  $u_{1i}$  et  $\bar{u}_{1i}$ , qui, étant d'ordre impair, ne peuvent les échanger (par transformation), sont permutables à  $X_2$  et à  $X_0$ . Donc, si  $n = p$  et  $m = 1$ ,  $X'_i = \{X_i, u_{1i}\}$  pour  $A = H$ , et  $X'_i = \{X_i, \bar{u}_{1i}\}$  pour  $A = \bar{H}$  (ici  $i = 0$  ou  $2$ ).

Cherchons enfin le normalisant  $X_i^0$  dans  $A$  de  $X_i^0$ , en exceptant d'abord, si  $z$  est impair, le cas  $A = G$ . Il est clair que  $X_i^0$  contient  $X_i^0$ . Donc  $X_i^0 = X_i$ . Si  $z$  est impair, le normalisant de  $X_i^0$  ( $i = 0, 1$ ) dans  $G(n, \pi)$  coïncide avec  $X_i^0$ . On le voit en considérant  $X_i^0$  comme diviseur de  $G(n, \pi^2)$ .

**29.** Supposons que  $A = Q$  [avec  $\sigma_{i,i-1}^i = (-1)^i$  (cf. 8)], et cherchons alors quand  $X_2$  divise  $A^0$  ou  $B$ .

$\mu_1$  est toujours dans  $A^0$ ;  $\gamma_2 = t_0^{p+1} H_2^2 t_l m_{l, \gamma_{n+1-l}}$  est dans  $A^0$  toujours et seulement si  $\nu$  est pair, c'est-à-dire si  $p \equiv 1 \pmod{4}$ .

Supposons  $p \equiv 1 \pmod{4}$ . Alors  $\mu_1$  est dans  $B$  toujours et seulement si  $K (= z)$  est pair, ou si  $\nu \equiv 0 \pmod{4}$  (7), c'est-à-dire si  $p \equiv 1 \pmod{8}$ .

D'autre part, on a ici

$$\frac{s_l}{s_{n+1-l}} = (-1)^{\nu+1-l}, \quad \text{donc} \quad \gamma_{n+1-l, l} = -\frac{(p-l-1)!}{(l-2)!},$$

ou, en multipliant haut et bas par  $(p-1) \dots (p-l) = (-1)^l l!$ ,

$$\gamma_{n+1-l, l} = (-1)^{l+1} \frac{l(l-1)}{(l!)^2}.$$

En particulier, pour  $l = 2$ ,  $\gamma_{n+1-l, l} = -\frac{1}{2} = -c$  (8). Comme  $t_{0,2} m_{2,-c}^{-1}$

et  $t_{ik}(i, k \neq 0)$  sont dans  $B(I, 52)$ ,  $\gamma_2$  est dans  $B$  si  $\nu = 2$ , et, si  $\nu \geq 4$ , il y est en même temps que  $\gamma' = \prod_{i=1}^{\nu} m_{ii-1}$ .

Si  $K$  est pair,  $\gamma'$  est évidemment dans  $B$ . Si  $K$  est impair,  $\gamma'$  n'est dans  $B$  que s'il est dans  $B(p, p)$ , car un élément  $i_1^2 = i_2^{2g}$  ( $g = \frac{p-1}{2}$ ) de  $\mathfrak{e}_1$  ne peut être ici carré dans  $\mathfrak{e}$  que s'il l'est dans  $\mathfrak{e}_1$ . Comme il y a, dans  $\mathfrak{e}_1$ ,  $\frac{p-1}{4}$  non carrés suivis d'un carré  $\neq 0$ , et  $\frac{p-1}{4}$  carrés  $\neq 0$  suivis d'un non carré (*E.*, 44), il y a, parmi les  $p-2$  produits  $1.2, 2.3, \dots, (p-2)(p-1)$   $\frac{p-1}{2}$  non carrés. Or, les  $\nu-1$  produits  $1.2, 2.3, \dots, (\nu-1)\nu$  ont respectivement les mêmes caractères quadratiques que les  $\nu-1$  produits  $(p-1)(p-2), (p-2)(p-3), \dots, (p-\nu+1)(p-\nu)$ , et  $\nu(\nu+1) = \frac{p^2-1}{4}$  est ici carré. Donc les  $\nu-1 = \frac{p-3}{2}$  produits  $1.2, \dots, (\nu-1)\nu$  contiennent ici  $\frac{p-1}{4}$  non carrés. Si 2 est carré, c'est-à-dire ici si  $p \equiv 1 \pmod{8}$ , le nombre des non carrés figurant parmi les produits  $2.3, \dots, (\nu-1)\nu$  est  $\frac{p-1}{4} \equiv 0 \pmod{2}$ . Si 2 est non carré, c'est-à-dire ici si  $p \equiv 5 \pmod{8}$ , ce nombre est  $\frac{p-3}{4} \equiv 0 \pmod{2}$ . Donc  $\gamma_2$  est toujours dans  $B$  si  $p \equiv 1 \pmod{4}$ .

Donc, pour que  $X_2$  divise  $B$ , il faut et suffit que  $K$  soit pair, ou que  $p \equiv 1 \pmod{8}$ . Si  $X_2$  ne divise pas  $B$ , son p. g. c. d. avec  $B$  est  $X_2^0$ , et  $X_2$  divise  $A^0$  ou  $\frac{1}{2}B$ ,  $\frac{1}{3}B$  suivant que  $p \equiv 1$  ou  $3 \pmod{4}$ .

