A MATRIX REPRESENTATION OF THE PRIMITIVE RESIDUE CLASSES (mod $2n$)

K. MAHLER

A problem[1] in the geometry of numbers recently lead me to consider some simple matrices with elements 0, 1, and -1. I found to my surprise that these matrices had inverses of the same kind, that they were commutative, and that they in fact formed an Abelian group. These matrices are discussed in the present note.

1. Let m and n be two positive integers such that

$$1 \leq m < n, \qquad (m, n) = 1.$$

Let further $s \neq 0$ be a parameter and t one of its nth roots,

$$t^n = s.$$

There are thus n distinct possible values for t, the values $t_1, t_2, \cdots, t_n$ say.

Now denote by

$$A(m, n) = (a_{hk}) \quad \text{and} \quad B(m, n) = (b_{hk})$$

the two $n \times n$ matrices with the following elements. For each pair of suffixes $h, k = 1, 2, \cdots, n$ determine integers i, j, q, and r such that

$$km - h \equiv i \pmod{n}, \qquad 0 \leq i \leq n-1, \; q = \frac{km - h - i}{n},$$

and

$$km + h \equiv j \pmod{n}, \qquad 1 \leq j \leq n, \; r = \frac{km + h - j}{n}.$$

Then put

$$a_{hk} = s^q \text{ if } 0 \leq i \leq m-1, \qquad a_{hk} = 0 \text{ if } m \leq i \leq n-1;$$
$$b_{hk} = s^{r-1} \text{ if } 1 \leq j \leq m, \qquad b_{hk} = 0 \text{ if } m+1 \leq j \leq n.$$

Thus, by way of example,

Received by the editors March 27, 1956.

[1] It has been conjectured that the symmetric convex domain in the plane of given lattice determinant and smallest area is bounded by line segments and osculating hyperbolae arcs. The discussion of such domains leads to systems of linear equations which have matrices just as considered in this note, and I found their group property when I tried to solve the equations.

$$A(3,5) = \begin{pmatrix} 1 & s & 0 & s^2 & 0 \\ 1 & 0 & s & s^2 & 0 \\ 1 & 0 & s & 0 & s^2 \\ 0 & 1 & s & 0 & s^2 \\ 0 & 1 & 0 & s & s^2 \end{pmatrix}, \qquad B(2,5) = \begin{pmatrix} 0 & 0 & 1 & 0 & s \\ 0 & 1 & 0 & 0 & s \\ 0 & 1 & 0 & s & 0 \\ 1 & 0 & 0 & s & 0 \\ 1 & 0 & s & 0 & 0 \end{pmatrix}.$$

We shall study these matrices mainly in the case when m is odd and s has the value -1, but, for the present, do not yet impose these restrictions.

2. Denote by

$$x = (x_h), \qquad y = (y_h), \qquad z = (z_h)$$

three variable $n \times 1$ matrices (column vectors) such that

$$y = A(m, n)x \quad \text{and} \quad z = B(m, n)x,$$

or in explicit form,

$$y_h = \sum_{k=1}^{n} a_{hk}x_k, \qquad z_h = \sum_{k=1}^{n} b_{hk}x_k.$$

Further put, for shortness,

$$Y = y_1 + ty_2 + t^2y_3 + \cdots + t^{n-1}y_n,$$
$$Z = t^{n-1}z_1 + t^{n-2}z_2 + \cdots + tz_{n-1} + z_n.$$

Then

$$Y = \sum_{h=1}^{n}\sum_{k=1}^{n} t^{h-1}a_{hk}x_k = \sum_{k=1}^{n} u_k x_k$$

where

$$u_k = \sum_{h=1}^{n} t^{h-1}a_{hk},$$

and similarly

$$Z = \sum_{h=1}^{n}\sum_{k=1}^{n} t^{n-h}b_{hk}x_k = \sum_{k=1}^{n} v_k x_k$$

where

$$v_k = \sum_{h=1}^{n} t^{n-h}b_{hk}.$$

3. These expressions can be replaced by simpler ones. From the definition of a_{hk} it is evident that

$$t^{h-1}a_{hk}=\begin{cases} s^q t^{h-1}=t^{nq+h-1}=t^{km-i-1} & \text{if } km-h=nq+i,\ 0\leq i\leq m-1, \\ 0 & \text{if } km-h=nq+i,\ m\leq i\leq n-1. \end{cases}$$

Therefore

$$u_h = \sum_{h=1}^{n} t^{h-1}a_{hk} = \sum_{i=0}^{m-1} t^{km-i-1} = t^{(k-1)m}\frac{1-t^m}{1-t},$$

whence

$$\begin{aligned} Y &= \sum_{k=1}^{n} t^{(k-1)m}\frac{1-t^m}{1-t}\, x_k \\ &= \frac{1-t^m}{1-t}(x_1+t^m x_2+t^{2m}x_3+\cdots+t^{(n-1)m}x_n). \end{aligned}$$

