"Memoirs and Proceedings of the Manchester Literary and Philosophical Society," Vol. XLIV., Pts. 2, 3; 1900.

"Proceedings of the Royal Irish Academy," Series 3, Vol. v., No. 4; Dublin, 1900.

Linear Substitutions Commutative with a Given Substitution.

By L. E. DICKSON, Ph.D. Received May 8th, 1900. Communicated May 10th, 1900.

1. The object of this note is to determine the explicit form of all m-ary linear homogeneous substitutions T with coefficients in the $GF[p^n]$ which are commutative with a particular one S. For the case $n = 1$, the number of such substitutions T has been determined by M. Jordan,* whose method of proof was, however, limited to the consideration of a particular example. By the use of convenient notations, we may treat the general case with equal ease and, moreover, avoid the separation of the proof into two successive stages. Following M. Jordan, I first give to S its canonical form† S_1.

2. Let the characteristic determinant of S be

$$\Delta(K) \equiv [F_k(K)]^\alpha [F_l(K)]^\beta \ldots \quad (m \equiv k\alpha + l\beta + \ldots),$$

where $F_k(K)$, $F_l(K)$, ... are distinct polynomials belonging to, and irreducible in, the $GF[p^n]$. We may exhibit the roots of $F_k(K) = 0$ and of $F_l(L) = 0$ in the following notation:—

$$K_0, \quad K_1 \equiv K_0^{p^n}, \quad \ldots, \quad K_{k-1} \equiv K_0^{p^{n(k-1)}};$$

$$L_0, \quad L_1 \equiv L_0^{p^n}, \quad \ldots, \quad L_{l-1} \equiv L_0^{p^{n(l-1)}}.$$

To simplify the formulæ, we suppose that F_k and F_l are the only irreducible factors of $\Delta(K)$. The method is, however, seen to be general.

Corresponding to each partition of α and β into positive integers,

---

* *Traité des Substitutions*, pp. 128–136.

† "Canonical Form of a Linear Homogeneous Substitution in a Galois Field," *American Journal of Mathematics*, Vol. XXII., No. 2, April, 1900. The proof of the generalization of Jordan's theorem is there made by induction.

we obtain a canonical form of an m-ary substitution in the $GF[p^n]$. Let

$$\alpha \equiv a_1+a_2+\ldots+a_{r+1}, \quad \beta \equiv b_1+b_2+\ldots+b_{s+1}.$$

It will be convenient to let e denote any one of the integers

$$(e) \qquad 1, \quad a_1+1, \quad a_1+a_2+1, \quad \ldots, \quad a_1+a_2+\ldots+a_r+1;$$

and E any one of the remaining integers $\leqq \alpha$. Let b denote any one of the integers $1, b_1+1, \ldots, b_1+b_2+\ldots+b_s+1$; and B any one of the remaining integers $\leqq \beta$. The general canonical form may now be written:

$$S_1: \begin{cases} \eta'_{ij} = K_i\eta_{ij} & (i=0,1,\ldots,k-1;\ j \text{ any } e) \\ \eta'_{ij} = K_i\eta_{ij}+K_i\eta_{ij-1} & (i=0,1,\ldots,k-1;\ j \text{ any } E) \\ \zeta'_{ij} = L_i\zeta_{ij} & (i=0,1,\ldots,l-1;\ j \text{ any } b) \\ \zeta'_{ij} = L_i\zeta_{ij}+L_i\zeta_{ij-1} & (i=0,1,\ldots,l-1;\ j \text{ any } B). \end{cases}$$

3. An arbitrary linear homogeneous substitution on these indices may be exhibited as follows:

$$(T'_1): \begin{cases} \eta'_{ij} = \Sigma\alpha^{ij}_{tu}\eta_{tu}+\Sigma\beta^{ij}_{vw}\zeta_{vw} & (i=0,\ldots,k-1;\ j=1,\ldots,\alpha) \\ \zeta'_{ij} = \Sigma\gamma^{ij}_{tu}\eta_{tu}+\Sigma\delta^{ij}_{vw}\zeta_{vw} & (i=0,\ldots,l-1;\ j=1,\ldots,\beta), \end{cases}$$

where, as henceforth, the summation indices t, u, v, w run through the series

$$t=0,1,\ldots,k-1; \quad v=0,1,\ldots,l-1; \quad u=1,\ldots,\alpha; \quad w=1,\ldots,\beta.$$

