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 9e série, tome 5 (1926), p. 67-124.

<http://www.numdam.org/item?id=JMPA_1926_9_5__67_0>

Sur les diviseurs de certains groupes galoisiens;

PAR J.-A. DE SÉGUIER.

Lorsqu'on cherche les diviseurs d'un groupe linéaire dans un champ galoisien $\mathfrak{S}$ d'ordre $\pi = p^\kappa$ (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 $\mathfrak{O}(2, p^m)$ 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 (¹).

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) (²) dont je rappellerai seulement quelques-unes.

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

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

(²) Au nº **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 $\mathfrak{B}(n, \pi)$, mais ne l'est pas dans $\mathcal{G}(2\nu, \pi)$. 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 a 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 a à un facteur près, par $\mathcal{A}(n, \pi)$ ce que devient A quand on regarde les variables comme homogènes.

Je supposerai a de l'une des formes suivantes :

1° $$\begin{cases} \Sigma_1^\nu (x_i\bar y_i - y_i\bar x_i) + \eta\omega x\bar x \ (^1), & \eta = 0 \text{ ou } 1, \\ \omega = \upsilon - \bar\upsilon, & \upsilon \text{ étant un élément définissant de } \mathfrak{S}' \end{cases}$$

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

2° $$\omega\left[\frac{1}{2}\Sigma_1^\nu (x_i\bar y_i + y_i\bar x_i) + \eta c x\bar x\right]$$

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

3° $$\begin{cases} \Sigma_1^\nu (x_i y_i' - y_i x_i'), \\ \text{les } x_i', y_i' \text{ étant cogrédients aux } x_i, y_i \end{cases}$$

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

4° $$\begin{cases} \Sigma_1^\nu x_i y_i + \psi(x, y), & \psi(x, y) = cx^2 + bxy + c'y^2, \\ \psi \text{ pouvant être réductible dans } \mathfrak{S} \end{cases}$$

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

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

I.

1. Rangeons les variables dans l'ordre $y_1, \dots, y_\nu, y, x, x_\nu, x_{\nu-1}, \dots, x_1$, 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 φ_{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 $\mathfrak{S}'$.

$\varphi_{r+2,2}, \ldots, \varphi_{n,n-r}$; $r^{\text{ième}}$ *sous-transversale* la rangée (parallèle à la transversale) formée des φ_{ik} où $i+k=n+r+1$, c'est-à-dire la suite d'éléments $\varphi_{n,r+1}, \varphi_{n-1,r+2}, \ldots, \varphi_{r+1,n}$. Supposons maintenant φ dans le groupe sylowien **P** défini précédemment (*G.*, **15**, **23**, **42**). Alors les φ_{ik} situés *au-dessus* de la diagonale sont nuls, et ceux de la diagonale égaux à 1. Les φ_{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 o ou à 1, et l'on a vu (*loc. cit.*) qu'on peut les choisir arbitrairement, dans $\mathfrak{S}'$ si $\mathbf{A} = \mathrm{H}$ ou $\overline{\mathrm{H}}$, dans $\mathfrak{S}$ si $\mathbf{A} = \mathrm{G}$ ou Q; les φ_{ik} de la transversale situés *au-dessous* de la diagonale sont les α'_{ii} de *G.*, **15**, **23**, **42**, et l'on a vu qu'on peut les choisir arbitrairement dans $\mathfrak{S}$ si $\mathrm{A} = \mathrm{H}$, $\overline{\mathrm{H}}$ ou G, mais qu'ils sont déterminés si $\mathrm{A} = \mathrm{Q}$. Une fois déterminés les φ_{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 **P** dont les substitutions $\neq 1$ n'ont qu'une suite canonique. Je dirai qu'une telle substitution est *irréductible*, et je supposerai $p \geqq n$, en sorte que toute substitution irréductible de **P** soit d'ordre p (*S.*, **10**). Soit $\sigma = |y_i, \Sigma_1^i \sigma_{ik} y_k| (\sigma_{ii} = 1)$ une s_p irréductible de **P**. Pour que le premier diviseur élémentaire $\neq 1$ de $\sigma - s\varepsilon$ (ε étant la matrice unité d'ordre n) soit $(s-1)^n$ (cf. *S.*, **5**), 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 $\sigma_{i,i-1}$ ($i = 2, \ldots, n$) soient $\neq$ o. *Si donc* $\mathrm{A} = \mathrm{Q}$, *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 $\varpi = \Sigma_1^{p^m} \sigma^{(\alpha)}$ un diviseur de **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 $i = r+1, r+2, \ldots$ qu'on détermine les éléments de la $r^{\text{ième}}$ sous-transversale ($r > 0$) situés au-dessous de la diagonale : ce sont les $\varphi_{n-i+r+1,i}$ $\Big($la valeur maxima de i est le plus grand entier tel que $n-i+r+1$, soit $\geqq i+1$, c'est-à-dire le plus grand entier $\leqq \dfrac{n+r}{2}\Big)$. La combinaison de chaque colonne avec elle-même détermine les éléments de la transversale dans la mesure où ils sont déterminés.

l'unité, et $\sigma^{(\alpha)} = (\sigma_{ik}^{(\alpha)})$. Si $\sigma^{(\alpha)}\sigma^{(\beta)} = \sigma^{(\gamma)}$, $\sigma_{ik}^{(\gamma)}$ est nul pour $i < k$, égal à 1 pour $i = k$, et à $\Sigma_k^i \sigma_{i\rho}^{(\beta)}\sigma_{\rho k}^{(\alpha)}$ 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* $\sigma^{(\alpha)}\sigma^{(\beta)} = 1$, $\sigma_{i,i-1}^{(\beta)} = -\sigma_{i,i-1}^{(\alpha)}$.

Donc 1° ϖ *est abélien*, car, la première sous-diagonale de

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

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

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

3° En désignant désormais par $\sigma_\alpha = (\sigma_{\alpha ik})$ la substitution de ϖ où $\sigma_{\alpha 21} = \alpha$, α parcourt un groupe additif de $\mathfrak{S}'$ (*E.*, 34) quand σ_α parcourt $\varpi = \Sigma\sigma_\alpha(\sigma_0 = 1)$. Or l'action du p. p. c. m. des V_{12}, V_{21} sur y_1 et y_2, est semblable à $L(2, \pi^2)$ si $A = H$ ou $\overline{H}$, et à $L(2, \pi)$ si $A = G$ ou Q (*G.*, **11, 40**). En transformant donc au besoin ϖ par ce p. p. c. m., *on peut supposer que* α *parcourt le champ* $\mathfrak{S}_m$ *d'ordre* p^m, m *divisant* $K = m\varkappa$ *si* $A = G$ *ou* Q, *et* $2K = m\varkappa'$ *si* $A = H$ *ou* $\overline{H}$.

Je poserai alors $\sigma_1 = \sigma = (\sigma_{ik})$. Comme $\sigma_\alpha\sigma_\beta = \sigma_{\alpha+\beta}$ (donc $\sigma_\alpha^{-1} = \sigma_{-\alpha}$), on voit que, dans l'isomorphisme de ϖ avec le groupe des substitutions $(z + \alpha)$ où α parcourt $\mathfrak{S}_m$, σ_α correspond à $z + \alpha$.

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

$$\Sigma_l^n \lambda_{k\rho}\sigma_{\alpha\rho l} = \Sigma_1^k \sigma_{\beta k\rho}\lambda_{\rho l}. \tag{1}$$

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

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

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

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

Donc $\dfrac{\lambda_1}{\lambda_2} = \dfrac{\lambda_2}{\lambda_3} = \ldots = \dfrac{\lambda_{n-1}}{\lambda_n}$, soit $= \rho$, ou $\lambda_k = \lambda_n\rho^{n-k}$.

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

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

Donc la multiplication λ_0 dont les multiplicateurs sont $\lambda_1, \ldots, \lambda_n$, est dans le p.p.c.m. **M** des m_i, et $\lambda_0^{-1}\lambda$, qui est dans A et a la forme des substitutions de **P**, est aussi dans **P**. Donc λ 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* $\mathfrak{S}$, *et n pair, c'est-à-dire si* $A = G$, ρ *est carré.*

Ainsi, en posant $\mu_0 = |y_k, \iota^k y_k|$, λ *est, quel que soit* A, *dans* $\{\mu_0\}\Gamma'$, *et, si* $A = G$, *dans* $\{\mu_0^2\}\Gamma'$.

Quel que soit A, μ_0 multiplie a par ι^{n+1} et est donc dans A'. Cherchons une similitude de multiplicateur $\xi_A = \xi$ telle que $[\xi^{-1}]\mu_0 = \mu_A = \mu$ ou, si $A = G$, μ^2 conserve a. ξ est évidemment dans $\mathfrak{S}'$. Posons $\xi = \iota'^{w}$, faisons $\iota = \iota'^{\pi+1}$, et désignons par w_0 le p.g.c.d. de w, $\pi^2 - 1$; l'ordre f de ξ sera $\frac{\pi^2-1}{w_0}$. Je désignerai encore par π' 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 $\mu = \Pi_1^\nu m_{i, \xi^{-1}\iota^{n+1-i}}$ est d'ordre $\pi - 1$.

Soit $n = 2\nu$. Alors $\mu = \Pi_1^\nu m_{i, \xi^{-1}\iota^{n+1-i}}$, et π' *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* $\overline{H}$. La condition $\xi^{\pi+1} = \iota^{n+1}$ donne $w = n + 1 + l(\pi - 1)$. *Déterminons l par la condition* $n + 1 - 2l = \frac{\pi+1}{2^t}$. On aura

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

$$w_0 = \frac{\pi+1}{2^t}\pi', \qquad f = 2^t \frac{\pi - 1}{\pi'}.$$

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

Soit $A = G$. La condition que μ^2 conserve a donne $\xi^4 = \iota^{2(n+1)}$

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

$$w_0 = \frac{\pi+1}{2} w', \qquad f = 2\frac{\pi-1}{\pi'}, \qquad s = 2, \qquad \mu^{\pi-1} = d \quad (^1).$$

Quel que soit A, μ est, comme μ_0, permutable à **P** (*G.*, **15**), et μ transforme **P** comme μ_0. Le p. g. c. d. de $\{\mu_A\} = M_A = M$, I′ est toujours $\{\mu^{\pi-1}\}$; car pour que μ^h soit dans I′, il faut et suffit que μ_0^h y soit, donc que $\iota^h = \iota^{2h} = \ldots = \iota^{nh}$, d'où $h \equiv 0 \bmod \pi - 1$.

Ainsi, en désignant par $\Omega\,(\geqq D)$ *le groupe des similitudes de* A, *par* Ω_0 *son groupe sylowien d'ordre pair, par* Δ *un groupe égal à* 1 *si* $n = 2\nu + 1$, *et à* Ω_0 *si* $n = 2\nu$, λ *est dans* **P**MΩ (*dans* P $\{\mu^2\}$ *si* A = G), *et le p. g. c. d. de* M, Ω (*qui est le groupe des similitudes de* **P**M) *est* Δ (^{2}).

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

---

(^{1}) Pour $\pi \equiv 3 \bmod 4$, on pourrait déterminer l de manière que $w' \equiv 0 \bmod 4$. Alors $w_0 = 2\pi'(\pi+1)$, $f = \frac{\pi-1}{2\pi'}$, $s = 1$, $\mu^{\pi-1} = 1$. 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 $\xi_H^{\pi+1} = \iota^{n+1} = \xi_G^2$, d'où $\mu_G^2 = \mu_H^{\pi+1}$. On remarquera que μ_G, qui multiplie l'invariant a de H par -1, n'est pas dans H. Mais, quelle que soit la racine $j = \iota^{h\frac{\pi-1}{2}}$ (h impair) de $j^{\pi+1} = -1$, $[j]\mu_G = \mu'$ est dans H, et $(j\xi_G)^{\pi+1} = \iota^{n+1} = \xi_H^{\pi+1}$.

Je dis de plus que $\{\mu'\}$ contient $\{\mu_H\}$. Il suffit de montrer que μ_H est une puissance de μ', c'est-à-dire qu'il y a un nombre α tel que

$$\xi_H^{-1}\iota^k = (j\,\xi_G^{-1}\iota^k)^\alpha \qquad (k = 1, \ldots, n).$$

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

$$\beta[h(\pi-1) - (n+1)(\pi+1)] + h + \frac{\pi+1}{2^t} \equiv 0 \qquad \bmod 2(\pi+1).$$

Or soient β_0 et γ_0 deux entiers vérifiant $\beta_0(\pi-1) + 1 = \gamma_0\frac{\pi+1}{2}$; γ_0 est néces-

$\iota^{r i}\varphi_{ik} = \varphi_{ik}\iota^{sk}\xi^{r-s}$. De là, pour $i = k$, $\iota^{i(r-s)} = \xi^{r-s}$. En faisant $i = 1, 2$, on voit que $\iota^{r-s} = 1$, d'où $r \equiv s \bmod \pi - 1$, et $\xi^{r-s} = 1$. Si donc $\varphi_{ik} \neq 0$ (alors k est $\leqq i \leqq n$), $i - k$ a la forme $f(\pi - 1)$, f étant entier. Mais $i - k$ est $\leqq n - 1 \leqq p - 1$. 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 φ est une u_1 ou une $\overline{u}_1$ (*G.*, **9**). Donc, n étant ici impair, $A = H$ ou $\overline{H}$. Alors, *en négligeant le cas* $A = \overline{H}$, *et en désignant par* $\{u_1\}$ *le p.p.c.m. des* u_1, *qui est le central de* **P**, *le normalisant de* M *dans* **PM** *est* $M\{u_1\}$, μ *étant permutable à chaque* u_1.

