BULLETIN DE LA S. M. F.

J. A. DE SÉGUIER

Sur la forme canonique des substitutions linéaires

Bulletin de la S. M. F., tome 30 (1902), p. 247-252
<http://www.numdam.org/item?id=BSMF_1902__30__247_1>

SUR LA FORME CANONIQUE DES SUBSTITUTIONS LINÉAIRES;

Par M. de Séguier.

On peut établir simplement comme il suit la forme canonique des substitutions linéaires et quelques-unes de ses conséquences :

1. On démontrera d'abord, comme M. Jordan dans son *Cours d'Analyse* (t. III, p. 173), le théorème suivant :

Étant donnée une substitution linéaire $\alpha = (\alpha_{ik})$ *des variables* $x_1, \ldots, x_n$, *on peut toujours trouver* n *fonctions linéaires indépendantes des* x *formant une ou plusieurs suites* $y_1, \ldots, y_m; y'_1, \ldots, y'_m; \ldots$ *telles que* α *remplace les* y *d'une même suite* $y_1, \ldots, y_\mu, \ldots, y_m$ *respectivement par* $s_i y_1, \ldots, s_i(y_\mu + y_{\mu-1}), \ldots, s_i(y_m + y_{m-1})$ $(\mu \geqq 2)$, s_i *étant racine du déterminant caractéristique* Δ_α *de* α, *qu'il y ait au moins une suite répondant à chaque racine et que le nombre des* y *figurant dans les suites répondant à une racine coïncide avec la multiplicité de cette racine.*

Considérons maintenant le corps C résultant de l'adjonction des α_{ik} au corps des nombres rationnels ou au corps des nombres $0, 1, \ldots, p-1$ mod. p (p premier). Il s'agit de démontrer la proposition suivante :

Soit $\Delta_\alpha = \Pi_l f_l(s)^{\sigma_l}$ $(l = 1, \ldots, \delta)$ *la décomposition de* Δ_α *en facteurs irréductibles dans* C, f_l *étant de degré* ν_l *et ayant les racines* s_{lk_l} $(k = 0, \ldots, \nu_l - 1)$. *On peut faire :* 1° *qu'il y ait une suite* $y_1, \ldots, y_{m_l}$ *où les coefficients des* x *dans* y_i *appartiennent au corps* C_l *résultant de l'adjonction de* s_{l0} *à* C; 2° *qu'il y ait* ν_l *suites* S_{lk_l} *conjuguées* $y_{l1k_l}, \ldots, y_{lm_lk_l}$ $(y_{li0} = y_i)$; 3° *que s'il y a plusieurs suites* $S_{lj_lk_l}$ $(j_l = 1, \ldots, \mu_l;\ S_{l1k_l} = S_{lk_l})$, $y_{lj_l1k_l}, \ldots, y_{lj_lh_{lj_l}k_l}, \ldots, y_{lj_lm_{lj_l}k_l}$ $(y_{l1m_{l1}k_l} = y_{lm_lk_l})$, *formées avec la même* *racine s_{lk_l}, on ait $\Sigma_{j_l} m_{lj_l} = \sigma_l$. On aura ainsi pour chaque valeur de k_l une série $\mathcal{S}_{lk_l}$ de σ_l variables (réparties en μ_l suites) et ν_l séries conjuguées formant le système $\mathcal{S}_l$ relatif à $f_l(\Sigma_1^\delta \nu_l \sigma_l = n)$; si α_l est l'effet de α sur $\mathcal{S}_l$, les α_l sont permutables et $\alpha = \Pi_l \alpha_l$.*

J'omettrai dans la démonstration l'indice l, sauf à α_l, et j'écrirai m_k, s_k, y_{jhk}, S_k, $\mathcal{S}_k$, $\mathcal{S}$ pour m_{lk_l}, s_{lk_l}, $y_{lj_lh_{lj_l}k_l}$, S_{lk_l}, $\mathcal{S}_{lk_l}$, $\mathcal{S}_l$ respectivement.