We investigate the conditions under which T_1 is commutative with S_1. Equating the functions by which T_1S_1 and S_1T_1 replace η_{ie}, we get

$$K_i\sum_{t,u}\alpha^{ie}_{tu}\eta_{tu}+K_i\sum_{v,w}\beta^{ie}_{vw}\zeta_{vw} \equiv \sum_{t,u}\alpha^{ie}_{tu}K_t\eta_{tu}+\sum_{t,E}\alpha^{ie}_{tE}K_t\eta_{tE-1} + \sum_{v,w}\beta^{ie}_{vw}L_v\zeta_{vw}+\sum_{v,B}\beta^{ie}_{vB}L_v\zeta_{vB-1}.$$

This identity in the variables η and ζ requires

$$\begin{aligned} K_i\alpha^{ie}_{tu} &= K_t\alpha^{ie}_{tu} && (u \neq E-1), \\ K_i\alpha^{ie}_{tE-1} &= K_t\alpha^{ie}_{tE-1}+K_t\alpha^{ie}_{tE}, \\ K_i\beta^{ie}_{vw} &= L_v\beta^{ie}_{vw} && (w \neq B-1), \\ K_i\beta^{ie}_{vB-1} &= L_v\beta^{ie}_{vB-1}+L_v\beta^{ie}_{vB}. \end{aligned}$$

For $t=i$, the first two equations give merely $\alpha^{ie}_{iE}=0$. For $t \neq i$,

$K_i \neq K_t$, and the first equation gives $\alpha_{t\,e'-1}^{i\,e} = 0$, e' being any integer > 1 of the set (e). If $e'-1$ is an E, the second equation gives $\alpha_{t\,e'-2}^{i\,e} = 0$; in the contrary case, $e'-2 \neq E-1$, and the same result follows from the first equation. Next, according as $e'-2$ is or is not an E, the second or first equation gives $\alpha_{t\,e'-3}^{i\,e} = 0$. Proceeding thus, we find that every $\alpha_{tc}^{ie} = 0$ $(t \neq i,\ c$ arbitrary$)$.

Since $K_i \neq L_v$, the third and fourth equations require, for similar reasons, that every $\beta_{vc}^{ie} = 0$ $(c$ arbitrary$)$.

It follows that T_1 replaces η_{ie} by $\sum_{e'} \alpha_{ie'}^{ie}\,\eta_{ie'}$.

Denote by e_1 (or by e_1') an arbitrary e such that e_1+1 is an E, and by $\bar{e}_1$ any one of the remaining e's, so that $\bar{e}_1+1$ is an e. Equating the functions by which T_1S_1 and S_1T_1 replace $\eta_{i\,e_1+1}$, we get

$$K_i \sum_{t,u} \alpha_{tu}^{i\,e_1+1}\,\eta_{tu} + K_i \sum_{e} \alpha_{ie}^{i\,e_1}\,\eta_{ie} + K_i \sum_{v,w} \beta_{vw}^{i\,e_1+1}\,\zeta_{vw}$$
$$\equiv \sum_{t,u} \alpha_{tu}^{i\,e_1+1} K_t\,\eta_{tu} + \sum_{t,E} \alpha_{tE}^{i\,e_1+1} K_t\,\eta_{t\,E-1} + \sum_{v,w} \beta_{vw}^{i\,e_1+1} L_v\,\zeta_{vw} + \sum_{v,B} \beta_{vB}^{i\,e_1+1} L_v\,\zeta_{v\,B-1}.$$

Equating the coefficients of the ζ's, we find, as above, that every $\beta_{vc}^{i\,e_1+1} = 0$ $(c$ arbitrary$)$. In the second sum of the second member, E extends over every $E = e_1'+1$ and every E' not an $e+1$. Hence

$$\alpha_{i\,\bar{e}_1}^{i\,e_1} = 0, \quad \alpha_{i\,e_1'}^{i\,e_1} = \alpha_{i\,e_1'+1}^{i\,e_1+1}, \quad \alpha_{iE'}^{i\,e_1+1} = 0 \quad (E' \neq e+1),$$
$$\alpha_{tu}^{i\,e_1+1} = 0 \qquad (t \neq i,\ u \neq E-1),$$
$$K_i\,\alpha_{t\,E-1}^{i\,e_1+1} = K_t\,\alpha_{t\,E-1}^{i\,e_1+1} + K_t\,\alpha_{tE}^{i\,e_1+1} \qquad (t \neq i).$$