Soit plus généralement $\{\mu^g\}$ un diviseur de M d'ordre $q \bmod \Delta$: 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 μ^{ug} pour μ^g, ce qui n'altère pas q, que $g = \frac{\pi - 1}{q}$. Pour que $\{\mu^g\}$ soit permutable à φ, il faut que $\varphi\mu^g$ ait la forme $\mu^s\varphi$. Comme tout à l'heure, cela exige que $\xi^{g-s} = 1$, et, μ ayant l'ordre de ξ, $\mu^s = \mu^g$. Donc $\mu^{-g}\varphi\mu^g = \varphi$ ou $\varphi_{ik}\iota^{g(i-k)} = \varphi_{ik}$. Si donc $\varphi_{ik} \neq 0$, on a $i - k \equiv 0 \bmod q$. *Donc les* φ *permutables à* $\{\mu^g\}$ *sont celles où les* φ_{ik} *situés hors des sous-diagonales de rang* $\equiv 0 \bmod q$ *sont tous nuls, et elles sont permutables à* μ^g. *Elles forment* a priori *un groupe* Γ^g. *Soient* l *et* l' *les nombres de* φ_{ik} *où* $i - k = fq > 0$ (f *entier*) *qui, dans une*

---

sairement impair, et l'on peut supposer β_0 pair. En posant alors $\beta = \beta_0 + u\frac{\pi+1}{2^t}$, la congruence précédente revient à

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

toujours résoluble en u.

Pour que $\{\mu'\} = \{\mu_{11}\}$, il faut et suffit que μ' soit d'ordre $2^t(\pi - 1)$. Or, la première puissance de μ' qui soit dans Γ' 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* $h = \frac{\pi+1}{2^t}h'$, h' *étant impair.*

φ *quelconque, sont respectivement au-dessus de la transversale et dans la transversale. L'ordre de* Γ^g *est* $\pi^{2l+l'}$ *si* $A = H$, $\pi^{l+l'}$ *si* $A = G$, $\pi^{l'}$ *si* $A = Q$ (cela résulte des relations fondamentales). *Si donc* $q \geqq p - 1$, $\Gamma^g = 1$ ou $\{u_1\}$ (en négligeant le cas $A = \overline{H}$) *selon que* n *est* $> p$ *ou* $= p$. μ *est évidemment permutable à* Γ^g. *Donc le normalisant de* $\{\mu^g\}$ *dans* $\mathbf{PM}$ *est* $\Gamma^g M$.

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

4. Soit $\mu^g \varphi$, $\varphi = (\varphi_{ik})$ étant dans $\mathbf{P}$, une substitution de $\mathbf{PM}$ permutable à ϖ, et soit q (premier à p) son ordre mod $\mathbf{P}\Delta$. On voit par récurrence que $(\mu^g \varphi)^s \equiv \mu^{gs}$ mod $\mathbf{P}$. Donc μ^g est d'ordre q mod $\mathbf{P}\Delta$. Mais μ^{gq} est d'ordre premier à p. Donc μ^{gq} est dans Δ, et gq est le p. p. c. m. de g et de $\pi - 1$. Donc $gq = g\dfrac{\pi - 1}{e}$, 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 $ug' + vq = 1$, on peut supposer, en prenant au besoin $(\mu^g \varphi)^u$ pour $\mu^g \varphi$, *que* $g = \dfrac{\pi - 1}{q}$. C'est ce que je ferai désormais.

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

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, $[\mu^g \varphi]$ est dans $A(n - 2, \pi)$. Car on voit de suite (et mieux encore avec l'ordre ancien des variables) que $[\mu^g \varphi]$ vérifie les relations fondamentales exprimant qu'elle conserve $a - x_1 y_1$. 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 $z''_{ik} = \Sigma_k^i z'_{i\rho} z_{\rho k}$ pour $k \leqq i$, d'où $[z''] = [z][z']$.

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

$$\Sigma_{s=k}^{i} \zeta_{is} \varphi_{sk} = \Sigma_{s=k}^{i} \varphi'_{is} \iota^{g(s-k)} \zeta_{sk} \qquad (k = 1 \text{ ou } i = n). \tag{3}$$

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

Il suffit donc de prendre pour ζ 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 $r \equiv 0 \bmod q$).

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

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

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

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

Comme toute substitution de **P** transforme σ_α en une substitution $\sigma'_\chi = (\sigma'_{\chi ik})$ où $\sigma'_{\chi,k+1,k} = \sigma_{\chi,k+1,k}$, et par suite ϖ en un groupe ayant les mêmes propriétés, on voit qu'*en transformant au besoin ϖ par une substitution de* **P**, *on peut supposer que son normalisant dans* **PM** *contient une substitution de la forme $\mu^g \varphi$ ($gq = \pi - 1$, q étant donné) où φ est dans* **P** *et permutable à μ^g*. Alors, $(\mu^g \varphi)^q = \mu^{gq} \varphi^q$ étant permutable à φ, et μ^{gq} dans Δ, φ^q est permutable à ϖ. *Donc φ et μ^g sont permutables* à ϖ.

Supposons désormais q maximum, et ϖ déterminé comme il vient d'être dit. Soient $\mu^{g_i} \varphi_i$ ($i = 1, 2, \ldots$; $g_1 = g$; $\varphi_1 = \varphi$) les substitutions de A permutables à ϖ, $\mu^{g_i} \varphi_i$ étant d'ordre $q_i \bmod \mathbf{P}\Delta$. Alors $(\mu^g \varphi)^u (\mu^{g_i} \varphi_i)^v$ sera l'une d'elles, telle que $\mu^{g_k} \varphi_k$, et $g_k = ug + vg_i$. Or on peut choisir u et v de manière que g_k soit le p. g. c. d. de g, g_i. Soit $g = lg_k$, et $g_k = \frac{\pi - 1}{q_k} g'_k$, g'_k étant premier à q_k. On aura $lqg'_k = q_k$. 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 μ^{g_i} est permutable à ϖ. Donc φ_i est aussi permutable à ϖ. *Si donc ϖ' est le normalisant de ϖ dans* **P**, *le normalisant de ϖ dans* **PM**, *et par suite dans* A(**2**), *est* $\{\mu^g\}\varpi'$.

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

On verra que *q est toujours égal à* Θ.

3. *Supposons que m divise* K *et admettons que* $q = p^m - 1$. — Écrivons alors ι_m, μ_{0m}, $\xi_{mA} = \xi_m$, $\mu_{mA} = \mu_m$, $M_{mA} = M_m$ pour ι^g, μ_0^g, ξ_A^g, μ_A^g, $\{\mu_A^g\}$, désignons par $\mathfrak{S}_m$ le champ d'ordre p^m, et posons

$$\{\varpi, \mu_{mA}\} = \Phi_A = \Phi, \qquad \{\varpi, \mu_{mA}^2\} = \Phi_A^0 = \Phi^0.$$

Remarquons de suite que, si $A = Q$, $\mu_m = \Pi_1^\nu m_{i,(\nu+1-i)g}$, qui est toujours dans A^0, n'est pas toujours dans B (*cf. G.*, **59**). Il y est évidemment si g ou $\varkappa$ ($\equiv g$ mod 2) est pair. Supposons donc $\varkappa$ impair, et soit l un des nombres $1, \ldots, \nu$. Si ν est pair $= 2\rho$, $\nu + 1 - i$ prend des valeurs de parité différente pour $i = l$ et $i = \nu + 1 - l$. Donc μ_m est alors dans B toujours et seulement quand ρ est pair. Si ν est impair $= 2\rho + 1$, $\nu + 1 - i$ prend des valeurs de même parité pour $i = l$ et $i = \nu + 1 - l$. Donc μ_m est alors dans B toujours et seulement quand ρ est impair. *Ainsi, pour* $A = Q$, *μ_m est dans* B *toujours et seulement si $\varkappa$ est pair ou si* $\nu \equiv 0, 3$ mod 4.

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

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

(¹) Ici $K = m'\varkappa'$, et $\frac{1}{2}(p^{m'} + 1)$ est premier à $\frac{1}{2}(p^K - 1)$. Car tout facteur θ 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 β est un des nombres $1, \ldots, p-1 \bmod p$, l'élément de $\Delta\varpi$ qui répond à $z + \alpha\beta = (z+\alpha)^\beta$ est $\Delta\sigma_{\alpha\beta} = \Delta\sigma_\alpha^\beta$.

Φ *est défini par les équations de* ϖ *et de* M_m *jointes à* $\mu_m^{-1}\sigma_\alpha\mu_m = \sigma_{\alpha:m}$, σ_α *parcourant les générateurs de* ϖ *qu'on peut supposer être* $\sigma = \sigma_{:\frac{0}{m}}$, $\sigma_{:\frac{1}{m}}, \ldots, \sigma_{:\frac{m-1}{m}}$. D'une part, en effet, il résulte de ces équations que $\mu_m^{\pi-1}$ est permutable aux σ_α (*S.*, 73). D'autre part, Φ vérifie ces équations et contient Δ (*cf. E.*, 18, 19).

Φ^0 *est défini par les équations de* ϖ *et de* $\{\mu_m^2\}$ *jointes à* $\mu_m^{-2}\sigma_\alpha\mu_m^2 = \sigma_{\alpha:\frac{2}{m}}$ (*S.*, 73).

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

$$(4) \qquad (\alpha+\beta)^{i-k}\sigma_{ik} = \Sigma_{\rho=i}^{\rho=k}\alpha^{\rho-k}\beta^{i-\rho}\sigma_{i\rho}\sigma_{\rho k} \qquad (i \geqq k),$$

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 $i-1, i-2, \ldots, k+1$, en multipliant les égalités ainsi obtenues, et en posant $\sigma_{21}\sigma_{32}\ldots\sigma_{l,l-1} = s_l$ si $l > 1$, $s_1 = 1$, on obtient

$$(5) \qquad (i-k)!\,\sigma_{ik} = \frac{s_i}{s_k} \qquad (i \geqq k \geqq 1;\ 0! = 1).$$

Donc les σ_{ik} *sont complètement déterminés par les* $\sigma_{j,j-1}$, *et* $\neq 0$ *pour* $i \geqq k$. On voit d'ailleurs de suite que *l'expression* (5) *de* σ_{ik} *vérifie* (4) *quels que soient les* $\sigma_{j,j-1}$. Or, en transformant au besoin ϖ par des m_i, on peut donner à $\sigma_{21}, \sigma_{32}, \ldots, \sigma_{\nu,\nu-1}$ si $n = 2\nu$, et à $\sigma_{21}, \sigma_{32}, \ldots, \sigma_{\nu+1,\nu}$ 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* $\mathrm{H}(n, \pi)$. — Les relations fondamentales donnent

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

et

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

Si donc $n = 2\nu$, on peut, en transformant au besoin ϖ par une $\Pi_{i=1}^{\nu} m_{i\rho}$

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

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

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

et par suite

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

Ainsi, quand m divise K, ϖ *est complètement déterminé. Mais on ne sait pas encore si* ϖ *divise* A, *c'est-à-dire s'il conserve a*. Or, en posant

$$S_{\alpha\beta} = \Sigma_1^{\nu}\, \sigma_{n+1-i,\alpha}\, \dot{\sigma}_{i\beta}, \qquad S'_{\alpha\beta} = \Sigma_1^{\nu}\, \sigma_{i\alpha}\, \dot{\sigma}_{n+1-i,\beta};$$
$$T_{\alpha\beta} = S_{\alpha\beta} - S'_{\alpha\beta}, \qquad \tau_{\alpha\beta} = \omega\, \sigma_{\nu+1,\alpha}\, \dot{\sigma}_{\nu+1,\beta},$$

cette condition, formulée dans G, **1**, s'écrit

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

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

Soit d'abord $n = 2\nu$. Les seuls termes $\neq 0$ de $S_{\alpha\beta}$ sont ceux où $i \geqq \beta$ et $n + 1 - i \geqq \alpha$. 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 β est $\leqq \nu$ (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 α est $\leqq \nu$ (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 β (si $\beta \leqq \nu$) jusqu'au plus petit μ des deux nombres ν, $n + 1 - \alpha$, et dans $S'_{\alpha\beta}$, de α (si $\alpha \leqq \nu$) jusqu'au plus petit μ' des deux nombres ν, $n + 1 - \beta$. Si alors $B \leqq \nu$ et $\alpha > \nu$, on a $S'_{\alpha\beta} = 0$, $\mu = n + 1 - \alpha$, et, en posant $i = \beta + h$,

$$S_{\alpha\beta} = (-1)^{\nu-\beta} \Sigma_0^f \frac{(-1)^h}{h!\,(f-h)!} = \frac{(-1)^{\nu-\beta}}{f!}(1-1)^\nu = 0.$$

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

Si α et β sont $\leqq \nu$, 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 $T_{\alpha\beta} = (-1)^{\nu-\beta}\Sigma_0^f \frac{(-1)^h}{h!\,(f-h)!} = 0$.

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 α est $\neq \beta$ (donc α ou β est $> \nu$) et l'on a $T_{\alpha\beta} = \theta$, $\tau_{\alpha\beta} = 0$, 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 μ et μ' comme précédemment. Si alors β est $\leqq \nu$ et $\alpha > \nu + 1$, ou si $\alpha \leqq \nu$ et $\beta > \nu + 1$, on a encore $T_{\alpha\beta} = \tau_{\alpha\beta} = 0$. Si $\beta \leqq \nu$ et $\alpha \leqq \nu + 1$, ou si $\alpha \leqq \nu$ et $\beta \leqq \nu + 1$, 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 ϖ dive A, et q est effectivement égal à $p^m - 1$.

