Canonical Form of a Linear Homogeneous Transformation in an Arbitrary Realm of Rationality.

BY LEONARD EUGENE DICKSON.

1. In volume XXII of the *American Journal of Mathematics*, the writer investigated the canonical forms of linear homogeneous transformations in a finite field (necessarily a Galois Field). It was shown that the type of canonical form obtained by M. Jordan for the case of the field of integers taken modulo p is capable of immediate generalization to an arbitrary Galois Field. Instead of the direct, but lengthy, method of proof employed by M. Jordan, the paper cited gives a proof by induction from a smaller to a greater number of irreducible factors of the characteristic determinant. The latter method leads to a canonical form of linear transformations in an arbitrary field F. The formal process of reduction is the same as in the case of a Galois Field.* But the proof that the reduced form has the desired properties† is necessarily more complicated for the general field F than for a Galois Field. Indeed, the content of the theorem is essentially greater for the general field, since the roots of an equation $F(K) = 0$, belonging to and irreducible in F, may not all be rational functions in F of a single root, as is the case when F is a Galois Field (see §4). The object of this paper is to give the desired additional proof and thereby establish the validity of the canonical form for an arbitrary field.‡ In §6 is given an example to illustrate the generalized theorem.

---

* *American Journal*, vol. XXII, pp. 121–127. The paper will be designated A. J.

† Properties (a) and (b) below (§3), corresponding to (a) and (b) of A. J., p. 123.

‡ The theorem is stated in a different, but more compact, form by the writer in the Transactions of the American Mathematical Society, vol. 2 (1901), p. 393.

2. Proceeding as in A. J., pp. 124–6, we obtain the preliminary form S_2:

$$\lambda_i' = K_i\lambda_i, \qquad (i = 0, 1, \ldots, k-1)$$

$$Y_{01}' = K_0 Y_{01} + \alpha_{10}\lambda_0, \qquad Y_{0j}' = K_0(Y_{0j} + Y_{0\,j-1}), \qquad (j = 2, \ldots, a_1)$$

$$Y_{0a_1+1}' = K_0 Y_{0a_1+1} + \beta_{10}\lambda_0, \qquad Y_{0a_1+j}' = K_0(Y_{0a_1+j} + Y_{0a_1+j-1}), \qquad (j = 2, \ldots, a_2)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$Z_{01}' = L_0 Z_{01}, \qquad Z_{0j}' = L_0(Z_{0j} + Z_{0\,j-1}), \qquad (j = 2, \ldots, b_1)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

the expressions for Y_{ij}', Z_{ij}' being conjugate to those for Y_{0j}', Z_{0j}'. We proceed to prove that α_{10}, β_{10} are polynomials in K_0 with coefficients in F, and that the variables Y_{ij}, Z_{ij} have the properties:

(a). The variables Y_{0j} are linear homogeneous functions of the initial variables $\xi_1, \ldots, \xi_m$ whose coefficients are polynomials in K_0 with coefficients in F. The Y_{ij} are derived from the Y_{0j} by replacing K_0 by K_i.

(b). The variables Z_{0j} are linear homogeneous functions of $\xi_1, \ldots, \xi_m$ whose coefficients are polynomials in L_0 with coefficients in F. The Z_{ij} are derived from the Z_{0j} by replacing L_0 by L_i.

By the hypothesis made for the induction, the variables η_{ij} have the properties (a), the variables ζ_{ij} have the properties (b). Also

$$\lambda_i = X_0 + K_i X_1 + K_i^2 X_2 + \ldots + K_i^{k-1} X_{k-1}, \tag{1}$$

where the X_j are linear homogeneous functions of $\xi_1, \ldots, \xi_m$ with coefficients in F. Hence, in the transformation $\overline{S}$ (A. J., bottom of p. 125), the sums

$$\sum_{i=0}^{k-1} \alpha_{ji}\lambda_i, \quad \sum_{i=0}^{k-1} \beta_{ji}\lambda_i$$

are linear functions of $\xi_1, \ldots, \xi_m$ whose coefficients are polynomials in K_0 with coefficients in F. Applying the lemma below (§3),

$$\alpha_{ji} = \phi_j(K_0, K_i), \quad \beta_{ji} = \psi_j(K_0, K_i), \tag{2}$$

where ϕ_j, ψ_j are rational functions of their arguments with coefficients in F. Similarly, $\sum_{i=0}^{k-1} \alpha'_{ji}\lambda_i$ is a linear function of $\xi_1, \ldots, \xi_m$ whose coefficients are polynomials in L_0 with coefficients in F. Hence,

$$\alpha'_{ji} = \chi_j(L_0, K_i), \tag{3}$$

where χ_j is a rational function with coefficients in F.

