	g	g^2	g^3	g^4	$\cdots$	g^n
g^{-1}	e	g	g^2	g^3	$\cdots$	g^{n-1}
g^{-2}	g^{n-1}	e	g	g^2	$\cdots$	g^{n-2}
g^{-3}	g^{n-2}	g^{n-1}	e	g	$\cdots$	g^{n-3}
g^{-4}	g^{n-3}	g^{n-2}	g^{n-1}	e	$\cdots$	g^{n-4}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g^{-n}	g	g^2	g^3	g^4	$\cdots$	e

Table 1. Multiplication table for a cyclic group of order n

PRODUCT OF CIRCULANT MATRICES and the Initial Introduction of Group Matrices

Roger Chalkley, December 26, 2014

Because the objects termed *group matrices* in various publications are the objects whose determinants Richard Dedekind in (click here, pages 423-425) and Georg Frobenius in (click here, page 1343) termed group determinants, the concept of a group matrix can be traced back to Richard Dedekind and, somewhat later, Georg Frobenius. However, a useful notation for group matrices like that of **Definition 1** occurred much later when we wrote (click here) in 1976. The use there of representation theory in reverse to derive diagonalization properties of group matrices for any finite abelian group was then extended and completed in (click here). Next, we shall motivate **Definition 1** by employing the special case of it applied to circulant matrices.

Theorem 1. *Suppose that A and B are $n \times n$ circulant matrices having components in a ring R. Then, the matrix product of A and B is a circulant matrix and, when R is a commutative ring, $BA = AB$.*

Proof. Let g be a generator for a cyclic group G of order n. Then, with e as the unit element of G and $g^n = e$, Figure 1 provides a multiplication table for the elements of G. Consequently, there is a function α: $G \to R$ such that the $(i,\, j)$-component of A is given by

$$[A]_{i,j} = \alpha\big(g^{-i} g^j\big), \quad \text{for } i,\, j = 1,\, 2,\, \ldots,\, n \tag{1}$$

and there is a function β: $G \to R$ such that the $(i,\, j)$-component of B is given by

$$[B]_{i,j} = \beta\big(g^{-i} g^j\big), \quad \text{for } i,\, j = 1,\, 2,\, \ldots,\, n. \tag{2}$$

Let γ denote the function γ: $G \to R$ defined for each x in G by

$$\gamma(x) = \sum_{r=1}^{n} \alpha\big(g^{-r}\big)\beta\big(g^r x\big). \tag{3}$$

For any fixed integers i and j, the elements g^r of G for $1 \le r \le n$ are also given by means of g^{i-k}, for $1 \le k \le n$ and by g^{k-j}, for $1 \le k \le n$. Hence, (3) yields

$$\gamma(x) = \sum_{k=1}^{n} \alpha\big(g^{k-i}\big)\beta\big(g^{i-k} x\big) = \sum_{k=1}^{n} \alpha\big(g^{j-k}\big)\beta\big(g^{k-j} x\big), \quad \text{for each } x \text{ in } G. \tag{4}$$

We use (1), (2), and (4) to see that the $(i,\, j)$-component of AB is given by

$$(5)\qquad \begin{aligned} [AB]_{i,j} &= \sum_{k=1}^{n} [A]_{i,k}[B]_{k,j} = \sum_{k=1}^{n} \alpha\big(g^{k-i}\big)\beta\big(g^{j-k}\big) \\ &= \sum_{k=1}^{n} \alpha\big(g^{k-i}\big)\beta\big(g^{i-k}(g^{-i}g^{j})\big) = \gamma\big(g^{-i}g^{j}\big), \end{aligned}$$

for $i,\, j = 1,\, 2,\, \dots,\, n$. Hence, AB is a circulant matrix.

Suppose that the ring R is commutative. Then, for $i, j = 1,\, 2,\, \dots,\, n$, we use (2), (1), (4), and (5) to obtain

$$\begin{aligned} [BA]_{i,j} &= \sum_{k=1}^{n} [B]_{i,k}[A]_{k,j} = \sum_{k=1}^{n} \beta\big(g^{k-i}\big)\alpha\big(g^{j-k}\big) \\ &= \sum_{k=1}^{n} \alpha\big(g^{j-k}\big)\beta\big(g^{k-j}(g^{-i}g^{j})\big) \\ &= \gamma\big(g^{-i}g^{j}\big) = [AB]_{i,j}. \end{aligned}$$

Thus, we have $BA = AB$. This completes the proof. □

Definition 1. *Let A be an $n \times n$ matrix having components in a set S and let G be a group of order n for which its n elements are denoted by $g_1,\, g_2,\, \dots,\, g_n$. Then, A is a group matrix for G and the ordering $g_1,\, g_2,\, \dots,\, g_n$ of its elements if and only if there is a function $\sigma\colon G \to S$ such that the $(i,\, j)$-component of A is given by*

$$(6)\qquad [A]_{i,j} = \sigma\big(g_i^{-1}g_j\big), \quad \text{for } i,\, j = 1,\, 2,\, \dots,\, n.$$

To illustrate how various algebraic properties of circulant matrices can be transferred directly to group matrix, we supply a proof for the following result.