7. *Supposons maintenant que* $A = G(n, \pi)$. En transformant ϖ par une $\Pi_{i=1}^\nu m_{i\rho}$, ρ étant dans $\mathfrak{S}'$, on peut ramener $\sigma_{\nu+1,\nu}$ à 1, $\sigma_{21}, \ldots, \sigma_{\nu,\nu-1}$ restant égaux à 1. On reconnaît alors, comme dans le cas $A = H$, l'existence, *dans* $A(n, \pi^2)$ du diviseur $\Phi = \{\varpi, \mu_m\}$ qui est contenu dans **PM** (**P** ayant toujours le même sens). *Donc q est encore effectivement égal à* $p^m - 1$. *Si* $\varkappa$ *est pair,* μ^g *est dans* $\{\mu^2\}$ ($g \equiv \varkappa \bmod 2$), *et* Φ *divise* A. *Si* $\varkappa$ *est impair, le p. g. c. d. de* Φ, A *est* Φ^0.

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

en ϖ_N. *Donc* ϖ_N *divise* A. En posant alors $s^{-1}\sigma_\alpha s = \sigma_\alpha^{(N)} = (\sigma_{\alpha ik}^{(N)})$ et $\sigma_1^{(N)} = \sigma^{(N)}$, $\sigma_{1ik}^{(N)} = \sigma_{ik}^{(N)}$, 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 $\leqq \nu$, et $\sigma_{\alpha ik}^{N} = N\sigma_{\alpha ik} = N\alpha^{i-k}\sigma_{ik}$ si $i > \nu$ et $k \leqq \nu$. Comme d'ailleurs s est permutable à μ, on voit que, si $\iota_m^r = \alpha$, $\mu_m^{-r}\sigma_\beta^{(N)}\mu_m^r = s^{-1}\mu_m^{-r}\sigma_\beta\mu_m^r s = s^{-1}\sigma_{\alpha\beta}s = \sigma_{\alpha\beta}^{(N)}$.

Supposons qu'il y ait dans A une substitution $\lambda = (\lambda_{ik})$ transformant ϖ en ϖ_N. Il y aura dans $\lambda\varpi_N$ une substitution *transformant* M_m *en lui-même* (et toujours ϖ en ϖ_N). Prenons-la pour λ. On voit comme au n° **2** que λ est dans $\lambda_0\mathbf{P} = \mathbf{P}\lambda_0$, λ_0 étant un produit de m_i, donc permutable à μ_m. Or, n étant ici pair, donc $> p$, toute substitution de $\mathbf{P}$ permutable à M_m se réduit à 1 (**5**). *Donc* λ *coïncide avec* λ_0. Supposons que $\lambda^{-1}\sigma\lambda = \sigma_\alpha^{(N)}$ (en prenant pour λ une substitution de $\lambda\,|\,\mu_m^2\,|$, on peut remplacer α par un élément quelconque de $\mathfrak{S}_m$ ayant le même caractère quadratique dans $\mathfrak{S}_m$). 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 $k = 2, \ldots, \nu$ ou $k = \nu + 2, \ldots, n$, et $\lambda_{\nu+1} = N\alpha\lambda_\nu$. Comme $\lambda_{\nu+1}\lambda_\nu = 1$, on a $N\alpha = \lambda_\nu^{-2}$, et α *est non carré dans* $\mathfrak{S}$. Or α a la forme $\iota_m^r = \iota^{gr}$, et g a la parité de $\varkappa$.

Donc, si $\varkappa$ *est pair,* ϖ *et* ϖ_N *ne sont pas conjugués dans* A.

Supposons donc $\varkappa$ *impair,* α non carré et $\lambda = \sqrt{N\alpha}$. On aura $\lambda_i = \alpha^{i-\nu}\lambda_\nu$ pour $i = 1, \ldots, \nu - 1$, et la condition $\lambda_k = \alpha\lambda_{k-1}$ $(\nu + 2 \leqq k \leqq n)$ qui, en posant $k = n + 1 - i$ $(1 \leqq i \leqq \nu - 1)$, 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 $i \leqq \nu$) et, λ étant permutable à μ, $\lambda^{-1}\sigma_\beta\lambda = \sigma_{\alpha\beta}^{(N)}$.

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

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

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

et

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

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

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

Le groupe ainsi obtenu se déduit de celui obtenu pour $A=H(n, \pi)$ par le changement de variables qui consiste à remplacer y_i par ωy_i pour $i=1, \ldots, \nu$ sans altérer les x_i (ce qui change H en $\overline{H}$). 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 $i=1, \ldots, \nu$. Alors $\sigma_{i,i-1}=(-1)^i$ pour $i=1, \ldots, n$, et $s_l=(-1)^{2+3+\ldots+l}=(-1)^{\frac{(l-1)(l-2)}{2}}$.

Pour que ϖ conserve a, qui peut s'écrire $\frac{\omega}{2}\Sigma_1^n(y_k\dot y_{n+1-k}+\dot y_k y_{n+1-k})$, il faut et suffit que la somme $S_{\alpha\beta}=\Sigma_{k=1}^n\sigma_{k\alpha}\dot\sigma_{n+1-k,\beta}$ soit égale à o pour $\alpha+\beta\neq n+1$, et à 1 pour $\alpha+\beta=n+1$. Or, ici encore, si $\alpha+\beta$ est $>n+1$, $S_{\alpha\beta}=0$. Si $\alpha+\beta=n+1$, $S_{\alpha\beta}$ se réduit à 1. Si $\alpha+\beta<n+1$, il suffit de faire varier k de α à $n+1-\beta$ ou, en posant $k=\alpha+h$, de faire varier h de o à $f=n+1-\alpha-\beta$. On a alors

$$S_{\alpha\beta}=\Sigma_0^f\frac{1}{h!(f-h)!}\frac{s_{\alpha+h}}{s_\alpha}\frac{\dot s_{n+1-\alpha-h}}{\dot s_{n+1-\alpha-f}}.$$

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* $n=2\nu$, ϖ n'existe pas.

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

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

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

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

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

ou

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

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

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

On voit que, pour $h = 2$, $\dfrac{\varphi_{l+2,l+1}}{\sigma_{l+2,l+1}} = \dfrac{\varphi_{l+1,l}}{\sigma_{l+1,l}}$ est indépendant de l. Soit donc $\varphi_{l+1,l} = \theta_1\sigma_{l+1,l}$, et admettons que l'on ait, pour $\rho = 1, \ldots, h-2$, $\varphi_{l+\rho,l} = \theta_\rho\sigma_{l+\rho,l}$, θ_ρ ne dépendant pas de l ($\theta_0 = 1$). L'équation précédente donne alors, en remplaçant généralement σ_{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 $(h-1)!\,\dfrac{s_l}{s_{l+h}}$,

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

c'est-à-dire que $\varphi_{l+h-1,l} = \theta_{h-1}\sigma_{l+h-1,l}$, θ_{h-1} étant indépendant de l. Mais les θ_i (qui sont dans $\mathfrak{S}$ si $A = G$ ou Q) doivent satisfaire à la condition que φ conserve la même forme a que τ. D'après la vérification faite au n° **5**, cette condition équivaut, quel que soit A, à

$$(1)\qquad \Sigma_{h=0}^{f}(-1)^h\binom{f}{h}\theta_h\dot{\theta}_{f-h}=0 \qquad (\theta_0=1 \text{ pour } f=1,\ \ldots,\ n-1),$$

qui s'écrit encore :

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

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

si f est pair $=2\mu$,

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

Soit $A=H$, $\nu=\dot{\nu}$, et $\theta_f=\theta'_f+\nu\theta''_f$, θ'_f et θ''_f étant dans $\mathfrak{S}$. 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* ϖ' *est d'ordre* π^{n-1}.

Si $\theta_1=\theta_2=\ldots=\theta_{n-2}=0$, on a $\theta_{n-1}=(-1)\dot{\theta}_{n-1}$. Or, on vérifie de suite que $\dot{s}_n=(-1)^n s_n$. Donc $\varphi_{n1}=\frac{s_n\theta_{n-1}}{(n-1)!}=\dot{\varphi}_{n1}$. Donc φ est une u_1 (si $A=\overline{H}$ on trouverait une $\overline{u}_1$) arbitraire. Donc ϖ' contient $\{u_1\}$, ce qui devrait être, *a priori*, puisque $\{u_1\}$ est le central de **P** (*G.*, **15**).

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* ϖ' *est d'ordre* π^{ν}.

Supposons θ_1, θ_3, …, $\theta_{2\nu-3}$ nuls. *Si alors* $n=2\nu$ ($A=G$), φ est une u_1 arbitraire [ici encore le central de **P** est $\{u_1\}$ (*G.*, **23**)]. *Si* $n=2\nu+1$ ($A=Q$), $\theta_{2\nu-2}$ et $\theta_{2\nu}$ sont nuls, et φ est une U_{12} arbitraire, c'est-à-dire que φ parcourt le central de **P** (*G.*, **42**).

Plus généralement, d'après (3), si θ_1, …, θ_{μ} sont nuls, $\theta_{2\mu}=0$. Donc, si tous les θ_f d'indice impair $\leqq\mu$ sont nuls, $\theta_{2\mu}=0$. Pour que θ_1, …, θ_f soient nuls, il faut donc et il suffit que tous les θ_i d'indice impair $\geqq f$ soient nuls.

12. *Déterminons encore le normalisant* Φ' et Φ *dans* A. Soit s

une substitution de A permutable à Φ. s, étant évidemment permutable à ϖ, est dans $\{\mu_m\}\varpi'$ (**3**), et, en prenant pour s une substitution convenable de Φs, on peut supposer s dans ϖ'. s transforme μ_m en une substitution de la forme $\sigma_\alpha^{-1}\mu_m^h\sigma_\alpha$. Donc $s\sigma_\alpha^{-1}=\varphi=(\varphi_{ik})$ est dans ϖ' et permutable à $\{\mu_m\}$. Or, on a vu (**3**) qu'une telle substitution n'existe hors de Φ que si $n=p$ avec $m=1$ et $A=H$ ou $\overline{H}$, et qu'alors elle peut être quelconque dans $\{u_{1:1_m}\}$ si $A=H$ ou dans $\{\overline{u}_{1,\omega:_m}\}$ si $A=\overline{H}$.

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

13. *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 $\overline{H}$, 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 $\overline{H}$, et cherchons si Φ ou, pour $A=G$ avec $\varkappa\equiv 1 \bmod 2$, Φ^0 divise $A(n, p^{mk})$. Par construction ϖ divise $A(n, p^{mk})$, sauf peut-être si $A=H$ avec $n=2\nu+1$ ou si $A=\overline{H}$ avec $n=2\nu$, à cause de la présence de ω. On pourrait négliger ces deux cas comme sans intérêt. Mais, comme $\frac{K}{mk}$ est impair, le champ $\mathfrak{S}_{mk}$ d'ordre p^{mk} contient un non carré N de $\mathfrak{S}$. En supposant donc que $\upsilon^2=N$, υ définit à la fois $\mathfrak{S}'$ relativement à $\mathfrak{S}$ et le champ $\mathfrak{S}'_{mk}$ d'ordre p^{2mk} relativement à $\mathfrak{S}_{mk}$. Alors ω est dans $\mathfrak{S}'_{mk}$, et ϖ divise toujours $A(n, p^{mk})$.

Il suffit donc de considérer μ_m ou, si $A=G$ avec $\varkappa\equiv 1 \bmod 2$, μ_m^2. On voit de suite *que $A(2\nu+1, p^{mk})$ contient toujours Φ, et que $G(2\nu, p^{mk})$, qui contient toujours Φ^0, contient Φ toujours et seulement si k est pair* $\left(\text{pour qu'il contienne } \Phi, \text{ il faut et suffit que } \xi_m^{p^{mk}-1}=1,\right.$ $\left.\text{d'où } \frac{p^{mk}-1}{p^m-1}\equiv 0 \bmod 2\right)$.

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

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

$H(n, p^{mk})$ par ι_m^{n+1}, la condition que μ_m soit dans $H(n, p^{mk})$ revient à $\xi_m^{p^{mk}+1} = \iota_m^{n+1}$ (ξ_m est alors dans $\mathfrak{S}'_{mk}$).

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

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

Donc tout diviseur $H(n, p^{mk})$ *de* H *contient* Φ [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 ι_{km}, ι'_{km}, $\mu_{0,km}$, μ_{km}, ξ_{km} les éléments qui remplacent alors ι, ι', μ_{0m}, μ_m, ξ_m, en faisant $\iota_{km} = \iota^{\frac{\pi-1}{p^{km}-1}}$, $\iota'_{km} = \iota'^{\frac{\pi^2-1}{p^{2km}-1}}$.

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

Soit donc $n = 2\nu$. 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 Γ', il faut et suffit que

$$\iota_m^{u-1} = \iota_m^{2(u-1)} = \ldots = \iota^{n(u-1)},$$

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

Soit d'abord $A = H$. Alors $\frac{\varkappa}{k}$ 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

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

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

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

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

14. Cherchons maintenant dans $\mathcal{A}$ un diviseur $\mathcal{X}$ 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 $\overline{X}$ un diviseur de A contenant Ω (**2**) et tel que $\overline{X} \mid \Omega \equiv \mathcal{X}$. De la structure des $g_{p^m, p^m - 1}$ de $\mathcal{X}$ et de l'analyse précédente il résulte : 1° que m divise $K = m\varkappa$, et si $A = G$, que $\varkappa$ est pair (**7**); 2° qu'en transformant au besoin $\overline{X}$ par A ou, si $A = G$ par A′, on peut supposer $\Phi = \{\varpi, \mu_m\}$ contenu dans $\overline{X}$.

