CONCERNING LINEAR SUBSTITUTIONS OF FINITE PERIOD WITH RATIONAL COEFFICIENTS*

BY

ARTHUR RANUM

INTRODUCTION.

If the coefficients of a linear homogeneous substitution (matrix, bilinear form) are unrestricted, i. e., belong to the continuous domain of all complex numbers, there is no upper limit to its finite period; † moreover, for all possible integral values of n and m there exist linear substitutions in n variables of period m . But if the coefficients are restricted to the domain of rational numbers, the finite period is limited to certain definitely prescribed values that depend on the number of variables. For instance, it is clear that in one variable the only linear homogeneous substitutions of finite period with rational coefficients are $x' = x$, of period one, and $x' = -x$, of period two. Again, in two variables the only finite periods will be shown to be 1, 2, 3, 4, and 6. This may be compared with the well-known result given by KLEIN and FRICKE ‡ that the finite periods of linear *fractional* substitutions of *determinant* 1 in one variable are 1, 2, and 3.

In the continuous domain of complex numbers, every linear substitution of finite period is completely reducible; i. e., its canonical form is axial; but in the domain of rational numbers, some linear substitutions are only partly reducible and some are entirely irreducible; hence their canonical forms are no longer so simple. Moreover, there is an intimate connection between the reducibility of a linear substitution and its period.

In §§ 1–4 of this paper the minimum degree (number of variables) of a linear substitution of given period m with rational coefficients is determined;

* Presented to the Society at the Ithaca meeting September 5, 1907. Received for publication September 5, 1907.

† In this paper I shall confine my attention to matrices whose determinants do not vanish and therefore define the period of a matrix and the identity matrix in the usual way; in another paper soon to be published elsewhere I shall consider groups of matrices whose determinants vanish, and arrive at a more general definition of the concepts *period* and *identity matrix*.

‡ *Modulfunktionen*, vol. 1, p. 182.

in §§ 5–9 the effect of its reducibility is found; in §§ 10–20 the inverse problem is solved of obtaining the values of the period of a linear substitution when its degree and reducibility are given; §§ 21–27 contain a method of constructing the canonical forms of all linear substitutions of finite period. The principal results are: (1) a complete determination of all the finite periods of n -ary linear substitutions having rational coefficients; (2) a precise classification of all n -ary linear substitutions of period m having rational coefficients, with respect to their reducibility and canonical forms. Finally, § 28 contains a brief summary of these results for linear substitutions of low degree.

THE MINIMUM DEGREE OF A MATRIX OF PERIOD m .

1. Let

$$L = (l_{ij}) = \begin{pmatrix} l_{11} & \cdots & l_{1n} \\ \vdots & \ddots & \vdots \\ l_{n1} & \cdots & l_{nn} \end{pmatrix}, \quad \text{where} \quad |l_{ij}| \neq 0,$$

be an n -ary matrix of period m whose elements are rational numbers, and let its characteristic equation be written in the form

$$\Phi(\lambda) \equiv |l_{ij} - \lambda \delta_{ij}| = 0, \quad \text{where} \quad \delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

If we denote the identity matrix (δ_{ij}) by I , then L satisfies the two symbolic equations $L^m = I$ and $\Phi(L) = 0$, whose degrees are m and n , respectively. FROBENIUS* has proved that a matrix is of finite period if, and only if, the elementary divisors of its characteristic determinant are all linear, and the roots of its characteristic equation are roots of unity. It follows that if its period is m , the L. C. M. of the orders of these roots of unity must be m .† Here the term *order* of a root of unity ϵ is defined as the lowest integer κ for which $\epsilon^\kappa = 1$.

2. We shall need the following:

LEMMA. Any rational, integral equation $\Phi(\lambda) = 0$, whose coefficients belong to a field‡ Ω , is the characteristic equation of some matrix whose elements belong to Ω .§

* Crelle's Journal, vol. 84 (1877), p. 16.

† It is incorrectly stated by MUTH (*Elementartheiler*, art. 91, p. 178) that at least one of these roots must be a primitive m -th root of unity.

‡ By the term *field* we shall understand, as usual, any set of elements that is closed under rational operations (excluding division by zero), while we shall confine the term *domain* to that particular kind of field whose elements, infinite in number, are ordinary real or complex numbers. The domain $(\epsilon_1, \epsilon_2, \dots)$ will be understood to mean the set of rational functions of the numbers $\epsilon_1, \epsilon_2, \dots$.

§ This lemma was given in substance by DICKSON in the *American Journal of Mathematics*, vol. 23 (1901), p. 37.

Proof. If $\Phi(\lambda) \equiv \lambda^n + d_1\lambda^{n-1} + \dots + d_n$, let $L = (l_{ij})$ be chosen as defined by the equations

$$l_{i,i+1} = 1 \quad (i = 1, \dots, n-1), \quad l_{n,j} = -d_{n-j+1} \quad (j = 1, \dots, n),$$

$$l_{ij} = 0 \quad (j \neq i+1; i \neq n; i, j = 1, \dots, n).$$

Then L is evidently a matrix whose elements belong to Ω , and whose characteristic equation is $\Phi(\lambda) = 0$, as required by the lemma.