Now (A. J., p. 126) $Z_{0s} \equiv \zeta_{0s} + \sum_{i=0}^{k-1} B_{si}\lambda_i$, where

$$B_{1i} = \frac{\alpha'_{1i}}{L_0 - K_i}, \quad B_{2i} = \frac{\alpha'_{2i}}{L_0 - (K_i)} - \frac{L_0\alpha'_{1i}}{(L_0 - K_i)^2}, \ldots$$

In view of (1) and (3), it follows that $\sum B_{1i}\lambda_i$, $\sum B_{2i}\lambda_i, \ldots$ are symmetric in $K_0, K_1, \ldots, K_{k-1}$, and hence are rational functions of $\xi_1, \ldots, \xi_m$ and L_0 with coefficients in F. A like result therefore holds for $Z_{01}, Z_{02}, \ldots$ In the field F a rational function of L_0 equals a polynomial in L_0.

Next (A. J., p. 126), $Y_{0s} \equiv \eta_{0s} + \sum_{i=0}^{k-1} A_{si}\lambda_i$, where

$$A_{10} = \frac{\alpha_{20}}{K_0}, \quad A_{1i} = \frac{\alpha_{1i}}{K_0 - K_i}, \quad A_{20} = \frac{\alpha_{30}}{K_0}, \quad A_{2i} = \frac{\alpha_{2i}}{K_0 - K_i} - \frac{K_0\alpha_{1i}}{(K_0 - K_i)^2},$$

etc., for $i = 1, 2, \ldots, k-1$, while A_{a_10}, $A_{a_1+a_20}, \ldots$ remain undetermined. In view of (1) and (2), it follows that A_{10}, $A_{20}, \ldots$ are rational functions of K_0 with coefficients in F, and that the sums

$$\sum_{i=1}^{k-1} A_{1i}\lambda_i, \quad \sum_{i=1}^{k-1} A_{2i}\lambda_i, \ldots$$

are symmetric in $K_1, \ldots, K_{k-1}$, and hence are rational functions of $\xi_1, \ldots, \xi_m$ and K_0 with coefficients in F. A like result therefore holds for $Y_{01}, Y_{02}, \ldots, Y_{0a_1-1}$. The only modification necessary for Y_{0a_1}, $Y_{0a_1+a_2}, \ldots$ is to *choose* A_{a_10}, $A_{a_1+a_20}, \ldots$ to be rational functions of K_0 with coefficients in F. It follows that every Y_{0j} is a linear function of $\xi_1, \ldots, \xi_m$ whose coefficients are polynomials in K_0 with coefficients in F.

Incidentally, it was shown that $\alpha_{10}, \beta_{10}, \ldots$ are polynomials in K_0 with coefficients in F. Denote them by $\phi(K_0), \psi(K_0), \ldots$ Proceeding as in A. J., p. 127, we obtain the desired canonical form upon variables possessing the properties (a) and (b).

3. LEMMA.—*Let the λ_i be defined by relations* (1), *and let the γ_i be independent of $\xi_1, \ldots, \xi_m$. If, in the linear function*

$$\lambda \equiv \sum_{i=0}^{k-1} \gamma_i \lambda_i$$

of $\xi_1, \ldots, \xi_m$, the coefficients are polynomials in σ with coefficients in the field F, then will

$$\gamma_i = f(\sigma, K_i), \qquad (i = 0, 1, \ldots, k-1)$$

where f is a polynomial in σ and K_i with coefficients in F.