On combining this formula with the definition of Y, we obtain the First Identity,

$$\begin{aligned} &(1-t)(y_1+ty_2+t^2y_3+\cdots+t^{n-1}y_n) \\ &\qquad = (1-t^m)(x_1+t^m x_2+t^{2m}x_3+\cdots+t^{(n-1)m}x_n). \end{aligned} \tag{1}$$

Similarly, by the definition of b_{hk},

$$t^{n-h}b_{hk}=\begin{cases} s^{r-1}t^{n-h}=t^{nr-h}=t^{km-j} & \text{if } km+h=nr+j,\quad 1\leq j\leq m, \\ 0 & \text{if } km+h=nr+j,\ m+1\leq j\leq n. \end{cases}$$

Thus now

$$v_k = \sum_{h=1}^{n} t^{n-h}b_{hk} = \sum_{j=1}^{m} t^{km-j} = t^{(k-1)m}\frac{1-t^m}{1-t},$$

hence

$$\begin{aligned} Z &= \sum_{k=1}^{n} t^{(k-1)m}\frac{1-t^m}{1-t}\, x_k \\ &= \frac{1-t^m}{1-t}(x_1+t^m x_2+t^{2m}x_3+\cdots+t^{(n-1)m}x_n), \end{aligned}$$

and therefore, from the definition of Z,

$$\begin{aligned} &(1-t)(t^{n-1}z_1+t^{n-2}z_2+\cdots+tz_{n-1}+z_n) \\ &\qquad = (1-t^m)(x_1+t^m x_2+t^{2m}x_3+\cdots+t^{(n-i)m}x_n). \end{aligned}$$

Here the left-hand side may also be written as

$$-t^n(1-t^{-1})(z_1+t^{-1}z_2+t^{-2}z_3+\cdots+t^{-(n-1)}z_n).$$

Since $t^n=s$, we obtain then the Second Identity,

$$\begin{aligned}(2)\qquad -s(1-t^{-1})&(z_1+t^{-1}z_2+t^{-2}z_3+\cdots+t^{-(n-1)}z_n)\\ &=(1-t^m)(x_1+t^mx_2+t^{2m}x_3+\cdots+t^{(n-1)m}x_n).\end{aligned}$$

4. Denote by τ an arbitrary parameter, by

$$\xi=(\xi_h)$$

an arbitrary $n\times 1$ matrix (column vector), and put

$$\Phi(\xi\mid\tau)=(1-\tau)(\xi_1+\tau\xi_2+\tau^2\xi_3+\cdots+\tau^{n-1}\xi_n).$$

In this notation, the two identities (1) and (2) take the simple form

$$\Phi(y\mid t)=\Phi(x\mid t^m)\quad\text{and}\quad -s\Phi(z\mid t^{-1})=\Phi(x\mid t^m),$$

respectively. Here, for $s\neq 0$, t may be any one of $t_1, t_2, \cdots, t_n$.

LEMMA 1. *Let σ be distinct from* 0 *and* 1, *and let $\tau_1, \tau_2, \cdots, \tau_n$ denote the n roots of the equation $\tau^n=\sigma$. For any n given numbers $\phi_1, \phi_2, \cdots, \phi_n$ there exists one and only one vector ξ such that*

$$\Phi(\xi\mid\tau_h)=\phi_h\qquad (h=1,2,\cdots,n).$$

PROOF. The expression Φ may also be written as

$$\begin{aligned}\Phi(\xi\mid\tau_h)=(\xi_1-\sigma\xi_n)&+\tau_h(\xi_2-\xi_1)\\ &+\tau_h^2(\xi_3-\xi_2)+\cdots+\tau_h^{n-1}(\xi_n-\xi_{n-1}).\end{aligned}$$

The hypothesis $\sigma\neq 0$ implies that the n roots $\tau_1, \tau_2, \cdots, \tau_n$ are all distinct, hence that the Vandermonde determinant

$$\left|\tau_h^{k-1}\right|_{h,k=1,2,\cdots,n}$$

does not vanish. The assertion is therefore proved if it can be shown that the n linear forms

$$\xi_1-\sigma\xi_n,\qquad \xi_2-\xi_1,\qquad \xi_3-\xi_2,\cdots,\xi_n-\xi_{n-1}$$

in $\xi_1, \xi_2, \cdots, \xi_n$ are linearly independent. However, the determinant of these forms evidently equals $1-\sigma$ and so, by $\sigma\neq 1$, does not vanish, whence the assertion.

LEMMA 2. *Let s^m, hence also s and s^{-1}, be distinct from* 0 *and* 1, *and let $t_1, t_2, \cdots, t_n$ be the roots of $t^n=s$. The n equations*

$$(3)\qquad \Phi(y\mid t_h)=\Phi(x\mid t_h^m)\qquad (h=1,2,\cdots,n)$$

define a nonsingular linear mapping of x on y and vice versa; and the n equations

$$-s\Phi(z \mid t_h^{-1}) = \Phi(x \mid t_h^m) \qquad (h = 1, 2, \cdots, n) \tag{4}$$

similarly define a nonsingular linear mapping of x on z and vice versa.