Si tous les σ sont égaux à 1, la démonstration du théorème précédent suffit. Si $\sigma > 1$, on peut y supposer $s_i = s_0$ et elle fournit pour α une forme où figure $\mathcal{S}_0$. Or α transforme évidemment un polynome $\varphi(x_1, \ldots, x_n, s_0) = \varphi(s_0)$ à coefficients dans C en un polynome de même nature $\psi(s_0)$ et par suite $\varphi(s_k)$ en $\psi(s_k)$. Les variables de $\mathcal{S}_0$ étant indépendantes, celles de $\mathcal{S}_k$ le seront donc aussi. Mais de plus, cela est bien connu, les variables de $\mathcal{S}$ le seront. Car supposons que

$$\begin{aligned}\varphi = c_{11r} y_{11r} + \ldots + c_{\mu m_\mu r} y_{\mu m_\mu r} + \ldots \\ + c_{1,1,r+\rho} y_{1,1,r+\rho} + \ldots + c_{\mu, m_\mu, r+\rho} y_{\mu, m_\mu, r+\rho} + \ldots\end{aligned}$$

soit nulle, les coefficients des variables de $\mathcal{S}_r$ n'étant pas tous nuls. Soit $c_{\lambda\tau\theta}$ le premier coefficient $\neq 0$ à partir de la droite $(\theta \neq r)$. En transformant φ par α et en retranchant du résultat $s_\theta \varphi$, on aura une fonction nulle ne contenant plus $y_{\lambda\tau\theta}$, mais contenant les variables de $\mathcal{S}_r$. En répétant l'opération, on arriverait à une relation entre les y de $\mathcal{S}_r$.

Supposons alors $\neq 0$ le déterminant des coefficients de $x_1, \ldots, x_{\nu\sigma}$ dans les y_{jhk} $(j = 1, \ldots, \mu; h = 1, \ldots, m_j; k = 0, \ldots, \nu - 1)$. $s_0, \ldots, s_{\nu-1}$ figurant symétriquement dans les équations qui lient les

$$x_a \quad (a = 1, \ldots, \nu\sigma)$$

aux y et aux $x_{\nu\sigma+b}$ $(b = 1, \ldots, n'; n' = n - \nu\sigma)$, on aura

$$x_a = \Sigma_k \eta_{ak} + T_a,$$

T_a étant une fonction des $x_{\nu\sigma+b}$ à coefficients dans C et η_{ak} une fonction des y de $\mathcal{S}_k$ dont les coefficients sont des polynomes en s_k à coefficients dans C indépendants de k; α remplace $x_{\nu\sigma+b}$ par une expression de la forme

$$\Sigma_k \zeta_{bk} + \Sigma_c \beta_{bc} x_{\nu\sigma+c} \quad (c = 1, \ldots, n'), \qquad \zeta_{bk} = \Sigma_{jh} z_{bjhk} y_{jhk},$$

β_{bc} étant dans C et z_{bjhk} étant un polynome en s_k à coefficients dans C indépendants de k. En prenant pour variables les y et les $x_{\nu\sigma+b}$, on voit que le déterminant caractéristique $\Delta_\beta(s)$ de la matrice des β est $\Delta f^{-\sigma}$ et que par suite $\Delta_\beta(s_k) \neq 0$. Prenons alors pour variables les y et les fonctions

$$x'_b = x_{\nu\sigma+b} + \Sigma_k \upsilon_{bk}, \qquad \upsilon_{bk} = \Sigma_{jh} u_{bjhk} y_{jhk},$$

u_{bjhk} étant un polynome à coefficients indéterminés dans C mais indépendants de k, en sorte que υ_{bk} *est une fonction linéaire des x à coefficients dans* C; α transforme x'_b en

$$\Sigma_k \zeta_{bk} + \Sigma_c \beta_{bc}(x'_c - \Sigma_k \upsilon_{ck}) + \Sigma_k s_k(\upsilon_{bk} + \Sigma_{jh} u_{b,j,h+1,k} y_{jhk})$$
$$(u_{b,j,m_j+1,k} = 0).$$