Applying the above argument, the last two equations give

$$\alpha_{tc}^{i\,e_1+1} = 0 \quad (t \neq i,\ c = 1, \ldots, \alpha).$$

Hence T_1 affects η_{ie} and $\eta_{i\,e+1}$ as follows:—

$$\eta'_{i\,e_1} = \sum_{e_1'} \alpha_{i\,e_1'}^{i\,e_1}\,\eta_{i\,e_1'}, \quad \eta'_{i\,\bar{e}_1} = \sum_{e} \alpha_{ie}^{i\,\bar{e}_1}\,\eta_{ie},$$

$$\eta'_{i\,e_1+1} = \sum_{e} \alpha_{ie}^{i\,e_1+1}\,\eta_{ie} + \sum_{e_1'} \alpha_{i\,e_1'}^{i\,e_1}\,\eta_{i\,e_1'+1}.$$

Denote by e_2 (or by e_2') an arbitrary e_1 such that e_2+2 is an E, and by $\bar{e}_2$ any one of the remaining e_1's so that every $\bar{e}_2+2$ is an e. Equating the functions by which T_1S_1 and S_1T_1 replace $\eta_{i\,e_2+2}$, we get

$$K_i \sum_{t,u} \alpha_{tu}^{i\,e_2+2}\,\eta_{tu} + K_i \sum_{v,w} \beta_{vw}^{i\,e_2+2}\,\zeta_{vw} + \sum_{e} \alpha_{ie}^{i\,e_2+1}\,\eta_{ie} + \sum_{e_1} \alpha_{i\,e_1}^{i\,e_2}\,\eta_{i\,e_1+1}$$
$$= \sum \alpha_{tu}^{i\,e_2+2} K_t\,\eta_{tu} + \sum \alpha_{tE}^{i\,e_2+2} K_t\,\eta_{t\,E-1} + \sum \beta_{vw}^{i\,e_2+2} L_v\,\zeta_{vw} + \sum \beta_{vB}^{i\,e_2+2} L_v\,\zeta_{v\,B-1}.$$

Equating the coefficients of the ζ's, we find, as above, that

$$\beta_{vc}^{ie_3+2} = 0 \quad (v = 0,1,\ldots,l-1;\ c = 1,\ldots,\beta).$$

Equating the coefficients of η_{tu} $(t \neq i)$, we find, as formerly, that every

$$a_{tu}^{ie_3+2} = 0 \quad (t \neq i).$$

For $t = i$, we note that

$$\sum_E a_{iE}^{ie_3+2}\eta_{iE-1} \equiv \sum_{e_1} a_{ie_1+1}^{ie_3+2}\eta_{ie_1} + \sum_{e'_2} a_{ie'_2+2}^{ie_3+2}\eta_{ie'_2+1} + \sum_{E'} a_{iE'}^{ie_3+2}\eta_{iE'-1},$$

where E' runs over the series of E's not of the forms e_1+1 or $e+2$. But an $\bar{e}_1+2 \equiv (\bar{e}_1+1)+1$ is an $e+1$, and an $\bar{e}_2+2$ is not an E. Hence E' extends over those integers $\leqq u$ which are of none of the forms e, e_1+1, e_3+2, all three of which are distinct. Hence every

$$a_{ie_1}^{ie_3+1} = a_{ie_1+1}^{ie_3+2}, \quad a_{i\bar{e}_1}^{ie_3+1} = 0, \quad a_{i\bar{e}_2}^{ie_3} = 0,$$
$$a_{ie'_2}^{ie_3} = a_{ie'_2+2}^{ie_3+2}, \quad a_{iE'}^{ie_3+2} = 0.$$

