

# 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](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  $\alpha$  remplace les  $y$  d'une même suite  $y_1, \dots, y_\mu, \dots, y_m$  respectivement par  $s_i y_1, \dots, s_i(y_\mu + y_{\mu-1}), \dots, s_i(y_m + y_{m-1})$  ( $\mu \geq 2$ ),  $s_i$  étant racine du déterminant caractéristique  $\Delta_\alpha$  de  $\alpha$ , 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  $\alpha_{ik}$  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  $\Delta_\alpha = \prod_l f_l(s)^{\sigma_l}$  ( $l = 1, \dots, \delta$ ) la décomposition de  $\Delta_\alpha$  en facteurs irréductibles dans  $C$ ,  $f_l$  étant de degré  $\nu_l$  et ayant les racines  $s_{lk}$  ( $k = 0, \dots, \nu_l - 1$ ). 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  $s_{l0}$  à  $C$ ; 2° qu'il y ait  $\nu_l$  suites  $S_{lk}$  conjuguées  $y_{l1k_1}, \dots, y_{lm_l k_1}$  ( $y_{li0} = y_i$ ); 3° que s'il y a plusieurs suites  $S_{lj_1 k_1}$  ( $j_1 = 1, \dots, \mu_l; S_{l1 k_1} = S_{lk_1}$ ),  $y_{lj_1 k_1}, \dots, y_{lj_1 h_{j_1} k_1}, \dots, y_{lj_1 m_{j_1} k_1}$  ( $y_{lj_1 m_{j_1} k_1} = y_{lm_l k_1}$ ), formées avec la même*

racine  $s_{lk_1}$ , on ait  $\sum_j m_{lj_1} = \tau_l$ . On aura ainsi pour chaque valeur de  $k_l$  une série  $s_{lk_1}$  de  $\sigma_l$  variables (réparties en  $\mu_l$  suites) et  $\nu_l$  séries conjuguées formant le système  $s_l$  relatif à  $f_l(\sum_i \nu_i \sigma_i = n)$ ; si  $\alpha_l$  est l'effet de  $\alpha$  sur  $s_l$ , les  $\alpha_l$  sont permutable et  $\alpha = \Pi_l \alpha_l$ .

J'omettrai dans la démonstration l'indice  $l$ , sauf à  $\alpha_l$ , et j'écrirai  $m_k, s_k, \gamma_{jkk}, S_k, s_k, s$  pour  $m_{lk_1}, s_{lk_1}, \gamma_{lj_1 k_1 k_1}, S_{lk_1}, s_{lk_1}, s_l$  respectivement.

Si tous les  $\sigma$  sont égaux à 1, la démonstration du théorème précédent suffit. Si  $\sigma > 1$ , on peut y supposer  $s_l = s_0$  et elle fournit pour  $\alpha$  une forme où figure  $s_0$ . Or  $\alpha$  transforme évidemment un polynome  $\varphi(x_1, \dots, x_n, s_0) = \varphi(s_0)$  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  $s_0$  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

$$\varphi = c_{11r} \gamma_{11r} + \dots + c_{\mu m_\mu r} \gamma_{\mu m_\mu r} + \dots + c_{1,1,r+\rho} \gamma_{1,1,r+\rho} + \dots + c_{\mu,m_\mu,r+\rho} \gamma_{\mu,m_\mu,r+\rho} + \dots$$

soit nulle, les coefficients des variables de  $s_r$  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  $\varphi$  par  $\alpha$  et en retranchant du résultat  $s_0 \varphi$ , on aura une fonction nulle ne contenant plus  $\gamma_{\lambda\tau\theta}$ , mais contenant les variables de  $s_r$ . En répétant l'opération, on arriverait à une relation entre les  $\gamma$  de  $s_r$ .

