THE DECOMPOSITION OF MODULAR SYSTEMS OF RANK n IN n VARIABLES.

(Presented to the Chicago Section of the American Mathematical Society, April 24, 1897.)

BY PROFESSOR ELIAKIM HASTINGS MOORE.

I.

THEOREM A. If in the realm \( \mathfrak{R} \) of integrity-rationality \( \mathfrak{R} = [x_1, \ldots, x_n] = (R_1', \ldots, R_s') \), where the \( x_1, \ldots, x_n \) are independent variables and the realm \( \mathfrak{R}' = (R_1', \ldots, R_s') \) is independent of the \( x_1, \ldots, x_n \), the modular system

\[
2 = \begin{bmatrix} a_1 & 1 \cdots a_n & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{bmatrix}
\]

is contained in the coefficient modular system \( \mathfrak{F} \)

\[
\mathfrak{F} = \begin{bmatrix} f_{x_1} & \cdots & f_{x_n} \\ (\cdots) & \cdots & (\cdots) \end{bmatrix}
\]

of the form

\[
F[u_1, \ldots, u_n] = \sum_{k_1, \ldots, k_n} f_{x_1}^{k_1} \cdots f_{x_n}^{k_n}
\]

where the \( f_{x_1}, \ldots, f_{x_n} \) belong to \( \mathfrak{R} \) and the \( \xi_{k_i} \) belong to \( \mathfrak{R}' \) or to a family-realm containing \( \mathfrak{R}' \), and where the \( s \) linear forms \( \sum_{k_i} (x_i - \xi_{k_i}) u_i (h = 1, 2, \ldots, s) \) are distinct, then in the realm \( \mathfrak{R}' = [x_1, \ldots, x_n] = (R_1', \ldots, R_s', \xi_{k_i} \; \text{for} \; i = 1, 2, \ldots, s) \) the system \( \mathfrak{F} \) decomposes (in the sense of equivalence) into relatively prime factors \( \mathfrak{L}, \mathfrak{D}_{a^n} \),

\[
\mathfrak{L} = \begin{bmatrix} \mathfrak{L} \; \mathfrak{D}_{a^n} \end{bmatrix},
\]

where

\[
\mathfrak{D}_{a^n} = [x_1 - \xi_{k_1}, \ldots, x_n - \xi_{k_n}],
\]

so that

\[
\mathfrak{D}_{a^n} \sim [1] \; (h \leftrightarrow h'; h, h' = 1, 2, \ldots, s).
\]

Every such modular system \( \mathfrak{F} \) is of rank \( n \) in \( n \) variables.

Every modular system \( \mathfrak{F} \) of rank \( n \) in \( n \) variables decomposes in this way in particular with respect to its resolvent form

\[
F[u_1, \ldots, u_n].
\]
1. **Kronecker** in connection with his general theory of elimination (l. c., § 20) the decomposition of modular systems of rank \( n \) in \( n \) variables with non-vanishing discriminant.

In elucidation and extension of certain of the Kronecker Festschrift theories Mr. **Molk** wrote the elaborate paper, *Sur une notion*...

In Ch. IV., § 1 (l. c., pp. 79–107) Mr. Molk discusses the general modular system

\[
\mathcal{Q} = [L_1[x, y], \ldots, L_m[x, y]]
\]

of rank 2 in 2 variables \([x, y]\). The resolvent form \( F[u, v] \) of this system \( \mathcal{Q} \)

\[
F[u, v] = \sum_{i=0}^{m} f_i u^i v^j \prod_{h=1, s} ((x - \xi_h) u + (y - \eta_h) v)^{e_h}
\]

\((t = \sum_{h=1, s} e_h)\)

is a certain homogeneous form in the adjoined indeterminates \( uv \), which factors into \( s \) distinct linear factors \( ((x - \xi_h) u + (y - \eta_h) v) \) each to its proper multiplicity \( e_h \).

