DISTRIBUTION OF MATRICES IN A FINITE FIELD

L. CARLITZ AND JOHN H. HODGES

1. Introduction and notation. This paper is mainly concerned with the distribution with respect to characteristic polynomial and factors of the characteristic polynomial, of square matrices with elements in a finite field $GF(q)$. The method employed is to investigate the properties of the polynomials in question, that is, the matric problems are reduced to problems concerning polynomials. In this connection see a recent paper by Walker [5] on Fermat's theorem for algebras; incidentally Walker's Theorem 3 had been proved earlier in [1; § 7].

The properties of matrices assumed here may be found in [4]. German capitals $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \cdots$ will denote square matrices with elements in $GF(q)$. Polynomials in an indeterminate x with coefficients in $GF(q)$ will be denoted by $F(x), M(x), \cdots$ in § 2 and simply by $F, M, \cdots$ elsewhere.

The number of partitions of the positive integer m into at most r parts will be denoted by $\pi_r(m)$, with $\pi_m(m)=\pi(m)$, the number of unrestricted partitions of m. The symbol $\pi'_r(m)$ will denote the *weighted* partition into at most r parts:

$$\pi'_r(m)=\sum_{k_1+2k_2+\cdots+rk_r=m} q^{k_1+k_2+\cdots+k_r}\ , \tag{1.1}$$

with $\pi'_m(m)=\pi'(m)$, the unrestricted weighted partition.

In Theorem 1 below the number of non-derogatory matrices of order m is given in terms of the Euler ϕ-function for $GF[q, x]$.

If $F=F(x)$ is a polynomial of degree m and $F=P_1^{r_1}\cdots P_s^{r_s}$, where the P_i are distinct irreducible polynomials, we find (Theorem 2) that the number of *classes* of similar matrices of order m with characteristic polynomial $F(x)$ is

$$C_m(F)=\pi(r_1)\cdots\pi(r_s)\ . \tag{1.2}$$

Theorem 3 determines the total number $N(m)$ of distinct classes of similar matrices of order m as

$$N(m)=\pi'(m)\ , \tag{1.3}$$

where $\pi'(m)$ is defined in (1.1) with $r=m$.

We also find (Theorem 4) the number of distinct classes of similar matrices of order m with minimum polynomial of degree r, where r is a fixed integer $\leqq m$. Finally in § 4 we consider a polynomial problem

Received May 16, 1955.