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

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

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

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

$T_a$  étant une fonction des  $x_{\nu\sigma+b}$  à coefficients dans C et  $\eta_{ak}$  une fonction des  $\gamma$  de  $s_k$  dont les coefficients sont des polynomes en  $s_k$  à coefficients dans C indépendants de  $k$ ;  $\alpha$  remplace  $x_{\nu\sigma+b}$  par une

expression de la forme

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

$\beta_{bc}$  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  $x_{v\sigma+b}$ , on voit que le déterminant caractéristique  $\Delta_\beta(s)$  de la matrice des  $\beta$  est  $\Delta f^{-\sigma}$  et que par suite  $\Delta_\beta(s_k) \neq 0$ . Prenons alors pour variables les  $y$  et les fonctions

$$x'_b = x_{v\sigma+b} + \Sigma_k v_{bk}, \quad v_{bk} = \Sigma_{jh} u_{bjhk} \mathcal{Y}_{jhk},$$

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

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

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  $u_{1jm_jk}, \dots, u_{n'jm_jk}$ . Ceux-là connus, les mêmes équations, pour  $h = m_j - 1$ , donnent  $u_{1,j,m_j-1,k}, \dots, u_{n',j,m_j-1,k}$ ; et ainsi de suite. Les  $u$  étant ainsi déterminés, on aura  $\alpha = \alpha_1 \alpha_{x'}$ ,  $\alpha_1$  étant l'effet de  $\alpha$  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

$$y'^{\lambda_{i_1} h_{i_1} k_{i_1}} = \Sigma_{i_1 i_2} u_{i_1 i_2}^{\lambda_{i_1} h_{i_1} k_{i_1}} y_{i_1 i_2}^{\lambda_{i_1} h_{i_1} k_{i_1}}$$

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

$$(1) \quad u_{i_1 i_2}^{\lambda_{i_1} h_{i_1} k_{i_1}} (s_{\lambda_{i_1}} - s_{\lambda_{i_2}}) = s_{\lambda_{i_2}} u_{i_1 i_2}^{\lambda_{i_1} h_{i_1} k_{i_1}} - s_{\lambda_{i_1}} u_{i_1 i_2}^{\lambda_{i_1} h_{i_1} k_{i_1}-1},$$

$u_{i_1 i_2}^{\lambda_{i_1} h_{i_1} k_{i_1}}$  étant nul si  $h_{\lambda_{i_1}}$  est  $< 1$  ou  $> m_{\lambda_{i_1}}$  ou si  $h_{i_2}$  est  $< 1$  ou  $> m_{i_2}$ .

Soit  $l \neq \lambda$  ou  $k_l \neq k_\lambda$ . En faisant  $h_{\lambda j_\lambda} = 1$  et successivement  $h_{l j_l} = m_{l j_l}, \dots, 1$ , on voit que  $u_{l_i h_{j_l} k_l}^{\lambda j_\lambda k_\lambda} = 0$  et, par récurrence, pour  $h_{\lambda j_\lambda} = 2, 3, \dots$ , que  $u_{l_i h_{j_l} k_l}^{\lambda j_\lambda k_\lambda} = 0$  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  $y'_{j' h' k'} = \sum_{j h k} u_{j h k}^{j' h' k'} y_{j h k}$  et la condition (1) qui devient (en ne considérant qu'une série et en omettant l'indice  $k$ )  $u_{j h}^{j' h'} = u_{j h-1}^{j' h'-1}$  (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,  $u_{j h}^{j' h'} = 0$  pour  $h > h'$ ,  $u_{j h}^{j' h'} = 0$  pour  $h' = 1, \dots, m_{j'} - m_j$  (si  $m_{j'} > m_j$ ) et ne laisse indéterminés que  $u_{j h}^{j' h'}$  pour  $h' > m_{j'} - m_j$ . Ainsi,  $\mu$  étant le nombre des suites de la série,

$$(2) \quad \begin{cases} y'_{j'1} = \sum_1^\mu u_{j'1}^{j'1} y_{j1}, \\ y'_{j'2} = \sum_1^\mu (u_{j'2}^{j'2} y_{j1} + u_{j'1}^{j'2} y_{j2}), \\ y'_{j'3} = \sum_1^\mu (u_{j'3}^{j'3} y_{j1} + u_{j'2}^{j'3} y_{j2} + u_{j'1}^{j'3} y_{j3}), \\ \dots \end{cases}$$

$$u_{j'1}^{j' h'} = 0 \text{ pour } h' = 1, \dots, m_{j'} - m_j \text{ si } m_{j'} > m_j.$$

