# Matrices with finite period

By Olga Taussky and John Todd.

(*Received 8th September*, 1939. *Read 25th November*, 1939.)

**1.** The study of the primitive solutions of the equation

$$A^r = 1, \tag{1}$$

where $A = (a_{ij})$ is an $n \times n$ matrix whose elements are rational integers, was begun a long time ago[1]. In most cases this equation occurred incidentally in another theory; for instance Jordan encountered it in connection with linear differential equations having algebraic solutions, Minkowski in connection with quadratic forms and Turnbull in geometry. An important fact about these matrices is that any unimodular matrix can be represented as the product of matrices with finite period.

In this note we point out a connection between (1) and algebraic number fields generated by roots of unity. The methods we adopt can be applied to the study of a much larger class of matrices. In § 2 we summarise those parts of Algebraic Number Theory which we require[2].

**2.1.** Let $\alpha$ be a root of an irreducible algebraic equation

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0 \tag{2}$$

of degree $n$ with rational coefficients. The set of all polynomials of degree less than $n$ in $\alpha$, having all their coefficients rational, forms a field, the algebraic number field $R(\alpha)$, generated by $\alpha$. This field is said to have degree $n$. We can say that $R(\alpha)$ is an $n$-dimensional modul, with rational coefficients and base elements $1, \alpha, \ldots, \alpha^{n-1}$. Any set of elements $\omega_1, \ldots, \omega_n$ obtained from $1, \alpha, \ldots, \alpha^{n-1}$ by a non-singular linear transformation with rational coefficients also forms a base for this modul. The field $R(\alpha)$ can also be regarded as a hypercomplex system, over the rational numbers, with base $\omega_1, \ldots, \omega_n$, when the "natural" multiplication is introduced. The regular representation of this hypercomplex system associates with every element of it a certain $n \times n$ matrix all of whose elements are rational.

**2.2.** Let $a^{(2)}, \ldots, a^{(n)}$ denote the other $n-1$ roots of (2). These are called the conjugates of $a\,(=a^{(1)})$. Let $\omega_1^{(i)}, \ldots, \omega_n^{(i)}$ denote the same functions of $a^{(i)}$ as $\omega_1, \ldots, \omega_n\,(=\omega_1^{(1)}, \ldots, \omega_n^{(1)})$ are of $a\,(=a^{(1)})$ (this for $i=2, \ldots, n$). It is known that

$$|\omega_j^{(i)}| \neq 0.$$

The two sets $\omega_1^{(i)}, \ldots, \omega_n^{(i)}$ and $\omega_1^{(j)}, \ldots, \omega_n^{(j)}$ are said to be conjugate bases.

**2.3.** An algebraic number which satisfies an equation of the form (2) where all the coefficients are integers and where $a_0 = 1$ is called an integral number. An algebraic number which satisfies an equation of the form (2), where all the coefficients are integers and where $a_0 = \pm 1$, $a_n = \pm 1$, is called a unit (its reciprocal is also an integral number). A special case of such units are the roots of unity.

A base $\omega_1, \ldots, \omega_n$ of a field $R(a)$ is called an integral base if every $\omega_i$ is an integral number and if every integral number in $R(a)$ can be expressed as $\Sigma b_i \omega_i$ where the $b_i$ are integers. An integral base exists for any field. Of any two integral bases for the same field either can be obtained from the other by a unimodular linear transformation all of whose coefficients are integers.

**2.4.** The field generated by a root of unity has the property that every element satisfies an irreducible algebraic equation, all of whose roots are contained in the field.

**3.1.** *A connection between the units of a field generated by a root of unity and the automorphisms of a certain form.* Let $\zeta$ be a primitive $r$th root of unity. The degree of the field $R(\zeta)$ generated by $\zeta$ is $\phi(r)$ (where $\phi(r)$ is Euler's function, the number of positive integers less than $r$ and prime to it). We put $\phi(r) = n$. Let $\omega_1, \ldots, \omega_n$ be an integral base for $R(\zeta)$. Consider the form

$$f = \prod_{i=1}^{n} (u_1 \omega_1^{(i)} + \ldots + u_n \omega_n^{(i)}) \equiv \Pi\, l_i(u) \tag{3}$$

in the $n$ variables $u_1, \ldots, u_n$. Let $A = (a_{ij})$ be an $n \times n$ matrix, $|A| = \pm 1$, which determines a linear transformation

$$(u) \to (u') \text{ where } (u) = (u')\,A \tag{4}$$

under which $f$ is invariant (apart from a factor $\pm 1$)[3]. The fact that

https://doi.org/10.1017/S0013091500024627 Published online by Cambridge University Press

$f$ is invariant means that the linear factors of $f$ are permuted and subjected to a multiplication by factors $\rho_1, \ldots, \rho_n$ where $\prod_{i=1}^{n} \rho_i = \pm 1$, when they undergo the transformation (4). Suppose, in fact, that we have

$$(5_i) \qquad l_i(u) = \rho_i l_{p_i}(u')$$

where $p_i (i = 1, 2, \ldots, n)$ is a permutation of $1, 2, \ldots, n$.