Pour que les y disparaissent de cette expression, il faut et il suffit que les u vérifient

$$\Sigma_c \beta_{bc} u_{cjhk} - s_k(u_{bjhk} + u_{b,j,h+1,k}) = z_{bjhk}.$$

Pour $h = m_j$, ces équations, dont le déterminant est $\Delta_\beta(s_k) \neq 0$, donnent $u_{1jm_jk}, \ldots, u_{n'jm_jk}$. Ceux-là connus, les mêmes équations, pour $h = m_j - 1$, donnent $u_{1,j,m_j-1,k}, \ldots, u_{n',j,m_j-1,k}$; et ainsi de suite. Les u étant ainsi déterminés, on aura $\alpha = \alpha_1 \alpha_{x'}$, α_1 étant l'effet de α sur les y, $\alpha_{x'}$ une substitution à coefficients dans C n'opérant que sur les x' (fonctions linéaires des x à coefficients dans C) et $|\alpha_{x'}| = \Delta_\alpha f^{-\sigma}$. On est donc ramené à canoniser $\alpha_{x'}$ et la proposition est démontrée.

2. Soient

$$y'_{\lambda j_\lambda h_{\lambda j_\lambda} k_\lambda} = \Sigma_{l j_l h_{l j_l} k_l} u_{l j_l h_{l j_l} k_l}^{\lambda j_\lambda h_{\lambda j_\lambda} k_\lambda} y_{l j_l h_{l j_l} k_l}$$

de nouvelles variables. Pour qu'elles soient canoniques, il faut d'abord que α leur fasse subir la même substitution qu'aux y, chaque y' *correspondant* à l'y de mêmes indices, d'où la condition

$$(1) \qquad u_{l j_l h_{l j_l} k_l}^{\lambda j_\lambda h_{\lambda j_\lambda} k_\lambda}(s_{\lambda k_\lambda} - s_{l k_l}) = s_{l k_l} u_{l j_l h_{l j_l}+1\, k_l}^{\lambda j_\lambda h_{\lambda j_\lambda} k_\lambda} - s_{\lambda k_\lambda} u_{l j_l h_{l j_l} k_l}^{\lambda j_\lambda h_{\lambda j_\lambda}-1\, k_\lambda},$$

$u_{l j_l h_{l j_l} k_l}^{\lambda j_\lambda h_{\lambda j_\lambda} k_\lambda}$ étant nul si $h_{\lambda j_\lambda}$ est < 1 ou $> m_{\lambda j_\lambda}$ ou si $h_{l j_l}$ est < 1 ou $> m_{l j_l}$.

Soit $l \neq \lambda$ ou $k_l \neq k_\lambda$. En faisant $h_{\lambda j_\lambda} = 1$ et successivement $h_{l j_l} = m_{l j_l}, \ldots, 1$, on voit que $u^{\lambda j_\lambda 1 k_\lambda}_{l j_l h_{l j_l} k_l} = 0$ et, par récurrence, pour $h_{\lambda j_\lambda} = 2, 3, \ldots$, que $u^{\lambda j_\lambda h_{\lambda j_\lambda} k_\lambda}_{l j_l h_{l j_l} k_l} = 0$ si $l \neq \lambda$ ou si $k_l \neq k_\lambda$. Les y' d'une série doivent donc être des fonctions des y correspondants seulement. Le changement de variables pourra donc s'écrire $y'_{j'h'k'} = \Sigma_{jh} u^{j'h'k'}_{jhk} y_{jhk}$ et la condition (1) qui devient (en ne considérant qu'une série et en omettant l'indice k) $u^{j'h'}_{jh} = u^{j'\,h'-1}_{j\,h-1}$ (établie pour $h = 2, \ldots, m_j + 1$, $h' = 1, \ldots, m_{j'}$, m_j et $m_{j'}$ étant les nombres de variables de la j^e et de la j'^e suite respectivement) donne, par récurrence, $u^{j'h'}_{jh} = 0$ pour $h > h'$, $u^{j'h'}_{j1} = 0$ pour $h' = 1, \ldots, m_{j'} - m_j$ (si $m_{j'} > m_j$) et ne laisse indéterminés que $u^{j'h'}_{j1}$ pour $h' > m_{j'} - m_j$. Ainsi, μ étant le nombre des suites de la série,