**50.** *Considérons maintenant le cas où  $p = 5$  avec  $m = 1$ , et les groupes  $\mathfrak{A} = \mathfrak{G}(4, 5^2)$  et  $\mathfrak{A} = \mathfrak{Q}(5, 5^2)$ .*

Soit d'abord  $\mathfrak{A} = \mathfrak{G}(4, 5^2)$ , et désignons par  $i, j$  les nombres 0, 1 dans un ordre déterminé quelconque. On peut faire correspondre les générateurs  $\sigma, \rho, \gamma_i$  de  $\mathfrak{A}_i$  (en écrivant 5 pour 0 et 6 pour  $\infty$ ) à

$$\sigma = 12345, \quad \rho = 1243, \quad \gamma_0 = 14, 56$$

de  $\mathfrak{L}(2, 5)$ . Or, il y a un isomorphisme de  $\mathfrak{L}(2, 5)$  avec le groupe symétrique  $S_5$  de champ 1, 2, 3, 4, 5, où 12345, 1243, 14, 56 de  $\mathfrak{L}(2, 5)$  répondent respectivement à 12345, 1243, 12, 34 de  $S_5(S., 53)$ .



Dans l'isomorphisme de  $\mathcal{X}_j$  avec  $S_5$ , faisons correspondre  $\sigma$  à 12345,  $\mu_1$  à 1243 et  $\gamma_j$  à 12.34. Regardons maintenant comme identiques les symboles 1, 2, 3, 4, 5 de  $\mathcal{X}(2,5)$  et de  $S_5$ . Alors  $\{\mathcal{X}(2,5), S_5\}$  est le groupe symétrique  $S_6$  de champ 1, 2, 3, 4, 5, 6 (*S.*, 42).

Je dis que  $\{\mathcal{X}_0, \mathcal{X}_1\} \cong S_6$ . Identifions en effet  $\sigma, \mu_1, \gamma_i, \gamma_j$  avec les substitutions correspondantes de  $S_6$ . On aura, avec les notations de *S.*, 69,

$$\begin{aligned} s_2 = \mu_1 \gamma_j = 23, & \quad s_1 = \sigma s_2 \sigma^{-1} = 12, & \quad s_5 = \sigma^{-1} s_2 \sigma = 34, \\ s_4 = \sigma^{-2} s_2 \sigma^2 = 45, & \quad s_3 = \gamma_j \mu_1 \gamma_j = 56. \end{aligned}$$

Pour établir la proposition, il suffit donc (*loc. cit.*) de vérifier que les substitutions  $s_k$  de  $\{\mathcal{X}_0, \mathcal{X}_1\}$  satisfont aux équations

$$\begin{aligned} s_k^2 = 1, & \quad (s_1 s_2)^3 = (s_2 s_3)^3 = (s_3 s_4)^3 = (s_4 s_5)^3 = 1, \\ (s_1 s_3)^2 = (s_1 s_4)^2 = (s_1 s_5)^2 = (s_2 s_4)^2 = (s_2 s_5)^2 = (s_3 s_5)^2 = 1. \end{aligned}$$

Les équations où ne figure pas  $s_5$  sont satisfaites *a priori* dans  $\mathcal{X}_j$ . Il reste donc seulement à vérifier les autres, ce qui se fait directement (<sup>1</sup>). Donc  $\{\mathcal{X}_0, \mathcal{X}_1\} \cong S_6$ , et l'on a une correspondance des générateurs.

D'autre part,

$$\sigma = 12345, \quad \mu_1^2 = 14.23, \quad \gamma_i = 14.56, \quad \gamma_j = 12.34$$

engendrent le groupe alterné  $A_6$  de même champ que  $S_6$  (*S.*, 42).

(<sup>1</sup>) Pour vérifier  $(s_1 s_3)^2 = 1$ ,  $(s_3 s_5)^2 = 1$ ,  $(s_4 s_5)^2 = 1$ , il est avantageux de transformer d'abord ces relations. On a

$$s_1 s_3 = \sigma \mu_1 (\gamma_j \sigma^{-1} \gamma_j) \mu_1 \gamma_i = \sigma \mu_1 (\sigma \gamma_j \sigma) \mu_1 \gamma_i,$$

d'où, en observant les relations  $\mu_1^{-1} \sigma \mu_1 = \sigma^2$ ,  $\mu_1 \gamma_i \mu_1 = \gamma_i$ ,

$$\mu_1^{-1} s_1 s_3 \mu_1 = \sigma^3 \gamma_j \sigma \gamma_i.$$

De même

$$s_3 s_5 = \sigma^{-1} \mu_1 (\gamma_j \sigma \gamma_j) \mu_1 \gamma_i = \sigma^{-1} \mu_1 (\sigma^{-1} \gamma_j \sigma^{-1}) \mu_1 \gamma_i$$

et

$$\mu_1^{-1} s_3 s_5 \mu_1 = \sigma^2 \gamma_j \sigma^{-1} \gamma_i;$$

$$s_1 s_5 = \sigma^{-2} \mu_1 \gamma_j \sigma^2 \gamma_j \mu_1 \gamma_i \quad \text{et} \quad \mu_1^{-1} s_1 s_5 \mu_1 = \sigma \gamma_j \sigma^2 \gamma_j \gamma_i.$$

Il suffit donc de vérifier

$$(\sigma^3 \gamma_j \sigma \gamma_i)^2 = 1, \quad (\sigma^2 \gamma_j \sigma^{-1} \gamma_i)^2 = 1, \quad (\sigma \gamma_j \sigma^2 \gamma_j \gamma_i)^2 = 1.$$

Donc  $\{\mathfrak{X}_0^0, \mathfrak{X}_1^0\} = \{\sigma, \mu_1^2, \gamma_0, \gamma_1\}$  est isomorphe à  $A_6$  et est le plus grand commun diviseur de  $\{\mathfrak{X}_0, \mathfrak{X}_1\}$  et de  $\mathfrak{G}(4, 5)$ .

Soit maintenant  $A = Q(5, 5^2)$ , et désignons par  $i, j$  les nombres 0, 2 dans un ordre déterminé quelconque;  $X_i$  et  $X_j$  (isomorphes à  $S_5$ ) divisent ici  $R(5, 5^2)$  (29) [ $R(5, 5^2)$  est isomorphe à  $\mathfrak{G}(4, 5^2)$  (1, 43)]. Comme précédemment  $\{X_0, X_2\}$  est isomorphe à  $S_6, \sigma, \mu_1, \gamma_0, \gamma_1$  correspondant respectivement à 12345, 1243, 14, 56, 12.34.