Hence T_1 affects the indices η_{ie}, η_{ie+1}, η_{ie+2} as follows:—

$$\eta'_{i\bar{e}_1} = \sum_e a_{ie}^{i\bar{e}_1}\eta_{ie},$$

$$\begin{cases} \eta'_{i\bar{e}_2} = \sum_{e_1} a_{ie_1}^{i\bar{e}_2}\eta_{ie_1}, \\ \eta'_{i\bar{e}_2+1} = \sum_e a_{ie}^{ie_2+1}\eta_{ie} + \sum_{e_1} a_{ie_1}^{ie_2}\eta_{ie_1-1}, \end{cases}$$

$$\begin{cases} \eta'_{ie_2} = \sum_{e'_2} a_{ie'_2}^{ie_2}\eta_{ie'_2}, \\ \eta'_{ie_2+1} = \sum_{e_1} a_{ie_1}^{ie_2+1}\eta_{ie_1} + \sum_{e'_2} a_{ie'_2}^{ie_2}\eta_{ie'_2+1}, \\ \eta'_{ie_2+2} = \sum_e a_{ie}^{ie_2+2}\eta_{ie} + \sum_{e_1} a_{ie_1}^{ie_2+1}\eta_{ie_1+1} + \sum_{e'_2} a_{ie'_2}^{ie_2}\eta_{ie'_2+2}. \end{cases}$$

Proceeding as before, we separate the e_2 into the categories e_3 and $\bar{e}_3$, such that every e_3+3 is an E and every $\bar{e}_3+3$ is an e. We find that no simplification takes place in $\eta'_{i\bar{e}_1}$, $\eta'_{i\bar{e}_2}$, $\eta'_{i\bar{e}_2+1}$, nor in η'_{ie_2}, η'_{ie_2+1}, η'_{ie_2+2}, when e_2 is an $\bar{e}_3$. Simplifications arise when e_2 is an e_3, viz.:

$$\begin{cases} \eta'_{ie_2} = \sum_{e'_2} a_{ie'_2}^{ie_2}\eta_{ie'_2}, \\ \eta'_{ie_2+1} = \sum_{e_2} a_{ie_2}^{ie_2+1}\eta_{ie_2} + \sum_{e'_2} a_{ie'_2}^{ie_2}\eta_{ie'_2+1}, \\ \eta'_{ie_2+2} = \sum_{e_1} a_{ie_1}^{ie_2+2}\eta_{ie_1} + \sum_{e_2} a_{ie_2}^{ie_2+1}\eta_{ie_2+1} + \sum_{e'_2} a_{ie'_2}^{ie_2}\eta_{ie'_2+2}, \\ \eta'_{ie_2+3} = \sum_e a_{ie}^{ie_2+3}\eta_{ie} + \sum_{e_1} a_{ie_1}^{ie_2+2}\eta_{ie_1+1} + \sum_{e_2} a_{ie_2}^{ie_2+1}\eta_{ie_2+2} + \sum_{e'_2} a_{ie'_2}^{ie_2}\eta_{ie'_2+3}. \end{cases}$$

The law of the formation of the η'_{ij} is now evident, and may be verified by simple induction. In particular, T_1 replaces each η_{ij} by a function of the η_{iu} alone. Similarly, T_1 replaces each ζ_{ij} by a function of the ζ_{iw} only.

4. Consider, as an example, a substitution S_1 which involves only the indices η_{ij}, and for which $a_1 = 3$, $a_2 = 3$, $a_3 = 2$. Then

$$e = 1, 4, 7; \quad E = 2, 3, 5, 6, 8;$$

$$e_1 = 1, 4, 7; \quad \text{no } \bar{e}_1; \quad e_2 = 1, 4; \quad \bar{e}_2 = 7; \quad \text{no } e_3.$$

