# THE ALGEBRAIC THEORY OF DIABOLIC MAGIC SQUARES

By Barkley Rosser and R. J. Walker

1. **Introduction.** For many centuries magic squares have attracted the attention of people interested in mathematics. However, no general theory of magic squares has ever been developed, principally because such a theory would have to involve partition problems of a peculiarly difficult character. If one relaxes the condition that the elements of the square shall be the first $n^2$ positive integers, the study of magic squares becomes a purely algebraical problem involving linear equations in $n^2$ variables. For diabolic magic squares, in which all diagonals have the same sum, the group of transformations which leave the algebraic conditions unchanged is much larger than it is for ordinary magic squares, in which only the two main diagonals have this sum, and the resulting theory is more interesting. Hence we have confined our attention to diabolic squares and their generalizations.

In the first part of the paper the general algebraic theory of diabolic squares is considered. A group of transformations which carries any diabolic square of order $n$ into a diabolic square is constructed; for $n$ a prime $\geqq 7$ it is shown that this is the largest group carrying the most general diabolic square into a diabolic square. The latter result is proved by obtaining, for a square of prime order, the general solution of the $4n$ linear equations which the elements of the square must satisfy.

The latter part of the paper is concerned with the applications of these results to squares whose elements are the integers $1, \cdots, n^2$. The principal result here is that there are precisely 28,800 diabolic squares of order 5, all of an easily constructed type which we have called regular. The existence or non-existence of regular and irregular diabolic squares is demonstrated for squares of all orders.

2. **Some definitions.** By a *square* of order $n$, $S_n$, we shall mean a square matrix of order $n$ whose elements are members of any field $K$ of characteristic prime to $n$. The elements of $S_n$ shall be denoted by $A_{ij}$ or by $A(i, j)$, $i$ denoting the row and $j$ the column, and whenever $i$ or $j$ is not in the range 1 to $n$ inclusive, we shall understand that it is to be reduced to its least positive residue modulo $n$. The square whose elements are $A_{ij}$ shall often be designated by $A$.

A *configuration* in $S_n$ is any linear combination of elements

$$\sum_{x=1}^{r} \alpha_x A(i_x, j_x),$$

the $\alpha_x$ being members of $K$. $S_n$ is said to *admit* the configuration if

$$\sum_{x=1}^{r} \alpha_x A(i + i_x, j + j_x) = N \sum \alpha_x$$

Received November 2, 1938; in revised form, September 25, 1939.