D'autre part,  $\mu_1$  est ici hors de  $R(5, 5)$  (3). Donc, comme précédemment,  $\{X_0^0, X_2^0\} = \{\sigma, \mu_1^2, \gamma_0, \gamma_1\}$  est isomorphe à  $A_6$  et est le p. g. c. d. de  $\{X_0, X_2\}$  et de  $R(5, 5)$ .

31. Arrêtons-nous désormais au cas  $A = Q$ , et négligeons le groupe exceptionnel  $X_2$ .

De même que  $\sigma$  conserve  $\alpha$ , la substitution formée par les  $2h + 1$  premières lignes de  $\sigma$  conserve la forme

$$\varphi^{2h+1} = \sum_{k=1}^h y_k y^{2h+2-k} + \frac{1}{2} y_{h+1}^2 = \frac{1}{2} \sum_{k=1}^{2h+1} y_k y^{2h+2-k} \quad (h = 0, 1, \dots, \nu),$$

en regardant la première somme comme nulle pour  $h = 0$ .

Considérons aussi la forme

$$\varphi^{2h} = \sum_{k=1}^h c_k^{2h} y_k y^{2h+1-k},$$

où les  $c_k^{2h}$  sont indéterminés, et convenons d'écrire aussi  $c_{2h+1-k}^{2h}$  pour  $c_k^{2h}$ ,  $c_k$  pour  $c_k^{2\nu}$ , et  $q$  pour  $2h + 1$ .

$\sigma_x$  transforme  $\varphi^{2h}$  en

$$\varphi_x^{2h} = \sum_{k=1}^h c_k^{2h} \sum_{i=1}^h \sigma_{ki, \gamma_i} \sum_{j=1}^{q-k} \sigma_{q-k, j} \alpha^{q-i-j} y_j.$$

Posons

$$\varphi_x^{2h} = \sum_{r=0}^{q=2} \alpha^r \varphi_x^{2h} \quad [\varphi_x^{2h} = \varphi^{2h} (1)].$$

(1) Comme  $i$  est  $\leq k$ , et  $j \leq q - k$ , on ne peut avoir  $i + j = q$  que si  $i = k$  et  $j = q - k$ . Le coefficient de  $\alpha^0$  est donc  $\varphi^{2h}$ .

et calculons le coefficient  $C_{i\lambda}^{2h}$  de  $y_\lambda y_\mu$  dans  $\varphi_{2r}^{2h}(\lambda + \mu = q - r)$ , en supposant  $\lambda \leq \mu$  (alors  $\lambda$  est  $\leq h$ , sans quoi  $\lambda + \mu$  serait  $> q$ ).

Soit d'abord  $\lambda < \mu$ . On peut alors supposer que  $i = \lambda$  ou que  $i = \mu$ . Si  $i = \lambda$ , donc  $j = \mu$ , on a  $\lambda + k = h$ ,  $\mu + q = k$ , donc  $\lambda \geq k = q - \mu$ , et  $k$  prend les valeurs  $\lambda, \lambda + 1, \dots, \lambda + r = q - \mu$  si  $\lambda + r \leq h$  (donc  $\mu > h$ ), les valeurs  $\lambda, \lambda + 1, \dots, h$  si  $\lambda + r > h$  (donc  $\mu \leq h$ ). Si  $j = \lambda$  et  $i = \mu$ , on a  $\lambda + q = k$ ,  $\mu + k = h$ , et  $k$  prend les valeurs  $\mu, \mu + 1, \dots, h$  ( $\mu + r = q - \lambda$  est  $> h$  sans quoi  $\lambda$  serait  $> h$ ; ici  $\lambda + r = q - \mu$  est  $> h$ ).

Donc, si  $\lambda + r \leq h$  (alors  $\mu > h$ ),

$$C_{i\lambda}^{2h} = \sum_{k=\lambda}^{\lambda+r} c_k^{2h} \sigma_{k\lambda} \sigma_{q-k,\mu}.$$

Si  $\lambda + r > h$  (alors  $\mu \leq h$ ),

$$C_{i\lambda}^{2h} = \sum_{k=\lambda}^h c_k^{2h} \sigma_{k\lambda} \sigma_{q-k,\mu} + \sum_{k=\mu}^h c_k^{2h} \sigma_{k\mu} \sigma_{q-k,\lambda},$$

ou, en changeant dans la seconde somme  $k$  en  $q - k$ ,

$$C_{i\lambda}^{2h} = \sum_{k=\lambda}^{\lambda+r} c_k^{2h} \sigma_{k\lambda} \sigma_{q-k,\mu}.$$

Soit maintenant  $\lambda = \mu$ , donc  $2\lambda = q - r$  (ce qui exige que  $r$  soit impair), et  $\lambda = h + \frac{r-1}{2}$ . On aura  $\lambda + k = h$ ,  $\lambda + q = k$ , donc

$$\lambda + k \geq q - \lambda + r.$$

Mais, comme  $\lambda + r = h + \frac{r+1}{2}$  est  $> h$ ,  $k$  prendra les valeurs  $\lambda, \lambda + 1, \dots, h = \lambda + \frac{r-1}{2}$ . Donc

$$C_{i\lambda}^{2h} = \sum_{k=\lambda}^h c_k^{2h} \sigma_{k\lambda} \sigma_{q-k,\lambda},$$

ou, en changeant  $k$  en  $q - k$ ,

$$C_{i\lambda}^{2h} = \sum_{k=\lambda}^{\lambda+r} c_k^{2h} \sigma_{k\lambda} \sigma_{q-k,\lambda}.$$