Example. If $n = 3$,

$$\Phi(\lambda) \equiv \lambda^3 + d_1\lambda^2 + d_2\lambda + d_3, \quad L = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -d_3 & -d_2 & -d_1 \end{pmatrix}.$$

3. Our object is to find, for any given value of the degree n of a matrix L with rational elements, all the values of its finite period m , which are not also periods of matrices with rational elements of degree lower than n ; we shall attain this object by first obtaining, for any given value of its period m , its minimum degree n . Since the degree of a matrix is equal to the degree of its characteristic equation, and since by the above lemma every rational, integral equation with rational coefficients is the characteristic equation of some matrix with rational elements, therefore we wish to find an equation $\Phi(\lambda) = 0$, whose coefficients are rational, whose roots are roots of unity, such that the L. C. M. of their orders is m , whose elementary divisors are linear (when it is regarded as the characteristic equation of some definite matrix), and whose degree n is a minimum.

As so defined, $\Phi(\lambda) = 0$ will not have multiple roots. If it had, then the equation

$$\frac{\Phi(\lambda)}{[\Phi(\lambda), \Phi'(\lambda)]} = 0,$$

where $[\Phi(\lambda), \Phi'(\lambda)]$ is the G. C. D. of $\Phi(\lambda)$ and its derivative, would not have multiple roots, and since its coefficients are rational, it would also be the characteristic equation of some matrix with rational elements; moreover, it would be satisfied by all the roots of $\Phi(\lambda) = 0$, its elementary divisors would be linear, and its degree would be less than that of $\Phi(\lambda) = 0$.

Suppose the function $\lambda^m - 1$ to be factored as far as possible in the domain (1). Corresponding to every divisor m_1 of m , there will be just one irreducible factor of $\lambda^m - 1$ that is annihilated by all the primitive m_1 -th roots of unity and no others; and in particular there will be one irreducible factor $\Phi_1(\lambda)$, that is annihilated by all the primitive m -th roots of unity and no others. It is clear,

therefore, that our problem will be solved by putting $\Phi(\lambda)$ equal to the product of irreducible factors of $\lambda^m - 1$ selected in such a way that the sum of their degrees is a minimum and the G. C. D. of the orders of the corresponding roots of unity is equal to m . Its elementary divisors will evidently be linear.

4. If now we impose the further restriction that the characteristic determinant $\Phi(\lambda)$ shall be irreducible, we plainly have to put $\Phi(\lambda) = \Phi_1(\lambda)$; and since the degree of $\Phi_1(\lambda)$ is $\phi(m)$ (EULER's ϕ -function), the latter is not merely the minimum degree, but the only possible degree of the corresponding matrix. Thus we have derived

THEOREM 1. *Every matrix of period m whose elements are rational and whose characteristic determinant is irreducible in the domain (1) is of degree $\phi(m)$. The characteristic determinant of every such matrix is that irreducible factor of $\lambda^m - 1$ which is annihilated by the primitive m -th roots of unity.*

Example. Every such matrix of period 12 is of degree 4, and its characteristic determinant is $\lambda^4 - \lambda^2 + 1$; a representative matrix is

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{bmatrix}.$$

5. On the other hand, if we place no limitation on the reducibility of the characteristic equation, we can, of course, find matrices of period m whose degree is higher than $\phi(m)$, but we can also in general find others of degree much lower than $\phi(m)$. Let $m = 2^a p_1^{a_1} \dots p_r^{a_r}$, where $p_1, \dots, p_r$ are the distinct odd prime factors of m (if any exist), where $a_1, \dots, a_r$ are positive integers, and where a is a positive integer or zero. We wish to find a set of integers $m_1, \dots, m_r$ whose L. C. M. is m , and the sum of whose ϕ -functions is a minimum. It will evidently be sufficient to take these integers prime to each other. For if any two of them are not prime to each other, their G. C. D. is at most 2, and $\phi(2\kappa) = \phi(\kappa)$ where κ is odd. Moreover, if m_1 and m_2 are prime to each other, $\phi(m_1 m_2) = \phi(m_1) \cdot \phi(m_2)$; and since the sum of two positive integers is less than, or equal to, their product, unless one of them is unity, it follows that $\phi(m_1) + \phi(m_2) \leq \phi(m_1 m_2)$, unless $\phi(m_1)$, say, is 1, i. e., unless $m_1 = 2$.

Therefore, if $a > 1$, the required integers can be taken to be $2^a, p_1^{a_1}, \dots, p_r^{a_r}$, and the required minimum degree of a matrix of period m is $\phi(2^a) + \phi(p_1^{a_1}) + \dots + \phi(p_r^{a_r})$; while if $a = 0$ or 1, the integers can be taken to be $2^a p_1^{a_1}, p_2^{a_2}, \dots, p_r^{a_r}$, and the minimum degree is $\phi(p_1^{a_1}) + \dots + \phi(p_r^{a_r})$.

If we define $\psi(m)$ by the equations

$$\psi(m) = \begin{cases} \phi(2^a) + \sum_{i=1}^r \phi(p_i^{a_i}), & \text{if } a > 1, \\ \sum_{i=1}^r \phi(p_i^{a_i}), & \text{if } a = 1 \text{ or } 0, \end{cases}$$

we have

THEOREM 2. *If the characteristic determinant of a matrix of period m , whose elements are rational, is reducible in the domain (1), its irreducible factors are those irreducible factors of $\lambda^m - 1$, which are annihilated respectively by the primitive m_1 -th $\dots$ m_r -th roots of unity, where $m_1, \dots, m_r$ are integers whose L. C. M. is equal to m . The minimum degree of a matrix of period m with rational elements is equal to $\psi(m)$.*

Example. If $m = 15$, the minimum degree is 6, and every matrix of period 15 and degree 6 has for its characteristic determinant

$$(\lambda^2 + \lambda + 1)(\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1),$$

a representative matrix is

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & -1 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & -1 \end{pmatrix}.$$

THE REDUCIBILITY OF MATRICES IN A GIVEN DOMAIN.