The \( \xi, \eta \) are independent of the \( x, y \). These factors correspond to the distinct solution systems \((x, y) = (\xi, \eta)\) of the system of equations \( L_j[x, y] = 0 \) \((j = 1, 2, \ldots, m)\), and their multiplicities are the multiplicities of those solution systems.

Now in all cases the coefficient modular system \( \mathcal{F} \) contains the system \( \mathcal{Q} \),

\[
\mathcal{F} = [f_0, f_1, \ldots, f_m] \equiv 0 \quad [\mathcal{Q}],
\]

and conversely, if the system \( \mathcal{Q} \) has a non-vanishing discriminant, that is, if every multiplicity \( e_h \) is 1, then \( \mathcal{Q} \) contains \( \mathcal{F} \),

\[
\mathcal{Q} \equiv 0 \quad [\mathcal{F}],
\]

so that \( \mathcal{Q} \) and \( \mathcal{F} \) are equivalent,

\[
\mathcal{Q} \sim \mathcal{F}.
\]

Mr. Molk's highly involved algebraic proof (l. c., pp. 91–97)
Decomposition of modular systems. [July,

of this converse is not above criticism. Then the decomposition of $\mathcal{L}$

$$\mathcal{L} \sim \mathcal{F} \sim \prod_{h=1}^{s} [x - \xi_h, y - \eta_h]_{a=1}^{s}$$

follows (l. c., p. 104) by resolvent considerations.

Similarly Kronecker for the general $n$ makes the decomposition of the system $\mathcal{L}$ with non-vanishing discriminant depend upon the equivalence of $\mathcal{L}$ with the resolvent system $\mathcal{F}$.

It is, however, possible, by pure-arithmetic process, for the general $n$ and whether the discriminant vanish or not, to effect first a decomposition of $\mathcal{F}$ and then a corresponding decomposition of $\mathcal{L}$, from which, if the discriminant does not vanish, follows the equivalence of $\mathcal{L}$ and $\mathcal{F}$. I proceed to prove the caption theorem A, from which these results follow easily.

2. A realm $\mathcal{R}$ of integrity-rationality* $\mathcal{R} = [\mathcal{R}_1, \ldots, \mathcal{R}_m]$ ($\mathcal{R}_{n+1}, \ldots, \mathcal{R}_{n+r}$) consists of all functions $F[\mathcal{R}_1, \ldots, \mathcal{R}_m]$ ($\mathcal{R}_{n+1}, \ldots, \mathcal{R}_{n+r}$) integral in $\mathcal{R}_1 \ldots \mathcal{R}_m$ and rational in $\mathcal{R}_{n+1} \ldots \mathcal{R}_{n+r}$, the coefficients being integers. The realm is closed under addition, subtraction, and multiplication, and likewise under division by any function not 0 of $\mathcal{R} = (\mathcal{R}_{n+1}, \ldots, \mathcal{R}_{n+r})$.

Any set of functions $F_1, \ldots, F_n$ of a realm $\mathcal{R}$ constitutes a modular system $\mathcal{F} = [F_1, \ldots, F_n]$ of that realm. The whole theory of such modular systems relates to this underlying realm.

Any set of modular systems $\mathcal{F}_i = [F_{i1}, \ldots, F_{ir}]$ ($i = 1, 2, \ldots, n$) determines a modular system $[F_{ij}, j = 1, 2, \ldots, n]$ for which we use the notation $[\mathcal{F}_1, \ldots, \mathcal{F}_n]$.

3. The very useful theorem: If $[\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}] \sim [1]$, then $[\mathcal{F}_1, \mathcal{F}] [\mathcal{F}_2, \mathcal{F}] \sim [\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}]$: may readily be proved by the use of the fundamental theorems concerning the composition and the equivalence of modular systems.