Donc

$$G_{\lambda}^{2h} = \frac{1}{2} \sum_{k=\lambda}^{\lambda+r} c_k^{2h} \sigma_{k\lambda} \sigma_{q-k,\lambda}.$$

Ainsi on a, en posant  $k = \lambda + i$ ,

$$G_{\lambda}^{2h} = \frac{(-1)^{\lambda+r-k} \binom{\lambda+r-k}{i}}{r! \delta^{\lambda+r-k}} \sum_{i=0}^r \binom{r}{i} c_{\lambda+i}^{2h};$$

$$\delta = 1 \quad \text{si } \lambda < h - \frac{r-1}{2}, \quad \delta = 2 \quad \text{si } \lambda = h - \frac{r-1}{2}.$$

Soit  $r = 1$ , et essayons d'identifier  $\varphi_{2\lambda}^{2h}$ , qui ne contient que les variables  $y_1, \dots, y_{2h-1}$  (puisque  $\lambda + \mu = q - 1$ ) avec  $\varphi_1^{2h-1}$ . On aura

$$G_{\lambda}^{2h} = (-1)^{\lambda+1} (c_{\lambda}^{2h} + c_{\lambda+1}^{2h}) \quad \text{pour } \lambda = 1, \dots, h-1 \quad (\text{si } h > 1)$$

et

$$G_{1/h}^{2h} = \frac{1}{2} (-1)^{h+1} (c_h^{2h} + c_{2h-1}^{2h}) = (-1)^{h+1} c_h^{2h}.$$

Donc,

$$c_1^{2h} + c_2^{2h} = 1, \dots, c_{\lambda}^{2h} + c_{\lambda+1}^{2h} = (-1)^{\lambda+1}, \dots, c_{h-1}^{2h} + c_h^{2h} = (-1)^h, \\ c_h^{2h} = (-1)^{h+1},$$

d'où, en multipliant la  $i^{\text{ème}}$  équation par  $(-1)^{i-1}$ , et en ajoutant les équations de rang  $\lambda, \lambda + 1, \dots, h$ ,

$$c_{\lambda}^{2h} = (-1)^{\lambda+1} \left( h + \frac{1}{2} - \lambda \right).$$

On a alors, en supprimant des sommes nulles,

$$G_{\lambda}^{2h} = \begin{cases} 0 & \text{pour } r > 1 \quad (1), \\ \frac{1}{\delta} & \text{pour } r = 1, \end{cases} \quad G_{\lambda}^{2h} = c_{\lambda}^{2h} = (-1)^{\lambda+1} \left( h + \frac{1}{2} - \lambda \right).$$

Donc, pour  $c_{\lambda}^{2h} = (-1)^{\lambda+1} \left( h + \frac{1}{2} - \lambda \right)$ , on a

$$\varphi_{2\lambda}^{2h} = \varphi_{\lambda}^{2h} = 2\varphi_{2h-1}^{2h-1} \quad (h = 1, \dots, 2).$$

(1) La somme  $\sum_0^r (-1)^i \binom{r}{i} i$  est ce que devient pour  $x = 1$  la dérivée du développement de  $(1-x)^r$ .

Donc  $\sigma_\alpha$ , qui conserve  $\varphi^{2h-1}$  et transforme  $\varphi^{2h}$  en  $\varphi_x^{2h}$ , conserve en particulier l'intersection des  $n-2$  quadriques  $\varphi^3 = 0, \dots, \varphi^n = 0$ .

Soit  $(y_1, \dots, y_n)$  un point de cette intersection, et d'abord  $y_1 \neq 0$ . Des  $n-2$  équations  $\varphi^3 = 0, \dots, \varphi^n = 0$ , on peut évidemment tirer successivement  $y_3, \dots, y_n$  qui seront des fonctions rationnelles de  $y_1, y_2$ . Je dis qu'on aura généralement

$$y_l = \frac{(-1)^{\frac{l-1}{2}}}{(l-1)!} \frac{y_2^{l-1}}{y_1^{l-2}} \quad \text{pour } l = 1, \dots, n.$$

Il suffit de montrer que cette solution vérifie  $\varphi^{2h-1} = 0$  et  $\varphi^{2h} = 0$ . Ces conditions s'écrivent, en faisant  $l = i+1$ ,

$$\sum_0^{2h-2} (-1)^i \binom{2h-2}{i} = 0, \quad \sum_0^{2h-1} (-1)^i \left(h - \frac{1}{2} - i\right) \binom{2h-1}{i} = 0.$$

La première de ces égalités est évidente. Dans la seconde, le changement de  $i$  en  $2h-1-i$  revient à remplacer les limites par  $h$  et  $2h-1$ . En ajoutant les deux expressions ainsi obtenues de cette seconde égalité, on obtient, après suppression de sommes nulles,

$$\sum_0^{2h-1} (-1)^i \binom{2h-1}{i} i = 0,$$

identité déjà rencontrée.

Regardons maintenant les variables comme homogènes. Les points  $(1, y_2, \dots, y_n)$  communs à  $\varphi^3 = 0, \dots, \varphi^n = 0$  forment avec le point  $(0, 0, \dots, 0, 1)$  une « courbe »  $s$  définie par les équations

$$\varphi^h = \sigma_3 z^l, \quad z \text{ parcourant } \mathbb{C}_m.$$

Si  $y_1 = 0$ , les équations  $\varphi^{2h+i} = 0$  ( $h = 1, \dots, v$ ) donnent successivement  $y_2 = 0, y_3 = 0, \dots, y_{v+1} = 0$ , et il est clair que les points  $(y_1, \dots, y_n)$  où  $y_1, \dots, y_{v+1}$  sont nuls, annulent *tous les*  $\varphi^i$ . Ils forment une « génératrice »  $\bar{s}$  commune à toutes ces quadriques. L'intersection des  $n-2$  quadriques  $\varphi^3 = 0, \dots, \varphi^n = 0$  (où les  $y_i$  sont regardés comme homogènes) se compose de  $s$  et de  $\bar{s}$ .

