SCALAR POLYNOMIAL EQUATIONS FOR MATRICES OVER A FINITE FIELD

By John H. Hodges

1. **Introduction and notation.** Let $GF(q)$ denote the finite field of order $q = p^n$. Greek capitals θ, ϕ, $\cdots$ will denote square matrices over $GF(q)$. If $E = E(x)$ is a monic polynomial over $GF(q)$, let $N(E, m)$ be the number of matrices θ of order m such that $E(\theta) = 0$. In this paper, the classical theory of the scalar polynomial equation for matrices over a field is combined with a theorem of L. E. Dickson [1], concerning commutativity of certain matrices over $GF(q)$, to give an explicit formula (Theorem 2) for $N(E, m)$. In §5, we illustrate the formula by considering the case $E(x) = x^e - 1$. Finally, in §6, we treat the even more special case where $E(x) = x^3 - 1$. We remark that the case $E(x) = x^2 - 1$ has been discussed in detail in another note [2].

The author wishes to express his thanks to L. Carlitz, who suggested the inclusion of §5 in this paper and advised in its preparation.

We will need the following well-known formula for the number $g(t, d)$ of non-singular matrices of order $t \geq 1$ over $GF(q^d)$:

$$g(t, d) = q^{dt^2} \prod_{i=1}^{t} (1 - q^{-di}) = \prod_{i=0}^{t-1} (q^{dt} - q^{di}). \tag{1.1}$$

We also define $g(0, d) = 1$.

2. **The number** $N(E, m)$. Let $E = E(x)$ be a monic polynomial over $GF(q)$ and suppose that

$$E = P_1^{h_1} P_2^{h_2} \cdots P_s^{h_s}, \tag{2.1}$$

where the P_i are distinct monic prime polynomials, $h_i \geq 1$ and $\deg P_i = d_i$ for $i = 1, 2, \cdots, s$. If θ is a matrix of order m such that $E(\theta) = 0$, since the minimum polynomial of θ must divide E, the elementary divisors of $xI - \theta$ are of the form $P_i^{n_i}$ with $1 \leq n_i \leq h_i$. Suppose that $xI - \theta$ has elementary divisors as follows:

$$k_{ij} \text{ elementary divisors of the form } P_i^j, \tag{2.2}$$

where $i = 1, 2, \cdots, s$ and for fixed i, $1 \leq j \leq h_i$ and $k_{ij} \geq 0$ for all i, j. Since the characteristic polynomial $F = F(x)$ of θ is of degree m and is the product of these elementary divisors, corresponding to θ we have a partition $\pi = \pi(m)$ defined by the formula

$$\pi(m)\colon m = \sum_{i=1}^{s} d_i \sum_{j=1}^{h_i} j \cdot k_{ij}, \qquad k_{ij} \geq 0. \tag{2.3}$$

Received July 1, 1957; in revised form, February 10, 1958. The research for this paper was supported by a National Science Foundation Research Grant, G-2990.