4. The decomposition (4) of theorem A depends upon the decomposition (12) in the same realm $\mathcal{R}^*$.

$$\mathcal{F} \sim \prod_{h=1}^{s} \mathcal{D}_h^{a_h}.$$ 

This is indeed a particular case of (4), viz., for $\mathcal{L} = \mathcal{F}$: for $\mathcal{F} \equiv 0 [\mathcal{F}]$ and $\mathcal{F} \equiv 0 [\mathcal{D}_h^{a_h}]$ and so $[\mathcal{F}, \mathcal{D}_h^{a_h}] \sim \mathcal{D}_h^{a_h}$ ($h = 1, 2, \ldots, s$). This decomposition (12) will appear below as the third corollary to the theorem B(II., § 7).

We have (5) $[\mathcal{D}_h, \mathcal{D}_h] \sim [1]$ ($h \rightarrow h'$; $h, h' = 1, 2, \ldots, s$), and hence ($\S 3$)

* A convenient refinement of Kronecker's realm of rationality.
Further since by hypothesis

we have from (14, 12, 13) by §3 the desired decomposition (4)

The $s$ factor systems $[\mathbb{D}, D_s^n]$ ($h = 1, 2, \ldots, s$) are by pairs relatively prime (13).

The system $D_s^n$ consists of the totality of homogeneous products of degree $e$ of the $n$ differences $x_1 - \xi_{s1}, \ldots, x_n - \xi_{sn}$. If the $m$ functions $L_i[x_1, \ldots, x_n]$ of $\mathbb{D}$ be arranged each according to these $n$ differences, then the system $[\mathbb{D}, D_s^n]$ is equivalent to the system obtained by retaining in each function of $\mathbb{D}$ only those terms of degree less than $e$. Hence, in particular $[\mathbb{D}, D_s^n] \sim [1]$, unless $\mathbb{D} \equiv 0 [D_s^n]$.

On another occasion I shall develop the theory of modular systems capable of such decomposition into relatively prime factors.

5. A modular system $\mathbb{D}$ of rank $n$ in $n$ variables has (Kronecker, l. c., §20) a form $F[u_1, \ldots, u_n]$—its resolvent form—of the kind called for by the hypothesis of theorem A, and indeed every system $\mathbb{D}$ to which theorem A applies is of rank $n$. For this form $F$ we have further

Thus the system $\mathbb{D}$ decomposes with respect to the resolvent $F$ according to theorem A.

For the particular case of non-vanishing discriminant we have Kronecker's decomposition and equivalence,

6. Let $e$ denote the largest multiplicity $e$. Let $D$ denote any function $D[x_1, \ldots, x_n]$ of $\mathbb{D}$ for which

Then, from (5, 18) and §3,

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
DECOMPOSITION OF MODULAR SYSTEMS. [July, 

Hence

(20) \[ D \equiv 0 \prod_{h=1}^{s} D_h, \quad D' \equiv 0 \prod_{h=1}^{s} D_h', \quad D'' \equiv 0 \prod_{h=1}^{s} D_h''. \]

Then from (20, 12, 14) we have

(21) \[ D' \equiv 0 \quad [\mathcal{C}]. \]

This theorem for the case \( n = 2 \) is due to Mr. Netto.*

II.

THEOREM B. In any realm \( \mathfrak{R} \) of integrity-rationality the product \( \mathfrak{S} \) of the coefficient modular systems \( \mathfrak{D}, \mathfrak{E} \) of two homogeneous \( n \)-ary forms \( D[u_1, \ldots, u_n], \quad E[u_1, \ldots, u_n] \) of the realm \( \mathfrak{R} \) is equivalent to the coefficient modular system of their product form \( F = DE \), if for any certain system of \( n \) integers \( a_1, \ldots, a_n \) whose greatest common divisor is 1 in the realm \( \mathfrak{R} \)

\[ [D[a_1, \ldots, a_n], \quad E[a_1, \ldots, a_n], \quad \mathfrak{S}] \sim [1]. \]

1. We set, calling \( m_d, m_e \) the degrees respectively of \( D, E, \)

\[ D[u_1, \ldots, u_n] = \sum_{i_1, \ldots, i_n \mid m_d} d_{i_1 \ldots i_n} u_1^{i_1} \cdots u_n^{i_n}, \]

\[ E[u_1, \ldots, u_n] = \sum_{j_1, \ldots, j_n \mid m_e} e_{j_1 \ldots j_n} u_1^{j_1} \cdots u_n^{j_n}, \]

\[ F[u_1, \ldots, u_n] = \sum_{k_1, \ldots, k_n \mid m_f} f_{k_1 \ldots k_n} u_1^{k_1} \cdots u_n^{k_n} \]