On voit que  $\bar{s} = \bar{s}_\infty$  coupe  $s$  en l'unique point  $z = \infty$ .

On vérifie de suite que  $\sigma_x, \mu_m$  et  $\gamma_0$  opèrent sur les points  $z \left( = \frac{y_2}{y_1} \right)$

de  $s$  les substitutions respectives  $z + \alpha, i_m z, \frac{-1}{z}$ . Donc  $\mathcal{N}$  conserve  $s$ , et son action sur les  $p^m + 1$  points de  $s$  est semblable à  $\mathcal{L}(2, p^m)$ .

Le diviseur  $\Phi$  de  $\mathcal{N}$ , qui fixe le point  $z = \infty$ , conserve  $\bar{\epsilon}_\infty$ . Toute substitution de  $\mathcal{N}$  qui transforme  $\infty$  en  $\alpha$  est dans  $\Phi s_\alpha$ ,  $s_\alpha$  étant l'une d'elles et toutes ces substitutions transforment  $\bar{\epsilon}_\infty$  en une génératrice  $\bar{\epsilon}_\alpha$  coupant  $s$  en l'unique point  $z = \alpha$ . Ainsi  $\gamma_0$  change  $\bar{\epsilon}_\infty$  en  $\bar{\epsilon}_0$  dont les équations sont  $y_{p-1} = \dots = y_0 = 0$ . On voit que  $\bar{\epsilon}_\infty$  et  $\bar{\epsilon}_0$  n'ont aucun point commun. Donc,  $\mathcal{N}$  changeant deux points distincts quelconques  $\alpha, \beta$  en  $0$  et  $\infty$ ,  $\bar{\epsilon}_\alpha$  et  $\bar{\epsilon}_\beta$  n'ont aucun point commun. Chaque  $\bar{\epsilon}_z$  contenant  $\frac{p^{2v}-1}{p^m-1}$  points (à coordonnées dans  $\mathcal{E}_m$ ), le système des  $p^m + 1$   $\bar{\epsilon}_z$  en contient  $\frac{(p^{2v}-1)(p^m+1)}{p^m-1}$ . Pour  $v > 1$ , ce nombre est moindre que celui  $\frac{p^{2v}-1}{p^m-1}$  des points de  $a = 0$  dans  $\mathcal{E}_m$  (II, 17).

52. *Considérons le cas  $n = 5$ . On a alors ( $p$  est ici  $\geq 5$ )*

$$\sigma_x = U_{20x} U_{10, \frac{x^2}{2}} V_{12, -x} U_{12, \frac{x^2}{6}},$$

$$\rho_m = m_{1, \frac{1}{6}} m_{2, \frac{1}{6}}, \quad \gamma_0 = t_{12} m_{1, \frac{1}{24}} m_{2, \frac{1}{6}}$$

et  $s$  est ici définie par les équations

$$(1) \quad \frac{x^2}{y_1} = z, \quad \frac{x}{y_1} = -\frac{z^2}{2}, \quad \frac{x^2}{y_1} = -\frac{z^3}{6}, \quad \frac{x^3}{y_1} = \frac{z^4}{24}.$$

D'après la correspondance des générateurs de  $B(5, \pi)$  et  $\mathcal{G}(4, \pi)$  indiquée dans I, 45 (dont je garderai ici les notations, en y faisant  $\gamma = c = \frac{1}{2}$ ), les substitutions répondant à  $\sigma_x, \rho_m, \gamma_0$  dans  $\mathcal{G}(4, \pi)$  sont respectivement, en fonction des générateurs de  $\mathcal{G}(4, \pi)$ ,

$$\sigma_x = U_{12x} V_{12, \frac{x^2}{2}} V_{2, x} U_{1, \frac{x^2}{6}},$$

$$\rho_m = m_{1, \frac{1}{6}} m_{2, \frac{1}{6}}, \quad \gamma_0 = \tau_1 \tau_2 m_{1, \frac{1}{6}} m_{2, \frac{1}{6}}$$

et je désignerai par  $\mathcal{N}_\pi^5$  le diviseur de  $\mathcal{G}(4, \pi)$  correspondant à  $\mathcal{N}_\pi^5$  de  $Q(5, \pi^2)$ .

La droite  $\mathcal{Q}_2$  dont le point courant est, en coordonnées homogènes,  $(\xi_1, \eta_1, \xi_2, \eta_2)$ , et dont les coordonnées  $Z_{ik}$  sont liées par (1) et par  $x_3 = 1$  (cf. I, 45) est

$$\frac{\xi_1}{\eta_2} = \frac{1}{3} - \frac{z^2}{6} \frac{\xi_2}{\eta_2} - \frac{z^3}{3}, \quad \frac{\eta_1}{\eta_2} = \frac{z}{3} \frac{\xi_2}{\eta_2} - \frac{z}{3^2}.$$

Appelons *enveloppe de  $\mathcal{Q}_2$*  la courbe  $s'$  déterminée de la même manière que dans le champ des nombres réels et complexes ( $\mathcal{Q}_2$  coupe ici encore  $s'$  en deux points confondus). Les équations de  $s'$  sont ici

$$(2) \quad \frac{\xi_1}{\eta_2} = \frac{z}{3}, \quad \frac{\eta_1}{\eta_2} = \frac{z}{z^2}, \quad \frac{\xi_2}{\eta_2} = \frac{z}{z}.$$

ou, en éliminant  $z$  entre la première équation et chacune des deux autres,

$$(3) \quad \frac{\xi_2}{\eta_2} = \frac{3}{z} \frac{\eta_2}{\xi_1}, \quad \frac{\eta_1}{\eta_2} = \frac{z}{9} \left( \frac{\eta_2}{\xi_1} \right)^2.$$

En remplaçant la seconde équation (3) par le quotient de ces deux équations, on voit que  $s'$  est la cubique gauche intersection des deux quadriques

$$(4) \quad 3\xi_1\xi_2 - 3\eta_2^2, \quad 3\xi_1\eta_1 - \xi_2\eta_2.$$

admettant la génératrice commune  $\xi_1 = \eta_2 = 0$ . Or  $\mathcal{X}_0^0$  transforme  $s'$  en elle-même (1). Quand on prend  $s'$  sous la forme (2),  $\sigma_x$ ,  $\mu_m$ ,  $\gamma_0'$  opèrent sur  $z$  ( $= \frac{3\eta_2}{\xi_2}$ ) les substitutions respectives  $\frac{z+\alpha}{z}$ ,  $\frac{z-1}{z}$ ,  $\gamma_m^2 z$ .