PROOF. The assertion is contained in Lemma 1 applied with $\sigma = s$, $\sigma = s^{-1}$, and $\sigma = s^m$, respectively.

COROLLARY. *If s^m is distinct from 0 and 1, then the two matrices $A(m, n)$ and $B(m, n)$ are both nonsingular.*

5. From now on we impose the additional conditions that

$$m \text{ is odd}, \quad \text{and} \quad s = -1.$$

Hence $t_1, t_2, \cdots, t_n$ now satisfy the equation

$$t^n = -1.$$

Thus, for odd n, $-t_1, -t_2, \cdots, -t_n$ are all the nth roots of unity, while, for even n, $t_1, t_2, \cdots, t_n$ are all those $(2n)$th roots of unity which are not also nth roots of unity. The equations (3) connecting x and y remain unchanged, but the equations (4) between x and z now become

$$\Phi(z \mid t_h^{-1}) = \Phi(x \mid t_h^m) \qquad (h = 1, 2, \cdots, n),$$

or equivalent to this,

$$\Phi(z \mid t_h) = \Phi(x \mid t_h^{-m}) \qquad (h = 1, 2, \cdots, n). \tag{5}$$

Since, by hypothesis, m is prime to n, and further m is odd, it is obvious that both the mth powers

$$t_1^m, t_2^m, \cdots, t_n^m,$$

and the $(-m)$th powers

$$t_1^{-m}, t_2^{-m}, \cdots, t_n^{-m}$$

of $t_1, t_2, \cdots, t_n$ are again these same roots, only possibly arranged in a different order.

For, first, $t^n = -1$ implies that also $(t^m)^n = (t^{-m})^n = -1$ because m is odd. Secondly, by $(m, n) = 1$, there exist integers M and N such that $mM + nN = 1$. Hence, if $t^n = t'^n = -1$ and $t \neq t'$, then

$$\left(\frac{t^m}{t'^m}\right)^M \left(\frac{t^n}{t'^n}\right)^N = \frac{t}{t'} \neq 1 \qquad \text{and therefore } t^m \neq t'^m,\ t^{-m} \neq t'^{-m}.$$

6. From now on we change the notation slightly and allow m to be a positive or negative integer such that

$$(m, n) = 1, \qquad 1 \leq |m| \leq n - 1, \qquad m \text{ is odd.} \tag{6}$$

In extension of the previous notation we then put

$$A(m, n) = \begin{cases} A(m, n) & \text{if } m > 0, \\ B(-m, n) & \text{if } m < 0. \end{cases}$$

Therefore, in either case, the mapping

$$y = A(m, n)x$$

is equivalent to the system of n formulae,

$$\Phi(y \mid t_h) = \Phi(x \mid t_h^m) \qquad (h = 1, 2, \cdots, n).$$

Next, let m' be a second integer satisfying the conditions (6); the case when $m'=m$ is not excluded. Further let

$$z = A(m', n)y$$

so that also

$$z = A(m', n)A(m, n)x.$$

The definition of z implies that

$$\Phi(z \mid t_h) = \Phi(y \mid t_h^{m'}) \qquad (h = 1, 2, \cdots, n).$$

Now, as we saw above, we can write

$$t_h^{m'} = t_{k(h)}$$

where

$$\begin{pmatrix} 1 & 2 \cdots n \\ k(1) & k(2) \cdots k(n) \end{pmatrix}$$

is a certain permutation. Therefore

$$\Phi(z \mid t_h) = \Phi(y \mid t_h^{m'}) = \Phi(y \mid t_{k(h)}) = \Phi(x \mid t_{k(h)}^m)$$

and finally

$$\Phi(z \mid t_h) = \Phi(x \mid t_h^{m'm}) \qquad (h = 1, 2, \cdots, n).$$

By the hypothesis, mm' is odd and prime to n, hence also prime to $2n$. Hence there exists a unique integer μ such that

$$\mu \equiv m'm \pmod{2n}, \qquad 1 \leq |\mu| \leq n-1$$

and therefore also

$$(\mu, n) = 1, \qquad \mu \text{ is odd.}$$

The congruence for μ implies in particular that

$$t_h^{m'm} = t_h^{\mu} \qquad (h = 1, 2, \cdots, n).$$

It follows then that

$$\Phi(z \mid t_h) = \Phi(x \mid t_h^{\mu}) \qquad (h = 1, 2, \cdots, n).$$

These equations show, however, that necessarily

$$z = A(\mu, n)x$$

and we obtain the final result that

$$A(m', n)A(m, n) = A(\mu, n).$$

The following theorem has thus been proved.

THEOREM. *The $\phi(2n)$ matrices $A(m, n)$, where*

$$(m, 2n) = 1, \qquad 1 \leq |m| \leq n-1,$$

form under multiplication an Abelian group which is isomorphic to the group of primitive residue classes (mod $2n$). *The isomorphism is defined by*

$$A(m, n) \leftrightarrow \{m \pmod{2n}\}.$$

MANCHESTER UNIVERSITY, MANCHESTER, ENGLAND