6. A classification of matrices with respect to their characteristic equations will now be considered, and the results will be obtained for matrices whose elements belong to any domain Ω , not necessarily the domain (1), and not merely for matrices of finite period, but for all matrices whose characteristic determinants have linear elementary divisors.

If the totality of all the n -ary matrices in Ω , whose determinants are not zero, is called the *chief linear group of Ω* , then two such matrices, L and L' , will be said to be *conjugate in Ω* , if they are conjugate in the chief group of Ω , i. e., if there exists a matrix M in the chief group, such that $M^{-1}LM = L'$. A matrix L will be said to be *reducible in Ω* , if it is conjugate, in Ω , to a matrix of the form

$$L' = \begin{pmatrix} L_1 & O_1 \\ O_2 & L_2 \end{pmatrix},$$

where L_1, L_2 are square matrices and O_1, O_2 are rectangular matrices whose elements are all zero. If the component matrices L_1 and L_2 are themselves irreducible, then L' will be called a *reduced* matrix. If not, then L' can be further transformed into a matrix having three or more components. When finally all the components are irreducible, the complete matrix is said to be *reduced* in Ω . If the reduced matrix is axial, i. e., if all its elements outside of the principal diagonal are zero, the original matrix L is said to be *completely reducible*. In the complete set of conjugates to a given matrix L a simple representative matrix may be chosen as the *canonical form* of L . The canonical form of a reducible matrix will naturally be chosen to be a reduced matrix.

7. It is well known * that in the continuous domain of complex numbers all matrices, except those whose characteristic determinant has only a single elementary divisor, are reducible and that every matrix whose characteristic determinant has only linear elementary divisors is completely reducible. In a smaller domain, however, matrices are in general less reducible and the number of irreducible matrices is larger.

Example. The ternary matrix

$$L = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

of period 3, is completely reducible in the domain of complex numbers, and its reduced form is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix},$$

where ϵ is a primitive cube root of unity; whereas in the domain (1) it is only partly reducible, and its canonical reduced form can be taken to be

$$L' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}.$$

It is easy to verify that

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$$

is a matrix that will transform L into L' .

8. The following statement can be given to a well-known result in the theory of elementary divisors: †

* MUTH, *Elementartheiler*, arts. 77-79.

† FROBENIUS, *Crelle's Journal*, vol. 86 (1878), p.

Two matrices belonging to a domain Ω are conjugate in Ω , if, and only if, the elementary divisors of their characteristic determinants coincide.

In the particular case in which the elementary divisors are linear, they will coincide if the characteristic determinants themselves coincide. Therefore, *if the characteristic determinants of two matrices belonging to Ω have linear elementary divisors, then the coincidence of these characteristic determinants is the necessary and sufficient condition that the matrices are conjugate in Ω .*

Among the matrices to which this theorem applies are those of finite period, since their elementary divisors are linear. Hence we see that *two matrices of finite period belonging to Ω are conjugate in Ω , if, and only if, they have the same characteristic determinant.*

Example. The above-mentioned ternary matrices of period 3 both have the same characteristic determinant, $\lambda^3 - 1$.

9. We are now prepared to prove

THEOREM 3. *A matrix L , whose characteristic determinant $\Phi(\lambda)$ has its elementary divisors all linear, is reducible in a given domain Ω , if, and only if, its characteristic determinant is reducible in that domain. If the irreducible factors of $\Phi(\lambda)$ are $\Phi_1(\lambda), \dots, \Phi_s(\lambda)$, of degrees $n_1, \dots, n_s$, respectively, then the reduced form of L is made up of irreducible components $L_1, \dots, L_s$, of degrees $n_1, \dots, n_s$, respectively, whose characteristic determinants are $\Phi_1(\lambda), \dots, \Phi_s(\lambda)$, respectively.*

Proof. (a) If L is reducible in Ω , it obviously has the same characteristic determinant as its reduced form. Moreover, the characteristic determinant of a reduced matrix is the product of the characteristic determinants of its components, and is therefore reducible in Ω .

(b) If $\Phi(\lambda)$, the characteristic determinant of L , is reducible in Ω , and its irreducible factors are $\Phi_1(\lambda), \dots, \Phi_s(\lambda)$, then, by the lemma of § 2, component matrices $L_1, \dots, L_s$ exist in Ω having the functions $\Phi_1(\lambda), \dots, \Phi_s(\lambda)$ as their characteristic determinants. Moreover, the latter, being irreducible, have no multiple roots, and their elementary divisors are linear. Therefore the reduced matrix L' , made up of the components $L_1, \dots, L_s$, has the same characteristic determinant, with the same linear elementary divisors, as L ; i. e., L and L' are conjugate in Ω and L is reducible in Ω .

Example.

$$L = \begin{bmatrix} 0 & 2 & 0 & 2 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

is a matrix whose characteristic determinant, $(\lambda^2 - 2)^2$, has the elementary divisors $(\lambda - \sqrt{2})$, $(\lambda - \sqrt{2})$, $(\lambda + \sqrt{2})$, and $(\lambda + \sqrt{2})$. Since this characteristic determinant is reducible in any domain, L is reducible in any domain. In the continuous domain, L is completely reducible and its canonical form is

$$\begin{pmatrix} \sqrt{2} & 0 & 0 & 0 \\ 0 & \sqrt{2} & 0 & 0 \\ 0 & 0 & -\sqrt{2} & 0 \\ 0 & 0 & 0 & -\sqrt{2} \end{pmatrix}.$$

In the domain (1), however, the irreducible factors of its characteristic determinant are $\lambda^2 - 2$ and $\lambda^2 - 2$ and its canonical form can be taken to be

$$\begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

COROLLARY. *A matrix of finite period is reducible in a given domain, if, and only if, its characteristic determinant is reducible in that domain.*

Example. The reducibility of the matrix mentioned in § 7 is due to the reducibility of its characteristic determinant $(\lambda - 1)(\lambda^2 + \lambda + 1)$.