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

$$\gamma^2 = 1, \qquad (\gamma\sigma)^3 \equiv 1, \qquad \gamma^{-1}\mu_m\gamma \equiv \mu_m^{-1};$$

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

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

L'équation $[\gamma\sigma]^3 \equiv 1 \bmod \Omega$ s'écrit $\sigma\gamma\sigma = \gamma\sigma^{-1}\gamma[\rho]$, $[\rho]$ étant dans Ω. En prenant $[\rho]\gamma$ pour γ (c'est-à-dire en posant $\gamma = [\rho^{-1}]\gamma'$, et en effaçant l'accent), on peut supposer que $\rho = 1$. Je poserai alors $\{\Phi_\Lambda, \gamma\} = X_\Lambda = X$, $\{\Phi_\Lambda^0, \gamma\} = X_\Lambda^0 = X^0$, et je désignerai par

$$\mathcal{X}_\Lambda^0 = \mathcal{X}^0 \equiv \mathfrak{P}(2, p^m)$$

ce que devient X^0 quand on y regarde les variables comme homogènes. L'équation précédente s'écrit encore $(\sigma\gamma)^3 = [\zeta^2]$, ou, en désignant par $Y_i = \Sigma_l\, c_{il}\, y_l$, $Y'_i = \Sigma_l\, c'_{il}\, y_l$ 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 $\gamma^{-1}\mu_m\gamma \equiv \mu_m^{-1} \bmod \Omega$ s'écrit, en introduisant

$$[\zeta_m^{-2}\iota_m^{n+1}] = \delta, \qquad \gamma^{-1}\mu_m\gamma = [s]\delta\mu_m^{-1}.$$

Si $A = H$ avec $n = 2\nu$ et $\varkappa \equiv 1 \bmod 2$, δ est d'ordre 2^t et engendre Δ. Dans tous les autres cas $\delta = 1$. On voit que $[s]$ est dans Ω. L'équation précédente s'écrit $\mu_{0m}\gamma = [s\iota_m^{n+1}]\mu_{0m}^{-1}$, ou, en développant, $\gamma_{ik}\iota_m^k = s\iota_m^{n+1-i}\gamma_{ik}$.

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

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

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

d'où $cg = f\frac{\pi - 1}{2}$ 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

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

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

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

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

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

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

ou

$$|h| \leq 2\frac{n - 1}{p^m - 1} < 2\frac{p - 1}{p^m - 1}.$$

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

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

ou

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

Donc, si $i \leqq \nu$, *h est* $\leqq \frac{\nu - 1}{\nu}$, *d'où* $h = -1$; *et si* $i > n - \nu$, *h est* > -1, *d'où* $h = 1$. *Donc, sauf si* $i = \nu + 1$ *avec* $n = 2\nu + 1$, γ_{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 $i \leqq \nu$, $k = \nu + 1 - i$; pour $i > \nu$, $k = 3\nu + 1 - i$. Donc γ remplace y_i $(i \leqq \nu)$ par $\gamma_{i,\nu+1-i}\, y_{\nu+1-i}$ et y_j $(j > \nu) = x_{n+1-j} = x_l$ $(l = n + 1 - j \leqq \nu)$ par $\gamma_{j,3\nu+1-j}\, y_{3\nu+1-j}$.

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

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

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

$$Y_1 = \gamma_{1\nu} \Sigma_1^\nu (-1)^{l+1} \sigma_{\nu,\nu+1-l}\, \gamma_{\nu+1-l,l}\, y_l, \qquad Y'_1 = \gamma_{1\nu} \Sigma_1^\nu \sigma_{\nu l}\, y_l.$$

Donc

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

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

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

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

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

Dans ce qui suit, toute somme $\Sigma_i f(i)$ dont les limites ne sont pas indiquées, s'étend à toutes les valeurs de i pour lesquelles $f(i)$ est défini. En particulier $\binom{u}{v} = \frac{u(u-1)\ldots(u-v+1)}{v!}$, 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 $\geqq 0$, $\binom{-u}{v} = (-1)^v \binom{u+v-1}{v}$, 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 :

$$(5)\qquad s_{n-k}=\begin{cases}(-1)^k\dfrac{s_n}{s_{k+1}} & \text{si } k\leqq\nu-1\\[2mm] (-1)^{k+1}\dfrac{s_n}{\dot s_{k+1}} & \text{si } k\geqq\nu\end{cases}\qquad(\dot s_n=s_n).$$

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

$$(6)\qquad \begin{cases}\gamma_{i,\nu+1-i}=(-1)^{\nu+i}\dfrac{s_i}{s_{\nu+1-i}}\dfrac{(\nu-i)!}{(i-1)!}\\[2mm] \gamma_{\nu+1-i,i}=(-1)^{i+1}\dfrac{s_{\nu+1-i}}{s_i}\dfrac{(i-1)!}{(\nu-1)!}\end{cases}\qquad(i\leqq\nu),$$

$$(7)\qquad \begin{cases}\gamma_{j,3\nu+1-j}=(-1)^{\nu}\dfrac{s_j\dot s_{j-\nu}}{s_n}\dfrac{(n-j)!}{(j-\nu-1)!}\\[2mm] \gamma_{3\nu+1-j,j}=-\dfrac{\dot s_n}{s_js_{j-\nu}}\dfrac{(j-\nu-1)!}{(n-j)!}\end{cases}\qquad(j>\nu).$$

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

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

d'où, en posant $\nu+1-k=l$,

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

Pour $j>\nu$, on a

$$Y_j=\gamma_{j,3\nu+1-j}\Bigg[\sum_{k=1}^{\nu}(-1)^{j+k+\nu+1}\sigma_{3\nu+1-j,k}\gamma_{k,\nu+1-k}y_{\nu+1-k}\\ +\sum_{k=\nu+1}^{3\nu+1-j}(-1)^{j+k}\sigma_{3\nu+1-j,k}\gamma_{k,3\nu+1-k}y_{3\nu+1-k}\Bigg],$$

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

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

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

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

$$Y'_i = \sum_{k=1}^{\nu} \sigma_{ik} \gamma_{k,\nu+1-k} \sum_{l=1}^{\nu} \sigma_{\nu+1-k,l} y_l,$$

ou, en échangeant les deux sommations, et en observant qu'il suffit de faire varier k de 1 au plus petit t des deux nombres i, $\nu+1-l$,

$$Y''_i = \sum_{l=1}^{\nu} \sum_{k=1}^{t} \frac{s_i}{s_l} (-1)^{\nu+k} \frac{(\nu-k)!}{(i-k)!\,(k-1)!\,(\nu+1-k-l)!} y_l,$$

d'où pour $l \leqq \nu$,

$$c'_{il} = \frac{s_i}{s_l} \frac{(l-1)!}{(i-1)!} \sum_{k=1}^{t} (-1)^{\nu+k} \binom{\nu-k}{l-1} \binom{i-1}{k-1},$$

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

$$\begin{aligned} Y'_j = & \sum_{k=1}^{\nu} \sigma_{jk} \gamma_{k,\nu+1-k} \sum_{l=1}^{\nu} \sigma_{\nu+1-k,l} y_l \\ & + \sum_{k=\nu+1}^{n} \sigma_{jk} \gamma_{k,3\nu+1-k} \sum_{r=1}^{n} \sigma_{3\nu+1-k,r} y_r. \end{aligned}$$

([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 $\geqq 0$) dans les deux membres donne, en supposant n entier $\geqq 1$,

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

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

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

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

$$\sum_t (-1)^{t+a} \binom{k}{t+a} \binom{r-t-a}{l} = \binom{r-k}{r-l} \qquad (r, l \text{ entiers, et } r \geqq l).$$

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 $r<\nu$, $u=j$),

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

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

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

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

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

ou, en observant que

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

et que

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

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

ou, puisque

$$\binom{n-1}{l-1} = \frac{(p-2)(p-3)\ldots(p-l)}{1.2\ldots(l-1)} = (-1)^{l-1}l \qquad (l \text{ entier} \geqq 1 \text{ et} \leqq n),$$

$$c'_{jl} = \frac{s_j}{s_l}(-1)^{l+1}\binom{j-l-1}{\nu-l}\frac{(l-1)!}{(j-1)!}\left(1-\frac{l}{j}\right) = \frac{s_j}{s_l}(-1)^{l+1}\frac{(j-l)!\,(l-1)!}{(\nu-l)!\,(j-\nu-1)!\,j!},$$

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

$$(-1)^l\frac{(j-l)!}{j!} = \frac{(n-j)!}{(n-j+l)!}, \qquad \text{c'est-à-dire à} \qquad (-1)^l = \frac{\binom{n}{j-l}}{\binom{n}{j}},$$

qui est vérifiée, puisque, d'après ce qu'on vient de voir, $\binom{n}{l} = (-1)^l$ [1].

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

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

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

$$\begin{aligned} c'_{ir} &= \frac{s_j}{s_r}(-1)^{\nu+1}\frac{(r-\nu-1)!}{(j-\nu-1)!}\sum_{k'}\binom{j'}{k'}\binom{\nu-1-k'}{r-\nu-1} \\ &= \frac{s_j}{s_r}(-1)^{\nu+1}\frac{(r-\nu-1)!}{(j-\nu-1)!}\binom{n-j}{n-r}, \end{aligned}$$

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

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

Ces équations, jointes à celles de Φ (**4**) *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 $l = \nu$, qui donne, en observant que

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

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

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

Je désignerai par γ_1, ζ_1, X_1, X_1^0, $\mathcal{X}_1$, $\mathcal{X}_1^0$, $\overline{X}_1$ les déterminations exceptionnelles de γ, ζ, X, X^0, $\mathcal{X}$, $\mathcal{X}^0$, $\overline{X}$ 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

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

Or i et k sont $\geqq 1$ et $\leqq n$. On a donc :

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

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* ± 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*, γ_{11} *et* γ_{nn} *ne sont pas tous deux nuls.*

On a ici

$$Y_1 = (\gamma_{11}^2 + \sigma_{n1}\gamma_{1n}\gamma_{11} + \gamma_{1n}\gamma_{n1})y_1 + \gamma_{1n}\sum_{i=2}^{n-1}\sigma_{ni}(-1)^{n-i}\gamma_{i,n+1-i}\,y_{n+1-i}$$
$$+ \gamma_{1n}(\gamma_{11} + \sigma_{n1}\gamma_{1n} + \gamma_{nn})y_n,$$

$$Y_1' = \gamma_{11}y_1 + \gamma_{1n}\sum_{i=1}^{n}\sigma_{ni}y_i.$$

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

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

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

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

Or, pour n impair, $\dot{s}_n = -s_n$. 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 θ devrait être égal à 1.

Donc $\gamma_{1n} = 0$. La condition que γ conserve a donne alors $\gamma_{11}\gamma_{nn} = 1$. La condition $c'_{11} = c_{11}$ donne $\gamma_{11}^2 = \gamma_{11}$. *Donc* $\gamma_{11} = \gamma_{nn} = 1$, et la condition $\gamma^2 = |\zeta|$ exige que $\gamma_{n1} = 0$.

Soit $A = Q$. Si γ_{1n} ou γ_{n1} est $\neq 0$, la condition $\gamma^2 = |\zeta|$ donne $\gamma_{11} + \gamma_{nn} = 0$, et la condition que γ conserve a donne $\gamma_{11} - \gamma_{nn} = 0$ contre l'hypothèse.

Donc $\gamma_{1n} = \gamma_{n1} = 0$. La condition que γ conserve a donne alors $\gamma_{11}\gamma_{nn} = 1$, et la condition $c'_{11} = c_{11}$ donne $\gamma_{11}^2 = \gamma_{11}$. *Donc* $\gamma_{11} = \gamma_{nn} = 1$.

Ainsi, pour $A = \overline{\Pi}$ ou Q, *on a ici* $\gamma_{11} = \gamma_{nn} = 1$, $\gamma_{1n} = \gamma_{n1} = 0$, *et* γ *remplace* y_j $(1 \leqq j \leqq n-1)$ *par* $\gamma_{j,n+1-j}\, y_{n+1-j}$.

La condition $\gamma^2 = |\zeta|$ donne

$$\zeta = \gamma_{11}^2 = \gamma_{nn}^2 = 1 \qquad \text{et} \qquad \gamma_{j,n+1-j}\,\gamma_{n+1-j,j} = 1 \qquad (2 \leqq j \leqq n-1).$$

La condition que γ 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 $c'_{1l} = c_{1l}$ *est alors satisfaite dans* ζ.

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

On a d'abord

$$Y_n = \sigma_{n1} y_1 + \sum_{l=2}^{n-1} (-1)^{l+1} \sigma_{n,n+1-l}\, \gamma_{n+1-l,l}\, y_l + y_n,$$

$$Y'_n = \sigma_{n1} y'_1 + \sum_{k=2}^{n-1} \sigma_{nk}\, \gamma_{k,n+1-k} \sum_{l=1}^{n-1} \sigma_{n+1-k,l}\, y_l + \sum_{l=1}^{n} \sigma_{nl}\, y_l,$$

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 $l = 2, \ldots, n-2$. Elle s'écrit $\left[\text{en multipliant par } (n-2)!\,\frac{s_l}{s_n}\right]$

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

ou ($n = 0$ dans $\mathfrak{S}$) (¹)

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

ou $\dfrac{(p-1)(p-2)\ldots(p-l)}{1.2\ldots l} = (-1)^l$. ce qui est évident.

(¹) Considérons la somme $S_{bh} = \sum_{s=0}^{h} \frac{(-1)^s}{s+b} \binom{h}{s}$ ($-b$ n'étant pas un des nombres $0, \ldots, h$). Je dis que $S_{bh} = \dfrac{\Gamma(b)\Gamma(h+1)}{\Gamma(b+h+1)}$. On a d'abord évidemment $S_{b0} = \dfrac{1}{b} = \dfrac{\Gamma(b)\Gamma(1)}{\Gamma(b+1)}$. 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 $-\dfrac{\Gamma(b+1)\Gamma(h+1)}{\Gamma(b+h+2)}$ (on le voit en posant $s = t+1$). Donc $S_{b,h+1} = \dfrac{\Gamma(b)\Gamma(h+2)}{\Gamma(b+h+2)}$.