Soient  $\mathcal{X}_0^0$ ,  $\sigma_x$ ,  $\mu_m$ ,  $\gamma_0'$ ,  $s''$  les transformées de  $\mathcal{X}_0^0$ ,  $\sigma_x$ ,  $\mu_m$ ,  $\gamma_0'$ ,  $s'$  par la

(1) En divisant la première équation (4) par la seconde [ou en éliminant  $z$  entre les deux dernières équations (3)], on obtient  $3\eta_1\eta_2 = \xi_2^2$ . C'est une nouvelle quadrique passant par  $s'$  et ayant avec chacune des quadriques (4) une génératrice commune. En transformant (4) par  $\sigma_x$ , on obtient des équations où les coefficients des puissances de  $\alpha$  sont nuls, soit identiquement, soit d'après les équations des trois quadriques. (Cf. LIE, *Theorie der Transformationsgruppen*, t. III, p. 183-190.)

substitution  $\tau_3^{-1}$  de  $\mathcal{G}(4, \pi)$  [qui répond à  $R_{1,2}^{-1} = d_2 T_{1,2}$  de  $B(5, \pi)$ ].

On aura

$$\sigma_x^{-1} = V_{1,2,-x} U_{1,2,\frac{x^2}{2}} U_{1,-\frac{x^2}{3}} U_{2,x} = \begin{vmatrix} \eta_1 & \eta_1 \\ \eta_2 & \alpha\eta_1 + \eta_2 \\ \xi_2 & \frac{\alpha^2}{2}\eta_1 - \alpha\eta_2 + \xi_2 \\ \xi_1 & \frac{\alpha^3}{6}\eta_1 + \frac{\alpha^2}{2}\eta_2 - \alpha\xi_2 + \xi_1 \end{vmatrix},$$

$$\mu_m^x = m_{1,1}^{-1} m_{2,1}, \quad \gamma_0^x = \tau_1 m_{1,1} m_{2,2} \tau_2,$$

et les équations de  $S''$  sont

$$3\xi_1 \eta_2 + 2\xi_2^2 = 0, \quad 3\xi_1 \eta_1 + \xi_2 \eta_2 = 0,$$

ou

$$\frac{\eta_2}{\xi_2} = -\frac{2}{3} \frac{\xi_2}{\xi_1}, \quad \frac{\eta_1}{\xi_2} = \frac{2}{9} \left( \frac{\xi_2}{\xi_1} \right)^2.$$

Si  $-1$  est non carré,  $\sigma_x^{-1}$  est la substitution  $\sigma_x^{(-1)}$  du n° 7, et est transformée en  $\sigma_x$  par la substitution de  $A'$  qui multiplie  $\eta_1$  et  $\eta_2$  par  $-1$  sans altérer les  $\xi$ .

Si  $-1$  est carré  $= \rho^2$ ,  $\sigma_x^{-1}$  est transformée en  $\sigma_x$  par  $m_{1,\rho} m_{2,\rho}$ .

**55.** Supposons maintenant, pour simplifier l'écriture, que  $p^m = \pi$ . Soient  $A_k, A_k^0, B_k$  les diviseurs respectifs de  $A, A^0, B$  qui laissent les variables  $x_i, y_1, \dots, x_k, y_k$  inaltérées, et  $X_k (\subseteq A_k^0), X_k^0 (\subseteq B_k), \sigma_{(k)\alpha}, \mu_{(k)}, \gamma_k, \Theta_k, \beta_{(k)}, \varpi_k$  les actions respectives de  $X, X^0, \sigma_\alpha, \mu, \gamma, \Theta, \beta, \varpi$  sur les variables autres que  $x_i, y_1, \dots, x_k, y_k$  quand on regarde, dans cette action,  $x_i, y_1, \dots, x_k, y_k$  comme nuls, c'est-à-dire l'action de ces groupes sur les points de la multiplicité  $x_i = y_1 = \dots = x_k = y_k = 0$ . On va voir que  $\{X^0, X_1^0, \dots, X_{n-1}^0\} = B$  (en entendant par là, si  $v = 1$ , que  $X^0 = B$ ).

Il est clair que  $\sigma_{(i)x}^{-1} \sigma_\alpha$  remplace  $y_k$  par  $y_k + \sigma_{\alpha k i} y_i$  pour  $k = 2, \dots, n-1$ , c'est-à-dire qu'elle opère sur  $y_2, \dots, y_{n-1}$  comme

$$\chi_x = U_{10, -\sigma_{\alpha, v+1}} \prod_{j=2}^v V_{1j, -\sigma_{\alpha j}} U_{1j, -\sigma_{\alpha, n+1-j}}$$

(les  $V_{ij}$  et les  $U_{ij}$  sont permutables). Donc  $\chi_x^{-1} \sigma_{(i)x}^{-1} \sigma_\alpha$  laisse  $y_1,$



$\gamma_2, \dots, \gamma_{n-1}$  inaltérés, et comme elle conserve  $a$ , elle laisse aussi  $\gamma_n$  inaltéré. Donc elle se réduit à  $\mathbf{1}$ , et  $\sigma_\alpha = \sigma_{(1)\alpha} \chi_\alpha^{(1)}$ .