**3.2.** We shall show that *each* $\rho_i$ *is a unit in* $R(\zeta)$. We begin by writing $(5_i)$ in full as

$$(5_i) \qquad u_1 \omega_1^{(i)} + \ldots + u_n \omega_n^{(i)} = \rho_i (u_1' \omega_1^{(p_i)} + \ldots + u_n' \omega_n^{(p_i)}).$$

Since the set $\omega_1^{(p_i)}, \ldots, \omega_n^{(p_i)}$ is also an integral base in the field $R(\zeta)$ we have, for a certain matrix $B_i = (b_{rs}^{(i)})$ all of whose elements are integers and for which $|B_i| = \pm 1$, that[4]

$$(6_r) \qquad \omega_r^{(p_i)} = b_{rs}^{(i)} \omega_s^{(i)}$$

—this for $i = 1, 2, \ldots, n$.

Substituting from (4) and (6) in (5) we find

$$a_{jk} \omega_k^{(i)} u' = \rho_i b_{rl}^{(i)} \omega_l^{(i)} u_r'$$

from which, on equating the coefficients of $u_j'$, we have

$$(7_i) \qquad (a_{jk} - \rho_i b_{jk}^{(i)}) \omega_k^{(i)} = 0.$$

It follows from $(7_i)$, since the $\omega_k^{(i)}$ are not all zero, that $\rho_i$ is a root of the determinantal equation

$$(8) \qquad |a_{jk} - x b_{jk}^{(i)}| = 0.$$

Because the coefficient of $x^n$ and the constant term in (8) are $\pm |b_{jk}^{(i)}|$ and $|a_{jk}|$ respectively (and therefore each is $\pm 1$) it follows (the remaining coefficients being integers) from the theorem of Gauss[5] that $\rho_i$ is a unit in a certain algebraic field. We can express $\rho_i$ rationally in terms of the $\omega_1^{(i)}, \ldots, \omega_n^{(i)}$ by using any one of the equations $(7_i)$. Hence $\rho_i$ is a unit in $R(\zeta)$.

**3.3.** Consider now any field of degree $n$ with base $\omega_1, \ldots, \omega_n$ and a special case of the transformation (4) in which each $l_i$ is transformed into itself, apart from the factor $\rho_i$. This means that each $p_i = i$ and that each matrix $B_i$ is the unit $n \times n$ matrix so that each $\rho_i$ satisfies the *same* algebraic equation

$$(9) \qquad |a_{jk} - \delta_{jk} x| = 0$$

which must be a power of the irreducible equation which they satisfy.

The equation $(7_i)$, in the special case under consideration, can be written as

$$(10_i) \qquad (\omega_1^{(i)}, \ldots, \omega_n^{(i)})\, A = \rho_i (\omega_1^{(i)}, \ldots, \omega_n^{(i)}),$$

from which it is clear that *if $A$ is of finite period*[6] (say $q$) *then $\rho_i$ is of finite period* ($r_i \leqq q$).

Since the $\rho_i$ are conjugates all the $r_i$ are equal, say to $r$. We show that $r = q$.

It follows from $(10_i)$ that

$$(11_i) \qquad (\omega_1^{(i)}, \ldots, \omega_n^{(i)})\, A^r = (\omega_1^{(i)}, \ldots, \omega_n^{(i)})$$

which means that the reduced characteristic function[7] of $A$ with respect to each of the $n$ vectors $(\omega^{(i)})$, $(i = 1, 2, \ldots, n)$, is a divisor of $A^r - 1$. These $n$ vectors are linearly independent because $|\omega_j^{(i)}| \neq 0$. Hence the reduced characteristic function of $A$ is a divisor of $A^r - 1$. Thus we have $q \leqq r$. Hence $q = r$.