THE FINITE PERIODS OF n -ARY MATRICES.

10. In all that follows, the domain (1) will be understood.* By means of Theorem 3 and its corollary, the results of Theorems 1 and 2 can now be expressed in the following form:

THEOREM 4. *Every irreducible matrix of period m with rational elements is of degree $\phi(m)$. Every reducible matrix of period m with rational elements is of degree $\phi(m_1) + \dots + \phi(m_s)$, where $m_1, \dots, m_s$ are integers whose L. C. M. is equal to m ; its reduced form is made up of irreducible components whose degrees are $\phi(m_1), \dots, \phi(m_s)$, respectively. The minimum degree of a matrix of period m with rational elements is $\psi(m)$.*

EXAMPLE. If $m = 20$, the irreducible matrices are of degree 8; the reducible matrices are of various degrees ranging upward from the minimum value, which is 6; for instance, by taking $m_1 = 1$, $m_2 = 4$, $m_3 = 4$, $m_4 = 10$, we get $1 + 2 + 2 + 4 = 9$ for the degree.

11. Theorem 4 is analogous to the following well-known properties of permutations (substitutions):

* In a future paper I hope to treat in a similar manner the domain (ϵ) , where ϵ is a root of unity.

Every transitive (cyclical) permutation of period m is of degree m . Every intransitive permutation of period m is of degree $m_1 + \dots + m_s$, where $m_1, \dots, m_s$ are integers whose L. C. M. is equal to m . The minimum degree of a permutation of period $2^a p_1^{a_1} \dots p_r^{a_r}$ is $2^a + p_1^{a_1} + \dots + p_r^{a_r}$, if $a > 0$, and $p_1^{a_1} + \dots + p_r^{a_r}$, if $a = 0$.

EXAMPLE. A permutation of period 20 and of minimum degree 9 has one cycle of 4 letters and one of 5.

12. COROLLARY 1. *The minimum degree of a matrix whose period m is a power of a prime, or twice a power of an odd prime, is $\phi(m)$. In particular, the minimum degree of a matrix of prime period p is $p - 1$.*

From Corollary 1, in view of the lemma of § 2, we derive

COROLLARY 2. *If p is a prime and a is an integer determined by the inequalities $p^{a-1}(p-1) \leq n < p^a(p-1)$, then n -ary matrices exist whose period is any power of p as high as the a -th, but no higher. In particular, if $p-1 \leq n < p(p-1)$, n -ary matrices exist of period p , but none of period a power of p higher than the first. The highest prime period of an n -ary matrix cannot be greater than $n+1$.*

Since, for most values of m , $\psi(m) < \phi(m)$, it follows that in general the minimum degree of matrices of period m is less than the degree of the irreducible matrices of that period; i. e., there exist reducible matrices of lower degree than the irreducible matrices of the same period.

But there are exceptional values of m for which $\psi(m) = \phi(m)$. The solutions of this equation are evidently

$$(1) \quad m = 2^a, \quad (2) \quad m = p^a, \quad (3) \quad m = 2p^a, \quad (4) \quad m = 12.$$

If m has any of these values, the minimum degree of matrices of period m is equal to the degree of the irreducible matrices of that period; and there are no reducible matrices of lower degree than the irreducible matrices of the same period.

Moreover, if $m = 2^a$, p^a , or $2p^a$, all the matrices of minimum degree $\phi(m)$ are irreducible. Hence, every matrix whose period m is a power of a prime or twice a power of an odd prime, and one whose degree is $\phi(m)$, is irreducible; the degree of every reducible matrix of the same period is greater than $\phi(m)$. In particular, every matrix of prime period p and of degree $p-1$ is irreducible; the degree of every reducible matrix of period p is greater than $p-1$.

On the other hand, if $m = 12$, $\phi(m) = 2 \cdot 2$ and $\psi(m) = 2 + 2$. Therefore some of the matrices of period 12 and of degree 4 are irreducible and some are reducible; every reducible matrix of period 12 is of degree 4 or more.

13. With the single exception, $\phi(2) = \psi(2) = 1$, an odd number cannot be a

value of $\phi(m)$ or of $\psi(m)$. Moreover, not every even number can be a value of $\phi(m)$; among the even numbers which are not values of $\phi(m)$ the smallest are 14, 26, 34, 38, and 50. However, it is easy to see that every even number is included among the values of $\psi(m)$.

From these data drawn from the theory of numbers the following conclusions can be immediately drawn. *The degree of an irreducible matrix of finite period cannot be an odd number greater than 1 or one of the even numbers 14, 26, 34, 38, 50, etc.; in other words, every matrix of finite period, whose degree is either an odd number greater than 1 or one of the even numbers 14, 26, 34, 38, 50, etc., is reducible. In particular, every ternary matrix of finite period is reducible in the domain (1)*.*

The minimum degree of a matrix of finite period can be any even number whatsoever, but cannot be an odd number greater than 1; in other words, every even number is the minimum degree of the matrices of some finite period, whereas, if a matrix of finite period is of odd degree (> 1), another matrix of the same period and of lower degree can be found.