Le groupe  $Z = \langle X^0, B_i \rangle$  contient  $\chi_\alpha$ . Or, pour  $k \geq 3$ ,  $V_{2k\lambda}$  transforme  $V_{12\mu}$  en  $V_{12\mu} V_{1k, -\lambda\mu}$ ,  $U_{1k\mu}$  en  $U_{1k\mu} U_{12, \lambda\mu}$ , et est permutable aux autres  $V_{1j}$ ,  $U_{1j}$  ( $j \geq 0$ ). Donc, pour un choix convenable de  $\lambda$ ,  $V_{23}^{-1} \chi_\alpha V_{23\lambda}$  est une substitution de même forme que  $\chi_\alpha$ , contenue dans  $Z$ , mais où ne figurera plus  $V_{13}$ . A l'aide de  $V_{24}, \dots, V_{2\nu}$ , on fera de même disparaître successivement  $V_{14}, \dots, V_{1\nu}$ . A l'aide de  $U_{23\lambda}$ , qui transforme  $V_{12\mu}$  en  $V_{12\mu} U_{13, -\lambda\mu}$ , et est permutable aux autres  $U_{1j}$ , on fera disparaître  $U_{13}$ . A l'aide de  $U_{24}, \dots, U_{2\nu}$ , on fera disparaître  $U_{14}, \dots, U_{1\nu}$ . Donc  $Z$  contient une substitution de la forme  $V_{12\alpha} U_{12} U_{10}$ . A l'aide de  $U_{02\lambda}$ , qui transforme (pour  $c = \frac{1}{2}$ )  $V_{12\alpha}$  en  $V_{12\alpha} U_{13, -\frac{\alpha\lambda}{2}} U_{10, \alpha\lambda}$ ,  $U_{10\mu}$  en  $U_{12, -\lambda\mu} U_{10\mu}$ , et est permutable à  $U_{12}$ , on peut faire disparaître  $U_{10}$ . Donc  $Z$  contient une substitution  $V_{12\alpha} U_{12\lambda}$ , et de même sa transformée  $V_{12, \alpha\mu} U_{12, \frac{\lambda}{\mu}}$  par  $m_{2,\mu}^{-1} m_{3,\mu}^{-1}$ , qui est dans  $B_i$  [I, 29, (29)], donc aussi le produit  $\prod_{i=1}^3 V_{12, \alpha\mu_i} U_{12, \frac{\lambda}{\mu_i}}^{\mu_1, \mu_2}$  et  $\mu_3$ , étant trois valeurs arbitraires de  $\mu$ . Or, en supposant d'abord  $p \geq 5$ , on peut résoudre les deux équations  $\sum_1^3 \mu_i = \xi$ ,  $\sum_1^3 \frac{1}{\mu_i} = 0$ ,  $\xi$  étant arbitraire, en prenant  $\mu_1 = -\frac{\xi}{3}$ ,  $\mu_2 = \mu_3 = \frac{2\xi}{3}$ . Donc  $Z$  contient  $V_{12, \alpha\xi}$ , c'est-à-dire toutes les  $V_{12}$ .

En transformant les  $V_{12}$  par  $d_k T_{2k}$  ( $k \geq 3$ ; cette opération est inutile si  $n = 5$ ), qui est dans  $B_i$  (I, 28), on obtient toutes les  $V_{1k}$ . En les transformant par  $\gamma = \Theta\beta$  ( $\beta$  est un produit de  $m_i$ ), on obtient toutes les  $V_{k1}$ . En transformant les  $V_{1k}$  et les  $V_{k1}$  par  $\gamma_i = \Theta_i \beta_{(i)}$ , on obtient toutes les  $U_{1k}$ ,  $W_{1k}$ . En transformant les  $U_{1k}$  par les  $V_{0k}$  et les  $W_{k0}$ , on

(1) En posant de même

$$\chi_{(k)\alpha} = U_{k+1, 0, -\sigma_{\alpha, \nu+1, k-1}} \prod_{j=k+2}^{\nu} V_{k-1, j, -\sigma_{\alpha, j, k-1}} U_{k-1, j, \sigma_{\alpha, n-1-j, k-1}}$$

$$\chi^{(0)\alpha} = \chi_\alpha,$$

on a

$$\sigma_{(1)\alpha} = \sigma_{(2)\alpha} \chi_{(1)\alpha}, \dots, \sigma_{(k)\alpha} = \sigma_{(k+1)\alpha} \chi_{(k)\alpha} \quad (k \leq \nu - 2), \dots, \sigma_{(\nu-1)\alpha} = U_{0\nu, \sigma_{\alpha, \nu+1, \nu}},$$

d'où l'expression de  $\sigma_\alpha$  par les  $U$ ,  $V$ .

obtient les  $U_{k_0}$  et les  $V_{0,k}$  (I, 29). Donc  $Z$  contient  $B$ . Or  $Z$  est  $\leq B$ .  
 Donc  $Z = \{X_0, B_1\} = B$ .

Donc, si  $p \geq 5$ ,  $\{X^0, X_1^0, \dots, X_{k-1}^0, B_k\} = B$ , et, comme

$$B_{v-1} = X_{v-1}^0 \quad \left[ X_{v-1}^0 \text{ et } B_{v-1} \cong B(3, \pi) \text{ ont l'ordre } \frac{\pi(\pi^2-1)}{3} \right],$$

on a

$$\{X^0, X_1^0, \dots, X_{v-1}^0\} = B.$$

Si  $p = 3$ ,  $n$ , qui est  $\leq p$  et impair, est égal à 3. Or  $B$  est alors isomorphe à  $v(2, \pi)$ . Donc  $B = X_0$ .