$$
(2) \qquad \begin{cases}
y'_{j'1} = \Sigma_1^{u}\, u^{j'1}_{j1} y_{j1}, \\
y'_{j'2} = \Sigma_1^{\mu} (u^{j'2}_{j1} y_{j1} + u^{j'1}_{j1} y_{j2}), \\
y'_{j'3} = \Sigma_1^{\mu} (u^{j'3}_{j1} y_{j1} + u^{j'2}_{j1} y_{j2} + u^{j'1}_{j1} y_{j3}), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{cases}
$$

$$u^{j'h'}_{j1} = 0 \text{ pour } h' = 1, \ldots, m_{j'} - m_j \text{ si } m_{j'} > m_j.$$

Il faut encore que dans $y'_{j'h'k'}$, considérée comme fonction linéaire des x, les coefficients soient des polynomes en s_k à coefficients dans C indépendants de k. Or, les μ y_{j1} étant indépendants, on peut supposer que le déterminant des coefficients de $x_1, \ldots, x_\mu$ y est $\neq 0$. En écrivant que les coefficients de $x_1, \ldots, x_\mu$ dans $y'_{j'1}$ ont la forme voulue, on a des équations montrant que les $u^{j'1}_{j1}$ sont des polynomes en s_k à coefficients dans C indépendants de k. On le verra de même ensuite pour $u^{j'2}_{j1}$, puis pour $u^{j'3}_{j1}, \ldots$.

Ce changement de variables définit la forme générale α' d'une substitution linéaire des x à coefficients dans C *permutable à α* [1]. Car (2) montre la forme nécessaire de α' avec les variables y, et pour que α' soit une substitution linéaire des x à coefficients dans C, on voit, comme tout à l'heure, que les $u^{j'h'}_{jh}$ doivent être des polynomes en s_k à coefficients dans C indépendants de k.

---

(1) JORDAN, *Traité*, p. 128; DICKSON, *Linear Groups*, p. 229.

3. Cherchons le nombre de ces changements de variables (ou des substitutions α') quand C est un corps d'imaginaires de Galois d'ordre $\pi = p^m$ (p premier).

Tout d'abord le nombre des $u_{jh}^{j'h'}$ non nécessairement nuls est, pour chaque couple j, j', le plus petit $m_{jj'}$ des deux nombres m_j, $m_{j'}$. Mais ces $\Sigma m_{jj'}$ coefficients sont liés par la condition que le déterminant D de (2) soit $\neq 0$. Pour calculer D, rangeons les y et les y' de manière que $m_j \geqq m_{j+1}$, $m_{j'} \geqq m_{j'+1}$ [alors

$$\Sigma_{jj'} m_{jj'} = 2\Sigma_{(j'<j)} m_{jj'} - \Sigma m_{jj} = \Sigma_j (2j-1) m_j],$$

et soit

$$\begin{gathered} m_1 = \ldots = m_{\varepsilon_1} > m_{\varepsilon_1+1} = \ldots = m_{\varepsilon_1+\varepsilon_2} > m_{\varepsilon_1+\varepsilon_2+1} = \ldots \\ > m_{\varepsilon_1+\ldots+\varepsilon_{q-1}+1} = \ldots = m_{\varepsilon_1+\ldots+\varepsilon_q} \quad (\varepsilon_1 + \ldots + \varepsilon_q = \mu). \end{gathered}$$