14. Let $\phi^{-1}(x)$ and $\psi^{-1}(x)$ be defined in the usual way as the inverse ϕ - and ψ -functions of x . As so defined they are multiple-valued for some integral values of x and do not exist at all for other values of x . Neither $\phi^{-1}(x)$ nor $\psi^{-1}(x)$ exists for any odd value of x greater than 1; $\phi^{-1}(x)$ exists for all even values of x except 14, 26, etc., and $\psi^{-1}(x)$ exists for all even values of x without exception.

The values of $\phi^{-1}(n)$ are evidently the finite periods of irreducible matrices of degree n ; while the values of $\psi^{-1}(n)$ are those finite periods of reducible or irreducible matrices of degree n which are not also periods of matrices of lower degree. To find all the finite periods of n -ary matrices, it is necessary, therefore, to include the totality of the values of $\psi^{-1}(x)$ for all integral values of x from 1 to n inclusive, i. e., if $n=2k$ or $2k+1$, to include the values of $\psi^{-1}(1)$, $\psi^{-1}(2)$, $\psi^{-1}(4)$, $\dots$, $\psi^{-1}(2k)$. In view of the lemma of § 2, we may state

THEOREM 5. *If $n=2k$ or $2k+1$, the finite periods of n -ary matrices with rational elements are the values of $\psi^{-1}(1)$, $\psi^{-1}(2)$, $\psi^{-1}(4)$, $\dots$, $\psi^{-1}(2k)$. There exist n -ary matrices having all these periods, but none having any other finite periods.*

COROLLARY. *The finite periods of matrices of degree $2k+1$ are exactly the same as those of degree $2k$.*

* On the other hand POINCARÉ has shown (*Les Fonctions fuchsienues et l'arithmétique*, Liouville's Journal, ser. 4, vol. 3 (1887), pp. 439-449) that within the group of ternary matrices whose determinants are equal to unity and whose elements are not only rational but integral, the matrices of finite period are not all reducible, although their characteristic determinants evidently break up into factors with rational, and therefore integral, coefficients.

are the required values of $\phi^{-1}(n)$. The work will be shortened somewhat by ignoring the case $n_0 = 1$ until the end and then multiplying every odd value of $\phi^{-1}(n)$ by 2 to form an additional even value.

18. Table of values of $\phi^{-1}(n)$.

The finite periods of n -ary irreducible matrices.

Degree = n		Period = $\phi^{-1}(n)$	Degree = n		Period = $\phi^{-1}(n)$	Degree = n		Period = $\phi^{-1}(n)$
n	$= n_0 \dots n_r$	$2^{a_0} p_1^{a_1} \dots p_r^{a_r} = m$	n	$= n_0 \dots n_r$	$2^{a_0} p_1^{a_1} \dots p_r^{a_r} = m$	n	$= n_0 \dots n_r$	$2^{a_0} p_1^{a_1} \dots p_r^{a_r} = m$
1	= 1	1 = 1	10	= 10	11 = 11	20	= 20	5 ² = 25
		2 = 2			2·11 = 22			2·5 ² = 50
2	= 2	3 = 3	12	= 12	13 = 13		= 2·10	3·11 = 33
		2·3 = 6			2·13 = 26			2·3·11 = 66
		2 ² = 4		= 2·6	3·7 = 21			2 ² ·11 = 44
4	= 4	5 = 5			2·3·7 = 42	22	= 22	23 = 23
		2·5 = 10			2 ² ·7 = 28			2·23 = 46
		2 ³ = 8			2 ² ·3 ² = 36	24	= 2·12	3·13 = 39
	= 2·2	2 ² ·3 = 12	16	= 16	17 = 17			2·3·13 = 78
6	= 6	7 = 7			2·17 = 34			2 ² ·13 = 52
		2·7 = 14			2 ⁵ = 32		= 4·6	5·7 = 35
		3 ² = 9		= 8·2	2 ⁴ ·3 = 48			2·5·7 = 70
		2·3 ² = 18		= 4·4	2 ³ ·5 = 40			2 ³ ·7 = 56
8	= 8	2 ⁴ = 16		= 2·2·4	2 ² ·3·5 = 60			2 ³ ·3 ² = 72
	= 2·4	3·5 = 15	18	= 18	19 = 19		= 6·4	3 ² ·5 = 45
		2·3·5 = 30			2·19 = 38			2·3 ² ·5 = 90
		2 ² ·5 = 20			3 ³ = 27		= 2·2·6	2 ² ·3·7 = 84
	= 4·2	2 ³ ·3 = 24			2·3 ³ = 54			

19. *Computation of $\psi^{-1}(n)$.* Let $m = \psi^{-1}(n)$. If $m = 2^{a_0} p_1^{a_1} \dots p_r^{a_r}$, where $a_0 > 1$, then $n = \phi(2^{a_0}) + \phi(p_1^{a_1}) + \dots + \phi(p_r^{a_r})$. Defining $n_0, n_1, \dots, n_r$, as before, by equations (1), we obtain the final equations $n = n_0 + n_1 + \dots + n_r$, and $\psi^{-1}(n) = \phi^{-1}(n_0) \cdot \phi^{-1}(n_1) \dots \phi^{-1}(n_r)$.

Therefore the computation of $\psi^{-1}(n)$ is strictly analogous to that of $\phi^{-1}(n)$. We first form all the possible partitions of n into even parts $n_0, n_1, \dots, n_r$, such that the values of their inverse ϕ -functions can be taken to be powers of distinct primes; then for every such partition of n we select those powers of distinct primes in every possible way and form their product. The products so formed, together with the doubles of those that are odd, are the required values of $\psi^{-1}(n)$.

