

BULLETIN DE LA S. M. F.

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>](http://www.numdam.org/item?id=BSMF_1902_30_247_1)

© Bulletin de la S. M. F., 1902, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>*

SUR 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, \dots, x_n , on peut toujours trouver n fonctions linéaires indépendantes des x formant une ou plusieurs suites $y_1, \dots, y_m; y'_1, \dots, y'_m; \dots$ telles que α remplace les y d'une même suite $y_1, \dots, y_m, \dots, y_m$ respectivement par $s_1 y_1, \dots, s_1(y_m + y_{m-1}), \dots, s_1(y_m + y_{m-1})$ ($\mu \geq 2$), 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 $0, 1, \dots, p-1 \text{ mod. } p$ (p premier). Il s'agit de démontrer la proposition suivante :

Soit $\Delta_\alpha = \prod_l f_l(s)^{\alpha_l}$ ($l = 1, \dots, \delta$) la décomposition de Δ_α en facteurs irréductibles dans C , f_l étant de degré ν_l et ayant les racines s_{l,k_l} ($k = 0, \dots, \nu_l - 1$). On peut faire : 1° qu'il y ait une suite y_1, \dots, y_{m_l} où les coefficients des x dans y_i appartiennent au corps C_l résultant de l'adjonction de $s_{l,0}$ à C ; 2° qu'il y ait ν_l suites S_{l,k_l} conjuguées $y_{11,k_l}, \dots, y_{1m_l,k_l}$ ($y_{1l,0} = y_1$); 3° que s'il y a plusieurs suites S_{l,j_l,k_l} ($j_l = 1, \dots, \mu_l$; $S_{l,k_l} = S_{l,1,k_l}$), $y_{1j_l,k_l}, \dots, y_{1j_lh_{j_l}k_l}, \dots, y_{1j_lm_{j_l}k_l}$ ($y_{11m_{j_l}k_l} = y_{1m_lk_l}$), formées avec la même

racine s_{lk_l} , on ait $\sum_{j_l} m_{lj_l} = \sigma_l$. On aura ainsi pour chaque valeur de k_l une série s_{lk_l} de σ_l variables (réparties en μ_l suites) et ν_l séries conjuguées formant le système s_l relatif à $f_l(\sum_i \nu_i \sigma_i = n)$; si α_l est l'effet de α sur s_l , les α_l sont permutable et $\alpha = \prod_l \alpha_l$.

J'omettrai dans la démonstration l'indice l , sauf à α_l , et j'écrirai $m_k, s_k, y_{j_h k}, S_k, s_k, s$ pour $m_{lk_l}, s_{lk_l}, y_{lj_l k_l}, S_{lk_l}, s_{lk_l}, s_l$ 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 s_0 . Or α transforme évidemment un polynôme $\varphi(x_1, \dots, x_n, s_0) = \varphi(s_0)$ à coefficients dans C en un polynôme de même nature $\psi(s_k)$ et par suite $\varphi(s_k)$ en $\psi(s_k)$. Les variables de s_0 étant indépendantes, celles de s_k le seront donc aussi. Mais de plus, cela est bien connu, les variables de s le seront. Car supposons que

$$\begin{aligned} \varphi = & c_{11r} y_{11r} + \dots + c_{\mu m \mu r} y_{\mu m \mu r} + \dots \\ & + c_{1,1,r+\rho} y_{1,1,r+\rho} + \dots + c_{\mu, m \mu, r+\rho} y_{\mu, m \mu, r+\rho} + \dots \end{aligned}$$

soit nulle, les coefficients des variables de s_r n'étant pas tous nuls. Soit $c_{\lambda \neq 0}$ le premier coefficient $\neq 0$ à partir de la droite ($\theta \neq r$). En transformant φ par α et en retranchant du résultat $s_0 \varphi$, on aura une fonction nulle ne contenant plus $y_{\lambda \neq 0}$, mais ~~contenant~~ les variables de s_r . En répétant l'opération, on arriverait à une relation entre les y de s_r .