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  $\mu y_{j1}$  étant indépendants, on peut supposer que le déterminant des coefficients de  $x_1, \dots, x_\mu$  y est  $\neq 0$ . En écrivant que les coefficients de  $x_1, \dots, x_\mu$  dans  $y'_{j'1}$  ont la forme voulue, on a des équations montrant que les  $u_{j'1}^{j'1}$  sont des polynomes en  $s_k$  à coefficients dans  $C$  indépendants de  $k$ . On le verra de même ensuite pour  $u_{j'1}^{j'2}$ , puis pour  $u_{j'1}^{j'3}, \dots$

Ce changement de variables définit la forme générale  $\alpha'$  d'une substitution linéaire des  $x$  à coefficients dans  $C$  permutable à  $\alpha$  (1). Car (2) montre la forme nécessaire de  $\alpha'$  avec les variables  $y$ , et pour que  $\alpha'$  soit une substitution linéaire des  $x$  à coefficients dans  $C$ , on voit, comme tout à l'heure, que les  $u_{j h}^{j' h'}$  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  $\alpha'$ ) quand C est un corps d'imaginaires de Galois d'ordre  $\pi = p^m$  ( $p$  premier).

Tout d'abord le nombre des  $u_{j'k}^{j'k}$  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

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

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

$$m_{\varepsilon_1+\dots+\varepsilon_r} \geq \rho > m_{\varepsilon_1+\dots+\varepsilon_{r+1}}$$

(en faisant  $m_{\mu+1} = 0$ ),  $\mu_\rho = \varepsilon_1 + \dots + \varepsilon_r$  suites contenant au moins  $\rho$  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

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

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

$$\begin{aligned} D_{\rho_1} &= \Delta_1 = |u_{j'1}^{j'1}| (j, j' = 1, \dots, \varepsilon_1), \\ D_{\rho_2} &= \Delta_2 = |u_{j'1}^{j'1}| (j, j' = \varepsilon_1 + 1, \dots, \varepsilon_1 + \varepsilon_2), \dots, \\ D_{\rho_r} &= \Delta_r = |u_{j'1}^{j'1}| (j, j' = \varepsilon_1 + \dots + \varepsilon_{r-1} + 1, \dots, \varepsilon_1 + \dots + \varepsilon_r). \end{aligned}$$

$\Delta_1$  entrera dans tous les  $D_\rho$  où  $\mu_\rho \geq \varepsilon_1$ , c'est-à-dire dans  $D_1, \dots, D_{m_{\varepsilon_1}}$ ;  $\dots$ ;  $\Delta_r$  entrera dans tous les  $D_\rho$  où  $\mu_\rho \geq \varepsilon_1 + \dots + \varepsilon_r$ , c'est-à-dire dans  $D_1, \dots, D_{m_{\varepsilon_1+\dots+\varepsilon_r}}$ . Donc  $\pm D = \prod_{r=1}^{r=q} \Delta_r^{m_{\varepsilon_1+\dots+\varepsilon_r}}$ .  $\Delta_r$  contenant  $\varepsilon_r^2$  éléments, il y a, hors de  $\Delta, K = \Sigma m_{jj'} - \Sigma \varepsilon_r^2$  arbitraires dont chacune a  $\pi^\nu$  déterminations,  $\nu$  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  $\Delta_r$  qui donnent  $\Delta_r \neq 0$  est

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

Donc le nombre des déterminations du système considéré des  $\mathcal{Y}'_{j'k'k'}$ , que je supposerai être le  $\lambda^0$ , est

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

Le nombre des changements de variables (ou des  $\alpha'$ ) est  $\prod_1^{\delta} \psi(\lambda)$ .

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

---