Theorem 2. Suppose that $n \times n$ matrices A and B with components in a ring R are both group matrices for a group G relative to a designation of its elements by $g_1,\, g_2,\, \dots,\, g_n$. Then, the matrix product AB is a group matrix of that same kind. Moreover, when R is a commutative ring and G is abelian, $BA = AB$.

Proof. There is a function $\alpha\colon G \to R$ such that the $(i,\, j)$-component of A is given by

$$(7)\qquad [A]_{i,j} = \alpha\big(g_1^{-1}g_j\big), \quad \text{for } i,\, j = 1,\, 2,\, \dots,\, n$$

and there is a function $\beta\colon G \to R$ such that the $(i,\, j)$-component of B is given by

$$(8)\qquad [B]_{i,j} = \beta\big(g_i^{-1}g_j\big), \quad \text{for } i,\, j = 1,\, 2,\, \dots,\, n.$$

Let γ denote the function $\gamma\colon G \to R$ defined for each x in G by

$$(9)\qquad \gamma(x) = \sum_{r=1}^{n} \alpha\big(g_r^{-1}\big)\beta\big(g_r x\big).$$

For any fixed integers i and j, the elements g_r of G for $1 \le r \le n$ are also given by means of $g_k^{-1}g_i$, for $1 \le k \le n$ and by g^{k-j}, for $1 \le k \le n$. Hence, (9) yields

$$(10)\qquad \gamma(x) = \sum_{k=1}^{n} \alpha\big(g_i^{-1}g_k\big)\beta\big(g_k^{-1}g_j x\big) = \sum_{k=1}^{n} \alpha\big(g^{j-k}\big)\beta\big(g^{k-j}x\big), \quad \text{for each } x \text{ in } G.$$

We use (7), (8), and (10) to see that the $(i,\, j)$-component of AB is given by

$$
\begin{aligned}
[AB]_{i,j} &= \sum_{k=1}^{n} [A]_{i,k}[B]_{k,j} = \sum_{k=1}^{n} \alpha\big(g_i^{-1} g_k\big)\beta\big(g_k^{-1} g_j\big) \\
&= \sum_{k=1}^{n} \alpha\Big(\big(g_k^{-1} g_i\big)^{-1}\Big)\beta\Big(\big(g_k^{-1} g_i\big)\big(g_i^{-1} g_j\big)\Big) = \gamma\big(g_i^{-1} g_j\big),
\end{aligned} \tag{11}
$$

for $i,\, j = 1,\, 2,\, \ldots,\, n$. Hence, AB is a group matrix of that same type.

Suppose that the ring R is commutative and G is abelian. Then, for $i, j = 1,\, 2,\, \ldots,\, n$, we use (8), (7), (10), and (11) to obtain

$$
\begin{aligned}
[BA]_{i,j} &= \sum_{k=1}^{n} [B]_{i,k}[A]_{k,j} = \sum_{k=1}^{n} \beta\big(g_i^{-1} g_k\big)\alpha\big(g_k^{-1} g_j\big) \\
&= \sum_{k=1}^{n} \alpha\Big(\big(g_j^{-1} g_k\big)^{-1}\Big)\beta\Big(\big(g_j^{-1} g_k\big)\big(g_i^{-1} g_j\big)\Big) \\
&= \gamma\big(g^{-i} g^{j}\big) = [AB]_{i,j}.
\end{aligned}
$$

Thus, we have $BA = AB$. This completes the proof. $\square$

Definition 1 is closely related to the following formulation.

Definition 2. Let A be an $n \times n$ matrix having components in a set S and let G be a group of order n for which its n elements are denoted by $h_1,\, h_2,\, \ldots,\, h_n$. Then, A is a group matrix for G and the ordering $h_1,\, h_2,\, \ldots,\, h_n$ of its elements if and only if there is a function $\tau\colon\, G \to S$ such that the $(i,\, j)$-component of A is given by

$$
[A]_{i,j} = \tau\big(h_i h_j^{-1}\big), \quad \text{for } i,\, j = 1,\, 2,\, \ldots,\, n. \tag{12}
$$

In fact, when $h_i = g_i^{-1}$, for $i = 1,\, 2,\, \ldots,\, n$, we see that an $n \times n$ matrix A is a group matrix for G and the ordering $g_1,\, g_2,\, \ldots,\, g_n$ of its elements according to **Definition 1** if and only if A is a grup matrix for G and the ordering $h_1,\, h_2,\, \ldots,\, h_n$ according to **Definition 2**.