By hypothesis, the expression

$$\lambda \equiv X_0 \Sigma\gamma_i + X_1 \Sigma K_i\gamma_i + X_2 \Sigma K_i^2 \gamma_i + \ldots + X_{k-1} \Sigma K_i^{k-1}\gamma_i$$

is a linear function of $\xi_1, \ldots, \xi_m$ whose coefficients are polynomials in σ with coefficients in F. Since $X_0, X_1, \ldots, X_{k-1}$ are linearly independent linear functions of $\xi_1, \ldots \xi_m$ with coefficients in F, it follows that

$$\Sigma\gamma_i = f_0, \quad \Sigma K_i\gamma_i = f_1, \quad \Sigma K_i^2\gamma_i = f_2, \ldots, \quad \Sigma K_i^{k-1}\gamma_i = f_{k-1},$$

where $f_0, f_1, \ldots, f_{k-1}$ are polynomials in σ with coefficients in F. Hence

$$\Delta_i\gamma_i = \begin{vmatrix} f_0 & 1 & 1 & \ldots 1 & 1 & \ldots 1 \\ f_1 & K_0 & K_1 & \ldots K_{i-1} & K_{i+1} & \ldots K_{k-1} \\ f_2 & K_0^2 & K_1^2 & \ldots K_{i-1}^2 & K_{i+1}^2 & \ldots K_{k-1}^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{k-1} & K_0^{k-1} & K_1^{k-1} & \ldots K_{i-1}^{k-1} & K_{i+1}^{k-1} & \ldots K_{k-1}^{k-1} \end{vmatrix} \equiv D_i,$$

where Δ_i is derived from D_i by replacing $f_0, f_1, f_2, \ldots, f_{k-1}$ by $1, K_i, K_i^2, \ldots, K_i^{k-1}$ respectively. Since Δ_i is a product of the differences of the K_j, it does not vanish. By the interchange of K_a with K_b, where a and b differ from i, Δ_i and D_i only change in sign. Hence γ_i is symmetric in $K_0, K_1, \ldots, K_{i-1}, K_{i+1}, \ldots, K_{k-1}$. It follows that γ_i is a rational function of $f_0, f_1, \ldots, f_{k-1}$ and K_i with coefficients in F,

$$\gamma_i = \omega(f_0, f_1, \ldots, f_{k-1}; K_i),$$

the form of the function ω being the same for each value of i. Moreover, ω is linear in $f_0, f_1, \ldots, f_{k-1}$. Hence γ_i is a polynomial in σ whose coefficients are rational functions (and hence polynomials) in K_i with coefficients in F.

4. For a finite field, the proof may be somewhat simplified. In that case, $K_0, K_1, K_2, \ldots, K_{k-1}$ are polynomials in a single root K_i. In view of their origin, the Y_{0j} are linear functions of $\xi_1, \ldots, \xi_m$ whose coefficients are rational functions of $K_0, K_1, \ldots, K_{k-1}$ with coefficients in F, and, therefore, are polynomials in K_0 with coefficients in F, if F be a finite field. But the Z_{0j} might involve $K_0, K_1, \ldots, K_{k-1}$ as well as L_0. By means of the above lemma, it was readily shown that the Z_{0j} involve only L_0. An independent proof* is given in §5. The method involved does not seem to apply to the case of the variables Y_{0j} for a general field F.

5. In view of the hypothesis for the induction, we may set

$$\eta_{ij} \equiv y_{0j} + K_i y_{1j} + K_i^2 y_{2j} + \ldots + K_i^{k-1} y_{k-1j}, \qquad (i = 0, 1, \ldots, k-1)$$

where the y_{ij} are linear homogeneous functions of $\xi_1, \ldots, \xi_m$ with coefficients in F. The y_{ij} are linearly independent since the η_{ij} are. Since the determinant $|K_i^j| \neq 0$, $y_{0j}, y_{1j}, \ldots, y_{k-1j}$ can be expressed as linear functions of $\eta_{0j}, \eta_{1j}, \ldots, \eta_{k-1j}$. Similarly, $\zeta_{0j}, \zeta_{1j}, \ldots, \zeta_{k-1j}$ depend upon independent functions $z_{0j}, z_{1j}. \ldots, z_{k-1j}$ belonging to F; while the latter depend upon the former. Set

$$\zeta_{ij} = f_i(z_{0j}, \ldots z_{k-1j}), \quad z_{ij} = f_i'(\zeta_{0j}, \ldots, \zeta_{k-1j}). \qquad (i = 0, 1, \ldots, k-1).$$

In view of formulæ (1), $\lambda_0, \lambda_1, \ldots, \lambda_{k-1}$ depend upon $X_0, X_1, \ldots, X_{k-1}$, and inversely.