20. Table of values of $\psi^{-1}(n)$.

Those finite periods of n -ary matrices which are not also periods of $(n-1)$ -ary matrices.

Degree = n		Period = $\psi^{-1}(n)$	Degree = n		Period = $\psi^{-1}(n)$	Degree = n		Period = $\psi^{-1}(n)$
n	$= n_0 + \dots + n_r$	$2^{a_0} p_1^{a_1} \dots p_r^{a_r} = m$	n	$= n_0 + \dots + n_r$	$2^{a_0} p_1^{a_1} \dots p_r^{a_r} = m$	n	$= n_0 + \dots + n_r$	$2^{a_0} p_1^{a_1} \dots p_r^{a_r} = m$
1	= 1	1 = 1	8	= 8	$2^4 = 16$	12	= 12	13 = 13
		2 = 2		= 2 + 6	$3 \cdot 7 = 21$			21 \cdot 3 = 26
2	= 2	3 = 3			$2 \cdot 3 \cdot 7 = 42$		= 2 + 10	3 \cdot 11 = 33
		2 \cdot 3 = 6			$2^2 \cdot 7 = 28$			2 \cdot 3 \cdot 11 = 66
		$2^2 = 4$			$2^2 \cdot 3^2 = 36$			$2^2 \cdot 11 = 44$
4	= 4	5 = 5		= 4 + 4	$2^3 \cdot 5 = 40$		= 8 + 4	$2^2 \cdot 5 = 80$
		2 \cdot 5 = 10		= 2 + 2 + 4	$2^2 \cdot 3 \cdot 5 = 60$		= 6 + 6	$3^2 \cdot 7 = 63$
		$2^3 = 8$	10	= 10	11 = 11			$2 \cdot 3^2 \cdot 7 = 126$
	= 2 + 2	$2^2 \cdot 3 = 12$			2 \cdot 11 = 22		= 2 + 4 + 6	3 \cdot 5 \cdot 7 = 105
6	= 6	7 = 7		= 8 + 2	$2^4 \cdot 3 = 48$			2 \cdot 3 \cdot 5 \cdot 7 = 210
		2 \cdot 7 = 14		= 4 + 6	5 \cdot 7 = 35			$2^2 \cdot 5 \cdot 7 = 140$
		$3^2 = 9$			$2 \cdot 5 \cdot 7 = 70$		= 4 + 2 + 6	$2^2 \cdot 3 \cdot 7 = 168$
		$2 \cdot 3^2 = 18$			$2^3 \cdot 7 = 56$		= 2 + 6 + 4	$2^2 \cdot 3^2 \cdot 5 = 180$
	= 2 + 4	3 \cdot 5 = 15			$2^3 \cdot 3^2 = 72$			
		$2 \cdot 3 \cdot 5 = 30$		= 6 + 4	$3^2 \cdot 5 = 45$			
		$2^2 \cdot 5 = 20$			$2 \cdot 3^2 \cdot 5 = 90$			
	= 4 + 2	$2^3 \cdot 3 = 24$		= 2 + 2 + 6	$2^2 \cdot 3 \cdot 7 = 84$			
				= 4 + 2 + 4	$2^3 \cdot 3 \cdot 5 = 120$			

CANONICAL FORMS.

21. We wish to determine the canonical forms of all n -ary matrices of period m in the domain (1). The canonical form of a reducible matrix must be a reduced form whose irreducible components are all in their canonical forms, but the latter, i. e., the canonical forms of irreducible matrices, can be chosen in a variety of ways, the desideratum being to have as large a number of zero elements as possible. One effective method is to use the lemma of § 2. Another method, which to some extent agrees with the former, and which makes every canonical form, at bottom, a permutation, will now be outlined; the canonical form of an irreducible matrix L will be determined for different values of its period m .

22. $m = p$, a prime. In this case L is of degree $p - 1$. Assume p letters $X_1, \dots, X_p$, connected by the symmetrical relation $X_1 + \dots + X_p = 0$ (geometrically, p coördinates, of which $p - 1$ are independent). Any cyclical permutation on all the letters is of period p and is equivalent to a linear substitution on the first $p - 1$ of them; in particular, the permutation $(X_1 \dots X_p)$ is equivalent to the linear substitution

$$X'_1 = X_2, X'_2 = X_3, \dots, X'_{p-1} = -X_1 - \dots - X_{p-1},$$

and therefore to the matrix

$$L' = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 \\ -1 & -1 & -1 & \dots & -1 \end{bmatrix},$$

of degree $p-1$.* L' will be taken to be the canonical form of L . For example, if $p=2$, $L' = (-1)$; if $p=3$, $L' = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.

23. $m = p^a$ (p a prime). In this case L is of degree $p^{a-1}(p-1)$. Assume p^a letters $X_1, \dots, X_{p^a}$ connected by the p^{a-1} symmetrical relations

$$(2) \quad \sum_{j=0}^{p-1} X_{i+jp^{a-1}} = 0 \quad (i=1, \dots, p^{a-1})$$

(geometrically, p^a coördinates, of which $p^{a-1}(p-1)$ are independent). Take any cyclical permutation on all the letters which leaves the relations (2) invariant and is therefore imprimitive, having the systems of letters entering into those relations as imprimitive systems. Such a permutation is of period p^a and is equivalent to a linear substitution on the $p^{a-1}(p-1)$ letters $X_1, \dots, X_{p^{a-1}(p-1)}$, which are obtained by omitting the last letter of each imprimitive system.