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

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

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 $0, \ldots, h$ tel que i, suppo-

La condition $c'_{n1} = c_{n1}$ s'écrit, en divisant par σ_{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

$$\binom{n-2}{s} = (-1)^s(s+1)\ (^1). \qquad \Sigma_1^{n-1}\frac{1}{s} = 0,$$

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 $j = 2, \ldots, n-1$.

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

$$Y_j = \gamma_{j,n+1-j}\left[(-1)^{j+1}\sigma_{n+1-j,1}y_1 + \sum_{k=2}^{n+1-j}(-1)^{j+k}\sigma_{n+1-j,k}\gamma_{k,n+1-k}y_{n+1-k}\right],$$

d'où, en posant $n+1-k = l$,

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

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

---

sons d'abord que $b = -i+\varepsilon$, pour faire ensuite tendre ε vers zéro. La somme S'_{ih} 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 $b(b+1)\ldots(b+h) = \varepsilon f(\varepsilon)$, 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 $S_n = \Sigma_1^n \frac{1}{s}$ et $S_0 = 0$. *Donc* $S_{ih}^{(i)} = \lim_{\varepsilon=0} S_{bh}^{(i)} = (-1)^i\binom{h}{i}(S_i - S_{h-i})$.

Les formules obtenues ici serviront dans la suite.

(1) On peut aussi se servir de la fin dela 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 t le plus petit des deux nombres j, $n+1-l$,

$$Y_j = y_1\left(\sigma_{j1} + \sum_{k=2}^{j} \sigma_{jk}\gamma_{k,n+1-k}\sigma_{n+1-k,1}\right) + \sum_{l=2}^{n-1}\sum_{k=2}^{t} \sigma_{jk}\gamma_{k,n+1-k}\sigma_{n+1-k,l}\, y_l.$$

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

$$\begin{aligned} c'_{jl} &= \frac{s_j}{s_l}\frac{(l-2)!}{(j-2)!}\sum_{k=2}^{t}(-1)^k\binom{j-2}{k-2}\binom{n-k-1}{l-2} \\ &= \frac{s_j}{s_l}\frac{(l-2)!}{(j-2)!}\binom{n-j-1}{n-l-1} = c_{jl}, \end{aligned}$$

et

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

ou, puisque $n = p$,

$$\begin{aligned} c'_{j1} &= s_j\left[\frac{1}{(j-1)!} - \frac{1}{(j-2)!}\sum_{k=2}^{t}\frac{(-1)^k}{k}\binom{j-2}{k-2}\right] \\ &= s_j\left[\frac{1}{(j-1)!} - \frac{1}{j!}\right] = \frac{s_j}{(j-2)!\,j} = c_{j1}. \end{aligned}$$

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 $\gamma^2 = 1$, $(\gamma\sigma)^3 = 1$, $\gamma^{-1}\mu_m\gamma = \mu_m^{-1}$. *Donc* $X = \mathfrak{X} \equiv \mathfrak{L}(2, p)$.

Je désignerai par γ_2, ζ_2, X_2, X_2^0, $\mathfrak{X}_2$, $\mathfrak{X}_2^0$, $\overline{X}_2$ les déterminations exceptionnelles de γ, ζ, X, X^0, $\mathfrak{X}$, $\mathfrak{X}^0$, $\overline{X}$ qui viennent d'être obtenues.

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

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

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 $\eta_1 = 0$). En posant $\Theta = \Pi_1^n \tau_i$, $\Theta\gamma$ a la forme

$$|y_j, \beta_j y_j| = \beta \qquad (j = 1, \ldots, n).$$

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

$$\gamma = \Theta^{-1}\beta = \left|\begin{array}{cc} y_i\ (i \leqq \nu) & \beta_i y_{n+1-i} \\ y_{n+1-i} & -\beta_{n+1-i} y_i \\ y_{\nu+1}\ (\text{si } n = 2\nu+1) & \beta_{\nu+1} y_{\nu+1} \end{array}\right|.$$

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

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

$$\begin{aligned}
Y_i = {} & \beta_i \sum_{k=1}^{\nu} (-1)^{n+1+i+k} \beta_k \sigma_{n+1-i,k} y_{n+1-k} \\
& - \beta_i \sum_{k=n-\nu+1}^{n-i+1} (-1)^{n+1+i+k} \beta_k \sigma_{n+1-i,k} y_{n+1-k} + \eta_1 (-1)^{n+\nu+i} \beta_i \dot{\beta}_{\nu+1} y_{\nu+1}, \\
Y_{n+1-i} = {} & - \beta_{n+1-i} \sum_{k=1}^{i} (-1)^{i+k} \beta_k \sigma_{ik} y_{n+1-k}, \\
Y_{\nu+1} = {} & \beta_{\nu+1} \sum_{k=1}^{\nu+1} (-1)^{k+\nu+1} \beta_k \sigma_{\nu+1,k} y_{n+1-k} \qquad (\text{si } n = 2\nu+1), \\
Y'_i = {} & \sum_{k=1}^{i} \sum_{l=1}^{n+1-k} \beta_k \sigma_{ik} \sigma_{n+1-k,l} y_l, \\
Y'_{n+1-i} = {} & S + S' + S'', \\
S = {} & \sum_{k=1}^{\nu} \sum_{l=1}^{n+1-k} \beta_k \sigma_{n+1-i,k} \sigma_{n+1-k,l} y_l, \\
S' = {} & - \sum_{k=n+1-\nu}^{n+1-i} \sum_{l=1}^{n+1-k} \beta_k \sigma_{n+1-i,k} \sigma_{n+1-k,l} y_l, \\
S'' = {} & \eta_1 \beta_{\nu+1} \sigma_{n+1-i,\nu+1} \sum_{l=1}^{\nu+1} \sigma_{\nu+1,l} y_l, \\
Y'_{\nu+1} = {} & \sum_{k=1}^{\nu+1} \sum_{l=1}^{n+1-k} \beta_k \sigma_{\nu+1,k} \sigma_{n+1-k,l} y_l \qquad (\text{si } n = 2\nu+1).
\end{aligned}$$

La condition $c'_{in} = c_{in}$ donne $\beta_i = (-1)^{i+n} \frac{\sigma_{i1}}{\sigma_{n+1-i,1}}$ $(i \leqq \nu)$. 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 β_i se réduit à $\beta_{\nu+1}$, et celle de β_{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,

$$Y_i = (-1)^{n+1} \sum_{l=i}^{n} \frac{\sigma_{i1}\sigma_{n+1-l,1}}{\sigma_{n+1-i,1}\sigma_{l1}} \sigma_{n+1-i,n+1-l}\, y_l \qquad (i = 1, \ldots, \nu),$$

$$Y_{n+1-j} = (-1)^{n+1} \sum_{l=n-\nu}^{n} \frac{\sigma_{n+1-j,1}\sigma_{n+1-l,1}}{\sigma_{j1}\sigma_{l1}} \sigma_{j,n+1-l}\, y_l \qquad (j = 1, \ldots, \nu + 1 = n - \nu),$$

$$Y'_i = \sum_{l=1}^{n} \sum_{k=1}^{t} (-1)^{k+n} \frac{\sigma_{k1}\sigma_{ik}}{\sigma_{n+1-k,1}} \sigma_{n+1-k,l}\, y_l \qquad (i = 1, \ldots, \nu),$$

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

$$Y'_{n+1-j} = \sum_{l=1}^{n} \sum_{k=1}^{u} f(j, k, l) + \sum_{l=1}^{n-\nu} \sum_{k=\nu+1}^{u'} f(j, k, l) \qquad (j = 1, \ldots, n - \nu),$$

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

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

On a donc

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

$$= (-1)^{n-1} \frac{s_i}{s_l} \frac{(l-1)!}{(i-1)!} \binom{n-i}{n-l} = c_{il},$$

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

$$c'_{n+1-j,l} = (-1)^n \frac{s_{n+1-j}}{s_l} \frac{(j-1)!}{(n-l)!} \sum_{k=1}^{n} (-1)^k \binom{n-k}{j-1} \binom{n-l}{k-1}$$

$$= (-1)^{n+1} \frac{s_{n+1-j}}{s_l} \frac{(j-1)!}{(n-l)!} \binom{l-1}{n-j} = c_{n+1-j,l},$$

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

$$c'_{n+1-j,l} = (-1)^n \frac{s_{n+1-j}}{s_l} \frac{(j-1)!}{(n-l)!} \sum_{k=1}^{n} (-1)^k \binom{n-k}{j-1} \binom{n-l}{k-1}$$

$$= (-1)^{n+1} \frac{s_{n+1-j}}{s_l} \frac{(j-1)!}{(n-l)!} \binom{l-1}{n-j}.$$

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 $c'_{n+1-j,l} = c_{n+1-j,l}$ pour $l \leq n - \nu$.

Le groupe X *est ici défini abstraitement par les équations de* Φ (4) *jointes à* $\gamma^2 = d^{n-1}$, $\gamma^{-1}\mu_m\gamma = \mu_m^{-1}\delta$, $\delta = 1$ *si* $n = 2\nu + 1$, $\delta^{2^{l-1}} = d^k$ *si* $n = 2\nu$ (2), $d^2 = 1$ *et aux équations exprimant que* δ *et* d *sont permutables aux autres générateurs.*

Le seul cas où $|\delta|$ *soit* $> D$ *est celui où* $A = H(2\nu, \pi)$ *avec* $\pi \equiv 3 \bmod 4$. *Alors* $\frac{p^m - 1}{2}$ *est impair, et le diviseur* $Y = \{\omega, d\mu_m^2, \gamma\}$ *de* X *est* $\cong U(2, p^m)$ (*S.*, 92). *Le groupe* $Z = \{Y, \delta\}$ ($Z|D$ *est produit direct de* $Y|D$ *par* $\Delta|D$) *est d'indice* 2 *dans* $X = Z + \mu_m^{\frac{p^m-1}{2}} Z$. *Dans tous les autres cas, le diviseur* $\{\varpi, \mu_m^2, Y\} = X^0$, *d'indice* 2 *dans* X, *est isomorphe à* $\mathfrak{V}(2, p^m)$ *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 $A = \overline{H}$ ou Q (on passe de $\overline{H}$ à Q en supposant tous les coefficients dans $\mathfrak{S}$). En posant $\Theta = \Pi_1^\nu t_i$, Θ_ν a la forme $|y_i, \beta_i y_i| = \beta$ ($\beta_{\nu+1} = \gamma_{\nu+1,\nu+1}$). Pour que β conserve a, 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 γ 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**,

$$Y'_i = \sum_{l=1}^{n} (-1)^{i+l} \frac{\beta_l}{\beta_i} \sigma_{n+1-i,\,n+1-l}\, Y_l,$$

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

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

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

$$\beta_i = (-1)^{i+1} \frac{\sigma_{i1}}{\sigma_{n+1-i,\,1}} = (-1)^{i-1} \frac{s_i}{s_{n+1-i}} \frac{(n-i)!}{(i-1)!},$$

et ces valeurs vérifient les relations $\beta_{n+1-i}\beta_i = 1$, $\beta_{\nu+1} = (-1)^{\nu}$. *Donc γ, si elle existe, est dans* A^0 (¹).

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

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

Je désignerai désormais par γ_0, ζ_0, X_0, X_0^0, $\mathfrak{X}_0$, $\mathfrak{X}_0^0$, $\bar{X}_0$, les déterminations de γ, ζ, X, X^0, $\mathfrak{X}$, $\mathfrak{X}^0$, $\bar{X}$ obtenues aux n^{os} **17-18**.

Supposons maintenant que $A = Q$ (alors $\Omega = D$). Comme γ, σ et μ_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 $X_0 \cong \mathfrak{L}(2, p^m)$. Dans cet isomorphisme σ, μ_m, γ_0 répondent respectivement à $z+1$, $\iota_m z$, $-z^{-1}$. *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, γ_0 est dans R [*voir G.*, **29**, formule (29), en observant que $\beta_{\nu+1} = (-1)^{\nu}$]. Donc, comme μ_m (**4**), X_0 *est dans* R *toujours et seulement si* $\varkappa$ *est pair ou si* $\nu \equiv 0, 3 \bmod 4$: X_0^0 *divise toujours* R.

(¹) Cela devait être *a priori*, puisque γ correspond à $\frac{-1}{z}$ qui est dans le groupe simple $\mathfrak{V}(2, p)$.

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

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

Si $n = 2\nu$, X_H (**14**) *divise tous les* $H(n, p^{mk})$ *qui divisent* $H(n, \pi)$. X_G *si* $\varkappa$ *est pair, ou* X'_G *si* $\varkappa$ *est impair divise tous les* $G(n, p^{mk})$ *qui divisent* $G(n, \pi)$.

De plus, comme $\mu_G^2 = \mu_G^{\pi-1}$ (**2**), *on a toujours* $X'_G = X'_H$, *et, si* $\varkappa$ *est pair* $\left(\text{alors } \frac{\pi - 1}{p^m - 1} \text{ est pair et } \mu_{mG} = \mu_{mH}^{\frac{\pi-1}{2}}\right)$, $X_G = X_H$.

II.