(2) so that

\[ f_{k_1 \ldots k_n} = \sum_{i_1, \ldots, i_n \mid m_d} d_{i_1 \ldots i_n} e_{i_1 \ldots i_n} \]

(3) where the summation remarks of (1, 2; 3) have the definitions (4; 5)

\[ h_1, \ldots, h_n \mid m_o \sim h_1, \ldots, h_n = 0, 1, \ldots, m_o; \quad h_1 + \cdots + h_n = m_c \]


† Or, more generally, the \( a_1, \ldots, a_n \) may be any column of an unimodular matrix \( (a_{st}) \) \( (s, s' = 1, 2, \ldots, n) \) of the realm \( \mathfrak{R}, [a_{st}] = 1. \) The proof then needs change only in \( \S 3. \)
For the corresponding coefficient modular systems we write

(6) \[ \mathcal{D} = \begin{bmatrix} \ldots & d_1 & \ldots & d_n \end{bmatrix}, \quad \mathcal{E} = \begin{bmatrix} \ldots & e_1 & \ldots & e_n \end{bmatrix}, \quad \mathfrak{F} = \begin{bmatrix} \ldots & f_1 & \ldots & f_n \end{bmatrix}; \]

and in general we denote the coefficient modular system of any form \( G [u, \ldots, u] \) of the realm \( \mathfrak{R} \) by the corresponding Gothic capital letter \( \mathfrak{G} \).

We are to prove that under a certain hypothesis \( H \)

\[ \mathcal{D} \mathcal{E} \sim \mathfrak{F}. \]

2. Under an unimodular linear homogeneous substitution

(8) \[ u_s = \sum_{s'=0}^n a_{ss'} u_{s'}, \quad |a_{ss'}| = 1 \quad (s, s' = 1, 2, \ldots, n) \]

whose coefficients \( a_{ss'} \) belong to the realm \( \mathfrak{R} \), the form \( G [u, \ldots, u] \) of the realm is transformed into the form \( G' [u', \ldots, u'_n] \), and the corresponding coefficient modular systems are equivalent, \( \mathfrak{G} \sim \mathfrak{G}' \).

Since identities in the \( u \)'s transform into identities in the \( u' \)'s in order to prove for the two forms \( D, E \) under the hypothesis \( H \) the equivalence (7) \( \mathcal{D} \mathcal{E} \sim \mathfrak{F} \) it is sufficient to prove for the two transformed forms \( D', E' \) under the transformed hypothesis \( H' \) the corresponding equivalence (7) \( \mathcal{D}' \mathcal{E}' \sim \mathfrak{F}' \).

3. By hypothesis \( H \) there exists a system of \( n \) integers \( a_1, \ldots, a_n \) of greatest common divisor 1 such that in \( \mathfrak{R} \)

(9) \[ [D [a_1, \ldots, a_n], E [a_1, \ldots, a_n], \mathfrak{F}] \sim [1]. \]

There exists* then a substitution (8) with integral coefficients in which

* We can pass from \( (a_1', a_2', \ldots, a_n') \) to \( (1, 0, \ldots, 0) \) by a sequence of elementary transformations, i.e., interchange of two elements with change of sign of one and addition to one element of another element. The application of the reverse sequence simultaneously to the \( n \) columns of the identity matrix

\[
\begin{bmatrix}
1 & 0 & \ldots & 0 \\
0 & 0 & \ldots & 1 \\
\vdots & \ddots & \ddots & \ddots \\
0 & \ldots & 0 & 1
\end{bmatrix}
\]

carries us to the matrix \( (a_{ss'}) \) desired.

