Journal of the Mathematical Society of Japan Vol. 7, No. 3, June, 1955

The number of solutions of some equations in a finite field.

By L. CARLITZ

(Received Dec. 25, 1953)

1. Introduction. The writer [1], [3] has determined the number of solutions of certain types of equations in a finite field. For example, making use of the well-known formulas for the number of solutions of $Q(\xi_1, \cdots, \xi_r)=\alpha$, where Q denotes a quadratic form with coefficients in $GF(q)$, q odd, such equations as

$$(1.1) \qquad Q(\xi_1, \cdots, \xi_r)=\eta_1^{e_1} \cdots \eta_s^{e_s}$$

and

$$(1.2) \qquad Q(\xi_1, \cdots, \xi_{2r})=f(\eta_1, \cdots, \eta_s),$$

where $f(\eta)$ donotes a polynomial that never vanishes, are readily handled. R. G. Pohrer [6] has found the number of solutions for a great many equations of this and other kinds.[1)]

In the present note we consider a few additional types. In general, when a quadratic form $Q(\xi_1, \cdots, \xi_r)$ occurs in an equation, the case r odd is more difficult; this is illustrated for example by (1.2). However for an equation of the type

$$(1.3) \qquad Q(\xi_1, \cdots, \xi_{2r+1})=g(\eta_1, \cdots, \eta_s),$$

it may be possible to find explicit formulas for the number of solutions when the polynomial $g(\eta)$ satisfies certain conditions. A particularly simple case is

$$(1.4) \qquad g(\eta)=\prod_{i=1}^{s}(\eta_i^2+\beta_i\eta_i+\gamma_i);$$

1) To find the number of solutions of such simultaneous equations in a finite field is also of interest in connection with the algebraic geometry, as was pointed out by A. Weil: Bull. Amer. Math. Soc. 55 (1949) pp. 497-508.