In particular, the permutation $(X_1 \dots X_{p^a})$ is equivalent to the linear substitution

$$X'_1 = X_2, X'_2 = X_3, \dots, X'_{p^{a-1}(p-1)} = - \sum_{j=0}^{p-2} X_{1+jp^{a-1}}.$$

The corresponding matrix will be taken to be the canonical form of every irreducible matrix of period p^a .

For example, if $m = 3^2$, we have nine letters $X_1, \dots, X_9$ connected by the three relations

$$X_1 + X_4 + X_7 = X_2 + X_5 + X_8 = X_3 + X_6 + X_9 = 0;$$

the permutation $(X_1 \dots X_9)$ is equivalent to the linear substitution

$$X'_1 = X_2, X'_2 = X_3, X'_3 = X_4, X'_4 = X_5, X'_5 = X_6, X'_6 = -X_1 - X_4,$$

* This method, for the case $m=p$, was given, in substance, in my paper in the Bulletin of the American Mathematical Society (1907), vol. 13, p. 343, § 14. Cf. also KLEIN's n -ary group of order $(n+1)!$ (KLEIN, *Mathematische Annalen*, vol. 4 (1871), pp. 346-358; MOORE, *American Journal of Mathematics* (1900), vol. 22, pp. 336-342.)

and is imprimitive, having the systems of letters entering into those relations as imprimitive systems. It is evidently equivalent to a linear substitution on the $\phi(m)$ letters (5), and therefore to a matrix of degree (m) .

In order to obtain a simple canonical form for the matrix, it will be convenient to extend the range of values of the suffixes $i_1, \dots, i_r$ to include all integers, and to define every new letter $X_{i_1, \dots, i_r}$ so obtained as equal to the old letter whose suffixes are the least positive residues of the suffixes of the new letter with respect to the moduli $p_1^{a_1}, \dots, p_r^{a_r}$. More precisely, we put $X_{i_1, \dots, i_r} = X_{i'_1, \dots, i'_r}$, if, and only if, $i_1 \equiv i'_1 \pmod{p_1^{a_1}}, \dots$, and $i_r \equiv i'_r \pmod{p_r^{a_r}}$. Then the letters

$$X_{i, i, \dots, i} \quad (i=1, 2, \dots, m)$$

are all distinct. For if $X_{i, i, \dots, i} = X_{j, j, \dots, j}$, then $i \equiv j \pmod{p_1^{a_1}}, \pmod{p_2^{a_2}}, \dots$, and $\pmod{p_r^{a_r}}$; and therefore $i \equiv j \pmod{m}$. So, being m in number, they are simply the letters (3) arranged in a particular order.

It is now clear that the permutation $(X_{1,1,\dots,1} \dots X_{m,m,\dots,m})$, of period m , has the required imprimitive systems, and is therefore equivalent to the following linear substitution on the $\phi(m)$ letters (5):

$$X'_{i_1, \dots, i_r} = X_{i_1+1, \dots, i_r+1} \quad [i_1=1, \dots, p_1^{a_1-1}(p_1-1); \dots; i_r=1, \dots, p_r^{a_r-1}(p_r-1)],$$

in which it is understood that every supernumerary letter is to be expressed in terms of the letters (5) by means of the relations (4). *The resulting matrix will be taken to be the canonical form of every irreducible matrix of period m .*

The §§ 22–24 are evidently special cases of this section.

26. Examples. (1) If $m = 3 \cdot 5$, so that $\phi(m) = 2 \cdot 4$, we have the 15 letters

$$X_{11}, X_{12}, X_{13}, X_{14}, X_{15},$$

$$X_{21}, X_{22}, X_{23}, X_{24}, X_{25},$$

$$X_{31}, X_{32}, X_{33}, X_{34}, X_{35},$$

conditioned by the vanishing of the sum of the letters in each row and in each column. The permutation $(X_{11} \dots X_{1515})$ becomes the octonary linear substitution $X'_{ij} = X_{i+1, j+1}$ ($i = 1, 2; j = 1, 2, 3, 4$), which may be written

$$\begin{aligned} X'_{1j} &= X_{2, j+1} & (j=1, 2, 3), & & X'_{14} &= - \sum_{j=1}^4 X_{2j}, \\ X'_{2j} &= - \sum_{i=1}^2 X_{i, j+1} & (j=1, 2, 3), & & X'_{24} &= \sum_{i=1, 2}^{j=1, 2, 3, 4} X_{ij}. \end{aligned}$$

Therefore the canonical form of an irreducible matrix of period 15 is

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\ 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

(2) If $m = 2^2 \cdot 3$, so that $\phi(m) = 2, 2$, we have the twelve letters X_{ij} ($i = 1, 2, 3; j = 1, 2, 3, 4$), connected by the relations

$$X_{i1} + X_{i3} = X_{i2} + X_{i4} = 0 \quad (i = 1, 2, 3), \quad X_{1j} + X_{2j} + X_{3j} = 0 \quad (j = 1, 2, 3, 4).$$

The permutation $(X_{11} \dots X_{1212})$ becomes the quaternary linear substitution $X'_{ij} = X_{i+1, j+1}$ ($i, j = 1, 2$), which may be written

$$X'_{11} = X_{22}, \quad X'_{12} = -X_{21}, \quad X'_{21} = -X_{12} - X_{22}, \quad X'_{22} = X_{11} + X_{21}.$$

Therefore the canonical form is

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

27. We are now prepared to find the canonical forms of all n -ary matrices of period m . Theorem 4 shows that we merely have to select in all possible ways integers $m_1, \dots, m_s$ such that their L. C. M. is m , and $\phi(m_1) + \dots + \phi(m_s) = n$. The number of canonical forms is equal to the number of ways of selecting these integers. The canonical form corresponding to any given selection is obtained by taking irreducible components of periods $m_1, \dots, m_s$ and of degrees $\phi(m_1), \dots, \phi(m_s)$, respectively, each in its canonical form as defined above, and combining them into a single reduced matrix.

