LINEAR AND QUADRATIC EQUATIONS IN A GALOIS FIELD WITH APPLICATIONS TO GEOMETRY

By Eckford Cohen

1. Introduction. Let F denote a Galois field of order q and *odd* characteristic p, and let a, b, a_i, b_i $(i = 1, \cdots, t)$ denote elements of F such that $a_1 \cdots a_t \neq 0$ and such that exactly s of the elements b_i are $\neq 0$ where $1 \leq s \leq t$. In this paper we wish to find the number $N_{s,t}(a, b)$ of common solutions in F of the equations,

$$\begin{cases} a = a_1x_1^2 + \cdots + a_tx_t^2 \\ b = b_1x_1 + \cdots + b_tx_t \, . \end{cases} \tag{1.1}$$

This problem was considered in the special case $s = t$ in [3] where explicit formulas for $N_{t,t}(a, b)$ were found. The method of that paper made lavish use of Gaussian sums. In the present paper we again make use of exponential sums, but only quite sparingly. More precisely, we require only two formal properties of Gaussian sums in F (see Remark 2, §2) and these are used merely to reduce the problem of the paper to the special cases for which $s \leq 3$. These cases are treated by arithmetical methods in §3, and a complete and explicit evaluation of $N_{s,t}(a, b)$ is obtained in Theorem 2. The only additional tool needed is the Jordan–Dickson formula for the number of solutions of a quadratic equation in F.

In §4 we apply the results of the preceding section to the following geometrical questions: (a) determination of the number of hyperplanes contained in the complement of a quadric in an affine space based on F, (b) establishment of criteria for a quadric to meet a hyperplane in a projective space with F as base field, (c) characterization of the "sum-altering" affine transformations on the set of vectors for which a given quadratic form assumes a fixed value of F.

2. Trigonometric sums and reduction of the problem. For an element a of F place

$$t(a) = a + a^p + \cdots + a^{p^r - 1}, \qquad q = p^r,$$

and define $e(a) = \exp\,(2\pi i t(a)/p)$. The function $e(a)$ is an additive character of F into the multiplicative group of the complex field. For arbitrary a, b in F put

$$S(a, b) = \sum_{x \in F} e(ax^2 + 2bx),$$

Received May 13, 1964. This research was supported in part by the National Science Foundation grant G-19012.