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

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

$$\gamma^2 = [\zeta], \qquad \gamma^{-1}\mu_m^2\gamma = \mu_m^2[s], \tag{1}$$

$$\sigma_{\mu_m^x}\gamma\mu_m^{p^m-1-2x}\sigma_{\mu_m^{-x}} = \gamma\sigma_{\mu_m^x}\gamma[\rho_x], \tag{2}$$

x parcourant toutes les valeurs entières mod $p^m - 1$, et $[\zeta]$, $[s]$, $[\rho_x]$ étant dans Ω. Posons $\frac{p^m - 1}{2} = q$ et $\rho_q = \rho$. En prenant au besoin $[\rho^{-1}]\gamma$ pour γ, *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

$$\sigma_{\mu_m^{-x}}\gamma\mu_m^{2x} = \gamma\sigma_{-\mu_m^{-x}}\gamma[\rho_{q-x}],$$

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

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

ou

$$\mu_m^{p^m-1} = \mu^{\pi-1} = |\zeta\rho_{q-x}\rho_x|,$$

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

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 $\mu_m^{-x}\sigma_x\mu_m^x = \sigma_{x(1,m)}$

$$\sigma_{1,m}\gamma\mu_m^{p^m-1-2x}\sigma_{1,m}|s^{-1}| = \gamma\sigma_{1,m}\gamma|\rho_{x+2}|. \tag{3}$$

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

En remplaçant $\mu_m^{p^m-1}$ par $|\zeta\rho_0|$, μ_m^{-2x} par $|\xi^{2x}|\mu_{0m}^{-2x}$, et ξ^2 par $e^{-1}\iota_m^{n+1}$ $|e = \pm 1$, sauf si $n = 2\nu$ avec $A = H$ et $\pi \equiv 3 \bmod 4$ (**2**)$|$, l'équation (2) s'écrit

$$\gamma\sigma_{1,m}^{-1}\gamma\mu_{0m}^{2x} = \left|\frac{\rho_x}{\rho_0}e^x\iota_m^{(n+1)x}\right|\sigma_{1,m}\gamma\sigma_{1,m}. \tag{4}$$

Je désignerai par $Y_{xi} = \Sigma_l c_{xil}y_l$ et $Y'_{xi} = \Sigma_l c'_{xil}y_l$ 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 $c'_{xil} = c_{xil}$ en partant de la condition $c'_{0il} = c_{0il}$.

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

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

Or, si γ existe, il y a pour chaque i, au moins un $\gamma_{ik} \neq 0$, et, pour $\gamma_{ik} \neq 0$, on a $s' = \iota_m^{2i+k-n-1}$. Donc s' a la forme $\iota_m^{2c}\left(0 \leqq c \leqq \frac{p^m-3}{2}\right)$. Supposons toujours que $\iota = \iota'^{\pi+1}$. On aura $s' = \iota'^{(2cg\pi+l)}$ (**5**). Mais $|s'|$ étant dans Ω, s' a la forme $\iota'^{(\pi-1)s}$. Donc

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

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 $f = 1$, $p^m \equiv 1 \bmod 4$). Ainsi, pour chaque valeur de i, les $\gamma_{ik} \neq 0$ vérifient la condition

$$\left\{\begin{array}{l} 2(i+k-n-1) = f\frac{p^m-1}{2} + f'(p^m-1), \\ (f = 0 \text{ ou } 1;\ \text{si } f = 1,\ p^m \equiv 1 \bmod 4\ (f' \text{ entier}), \end{array}\right. \tag{5}$$

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

21. *Supposons d'abord $f = 1$, donc $p^m \equiv 1 \bmod 4$, 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 ≥ 2 et $\leq 2n$. Donc

$$1 - n \leq h\frac{p^m-1}{4} \leq n - 1, \qquad \text{ou} \qquad |h| \leq 4\frac{n-1}{p^m-1} < 4\frac{p-1}{p^m-1}.$$

Donc, h étant impair, on a :

si $p > 3$, $\quad m = 1$ (donc $p \equiv 1 \bmod 4$), $\quad |h| = 1$ ou 3, $\quad n \geq |h|\frac{p-1}{4} + 1$;

si $p = 3$, $\quad m = 2$, $\quad |h| = 1$, $\quad n \geq 3$, $\quad$ donc $n = 3$.

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

Soit donc $p = 4q' + 1$, $m = 1$, $n = |h|q' + r$ $(r \geq 1)$. Si h ne prend que les deux valeurs ± 1, les seuls γ_{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 ± 3, et $n = 3q' + r$ $(1 \leq r \leq q' + 1)$. Les seuls γ_{ik} pouvant être $\neq 0$ sont ceux de quatre parallèles à la transversale passant par les éléments $\gamma_{1,r}$, $\gamma_{1,2q'+r}$, $\gamma_{n,q'+1}$, $\gamma_{n,3q'+1}$.

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

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 $\alpha, \beta = 1, \ldots, q'$,

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

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 $\gamma_{q'+\beta,p-\beta}$ sont nuls; mais alors les $\gamma_{3q'+\beta,p-\beta}$ sont tous $\neq 0$ (sans quoi γ 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 $\alpha=1, \ldots, q'$, 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* $\gamma_{q'+\beta,p-\beta}$ *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 $\geqq 2$ et $\leqq 2n$, on a

$$1-n \leqq f'\frac{p^m-1}{2} \leqq n-1, \qquad \text{ou} \qquad |f'| \leqq 2\frac{n-1}{p^m-1} \leqq 2\frac{p-1}{p^m-1}.$$

Si $f'=0$ *pour chaque couple* i, k, *on est ramené au cas des* n^{os} **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 $\frac{p^m-1}{p-1} \leqq 2$. Donc $m=1$, $|f'| \leqq 2$, $n \geqq |f'|\frac{p-1}{2}+1$.

Supposons d'abord que $|f'|$ *reste* <2. Alors n est $\geqq \frac{p+1}{2}$. Posons $n=q+r$ $(p=2q+1)$. Les seuls γ_{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 γ_{1r}, γ_{1n}, $\gamma_{n,q-1}$.

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

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

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

et l'équation $c'_{1jq}=c_{1jq}$ s'écrit $\frac{e\rho_1}{\rho_0}c'_{0jq}=c_{0jq}$, d'où, par comparaison avec $c'_{0jq}=c_{0jq}$ ($\gamma_{j,n+1-j}$ et $\gamma_{n+1-q,q}$ sont $\neq 0$, sans quoi $|\gamma|$ serait nul), $\frac{e\rho_1}{\rho_0}=1$.

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

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

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

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 $e\rho_1 = \rho_0$,

$$\sum_{h=1}^{\alpha} \sigma_{\alpha h}\gamma_{h,r+1-h}\sigma_{r+1-h,\beta} = 0, \tag{6}$$

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

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

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

23. *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

$$\begin{aligned} \left(1 + \frac{e\rho_1}{\rho_0}\right) &\sum_{h=1}^{\alpha} \sigma_{\alpha h}\gamma_{h,n+1-h}\sigma_{n+1-h,\beta} \\ &= (-1)^{\alpha+\beta} 2\gamma_{\alpha,n+1-\alpha}\sigma_{n+1-\alpha,n+1-\beta}\gamma_{n+1-\beta,\beta}. \end{aligned} \tag{7}$$

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

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

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 $\alpha = 1$), $\frac{e\rho_1}{e_0} = 1$, puis $\gamma_{\alpha,n+1-\alpha} = \frac{(-)^\alpha\sigma_{\alpha 1}}{\sigma_{n+1-\alpha,1}}$. En portant ces valeurs dans la somme des deux relations $c'_{0\alpha\alpha} = c_{0\alpha\alpha}$,

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

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

Le premier membre est égal à

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

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

$$\gamma_{\alpha,n+1-\alpha}(\gamma_{n+1-\alpha,\alpha}y_\alpha+\gamma_{n+1-\alpha,\alpha+\nu}y_{\alpha+\nu}).$$

Donc $\gamma_{n+1-\alpha,\alpha+\nu}=0$, 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* γ, *et le groupe obtenu ici est* X_0^0 (**18**).

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

$$\left(1+\frac{e\rho_1}{\rho_0}\right)\sigma_{n+1-\alpha,\beta}=(-1)^{\alpha+\beta}\gamma_{n+1-\beta,\beta}\sigma_{n+1-\alpha,n+1-\beta}.$$

Mais $\gamma_{n+1-\beta,\beta}$ est nul pour $\beta=n$, et $\neq 0$ pour $\beta=n+1-\alpha$. Donc $1+\frac{e\rho_1}{\rho_0}$ serait à la fois nul et non nul.

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

$$\gamma_{1\nu}\sigma_{\nu l}+\frac{e\rho_1}{\rho_0}\gamma_{1\nu}\sigma_{\nu l}=(-1)^{l+1}\sigma_{\nu,\nu+1-l}\gamma_{\nu+1-l,l}.$$

Donc $e\rho_1=-\rho_0$, et $\gamma_{\nu+1-l,l}=\frac{(-1)^{l+1}\sigma_{\nu l}}{\sigma_{\nu,\nu+1-l}}$ ($l\leqq\nu$).

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

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

Or, les σ du second membre sont nuls pour $l<\nu$, et, pour $l=\nu$, le second membre est le coefficient de y_ν dans la fonction que γ^2 substitue à y_n. Donc le second membre est nul pour $l \leqq \nu$. En faisant $l = \nu$, $\nu - 1, \ldots, 1$, on a donc, entre les $\sigma_{nh}\gamma_{h,n+1-h}$, ν équations homogènes de déterminant 1 (tous les éléments situés au-dessus de la diagonale, composée d'unités, sont nuls). Donc les $\gamma_{h,n+1-h}$ ($h > \nu$) sont nuls, et *l'on rentre dans le cas traité au n° 15. On a la même détermination de γ, et le groupe obtenu ici est X_1^0.*

24. *Soit $r = q + 1$, donc $n = p = 2q + 1$ et $q = \nu$.* Les seuls γ_{ik} pouvant être $\neq 0$ sont ceux de trois parallèles à la transversale, passant par les éléments $\gamma_{1,\nu+1}$, γ_{1n}, $\gamma_{n,\nu+1}$. La combinaison de la première ligne avec elle-même montre que $\gamma_{1,\nu+1} = 0$. Donc γ_{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 $\leqq |f'|\dfrac{p-1}{2} + 1$ et $\geqq p$, *on a $n = p$*. Les seuls γ_{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 γ_{11}, $\gamma_{1,\nu+1}$, γ_{1n}, $\gamma_{n,\nu+1}$, γ_{nn} (la première et la cinquième ne contenant qu'un élément).

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

$$\frac{1}{2}\left(1 + \frac{e\rho_1}{\rho_0}\right) = u, \qquad \frac{1}{2}\left(1 - \frac{e\rho_1}{\rho_0}\right) = v,$$

$$u\gamma_{1n} = \gamma_{1n}^2\sigma_{n1} + \gamma_{11}\gamma_{1n} + \gamma_{1,\nu+1}\gamma_{\nu+1,n} + \gamma_{1n}\gamma_{nn}, \tag{9}$$

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

La somme et la différence des équations

$$c'_{0,1,\nu+1} = c_{0,1,\nu+1}, \qquad c'_{1,1,\nu+1} = c_{1,1,\nu+1}$$

donnent

$$u\gamma_{1,\nu+1} + v\gamma_{1n}\sigma_{n,\nu+1} = \gamma_{1n}\gamma_{1,\nu+1}\sigma_{n1} + \gamma_{11}\gamma_{1,\nu+1} + \gamma_{1,\nu+1}\gamma_{\nu+1,\nu+1} + \gamma_{1n}\gamma_{n,\nu+1}, \tag{11}$$

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

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

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

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

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

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

$$e=s=1,\qquad \rho_{2r}=\rho_0,\qquad \rho_{2r+1}=\rho_1,\qquad [\zeta\rho_{q-r}\rho_r]=1.$$

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 $\gamma_{\nu+1,n}=0$; (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 $c'_{0\alpha n}=c_{0\alpha n}$, $c'_{1\alpha n}=c_{1\alpha n}$ $(2\leqq\alpha\leqq n)$ donne maintenant

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

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

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

d'où, comme au n° **23**, $\gamma_{\alpha,\nu+2-\alpha} = 0$. Mais alors γ^2 remplace y_α par

$$\gamma_{\alpha,n+1-\alpha}(\gamma_{n+1-\alpha,\alpha}y_\alpha + \gamma_{n+1-\alpha,\alpha+\nu}y_{\alpha+\nu}),$$

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

Soit maintenant $\gamma_{1n} = 0$. 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 $c'_{0,\alpha,n-1} = c_{0,\alpha,n-1}$, $c'_{1,\alpha,n-1} = c_{1,\alpha,n-1}$ $(2 < \alpha < n-1)$ donne maintenant

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

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

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

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

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

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

En effet, si $\mathfrak{X}_0$ est conjugué de $\mathfrak{X}_i$ $(i = 1, 2)$ dans $\mathfrak{A}$, il y a dans A une substitution s telle que $s^{-1}\overline{X}_i s = \overline{X}_0$ (et réciproquement). Donc $s^{-1}X_i s = X_0\Theta$, Θ étant dans Ω. Or, suivant que $n = p - 1 \equiv 0 \bmod 4$ ou que $n = p$, on a $X_1|D = X_0|D = \mathfrak{L}(2, p)$, ou $X_2 = X_0 \equiv \mathfrak{L}(2, p)$. Donc $\Theta = 1$. D'ailleurs, dans le groupe de degré $p + 1$ deux fois transitif $\mathfrak{L}(2, p)$, les diviseurs d'ordre $p(p-1)$ qui fixent un symbole sont tous conjugués de $|z+1, \iota_1 z|$. On peut donc supposer s permutable à Φ, donc à ϖ. De même les diviseurs d'ordre $p-1$ de $|z+1, \iota_1 z|$ y étant tous conjugués de $|\iota_1 z|$, on peut supposer s permutable à M_1. Mais alors s transforme γ_i en une s_2 de X_0 permutable à M_1 et située hors de M_1. Or le normalisant de $|\iota_1 z|$ dans $\mathfrak{L}(2, p)$ est $|\iota_1 z, z^{-1}|$ [1], et ses s_2 autres que $-z$ y forment deux classes représentées par z^{-1} et $\iota_1 z$. On peut donc supposer que s transforme γ_i en $\mu_1^\alpha \gamma_0 d^\beta$ ($\alpha, \beta = 0$ ou 1) [2] ou que $s\mu_1^\alpha\gamma_0 s^{-1} = \gamma_i d^\beta$. Or s, étant permutable à ϖ, a la forme $s = \mu_1^l \varphi$, φ étant dans ϖ' (**4**); et φ, étant donc permutable à M_1, a la forme u_{1l} ou $\overline{u}_{1l}$ (**5**) ($l = 0$ si $n \neq p$). Donc $s\mu_1^\alpha\gamma_0 s^{-1}$ remplace y_1 par une fonction où le coefficient de $y_\varkappa$ 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 $\varkappa$ est pair*, toute substitution de A' qui transforme ϖ en $\varpi_\varkappa$ (**7**) transforme X_1 et X_0 en deux autres diviseurs de A qui contiennent $\varpi_\varkappa$, 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 $\varkappa$ impair. Considérons alors $G(n, \pi^2)$, et faisons jouer à π^2 le rôle de π. 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 (**20-25**) 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' dans A de X_i ($i = 0, 1, 2$; $A \neq G$ si $\varkappa$ est impair).*