Example. If $n = 3$ and $m = 6$, we find three pairs of values of m_1 and m_2 , namely 3 and 2, 6 and 1, 6 and 2, and therefore three canonical forms of ternary matrices of period 6, namely,

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}.$$

It will be noticed that every canonical form, as we have defined it, is a matrix whose elements are equal to 0, 1, or -1 and whose determinant is equal to ± 1 .

RESULTS FOR MATRICES OF LOW DEGREE.

28. The results of the foregoing theory may be applied to matrices of a few of the lowest degrees and summarized as follows:

$n = 2$. Apart from the trivial case $m = 1$, *the only finite periods of binary matrices with rational elements are 2, 3, 6, and 4*. The matrices of period 2 are all reducible; their canonical forms are $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, whose characteristic determinant is $(\lambda + 1)^2$, and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, whose characteristic determinant is $(\lambda - 1)(\lambda + 1)$. The matrices of periods 3, 6, and 4 are all irreducible; their canonical forms and characteristic determinants are $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ and $\lambda^2 + \lambda + 1$, $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ and $\lambda^2 - \lambda + 1$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\lambda^2 + 1$, respectively.

$n = 3$. *In the field (1) ternary matrices have the same finite periods as binary matrices, and all ternary matrices of finite period are reducible*. Those of period 2 have three canonical forms, namely,

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

whose characteristic determinants are $(\lambda + 1)^3$, $(\lambda - 1)(\lambda + 1)^2$, and $(\lambda - 1)^2(\lambda + 1)$, respectively. Those of period 3 can all be transformed into the single canonical form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix},$$

whose characteristic determinant is $(\lambda - 1)(\lambda^2 + \lambda + 1)$. Those of period 4 have the two canonical forms

$$\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix},$$

whose characteristic determinants are $(\lambda \mp 1)(\lambda^2 + 1)$. Finally, those of period 6 have the three canonical forms mentioned in § 27, the corresponding characteristic determinants being $(\lambda + 1)(\lambda^2 + \lambda + 1)$ and $(\lambda \mp 1)(\lambda^2 - \lambda + 1)$, respectively.*

$n = 4$. *Quaternary matrices have the periods 5, 10, 8, and 12, in addition to those of binary matrices*. All quaternary matrices of periods 5, 10, and 8,

* Contrast these nine canonical forms of ternary matrices, all of which are reduced, with the eight canonical forms, four reduced and four irreducible, obtained by POINCARÉ (l. c., p. 448).

and some of period 12, are irreducible; all those of periods 2, 3, 6, and 4, and some of period 12, are reducible. Those of period 2 have four canonical forms, which require no further mention. Those of period 3 have two canonical forms, whose characteristic determinants are $(\lambda - 1)^2(\lambda^2 + \lambda + 1)$ and $(\lambda^2 + \lambda + 1)^2$, respectively. Those of period 6 have seven canonical forms, and those of period 4 have four canonical forms.

Those whose periods are 5, 10, and 8 have the canonical forms and characteristic determinants

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \end{pmatrix} \quad \text{and} \quad \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1,$$

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \lambda^4 - \lambda^3 + \lambda^2 - \lambda + 1,$$

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \lambda^4 + 1,$$

respectively. Those matrices of period 12 which are irreducible have the canonical form

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

and the characteristic determinant $\lambda^4 - \lambda^2 + 1$, while those which are reducible have the two canonical forms

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

whose characteristic determinants are $(\lambda^2 + 1)(\lambda^2 + \lambda + 1)$ and $(\lambda^2 + 1)(\lambda^2 - \lambda + 1)$, respectively.

$n = 5$. Quinary matrices have the same finite periods as quaternary matrices; all quinary matrices of finite period are reducible.

$n = 6$. Senary matrices have eight additional periods, viz., 7, 14, 9, 18, 15, 30, 20, and 24, making seventeen periods in all. Those whose periods are 7, 14, 9, and 18, are irreducible; those whose periods are 15, 30, 20, and 24 are reducible, and their reduced forms are each made up of two components, one binary and one quaternary. There is a single canonical form corresponding to each of the periods 7, 14, 9, 18, 15, 20, and 24, while there are three canonical forms corresponding to the period 30.

$n = 7$. Septenary matrices have the same finite periods as senary matrices; all septenary matrices of finite period are reducible.

$n = 8$. Octonary matrices have seven additional periods, 16, 21, 42, 28, 36, 40, and 60. Here for the first time we meet with irreducible matrices of periods 15, 30, 20, and 24. Besides these, there are also reducible octonary matrices of periods 15, 30, 20, and 24. For example, the irreducible matrices of period 20 have the characteristic determinant $\lambda^8 - \lambda^6 + \lambda^4 - \lambda^2 + 1$, while the reducible matrices of period 20 have eight different characteristic determinants, one of which is $(\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1)(\lambda^2 + 1)^2$.

This classification can easily be extended to cover matrices of any given degree whatever.*

CORNELL UNIVERSITY,
August, 1907.

* I wish to acknowledge my obligation to Professor FITE for valuable assistance in correcting errors and omissions in this paper.