We have therefore established the following result:—

I. *An $n \times n$ matrix which determines an automorphism (of the special type in question) of the form* (3) *can only have such periods as are possessed by the roots of unity contained in the field.*

**3.4.** All the possibilities allowed by I can be realised. We shall establish:

II. *Let $R(\alpha)$ be a field of degree $n$. Let $r$ be the order of a root of unity contained in $R(\alpha)$. Then there exists an $n \times n$ matrix with period $r$.*

Proof. Let $\eta$ be a primitive $r$-th root of unity contained in $R(\alpha)$. Let $\omega_1, \ldots, \omega_n$ be an integral base for $R(\alpha)$. Since each $\eta\omega_j$ is an integral number there is a matrix $C = (c_{jk})$, all of whose elements are integers, such that

$$\eta\omega_j = c_{jk}\, \omega_k$$

which we may write in the form

$$\eta\, (\omega_1, \ldots, \omega_n) = (\omega_1, \ldots, \omega_n)\, C.$$

From this it follows that

$$(\omega_1, \ldots, \omega_n) = (\omega_1, \ldots, \omega_n)\, C^r.$$

This last result is also true when we replace $(\omega)\,(= (\omega^{(1)}))$ by any of its conjugates $(\omega^{(i)})$. Using the method of proof of I and the fact that $\eta$ is a primitive root we conclude that $C$ has period $r$.

https://doi.org/10.1017/S0013091500024627 Published online by Cambridge University Press

An alternative proof of II depending on the regular representation of the field can be given. We observe that if we do not take the regular representation relative to an *integral* base we must use the following lemma which is, however, of interest independently[8].

LEMMA. *Every matrix with finite period, all of whose elements are rational, is similar to a matrix all of whose elements are integers.*

**4.** The matrices we have considered do not exhaust the class of matrices with finite period. In fact the characteristic polynomial of such a matrix is not, in general, the power of an irreducible polynomial (*cf.* **11** below). We shall now consider the general form of such matrices.

If $A$ is an $n \times n$ matrix with period $r$ then it is known[9] that the characteristic equation of $A$ is of the form

$$\Pi f_{d_i}(n) = 0,$$

where $f_{d_i}(n) = 0$ is the irreducible equation of which the $d_i$th root of unity is a root and where the $d_i$ are divisors of $r$. Hence

$$n = \Sigma \phi(d_i).$$

From this it follows that

III. *Corresponding to an assigned $n$ only a finite number of values of $r$ are possible.*

We shall now establish

IV. *Let $A$ be an $n \times n$ matrix, irreducible in the rational field, and of period $r$. Then $\phi(r) = n$.*

This implies that *the only possible periods of irreducible $n \times n$ matrices are those which occur among the orders of the roots of unity generating fields of degree $n$.*

Proof. $A$ being irreducible the characteristic polynomial of $A$ must be the power of an irreducible polynomial[10]. Every latent root $\rho$ of $A$ is a root of unity and all these have the same order. This order must be $r$. For, if we had $\rho^s = 1$, where $s$ is a proper divisor of $r$, then the matrix $A$ would satisfy the equation $A^s = 1$ because the reduced characteristic equation of which $A$ is a root must be a divisor of the characteristic equation. Hence the irreducible polynomial in question is of degree $\phi(r)$ and so $\phi(r)/n$. To show that $\phi(r) = n$ it is enough to show that the characteristic polynomial of $A$ is itself irreducible. This follows from the fact[10] that an irreducible matrix

has its characteristic polynomial and its reduced characteristic polynomial identical, and the fact that the matrix $A$ satisfies $x^r - 1 = 0$, which has no multiple roots[11].

5.1. *Applications.* By using the regular representation of an associative hypercomplex system with a unit, with integers as coefficients, and having $n$ base elements it follows from III that if $r$ is a period of a unit in any such system then $r \leqq K = K(n)$, a constant depending only on $n$. In particular we have[12].

*If $r$ is the order of a unit in a group-ring (the group being of order $n$ and the ring that of the integers) then $r \leqq K = K(n)$, a constant depending only on $n$.*

5.2. The result III, established for matrices whose elements are rational integers, can be extended. In fact this result is true for matrices with elements in an (associative) hypercomplex system $S$ with integers as coefficients and having $f$ base elements. To see this we use the regular representation of the elements of $S$ as $f \times f$ matrices and we observe that every $n \times n$ matrix with elements in $S$ having period $r$ gives rise to an $fn \times fn$ matrix[13], whose elements are integers, which has the same period $r$—and the number of these periods is finite by III.

Particular cases of $S$ which are of interest are the complex integers and the quaternion integers (in the sense of Dickson). Some of these will be discussed in another paper.