Soit s une substitution de A permutable à X_i, et $s^{-1}\varpi s = \varpi_i$. X_1 contient une substitution s_1 transformant ϖ en ϖ_1. Donc ss_1^{-1} est permutable à ϖ et a la forme $\varphi\mu_m^l$, φ étant dans ϖ' (**4**). Donc s est

---

[1] $\mathfrak{L}(2, p)$ étant deux fois transitif, le diviseur fixant deux symboles a $\dfrac{p(p+1)}{2}$ 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 $\not\equiv |M_1, \gamma_0|$ $[\gamma_1^2 = \gamma_0^2 = d,\ \gamma_1^{-1}\mu_1\gamma_1 = \mu_1^{-1} d^{\mathrm{K}+1},\ \gamma_0^{-1}\mu_1\gamma_0 = \mu_1^{-1} d^{\mathrm{K}}]$ (**16**, **17**).

dans φX_i, et φ est permutable à X_i. Donc φ, qui est permutable à ϖ, l'est au normalisant Φ de ϖ dans X_i. Comme d'ailleurs Φ détermine X_i, il suffit que φ soit dans Φ' (**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 $\overline{H}$, X'_i coïncide avec X_i.* Si l'on a à la fois $n = p$, $m = 1$ et $A = H$ ou $\overline{H}$, on peut seulement affirmer que X'_i divise $\{X_i, u_{11_1}\}$ si $A = H$, ou $\{X_i, \overline{u}_{11_1}\}$ si $A = \overline{H}$ (**12**). Mais u_{11_1} et $\overline{u}_{11_1}$ sont ici permutables à Φ, et quand Φ est donné, X n'a qu'une des deux déterminations X_2 et X_0. Donc u_{11_1} et $\overline{u}_{11_1}$, 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 $m = 1$, $X'_i = \{X_i, u_{11_1}\}$ pour $A = H$, et $X'_i = \{X_i, \overline{u}_{11_1}\}$ pour $A = \overline{H}$ (ici $i = 0$ ou 2).*

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

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

μ_1 *est toujours dans* A^0; $\gamma_2 = t_0^{\nu+1} \Pi_2^\nu t_l m_{l,\gamma_{n+1-l,l}}$ *est dans* A^0 *toujours et seulement si ν est pair, c'est-à-dire si* $p \equiv 1 \bmod 4$.

Supposons $p \equiv 1 \bmod 4$. *Alors μ_1 est dans B toujours et seulement si* $K (= \varkappa)$ *est pair, ou si* $\nu \equiv 0 \bmod 4$ (**7**), *c'est-à-dire si* $p \equiv 1 \bmod 8$.

D'autre part, on a ici

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

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 $t_{02} m_{2,-c}^{-1}$

et $t_{ik}(i, k \neq 0)$ sont dans B(I, **32**), γ_2 est dans B si $\nu = 2$, et, si $\nu \geq 4$, il y est en même temps que $\gamma' = \Pi_3^{\nu} m_{\mu\mu-\nu}$.

Si K est pair, γ' est évidemment dans B. Si K est impair, γ' n'est dans B que s'il est dans $B(p, p)$, car un élément $\iota_1^x = \iota^{xg}$ $\left(g = \frac{\pi - 1}{p - 1}\right)$ de $\mathfrak{S}_1$ ne peut être ici carré dans $\mathfrak{S}$ que s'il l'est dans $\mathfrak{S}_1$. Comme il y a, dans $\mathfrak{S}_1$, $\frac{p-1}{4}$ 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, $2.3, \ldots, (p-2)(p-1)$ $\frac{p-1}{2}$ non carrés. Or, les $\nu - 1$ produits 1.2, $2.3, \ldots, (\nu - 1)\nu$ ont respectivement les mêmes caractères quadratiques que les $\nu - 1$ produits $(p-1)(p-2)$, $(p-2)(p-3)$, $\ldots$, $(p - \nu + 1)(p - \nu)$, et $\nu(\nu + 1) = \frac{p^2 - 1}{4}$ est ici carré. Donc les $\nu - 1 = \frac{p-3}{2}$ produits $1.2, \ldots, (\nu - 1)\nu$ contiennent ici $\frac{p-1}{4}$ non carrés. Si 2 est carré, c'est-à-dire ici si $p \equiv 1 \bmod 8$, le nombre des non carrés figurant parmi les produits $2.3, \ldots, (\nu - 1)\nu$ est $\frac{p-1}{4} \equiv 0 \bmod 2$. Si 2 est non carré, c'est-à-dire ici si $p \equiv 5 \bmod 8$, ce nombre est $\frac{p-5}{4} \equiv 0 \bmod 2$. *Donc γ_2 est toujours dans* B *si* $p \equiv 1 \bmod 4$.

Donc, pour que X_2 divise B, *il faut et suffit que* K *soit pair, ou que $p \equiv 1$ mod 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 $\{B, t_1\}$ suivant que $p \equiv 1$ ou* 3 mod 4.

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

Soit d'abord $\mathcal{A} = \mathfrak{G}(4, 5^2)$, et désignons par i, j les nombres 0, 1 dans un ordre déterminé quelconque. *On peut faire correspondre les générateurs σ, μ_1, γ_i de $\mathfrak{X}_i$ (en écrivant 5 pour 0 et 6 pour ∞) à*

$$\sigma + 1 = 12345, \qquad 2\sigma = 1243, \qquad -\frac{1}{\sigma} = 14.56$$

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 $\mathcal{N}_j$ *avec* S_5, *faisons correspondre* σ *à* 12345, μ_1 *à* 1243 *et* γ_j *à* 12.34. Regardons maintenant comme identiques les symboles 1, 2, 3, 4, 5 de $\mathfrak{g}(2,5)$ et de S_5. Alors $\{\mathfrak{g}(2,5), S_5\}$ est le groupe symétrique S_6 de champ 1, 2, 3, 4, 5, 6 (*S.*, 42).

Je dis que $\{\mathcal{N}_0, \mathcal{N}_1\} \equiv S_6$. Identifions en effet σ, μ_1, γ_i, γ_j avec les substitutions correspondantes de S_6. On aura, avec les notations de *S.*, 69,

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

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

$$s_k^2 = 1, \qquad (s_1 s_2)^3 = (s_2 s_3)^3 = (s_3 s_4)^3 = (s_4 s_5)^3 = 1,$$
$$(s_1 s_3)^2 = (s_1 s_4)^2 = (s_1 s_5)^2 = (s_2 s_4)^2 = (s_2 s_5)^2 = (s_3 s_5)^2 = 1.$$

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

D'autre part,

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

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

(¹) Pour vérifier $(s_1 s_5)^2 = 1$, $(s_3 s_5)^2 = 1$, $(s_4 s_5)^3 = 1$, il est avantageux de transformer d'abord ces relations. On a

$$s_1 s_5 = \sigma\mu_1(\gamma_j \sigma^{-1} \gamma_j)\mu_1\gamma_i = \sigma\mu_1(\sigma\gamma_j\sigma)\mu_1\gamma_i,$$

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

$$\mu_1^{-1} s_1 s_5 \mu_1 = \sigma^3 \gamma_j \sigma \gamma_i.$$

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

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

$$s_4 s_5 = \sigma^{-2}\mu_1\gamma_j\sigma^2\gamma_j\mu_1\gamma_i, \qquad \text{et} \qquad \mu_1^{-1} s_4 s_5 \mu_1 = \sigma\gamma_j\sigma^2\gamma_j\gamma_i.$$

Il suffit donc de vérifier

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

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* $\mathcal{G}(4, 5)$.

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 $\mathcal{G}(4, 5^2)$ (**I, 43**)]. Comme précédemment $\{X_0, X_2\}$ *est isomorphe à* S_6, σ, μ_1, γ_i, γ_j *correspondant respectivement à* 12345, 1243, 14.56, 12.34.

D'autre part, μ_1 est ici hors de $R(5, 5)$ (**5**). Donc, comme précédemment, $\{X_0^0, X_2^0\} = \{\sigma, \mu_1^2, \gamma_0, \gamma_2\}$ *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 σ conserve a, la substitution formée par les $2h + 1$ premières lignes de σ conserve la forme

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

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

Considérons aussi la forme

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

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 $2h + 1$.

σ_α transforme φ^{2h} en

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

Posons

$$\varphi_\alpha^{2h} = \sum_{r=0}^{q-2} \alpha^r \varphi_{\alpha r}^{2h} \qquad [\varphi_{\alpha 0}^{2h} = \varphi^{2h} \text{ (1)}].$$

---

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

et calculons le coefficient $C_{r\lambda}^{2h}$ de $x_\lambda x_\mu$ dans $\varphi_{2r}^{2h}(\lambda+\mu=q-r)$, en supposant $\lambda\leqq\mu$ (alors λ est $\leqq h$, 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 $\lambda\leqq k\leqq h$, $\mu\leqq q-k$, donc $\lambda\leqq k\leqq q-\mu$, et k prend les valeurs $\lambda, \lambda+1,\ldots, \lambda+r=q-\mu$ si $\lambda+r\leqq h$ (donc $\mu>h$), les valeurs $\lambda, \lambda+1,\ldots, h$ si $\lambda+r>h$ (donc $\mu\leqq h$). Si $j=\lambda$ et $i=\mu$, on a $\lambda\leqq q-k$, $\mu\leqq k\leqq h$, et k prend les valeurs $\mu, \mu+1,\ldots, h$ ($\mu+r=q-\lambda$ est $>h$ sans quoi λ serait $>h$; ici $\lambda+r=q-\mu$ est $>h$).

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

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

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

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

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

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

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 $\lambda\leqq k\leqq h$, $\lambda\leqq q-k$, donc

$$\lambda\leqq k\leqq q-\lambda=\lambda+r.$$

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

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

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

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

Donc

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

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

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

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

Soit $r = 1$, et essayons d'identifier $\varphi_{\lambda 1}^{2h}$, qui ne contient que les variables $x_1, \dots, x_{2h-1}$ (puisque $\lambda + \mu = q - 1$) avec φ^{2h-1}. On aura

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

et

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

Donc,

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

d'où, en multipliant la $i^{\text{ième}}$ 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,

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

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

$$\varphi_\lambda^{2h} = \varphi^{2h} + \chi\varphi^{2h-1} \qquad (h = 1, \dots, \nu).$$

---

(1) La somme $\Sigma_0^r(-1)^i\binom{r}{i} i$ est ce que devient pour $x = 1$ la dérivée du développement de $(1-x)^r$.

Donc σ_α, qui conserve φ^{2h-1} et transforme φ^{2h} en φ^{2h}_α, conserve en particulier l'intersection des $n-2$ quadriques $\varphi^3 = 0, \ldots, \varphi^n = 0$.

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

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

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

$$\Sigma_0^{2h-2}(-1)^i\binom{2h-2}{i} = 0, \qquad \Sigma_0^{h-1}(-1)^i\left(h-\frac{1}{2}-i\right)\binom{2h-1}{i} = 0.$$

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,

$$\Sigma_0^{2h-1}(-1)^i\binom{2h-1}{i}\,i = 0,$$

identité déjà rencontrée.

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

$$\rho y_l = \sigma_l z^l, \qquad z \text{ parcourant } \mathfrak{C}_n.$$

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

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

On vérifie de suite que σ_α, μ_m et γ_0 opèrent sur les points $z\left(=\frac{y_2}{y_1}\right)$

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

Le diviseur Φ de $\mathfrak{X}$, qui fixe le point $z=\infty$, conserve $\mathfrak{E}_\infty$. Toute substitution de $\mathfrak{X}$ qui transforme ∞ en α est dans Φs_α, s_α étant l'une d'elles et toutes ces substitutions transforment $\mathfrak{E}_\infty$ en une génératrice $\mathfrak{E}_\alpha$ *coupant $\mathcal{S}$ en l'unique point $z=\alpha$*. Ainsi γ_0 change $\mathfrak{E}_\infty$ en $\mathfrak{E}_0$ dont les équations sont $y_{\nu+1}=\ldots=y_n=0$. On voit que $\mathfrak{E}_\infty$ et $\mathfrak{E}_0$ n'ont aucun point commun. Donc, $\mathfrak{X}$ changeant deux points distincts quelconques α, β en 0 et ∞, $\mathfrak{E}_\alpha$ et $\mathfrak{E}_\beta$ *n'ont aucun point commun*. Chaque $\mathfrak{E}_z$ contenant $\frac{p^{m\nu}-1}{p^m-1}$ points (à coordonnées dans $\mathfrak{C}_m$), le système des p^m+1 $\mathfrak{E}_z$ en contient $\frac{(p^{m\nu}-1)(p^m+1)}{p^m-1}$. Pour $\nu>1$, ce nombre est moindre que celui $\frac{p^{2m\nu}-1}{p^m-1}$ des points de $u=0$ dans $\mathfrak{C}_m$ (II, **17**).