The most general substitution T_1 commutative with S_1 has the form

	η_{i1}	η_{i4}	η_{i7}	η_{i2}	η_{i5}	η_{i8}	η_{i3}	η_{i6}
$\eta'_{i7} =$	a_{i1}^{i7}	a_{i4}^{i7}	a_{i7}^{i7}					
$\eta'_{i8} =$	a_{i1}^{i8}	a_{i4}^{i8}	a_{i7}^{i8}	a_{i1}^{i7}	a_{i4}^{i7}	a_{i7}^{i7}		
$\eta'_{i1} =$	a_{i1}^{i1}	a_{i4}^{i1}						
$\eta'_{i2} =$	a_{i1}^{i2}	a_{i4}^{i2}	a_{i7}^{i2}	a_{i1}^{i1}	a_{i4}^{i1}			
$\eta'_{i3} =$	a_{i1}^{i3}	a_{i4}^{i3}	a_{i7}^{i3}	a_{i1}^{i2}	a_{i4}^{i2}	a_{i7}^{i2}	a_{i1}^{i1}	a_{i4}^{i1}
$\eta'_{i4} =$	a_{i1}^{i4}	a_{i4}^{i4}						
$\eta'_{i5} =$	a_{i1}^{i5}	a_{i4}^{i5}	a_{i7}^{i5}	a_{i1}^{i4}	a_{i4}^{i4}			
$\eta'_{i6} =$	a_{i1}^{i6}	a_{i4}^{i6}	a_{i7}^{i6}	a_{i1}^{i5}	a_{i4}^{i5}	a_{i7}^{i5}	a_{i1}^{i4}	a_{i4}^{i4}

holding for $i = 0, 1, \ldots, k-1$. By inspection, its determinant equals

$$(a_{i7}^{i7})^2 \begin{vmatrix} a_{i1}^{i1} & a_{i4}^{i1} \\ a_{i1}^{i4} & a_{i4}^{i4} \end{vmatrix}^3.$$

5. The indices $\eta_{i1}, \ldots, \eta_{i\alpha}$ are linear functions of the initial indices $\xi_1, \ldots, \xi_m$, having as coefficients polynomials in K_i. Likewise, $\zeta_{i1}, \ldots, \zeta_{i\beta}$ are linear functions of $\xi_1, \ldots, \xi_m$ involving L_i. Let us return from the indices η_{ij}, ζ_{ij} to the initial indices ξ_i. By hypothesis, S_1 becomes S, a substitution having its coefficients in the $GF[p^n]$. Let T_1

become T. Under what conditions will T have its coefficients in the same field? Remembering that T_1 replaces η_{ij}, ζ_{ij} by functions of the respective forms

$$\sum_{u=1}^{\alpha} a_{iu}^{ij}\eta_{iu}, \quad \sum_{w=1}^{\beta} \delta_{iw}^{ij}\zeta_{iw},$$

it is evidently necessary and sufficient that a_{iu}^{ij} be the same function of K_i for $i = 1, \ldots, k-1$ that a_{0u}^{0j} is of K_0, and that δ_{iw}^{ij} be the same function of L_i for $i = 1, \ldots, l-1$ that δ_{0w}^{0j} is of L_0. Expressed otherwise, these conditions are

$$a_{iu}^{ij} = (a_{0u}^{0j})^{p^{ni}}, \quad \delta_{iw}^{ij} = (\delta_{0w}^{0j})^{p^{ni}}.$$

Hence T_1 is completely determined from the functions by which it replaces η_{0j} $(j = 1, \ldots, \alpha)$ and ζ_{0j} $(j = 1, \ldots, \beta)$. The final theorem is as follows:—

To determine the most general m-ary linear homogeneous substitution T with coefficients in the $GF[p^n]$ which is commutative with a particular one S, we give to S its canonical form S_1, which may be expressed as a product,

$$S_1 \equiv y_0 y_1 \cdots y_{k-1} z_0 z_1 \cdots z_{l-1} \cdots,$$

y_i, z_i denoting the respective substitutions—

$$y_i: \quad \eta_{ie} = K_i \eta_{ie}, \quad \eta_{iE} = K_i(\eta_{iE} + \eta_{iE-1}),$$

$$z_i: \quad \zeta_{ib} = L_i \zeta_{ib}, \quad \zeta_{iB} = L_i(\zeta_{iB} + \zeta_{iB-1}).$$

Then must T_1 (T written in the indices η_{ij}, ζ_{ij}) be expressible as a product

$$T_1 \equiv Y_0 Y_1 \cdots Y_{k-1} Z_0 Z_1 \cdots Z_{l-1} \cdots,$$

where Y_0 affects only the indices η_{0u}, the coefficients being given by the law explained at the end of § 3, and where Y_i is obtained from Y_0 by raising its coefficients to the power p^{ni}; with similar remarks for the substitutions Z_i.