Il y aura ε_r suites contenant $m_{\varepsilon_1+\ldots+\varepsilon_r}$ variables et, si

$$m_{\varepsilon_1+\ldots+\varepsilon_r} \geqq \rho > m_{\varepsilon_1+\ldots+\varepsilon_r+1}$$

(en faisant $m_{\mu+1} = 0$), $\mu_\rho = \varepsilon_1 + \ldots + \varepsilon_r$ suites contenant au moins ρ variables ($\mu_1 = \mu$). Rangeons alors les y' de manière que les $\mu_\rho\, y'_{j'\rho}$ se suivent dans l'ordre croissant des j' et que $y'_{1\,\rho+1}$ suive $y'_{\mu_\rho \rho}$, puis ordonnons $y'_{j'\rho}$ de manière que les $\mu_\rho\, y_{j\rho}$ se suivent dans l'ordre croissant des j et que $y_{1\,\rho+1}$ suive $y_{\mu_\rho \rho}$. $\pm$ D se réduira évidemment à un produit de mineurs principaux

$$D_\rho = |u_{j1}^{j'1}| (j, j' = 1, \ldots, \mu_\rho;\ \rho = m_1, \ldots, 1).$$

Or, dans D_ρ, $u_{j1}^{j'1} = 0$ pour $1 \leqq m_{j'} - m_j$, c'est-à-dire pour $m_j < m_{j'}$. Donc D_ρ se réduit aussi à un produit des mineurs principaux

$$\begin{aligned} D_{\rho 1} &= \Delta_1 = |u_{j1}^{j'1}| \ (j, j' = 1, \ldots, \varepsilon_1), \\ D_{\rho 2} &= \Delta_2 = |u_{j1}^{j'1}| \ (j, j' = \varepsilon_1 + 1, \ldots, \varepsilon_1 + \varepsilon_2), \ldots, \\ D_{\rho r} &= \Delta_r = |u_{j1}^{j'1}| \ (j, j' = \varepsilon_1 + \ldots + \varepsilon_{r-1} + 1, \ldots, \varepsilon_1 + \ldots + \varepsilon_r). \end{aligned}$$

Δ_1 entrera dans tous les D_ρ où $\mu_\rho \geqq \varepsilon_1$, c'est-à-dire dans $D_1, \ldots, D_{m_{\varepsilon_1}}$; $\ldots$; Δ_r entrera dans tous les D_ρ où $\mu_\rho \geqq \varepsilon_1 + \ldots + \varepsilon_r$, c'est-à-dire dans $D_1, \ldots, D_{m_{\varepsilon_1+\ldots+\varepsilon_r}}$. Donc $\pm D = \Pi_{r=1}^{r=q} \Delta_r^{m_{\varepsilon_1+\ldots+\varepsilon_r}}$. Δ_r contenant ε_r^2 éléments, il y a, hors de Δ, $K = \Sigma m_{jj'} - \Sigma_1^q \varepsilon_r^2$ arbitraires dont chacune a π^ν déterminations, ν étant le degré du facteur irréductible annulé par s_k, et l'on sait que le nombre des déterminations du Tableau des éléments de Δ_r qui donnent $\Delta_r \neq 0$ est

$$\Pi_{i=0}^{\varepsilon_r-1}(\pi^{r\varepsilon_r} - \pi^{\nu i}) = \varpi(r, \nu).$$

Donc le nombre des déterminations du système considéré des $y'_{j'h'k'}$, que je supposerai être le λ^e, est

$$\pi^{k\nu}\,\Pi_{r=1}^{q}\,\varpi(r, \nu) = \psi(\lambda).$$

Le nombre des changements de variables (ou des α') est $\Pi_1^{\delta}\psi(\lambda)$.

L'ordre du groupe L formé par les substitutions linéaires à coefficients dans C, étant $\Pi_{i=0}^{n-1}(\pi^n - \pi^i)$, on connaîtra par là le nombre des conjuguées de α dans L.