Take as independent variables the functions X, y, z. Then $\bar{S}$ replaces each X by a function of the X only, each y by a function of the X and the y only, each z by a function of the X and the z only, the coefficients of these functions being in F. Let $\bar{S}$ replace z_{ij} by $\sum_{r,s} m_{rs} z_{rs} + \sum_r n_r X_r$. It is possible to

---

*** It is merely a new form of that by Jordan, "Traité," pp. 121–122.**

determine a set of functions

$$\bar{z}_{ij} \equiv z_{ij} + \sum_r x_{ijr} X_r, \tag{4}$$

such that $\bar{S}$ replaces $\bar{z}_{ij}$ by $\sum_{r,s} m_{rs} \bar{z}_{rs}$. One set is given by

$$\bar{\bar{z}}_{ij} \equiv f'_i(Z_{0j}, \ldots, Z_{k-1j}),$$

where the Z_{is} are the functions determined in A. J., p. 126. To show that this is the only set, consider any set (4). In terms of the variables λ_i, η_{ij}, $\bar{\zeta}_{ij} \equiv f_i(\bar{z}_{0j}, \ldots, \bar{z}_{k-1j})$, the transformation $\bar{S}$ replaces each by ζ_{ij} by a linear function of the $\bar{\zeta}_{is}$ only. Now $\bar{\zeta}_{ij}$ has the form $\zeta_{ij} + \sum_r \gamma_{ijr} X_r$. But the only set of functions of this form which $\bar{S}$ replaces by functions in which the coefficients of the X_r vanish was shown to be the set Z_{ij}. Hence $\bar{\zeta}_{ij} \equiv Z_{ij}$, so that $\bar{z}_{ij} \equiv f'_i(\bar{\zeta}_{0j}, \ldots, \bar{\zeta}_{k-1j}) = \bar{\bar{z}}_{ij}$. But, when $\bar{S}$ is expressed in terms of the variables K, y, z, the unique set (4) can be determined by the method of undetermined coefficients, so that the x_{ir} will belong to the field F. Hence the functions $\bar{z}_{ij}$ belong to F. But the coefficients in $f_i(z_{0j}, \ldots . z_{k-1j})$ are polynomials in L_i with coefficients in F. Hence the same is true for

$$f_i(\bar{z}_{0j}, \ldots, \bar{z}_{k-1j}) \equiv \bar{\zeta}_{ij} = Z_{ij}.$$

6. EXAMPLE.—The general theory is well illustrated by the following example: Consider a linear transformation whose characteristic determinant is $(\rho^3 - 2)^2$. By a general theorem (*Amer. Journ.*, vol. XXIII, p. 37), one such transformation is

$$A: \xi'_1 = 4\xi_3 - 4\xi_6, \ \xi'_2 = \xi_1, \ \xi'_3 = \xi_2, \ \xi'_4 = \xi_3, \ \xi'_5 = \xi_4, \ \xi'_6 = \xi_5.$$

The functions which A multiplies by ρ, where $\rho^3 = 2$, are

$$\xi_1 + \rho\xi_2 + \rho^2\xi_3 - 2\xi_4 - 2\rho\xi_5 - 2\rho^2\xi_6.$$

Denote the function by λ_1, λ_2 or λ_3 according as $\rho = \sqrt[3]{2}$, $\rho = \omega\sqrt[3]{2}$, or $\rho = \omega^2\sqrt[3]{2}$ respectively, where $\omega \equiv -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ is an imaginary cube root of unity. Taking as new variables the linearly independent functions λ_1, λ_2, λ_3, ξ_4, ξ_5, ξ_6, the transformation A becomes

$$\begin{cases} \lambda_1' = \sqrt[3]{2}\lambda_1, \quad \lambda_2' = \omega\sqrt[3]{2}\lambda_2, \quad \lambda_3' = \omega^2\sqrt[3]{2}\lambda_3, \\ \xi_4' = 2\xi_6 + f, \quad \xi_5' = \xi_4, \quad \xi_6' = \xi_5, \end{cases} \qquad [f \equiv \tfrac{1}{6}\sqrt[3]{2}(\lambda_1 + \omega\lambda_2 + \omega^2\lambda_3)].$$