---

## NOTES AND REFERENCES.

**1**. It will be understood throughout this note that every matrix considered, unless otherwise stated, has all its elements rational integers. Further we shall understand by integer rational integer unless some other meaning is given explicitly.

Among the papers dealing with the problem under consideration are

H. F. Baker, *Proc. London Math. Soc.* (1), **35** (1903), 379-384.

C. Jordan, *Journ. f. Math.* **84** (1878), 89-215, especially 112.

R. Lipschitz, *Acta Math.* **10** (1887), 137-144.

H. Minkowski, *Journ. f. Math.* **101** (1887), 196-202; also in *Gesammelte Abhandlungen* 1 (Leipzig-Berlin, 1911), 212-218. (*Cf.* A. Speiser, *Theorie der Gruppen von endlicher Ordnung* ((3), Berlin, 1937), §67).

H. W. Turnbull, *Journ. London Math. Soc.* **2** (1927), 242-244.

R. Vaidyanathaswamy, *Journ. London Math. Soc.* **3** (1928), 121-124 and 268-272.

A more complete bibliography is available in the reports of: J. H. M. Wedderburn, *Lectures on Matrices* (American Math. Soc. Coll. Publications, 17, New York, 1934); B. L. van der Waerden, *Gruppen von linearen Transformationen* (Berlin, 1935); C. C. MacDuffee, *The Theory of Matrices* (Berlin, 1933).

**2.** Proofs of the results stated in § 2 will be found in any account of Algebraic Number Theory, *e.g.* in D. Hilbert, *Gesammelte Abhandlungen*, 1 (Berlin, 1932), 63-363 or in a forthcoming book by one of us (O. T.): *Algebraic Numbers* (Oxford, 1940).

**3.** It is interesting to observe that it is always possible to find a form of degree $n$ in $n$ variables which is invariant under the transformation determined by an assigned $n \times n$ matrix $A$ with $|A| = \pm 1$. To see this denote the latent roots of $A$ by $\rho_1, \ldots\ldots, \rho_n$ and denote by $(x_1^{(i)}, \ldots\ldots, x_n^{(i)})$ a non-trivial solution of the system of equations

$$\rho_i(x_1^{(i)}, \ldots\ldots, x_n^{(i)}) = (x_1^{(i)}, \ldots\ldots, x_n^{(i)})A.$$

Then the form

$$\prod_{i=1}^{n} (u_1 x_1^{(i)} + \ldots\ldots + u_n x_n^{(i)})$$

in the $n$ variables $u_1, \ldots\ldots, u_n$ is easily shown to be invariant under the transformation determined by $A$.

**4.** Here and elsewhere we find it convenient to use the summation convention.

**5.** See *e.g.* A. A. Albert, *Modern Higher Algebra* (Chicago-Cambridge, 1937), 37.

**6.** When we say that $A$ has period $r$ we understand that $A^r = 1$ and that $A^s \neq 1$ for any $s = 1, 2, \ldots\ldots, r-1$.

**7.** See *e.g.* H. W. Turnbull and A. C. Aitken, *The Theory of Canonical Matrices* (London-Glasgow, 1932), Ch. 5.

**8.** See *e.g.* the book of Speiser referred to in **1**, § 67 or W. Burnside, *Proc. London Math. Soc.* (2), **7** (1909), 8-13.

**9.** See the papers of Vaidyanathaswamy referred to in **1**. The case $r = n$ corresponds to the cyclic permutation of $n$ elements; in this case we have to use the well-known relation

$$n = \sum_{d/n} \phi(d).$$

**10.** See the book of Albert referred to in **5**, Ch. 4, § 5.

**11.** Similarly it can be seen that an $n \times n$ matrix of period $r$, whose characteristic polynomial is the power of an irreducible polynomial, must be the direct sum of irreducible matrices each of which has its characteristic function of degree $\phi(r)$. Such a matrix can always be obtained as the regular representation of a root of unity contained in an algebraic number field of degree $n$. *Cf.* Olga Taussky and John Todd, *Proc. Royal Irish Academy*, **46**A (1940), 1-11.

**12.** This result is in accordance with a result established by Higman, *Proc. London Math. Soc.* (2), **46** (1940), 231-248. Here it is shown that the only units of finite order in the group-ring of an abelian group are the elements of the group itself.

**13.** See *e.g.* the book of Turnbull and Aitken referred to in **7**, Ch. 1, § 6.

JOHN TODD,
KING'S COLLEGE, LONDON, W.C. 2.

OLGA TAUSSKY,
WESTFIELD COLLEGE, LONDON, N.W. 3