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

$$x_\alpha \quad (\alpha = 1, \dots, \nu \sigma)$$

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

$$x_\alpha = \sum_k \eta_{\alpha k} + T_\alpha,$$

T_α étant une fonction des $x_{\nu \sigma + b}$ à coefficients dans C et $\eta_{\alpha k}$ une fonction des y de s_k dont les coefficients sont des polynômes en s_k à coefficients dans C indépendants de k ; α remplace $x_{\nu \sigma + b}$ par une

expression de la forme

$$\Sigma_k \zeta_{bk} + \Sigma_c \beta_{bc} x_{v\sigma+c} \quad (c = 1, \dots, n'), \quad \zeta_{bk} = \Sigma_{jh} z_{bjhk} y_{jhhk},$$

β_{bc} étant dans C et z_{bjhk} étant un polynôme en s_k à coefficients dans C indépendants de k . En prenant pour variables les y et les $x_{v\sigma+b}$, 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

$$x'_b = x_{v\sigma+b} + \Sigma_k v_{bk}, \quad v_{bk} = \Sigma_{jh} u_{bjhk} y_{jhhk},$$

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

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

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 $u_{tjm_jk}, \dots, u_{n'jm_jk}$. Ceux-là connus, les mêmes équations, pour $h = m_j - 1$, donnent $u_{t,j,m_j-1,k}, \dots, u_{n',j,m_j-1,k}$; et ainsi de suite. Les u étant ainsi déterminés, on aura $\alpha = \alpha_x, \alpha_{x'}$, α_x 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

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

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

$$(1) \quad u_{l j_l h_{j_l} k_l}^{\lambda j_h h_{\lambda j_h} k_h} (s_{\lambda k_h} - s_{l k_l}) = s_{l k_l} u_{l j_l h_{j_l} k_l}^{\lambda j_h h_{\lambda j_h} k_h} - s_{\lambda k_h} u_{l j_l h_{j_l} k_l}^{\lambda j_h h_{\lambda j_h} k_h},$$

$u_{l j_l h_{j_l} k_l}^{\lambda j_h h_{\lambda j_h} k_h}$ étant nul si $h_{\lambda j_h}$ est < 1 ou $> m_{\lambda j_h}$ 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 $h_{lj_l} = m_{lj_l}, \dots, 1$, on voit que $u_{ij_l h_{lj_l} k_l}^{\lambda j_l h_{lj_l} k_l} = 0$ et, par récurrence, pour $h_{\lambda j_\lambda} = 2, 3, \dots$, que $u_{ij_l h_{lj_l} k_l}^{\lambda j_l h_{lj_l} k_l} = 0$ 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 $y'_{jh'k} = \sum_{jh} u_{jh'k}^{jh'k} y_{jhk}$ et la condition (1) qui devient (en ne considérant qu'une série et en omettant l'indice k) $u_{jh}^{jh'} = u_{jh-1}^{jh'-1}$ (établie pour $h = 2, \dots, m_j + 1, h' = 1, \dots, m_{j'}, m_j$ et $m_{j'}$ étant les nombres de variables de la j^e et de la j'^e suite respectivement) donne, par récurrence, $u_{jh}^{jh'} = 0$ pour $h > h'$, $u_{j1}^{jh'} = 0$ pour $h' = 1, \dots, m_{j'} - m_j$ (si $m_{j'} > m_j$) et ne laisse indéterminés que $u_{j1}^{jh'}$ pour $h' > m_{j'} - m_j$. Ainsi, μ étant le nombre des suites de la série,

$$(2) \quad \begin{cases} y'_{j1} = \Sigma_1^\mu u_{j1}^{j1} y_{j1}, \\ y'_{j2} = \Sigma_1^\mu (u_{j1}^{j2} y_{j1} + u_{j1}^{j1} y_{j2}), \\ y'_{j3} = \Sigma_1^\mu (u_{j1}^{j3} y_{j1} + u_{j1}^{j2} y_{j2} + u_{j1}^{j1} y_{j3}), \\ \dots \\ u_{j1}^{jh'} = 0 \text{ pour } h' = 1, \dots, m_{j'} - m_j \text{ si } m_{j'} > m_j. \end{cases}$$