The following transformation of determinant 2

$$\xi_4' = 2\xi_6, \quad \xi_5' = \xi_4, \quad \xi_6' = \xi_5,$$

multiplies the function $\xi_4 + \rho\xi_5 + \rho^2\xi_6\,(\rho^3 = 2)$ by ρ. Set

$$\begin{aligned} y_1 &= \xi_4 + \sqrt[3]{2}\,\xi_5 + \sqrt[3]{4}\,\xi_6, \\ y_2 &= \xi_4 + \omega\sqrt[3]{2}\,\xi_5 + \omega^2\sqrt[3]{4}\,\xi_6, \\ y_3 &= \xi_4 + \omega^2\sqrt[3]{2}\,\xi_5 + \omega\sqrt[3]{4}\,\xi_6. \end{aligned}$$

Then A replaces y_1, y_2, y_3 by, respectively,

$$\sqrt[3]{2}\,y_1 + f, \quad \omega\sqrt[3]{2}\,y_2 + f, \quad \omega^2\sqrt[3]{2}\,y_3 + f.$$

By introducing as new variables

$$\begin{aligned} x_1 &= \tfrac{1}{6}\lambda_1, & \eta_1 &= y_1 + ax_1 + (\omega x_2 - x_3)/(1-\omega), \\ x_2 &= \tfrac{1}{6}\lambda_2, & \eta_2 &= y_2 + bx_2 + (\omega x_3 - x_1)/(1-\omega), \\ x_3 &= \tfrac{1}{6}\lambda_3, & \eta_3 &= y_3 + cx_3 + (\omega x_1 - x_2)/(1-\omega), \end{aligned}$$

we obtain the canonical form

$$\begin{aligned} x_1' &= \sqrt[3]{2}\,x_1, & x_2' &= \omega\sqrt[3]{2}\,x_2, & x_3' &= \omega^2\sqrt[3]{2}\,x_3, \\ \eta' &= \sqrt[3]{2}(\eta_1 + x_1), & \eta_2' &= \omega\sqrt{2}\,(\eta_2 + x_2), & \eta_3' &= \omega^2\sqrt[3]{2}(\eta_3 + x_3). \end{aligned}$$

Here x_1, x_2, x_3 are of the respective forms

$$\theta(\xi_1, \ldots, \xi_6;\ \sqrt[3]{2}), \quad \theta(\xi_1, \ldots, \xi_6;\ \omega\sqrt[3]{2}), \quad \theta(\xi_1, \ldots, \xi_6,\ \omega^2\sqrt[3]{2}), \tag{5}$$

where θ is a linear function of its arguments, the coefficients being rational numbers. Again, we have

$$\eta_1 = \xi_4 + \sqrt{2}\,\xi_5 + \sqrt[3]{4}\,\xi_6 + \frac{a}{6}\lambda_1 + \tfrac{1}{6}(-\xi_1 + \sqrt[3]{4}\,\xi_3 + 2\xi_4 - 2\sqrt[3]{4}\,\xi_6),$$

$$\eta_2 = \xi_4 + \omega\sqrt[3]{2}\,\xi_5 + \omega^2\sqrt[3]{4}\,\xi_6 + \frac{b}{6}\lambda_2 + \tfrac{1}{6}(-\xi_1 + \omega^2\sqrt[3]{4}\,\xi_3 + 2\xi_4 - 2\omega^2\sqrt[3]{4}\,\xi_6),$$

$$\eta_3 = \xi_4 + \omega^2\sqrt[3]{2}\,\xi_5 + \omega\sqrt[3]{4}\,\xi_6 + \frac{c}{6}\lambda_3 + \tfrac{1}{6}(-\xi_1 + \omega\sqrt[3]{4}\,\xi_3 + 2\xi_4 - 2\omega\sqrt[3]{4}\,\xi_6).$$

Hence η_1, η_2, η_3 will be of the respective forms (5), if we take

$$a = f(\sqrt[3]{2}),\quad b = f(\omega\sqrt[3]{2}),\quad c = f(\omega^2\sqrt{2}),$$

where f is a rational function with coefficients in F. Whatever be the field F the variables in the canonical form have the desired properties (a).*

THE UNIVERSITY OF CHICAGO, *October*, 1901.

---

*I take this occasion to note certain errata in my article in vol. XXIII:

Page 351, line 25, *for* $\lambda\xi_1$ *read* $\gamma\xi_1$.
Page 364, line 20, *for* 2^m *read* $2m$.
Page 366, bottom, *for*), *read*).
Page 373, bottom, *for* F^λ *read* F_λ.