54. Pour  $n \geq 7$ , on a  $\{X^0, X_1^0, \dots, X_{v-2}^0\} = B$ .

En effet, considérons d'abord le cas  $n = 7$ . Le groupe  $\{X, X_1\}$  contient

$$Z_x = V_{10, -\frac{x^2}{6}} V_{12, -x} U_{12, -\frac{x^2}{120}} V_{13, \frac{x^2}{2}} U_{13, -\frac{x^2}{24}}$$

donc aussi

$$Z_x Z_{-x} = V_{13, x^2} U_{13, \dots, \frac{x^2}{12}} = s_x.$$

et

$$s_{x_1} s_{x_1'} = V_{13, \lambda} U_{13, \mu},$$

$$\lambda = x_1^2 + x_2^2, \quad \mu = -\frac{1}{12} (x_1^2 + x_2^2) = -\frac{1}{12} (\lambda^2 - 2\lambda x_1^2 + x_1^4).$$

$\alpha_1$  et  $\alpha_2$  sont  $\neq 0$ . Mais on peut supposer  $\lambda$  quelconque dans  $\mathcal{E}$ . Car si  $\lambda$  est non carré,  $\alpha_1$  et  $\alpha_2$  sont  $\neq 0$  dans toutes les solutions  $(\alpha_1, \alpha_2)$  de l'équation  $\alpha_1^2 + \alpha_2^2 = \lambda$ , et si  $\lambda$  est carré, le nombre total des solutions est  $\pi \pm 1 \geq 6$  (E., 44) ( $p$  est  $\geq n$ ), celui des solutions où  $\alpha_1, \alpha_2 = 0$  étant évidemment 4.

Or, soient  $\alpha_1', \alpha_2'$  des déterminations de  $\alpha$  analogues à  $\alpha_1, \alpha_2$  et  $\lambda', \mu'$  les déterminations correspondantes de  $\lambda, \mu$ . Supposons que  $\lambda' = -\lambda$ ,  $\lambda$  étant tel que

$$\mu + \mu' = -\frac{1}{6} [\lambda^2 - \lambda(\alpha_1^2 - \alpha_2^2) + \alpha_1^4 + \alpha_2^4]$$

soit  $\neq 0$ . On a alors

$$s_{\alpha_1} s_{\alpha_1'} s_{\alpha_2} s_{\alpha_2'} = V_{13, \lambda + \lambda'} U_{13, \mu + \mu'} = U_{13, \mu + \mu'}.$$

Or  $\{X, X_1\}$  contient

$$\sigma_{(1)x} = U_{30, x} U_{10, -x} V_{23, -x} U_{\dots, -\frac{x^2}{6}}$$

donc aussi (I, 29)

$$\sigma_{(0)\alpha}^{-1} U_{13, \mu+\mu'} \sigma_{(0)\alpha} U_{13, \mu+\mu'}^{-1} = U_{13, \mu+\mu'},$$

donc toutes les  $U_{12}$ , donc aussi leurs transformées par  $\gamma_0$ , qui sont les  $W_{12}$ , donc aussi  $W_{12}$  (I, 40), que  $\gamma_0 \gamma_1 (= m_{13}, t_1)$  transforme en  $V_{12}$ . Donc  $\{X^0, X_1^0\}$  contient  $B_{12}$ , donc aussi

$$\sigma_{(0)\alpha}^{-1} V_{12\lambda} \sigma_{(0)\alpha} = V_{12\lambda} U_{12, \frac{\lambda\alpha^2}{5} - \frac{\lambda\alpha^2}{2}} V_{13, \lambda\alpha} U_{13, -\frac{\lambda\alpha^2}{6}} U_{10, \lambda\alpha},$$

donc aussi  $V_{13, \lambda\alpha} U_{13, -\frac{\lambda\alpha^2}{6}} U_{10, \lambda\alpha}$ , ou, en écrivant  $\lambda$  pour  $\lambda\alpha$ , toutes les substitutions  $V_{13\lambda} U_{13, -\frac{\lambda\alpha^2}{6}} U_{10\lambda} = s'_\alpha$ , et  $s'_\alpha, s'_{\alpha_1}, s'_{\alpha_2}, s'_{\alpha_3}$ ,  $\alpha_1, \alpha_2, \alpha_3$  étant quelconques  $\neq 0$ . Or, on peut choisir les  $\alpha_i$  de manière que  $\sum_1^3 \alpha_i^3 = 0$  (1), et on voit alors que  $\{X^0, X_1^0\}$  contient toutes les  $V_{13\lambda} U_{10\lambda}$ . En les multipliant par des  $s'_\alpha^{-1}$ , on voit que  $\{X^0, X_1^0\}$  contient toutes les  $U_{13, \frac{\lambda\alpha^2}{6}}$ , c'est-à-dire toutes les  $U_{13}$ , que  $\gamma_0$  transforme en  $W_{13}$ , donc  $W_{13}$ , que  $\gamma_0 \gamma_1$  transforme en  $V_{13}$ . Donc  $\{X^0, X_1^0\}$  contient  $B_{13}$ . Donc  $\{X^0, X_1^0\}$ , contenant les  $s'_\alpha$ , contient les  $U_{10}$ , que  $\gamma_0$  transforme en  $V_{01}$ . Donc  $\{X^0, X_1^0\}$  contient  $B_{10}, B_{12}$  et  $B_{13}$ . Donc  $\{X^0, X_1^0\} = B$ .

En partant, pour  $n \geq 7$ , de la formule  $\{X^0, B_1\} = B$ , on voit alors par récurrence que  $\{X^0, X_1^0, \dots, X_{n-2}^0\} = B$ .

(1) L'équation  $\sum_1^3 \alpha_i^3 = 0$  a toujours des solutions où  $\alpha_1, \alpha_2$  et  $\alpha_3$  sont  $\neq 0$ . Car le nombre total des solutions est  $\pi^2$ , et celui des solutions où  $\alpha_1 = 0$  est au plus  $2\pi - 1$  (E., 44). Il y a donc au plus  $3(2\pi - 1)$  solutions où un des  $\alpha_i$  est nul. Or, la condition  $\pi^2 > 3(2\pi - 1)$  est toujours remplie pour  $p \geq 7$ .