This determination of \( (a_{ss'}) \) is suggested by Kronecker's Reduction der Systeme von \( n^2 \) ganzzahligen Elementen (Journal für die Mathematik, vol. 107, pp. 135-136, 1891).
DECOMPOSITION OF MODULAR SYSTEMS. [July, 1970]

(10) \[ a_{s1} = a_s \quad (s = 1, 2, \ldots, n). \]

For this substitution (8), since

(11) \( (u_1, u_2, \ldots, u_n) = (a_1, a_2, \ldots, a_n) \sim (u'_1, u'_2, \ldots, u'_n) = (1, 0, \ldots, 0), \)

the transformed hypothesis \( H' \) affirms the equivalence in \( \mathfrak{R} \)

(12) \[ [D' [1, 0, \ldots, 0], E' [1, 0, \ldots, 0], \mathfrak{R}] \sim [D' [1, 0, \ldots, 0], E' [1, 0, \ldots, 0], \mathfrak{R}] \sim [d_{m0} \ldots 0, e_{m0} \ldots 0, \mathfrak{R}] \sim [1]. \]

4. Thus the theorem holds if it holds for the special case \( (a_1, a_2, \ldots, a_n) = (1, 0, \ldots, 0) \), when

(13) \[ [d_{m0} \ldots 0, e_{m0} \ldots 0, \mathfrak{R}] \sim [1], \]

so that, by I. §3,

(14) \[ [d_{m0} \ldots 0, e_{m0} \ldots 0, \mathfrak{R}] \sim [1]. \]

The equivalence

(15) \[ \mathcal{D} \mathcal{C} \sim \mathfrak{R} \]

in \( \mathfrak{R} \) is nothing but the two congruences

(16) \[ \mathcal{D} \mathcal{C} \equiv 0 \quad [\mathfrak{R}], \quad \mathcal{E} \equiv 0 \quad [\mathcal{D} \mathcal{C}]. \]

Of these the second holds by (3), and the first holds by (14) if

(17) \[ \mathcal{D} \mathcal{C} [d_{m_d \ldots 0}, e_{m_d \ldots 0}, \mathfrak{R}] \equiv 0 \quad [\mathfrak{R}], \]

and this holds if simultaneously

(18) \[ \mathcal{D} [e_{m_d \ldots 0}, \ldots, d_{l1 \ldots l_n}, e_{m_d \ldots 0}, \ldots] \equiv 0 \quad [\mathfrak{R}], \]

(19) \[ \mathcal{E} [d_{m_d \ldots 0}, \ldots, e_{l1 \ldots l_n}, d_{m_d \ldots 0}, \ldots] \equiv 0 \quad [\mathfrak{R}]. \]

We prove that (18) holds; the similar proof applies to (19). We have from (3) for \( d_{l1 \ldots l_n}, i_l = m_d \) (20), \( i_l = m_d \) (21):

(20) \[ d_{m_d \ldots 0, \ldots, 0} = f_{m_d \ldots 0, \ldots, 0} \equiv 0 \quad [\mathfrak{R}], \]

(21) \[ d_{l1 \ldots l_n, e_{m_d \ldots 0, \ldots, 0} = f_{l1 \ldots l_n, \ldots, 0} - \sum \delta_{l1 \ldots l_n, \ldots, 0} e_{l1 \ldots l_n} \rightarrow, \]
Hence, applying (21') \( m_d - i \) times and (20) once, we see that

\[
(22) \quad d_{i_1 i_2 \ldots i_n} e_{m_d 0 \ldots 0} \equiv - \sum^* d_{h_1 h_2 \ldots h_n} e_{i_1 i_2 \ldots i_n} [\mathfrak{F}].
\]

and so that (18) does hold.