32. *Considérons le cas $n=5$.* On a alors (p est ici ≥ 5)

$$\sigma_\alpha = U_{20\alpha} U_{10,\frac{\alpha^2}{2}} V_{12,-\alpha} U_{12,\frac{\alpha^3}{6}},$$

$$\mu_m = m_{1,i_m} m_{2,i_m}, \qquad \gamma_0 = t_{12} m_{1,\frac{1}{24}} m_{2,\frac{1}{6}},$$

et $\mathcal{S}$ est ici définie par les équations

$$\frac{y_2}{y_1}=z, \qquad \frac{x_3}{y_1}=-\frac{z^2}{2}, \qquad \frac{x_2}{y_1}=-\frac{z^3}{6}, \qquad \frac{x_1}{y_1}=\frac{z^4}{24}. \tag{1}$$

D'après la correspondance des générateurs de $B(5,\pi)$ et $\mathcal{G}(4,\pi)$ indiquée dans I, **45** $\left(\text{dont je garderai ici les notations, en y faisant } \gamma=c=\frac{1}{2}\right)$, les substitutions répondant à σ_α, μ_m^2, γ_0 dans $\mathcal{G}(4,\pi)$ sont respectivement, *en fonction des générateurs de* $\mathcal{G}(4,\pi)$,

$$\sigma'_\alpha = U_{12\alpha} V_{12,\frac{\alpha^2}{2}} V_{2,\alpha} U_{1,\frac{\alpha^3}{3}},$$

$$\mu_m = m_{1,i_m} m_{2,i_m}^{\frac{1}{2}}, \qquad \gamma_0 = \tau_1\tau_2 m_{1,\frac{1}{6}} m_{2,2},$$

et je désignerai par $\mathfrak{X}''_0$ le diviseur de $\mathcal{G}(4,\pi)$ correspondant à X''_0 de $Q(5,\pi^2)$.

La droite ω_z 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 $x_3 = y_3$ (*cf.* I, **43**) est

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

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

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

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

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

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

$$(4) \qquad 3\xi_1\xi_2 = 2\eta_2^2, \qquad 3\xi_1\eta_1 = \xi_2\eta_2,$$

admettant la génératrice commune $\xi_1 = \eta_2 = 0$. Or $\mathfrak{N}_0''$ transforme s' en elle-même (¹). Quand on prend s' sous la forme (2), σ_α, μ_m', γ_0' opèrent sur $z \left(= \frac{2\eta_2}{\xi_2}\right)$ les substitutions respectives $z+\alpha$, $-\frac{1}{z}$, $t_m^2 z$.

Soient $\mathfrak{N}_0'''$, σ_α, μ_m'', γ_0'', s'' les transformées de $\mathfrak{N}_0''$, σ_α', μ_m', γ_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 $2\eta_1\eta_2 = \xi_2^2$. C'est une nouvelle quadrique passant par s' et ayant avec chacune des quadriques (4) une génératrice commune. En transformant (4) par σ_α', on obtient des équations où les coefficients des puissances de α sont nuls, soit identiquement, soit d'après les équations des trois quadriques. (*Cf.* Lie, ***Theorie der Transformationsgruppen***, t. III, p. 182-190.)

substitution τ_2^{-1} de $\mathcal{G}(4, \pi)$ [qui répond à $R_{121}^{-1} = d_2 T_{12}$ de $B(5, \pi)$]. On aura

$$\sigma''_\alpha = V_{12,-\alpha} U_{12, \frac{\alpha^2}{2}} u_{1,-\frac{\alpha^3}{3}} u_{2,\alpha} = \left| \begin{array}{ll} \eta_1 & \eta_1 \\ \eta_2 & \alpha\eta_1 + \eta_2 \\ \xi_2 & \frac{\alpha^2}{2}\eta_1 - \alpha\eta_2 + \xi_2 \\ \xi_1 & \frac{\alpha^3}{6}\eta_1 + \frac{\alpha^2}{2}\eta_2 - \alpha\xi_2 + \xi_1 \end{array} \right|,$$

$$\mu''_m = m_{1,\frac{1}{m}}^{-1} m_{2,1,m}, \qquad \gamma''_0 = \tau_1 m_{1,\frac{1}{6}} m_{2,2} \tau_2,$$

et les équations de S'' sont

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

ou

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

Si -1 *est non carré*, σ''_α est la substitution $\sigma_\alpha^{(-1)}$ du n° **7**, et est transformée en σ_α par la substitution *de* A' qui multiplie η_1 et η_2 par -1 sans altérer les ξ.

Si -1 *est carré* $= \rho^2$, σ''_α est transformée en σ_α par $m_{1\rho} m_{2\rho}$.

33. 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 $x_1, y_1, \ldots, x_k, y_k$ inaltérées, et X_k ($\leq A_k^0$), X_k^0 ($\leq B_k$), $\sigma_{(k)\alpha}$, $\mu_{(k)}$, γ_k, Θ_k, $\beta_{(k)}$, ϖ_k les actions respectives de X, X^0, σ_α, μ, γ, Θ, β, ϖ sur les variables autres que $x_1, y_1, \ldots, x_k, y_k$ quand on regarde, dans cette action, $x_1, y_1, \ldots, x_k, y_k$ comme nuls, c'est-à-dire l'action de ces groupes sur les points de la multiplicité $x_1 = y_1 = \ldots = x_k = y_k = 0$. *On va voir que* $\{X^0, X_1^0, \ldots, X_{\nu-1}^0\} = B$ (*en entendant par là, si* $\nu = 1$, *que* $X^0 = B$).

Il est clair que $\sigma_{(1)\alpha}^{-1}\sigma_\alpha$ remplace y_k par $y_k + \sigma_{\alpha k 1} y_1$ pour $k = 2, \ldots, n-1$, c'est-à-dire qu'elle opère *sur* $y_2, \ldots, y_{n-1}$ comme

$$\chi_\alpha = U_{10,-\sigma_{\alpha,\nu+1,1}} \Pi_{j=2}^{\nu} V_{1j,-\sigma_{\alpha j 1}} U_{1j,-\sigma_{\alpha,n+1-j,1}}$$

(les V_{1j} et les U_{1j} sont permutables). Donc $\chi_\alpha^{-1}\sigma_{(1)\alpha}^{-1}\sigma_\alpha$ laisse y_1,

$y_2, \ldots, y_{n-1}$ inaltérés, et comme elle conserve a, elle laisse aussi y_n inaltéré. Donc elle se réduit à 1, et $\sigma_\alpha = \sigma_{(1)\alpha}\chi_\alpha$ (¹).

Le groupe $Z = \{X^0, B_1\}$ contient χ_α. Or, pour $k \geqq 3$, $V_{2k\lambda}$ 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} $(j \geqq 0)$. Donc, pour un choix convenable de λ, $V_{23\lambda}^{-1}\chi_\alpha V_{23\lambda}$ est une substitution de même forme que χ_α, contenue dans Z, mais où ne figurera plus V_{13}. A l'aide de $V_{24}, \ldots, V_{2\nu}$, on fera de même disparaître successivement $V_{14}, \ldots, V_{1\nu}$. 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 $U_{24}, \ldots, U_{2\nu}$, on fera disparaître $U_{14}, \ldots, U_{1\nu}$. *Donc Z contient une substitution de la forme* $V_{12\alpha}U_{12}U_{10}$. A l'aide de $U_{02\lambda}$, qui transforme $\left(\text{pour } e = \frac{1}{2}\right)$ $V_{12\alpha}$ en $V_{12\alpha}U_{12,-\frac{\alpha\lambda^2}{2}}U_{10,\alpha\lambda}$, $U_{10\mu}$ en $U_{12,-\lambda\mu}U_{10\mu}$, et est permutable à U_{12}, on peut faire disparaître U_{10}. *Donc Z contient une susbtitution* $V_{12\alpha}U_{12\lambda}$, 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_1 [I, **29**, (29)], donc aussi le produit $\Pi_{i=1}^{3} V_{12,\alpha\mu_i}U_{12,\frac{\lambda}{\mu_i}}$, μ_1, μ_2 et μ_3 étant trois valeurs arbitraires de μ. Or, *en supposant d'abord* $p \geqq 5$, on peut résoudre les deux équations $\Sigma_1^3 \mu_i = \xi$, $\sum_1^3 \frac{1}{\mu_i} = 0$, ξ 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 $d_k T_{2k}$ ($k \geqq 3$; cette opération est inutile si $n = 5$), qui est dans B_1 (I, **28**), on obtient toutes les V_{1k}. En les transformant par $\gamma = \Theta\beta$ (β est un produit de m_i), on obtient toutes les V_{k1}. En transformant les V_{1k} et les V_{k1} par $\gamma_1 = \Theta_1\beta_{(1)}$, 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

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

on a

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

d'où l'expression de σ_α par les U, V.

obtient les U_{k0} et les V_{0k} (I, **29**). *Donc* Z *contient* B. Or Z est $\leqq$ B. *Donc* $Z = \{X_0, B_1\} = B$.

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

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

on a

$$\{X^0, X_1^0, \ldots, X_{\nu-1}^0\} = B.$$

Si $p = 3$, n, qui est $\leqq p$ et impair, est égal à 3. Or B est alors isomorphe à $\mathfrak{C}(2, \pi)$. *Donc* $B = X_0$.

34. *Pour* $n \geqq 7$, *on a* $\{X^0, X_1^0, \ldots, X_{\nu-2}^0\} = B$.

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

$$\chi_\alpha = V_{10, -\frac{\alpha^3}{6}} V_{12, -\alpha} U_{12, -\frac{\alpha^5}{120}} V_{13, \frac{\alpha^2}{2}} U_{13, -\frac{\alpha^4}{24}},$$

donc aussi

$$\chi_\alpha \chi_{-\alpha} = V_{13, \alpha^2} U_{13, -\frac{\alpha^4}{12}} = s_\alpha,$$

et

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

$$\lambda = \alpha_1^2 + \alpha_2^2, \qquad \mu = -\frac{1}{12}(\alpha_1^4 + \alpha_2^4) = -\frac{1}{12}(\lambda^2 - 2\lambda\alpha_1^2 + 2\alpha_1^4).$$

α_1 et α_2 sont $\neq 0$. *Mais on peut supposer* λ *quelconque dans* $\mathfrak{S}$. Car si λ est non carré, α_1 et α_2 sont $\neq 0$ dans toutes les solutions (α_1, α_2) de l'équation $\alpha_1^2 + \alpha_2^2 = \lambda$, et si λ est carré, le nombre total des solutions est $\pi \pm 1 \geqq 6$ (*E.*, 44) (p est $\geqq n$), celui des solutions où $\alpha_1 \alpha_2 = 0$ étant évidemment 4.

Or, soient α'_1, α'_2 des déterminations de α analogues à α_1, α_2 et λ', μ' les déterminations correspondantes de λ, μ. Supposons que $\lambda' = -\lambda$, λ étant tel que

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

soit $\neq 0$. On a alors

$$s_{\alpha_1} s_{\alpha_2} s_{\alpha'_1} s_{\alpha'_2} = V_{13, \lambda+\lambda'} U_{13, \mu+\mu'} = U_{13, \mu+\mu'}.$$

Or $\{X, X_1\}$ contient

$$\sigma_{(1)\alpha} = U_{30, \alpha} U_{20, -\alpha} V_{23, -\alpha} U_{\ , -\frac{\alpha^3}{6}},$$

donc aussi (I, **29**)

$$\sigma_{(1)\alpha}^{-1} U_{13,\mu+\mu'} \sigma_{(1)\alpha} U_{13,\mu+\mu'}^{-1} = U_{12,\alpha(\mu+\mu)'},$$

donc toutes les U_{12}, donc aussi leurs transformées par γ_0, qui sont les $\mathbf{W}_{12}$, donc aussi $\mathbf{W}_{12}$ (I, **40**), que $\gamma_0\gamma_1 (= m_{13_1} t_1)$ transforme en $\mathbf{V}_{12}$. *Donc* $\{X^0, X_1^0\}$ *contient* B_{12}, donc aussi

$$\sigma_{(1)\alpha}^{-1} V_{12\lambda} \sigma_{(1)\alpha} = V_{12\lambda} U_{12, \frac{\lambda\alpha^4}{5} - \frac{\lambda\alpha^2}{2}} V_{13,\lambda\alpha} U_{13,-\frac{\lambda\alpha^3}{6}} U_{10,\lambda\alpha},$$

donc aussi $V_{13,\lambda\alpha} U_{13,-\frac{\lambda\alpha^3}{6}} U_{10,\lambda\alpha}$, ou, en écrivant λ pour $\lambda\alpha$, toutes les substitutions $V_{13\lambda} U_{13,-\frac{\lambda\alpha^2}{6}} U_{10\lambda} = s'_\alpha$, et $s'_{\alpha_1} s'_{\alpha_2} s'_{\alpha_3}$, α_1, α_2, α_3 étant quelconques $\neq 0$. Or, on peut choisir les α_i de manière que $\Sigma_1^3 \alpha_i^3 = 0$ (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'^{-1}_α, 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 γ_0 transforme en W_{13}, donc $\mathbf{W}_{13}$, que $\gamma_0\gamma_1$ transforme en $\mathbf{V}_{13}$. Donc $\{X^0, X_1^0\}$ contient B_{13}. Donc $\{X^0, X_1^0\}$, contenant les s'_α, contient les U_{10}, que γ_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 $n \geqq 7$, de la formule $\{X^0, B_1\} = B$, on voit alors par récurrence que $\{X^0, X_1^0, \ldots, X_{\nu-2}^0\} = B$.

(¹) L'équation $\Sigma_1^3 \alpha_i^3 = 0$ a toujours des solutions où α_1, α_2 et α_3 sont $\neq 0$. Car le nombre total des solutions est π^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 α_i est nul. Or, la condition $\pi^2 > 3(2\pi - 1)$ est toujours remplie pour $p \geqq 7$.