Il faut encore que dans $y'_{jh'k}$, 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_{ji} étant indépendants, on peut supposer que le déterminant des coefficients de x_1, \dots, x_μ dans y'_{j1} est $\neq 0$. En écrivant que les coefficients de x_1, \dots, x_μ dans y'_{j1} ont la forme voulue, on a des équations montrant que les u_{j1}^{j1} sont des polynomes en s_k à coefficients dans C indépendants de k . On le verra de même ensuite pour u_{j1}^{j2} , puis pour u_{j1}^{j3}, \dots

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 $u_{jh}^{jh'}$ 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 $u_{jk}^{ij'}$ 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 $m_j \geq m_{j+1}, m_{j'} \geq m_{j'+1}$ [alors

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

et soit

$$\begin{aligned} m_1 &= \dots = m_{\epsilon_1} > m_{\epsilon_1+1} = \dots = m_{\epsilon_1+\epsilon_2} > m_{\epsilon_1+\epsilon_2+1} = \dots \\ &> m_{\epsilon_1+\dots+\epsilon_{q-1}+1} = \dots = m_{\epsilon_1+\dots+\epsilon_q} \quad (\epsilon_1 + \dots + \epsilon_q = \mu). \end{aligned}$$

Il y aura ϵ_r suites contenant $m_{\epsilon_1+\dots+\epsilon_r}$ variables et, si

$$m_{\epsilon_1+\dots+\epsilon_r} \geq \rho > m_{\epsilon_1+\dots+\epsilon_{r+1}}$$

(en faisant $m_{\mu+1} = 0$), $\mu_r = \epsilon_1 + \dots + \epsilon_r$ suites contenant au moins ρ variables ($\mu_1 = \mu$). Rangeons alors les y' de manière que les $\mu_r y'_{j\rho}$ se suivent dans l'ordre croissant des j' et que $y'_{1\rho+1}$ suive $y'_{\mu_r \rho}$, puis ordonnons $y'_{j\rho}$ de manière que les $\mu_r y_{j\rho}$ se suivent dans l'ordre croissant des j et que $y_{1\rho+1}$ suive $y_{\mu_r \rho}$. $\pm D$ se réduira évidemment à un produit de mineurs principaux

$$D_\rho = | u_{j1}^{i1} | (j, j' = 1, \dots, \mu_r; \rho = m_1, \dots, 1).$$

Or, dans D_ρ , $u_{j1}^{i1} = 0$ pour $i \leq m_{j'} - m_j$, c'est-à-dire pour $m_j < m_{j'}$. Donc D_ρ se réduit aussi à un produit des mineurs principaux

$$D_{\rho_1} = \Delta_1 = | u_{j1}^{i1} | (j, j' = 1, \dots, \epsilon_1),$$

$$D_{\rho_2} = \Delta_2 = | u_{j1}^{i1} | (j, j' = \epsilon_1 + 1, \dots, \epsilon_1 + \epsilon_2), \dots,$$

$$D_{\rho_r} = \Delta_r = | u_{j1}^{i1} | (j, j' = \epsilon_1 + \dots + \epsilon_{r-1} + 1, \dots, \epsilon_1 + \dots + \epsilon_r).$$

Δ_1 entrera dans tous les D_ρ où $\mu_r \geq \epsilon_1$, c'est-à-dire dans $D_1, \dots, D_{m_{\epsilon_1}}$; Δ_r entrera dans tous les D_ρ où $\mu_r \geq \epsilon_1 + \dots + \epsilon_r$, c'est-à-dire dans $D_1, \dots, D_{m_{\epsilon_1+\dots+\epsilon_r}}$. Donc $\pm D = \prod_{r=1}^{r=q} \Delta_r^{m_{\epsilon_1+\dots+\epsilon_r}}$. Δ_r contenant ϵ_r^2 éléments, il y a, hors de Δ , $K = \Sigma m_{jj'} - \Sigma \epsilon_r^2$ arbitraires dont chacune a π^v déterminations, v étant le degré du facteur irréductible annulé par s_k , et l'on sait que le nombre des détermina-

tions du Tableau des éléments de Δ_r , qui donnent $\Delta_r \neq 0$ est

$$\Pi_{i=0}^{\varepsilon_r-1} (\pi^{r\varepsilon_r} - \pi^{v_i}) = w(r, v).$$

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

$$\pi^{kv} \Pi_{r=1}^q w(r, v) = \psi(\lambda).$$

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.