5. Cor. 1. The product of the coefficient modular systems \( \mathfrak{D}, \ldots, \mathfrak{D} \) of \( t \) \( n \)-ary forms \( D_{i_1}, \ldots, D_i \) of the realm \( \mathfrak{R} \) is equivalent to the modular system of their product-form \( F \), if for any certain system of \( n \) integers \( a_1, \ldots, a_n \) with greatest common divisor 1

\[
(23) \quad D_g [a_1, \ldots, a_n], D_{g'} [a_1, \ldots, a_n] \sim [1] \quad (g \nmid g'; g, g' = 1, 2, \ldots, t)
\]

6. Cor. 2. The \( s \) linear forms

\[
(24) \quad D_h [u_1, \ldots, u_n] = \sum_{i=1}^n d_{h i} u_i \quad (h = 1, 2, \ldots, s)
\]

belong to the realm \( \mathfrak{R} \) and have leading coefficients by pairs relatively prime

\[
(25) \quad [d_{h i}, d_{h' i}] \sim [1] \quad (h \nmid h'; h, h' = 1, 2, \ldots, s).
\]

Then, setting

\[
(26) \quad D_h [u_1, \ldots, u_n]^* = F_h [u_1, \ldots, u_n], \quad (h = 1, 2, \ldots, s),
\]

\[
(27) \quad \prod_{h=1, s} F_h [u_1, \ldots, u_n] = F [u_1, \ldots, u_n],
\]

we have the equivalence in \( \mathfrak{R} \)

\[
(28) \quad \prod_{h=1, s} \mathfrak{D}_h^* \sim \prod_{h=1, s} \mathfrak{F}_h \sim \mathfrak{F}
\]

This appears from Cor. 1 for \((a_1, a_2, \ldots, a_n) = (1, 0, \ldots, 0)\) since obviously for any linear form \( D_a \) and its power \( D_a^* = F \) we have \( \mathfrak{D}_a^* \sim \mathfrak{F}_a \) and since from (25) by I § 3

\[
[d_{h i}, d_{h' i}] \sim [1] \quad (h \nmid h'; h, h' = 1, 2, \ldots, s).
\]
7. Cor. 3. We consider the realm $\mathcal{R}$ of integrity-rationality

$$\mathcal{R} = [x_1, \ldots, x_n] \left( \xi_{hl} \quad h = 1, 2, \ldots, s \right)$$

where the $x_1, \ldots, x_n$ are indeterminates and where the $\xi_{hl}$ belong to a realm $\mathcal{R}^{s}$ not containing the indeterminates $x$ and in that realm are such that the $s$ forms

$$D_h[u_1, \ldots, u_n] = \sum_{i=1}^{n} (x_i - \xi_{hi}) u_i \quad (h = 1, 2, \ldots, s)$$

are distinct linear forms. Then we have (in the notations of Cor. 2) the equivalence (28).

The particular case, in which

$$\left[ x_1 - \xi_{hi}, x_1 - \xi_{hi} \right] \sim [1]$$

$(h \neq h'; h, h' = 1, 2, \ldots, s)$,

follows at once from Cor. 2.

The general case is reduced to this particular case by transformation of the $u_1, \ldots, u_n$ by a properly chosen unimodular substitution in the realm $[1]$

$$u_i = \sum_{t=1}^{n} a_{it} u'_t \quad (i = 1, \ldots, n)$$

and simultaneously of the $x_1, \ldots, x_n$ and the $\xi_{1}, \ldots, \xi_{s}$ by the substitutions contragredient to (32)

$$x_i' = \sum_{t=1}^{n} a_{it} x_t' \quad (i = 1, \ldots, n),$$

$$\xi_{hi}' = \sum_{t=1}^{n} a_{it} \xi_{hi} \quad (i = 1, \ldots, n).$$

Since the forms $D_h$ (30) are distinct we can determine integers $a_1, \ldots, a_n$ with greatest common divisor 1 such that

$$\sum_{t=1}^{n} \xi_{hi} a_{it} = \sum_{t=1}^{n} \xi_{hi} a_{it} \quad (h \neq h'; h, h' = 1, \ldots, s).$$

Then any unimodular matrix $(a_{it})$ in $[1]$ having $a_{it} = a_i'$ ($i = 1, \ldots, n$) will yield satisfactory reducing substitutions (32, 33, 34).

The University of Chicago, April 20, 1897.