LINEAR FORMS AND POLYNOMIALS IN A GALOIS FIELD

By L. CARLITZ

1. Introduction. Let t_1, u_0, u_1, \cdots be indeterminates over the Galois field $GF(p^n)$, and put

$$(1.1) \quad f_m(t) = f_m(t; u_0, \ldots, u_{m-1}) = \prod_{(c)} (t + c_0 u_0 + \ldots + c_{m-1} u_{m-1}),$$

the product extending over all sets (c_0, \dots, c_{m-1}) in $GF(p^n)$. Then by a formula due to E. H. Moore¹ we may express $f_m(t)$ as the quotient of two determinants:

(1.2)
$$f_m(t; u_0, \ldots, u_{m-1}) = \frac{D(u_0, \ldots, u_{m-1}, t)}{D(u_0, \ldots, u_{m-1})},$$

where

(1.3)
$$D_m = D(u_0, \ldots, u_m) = \begin{vmatrix} u_0 & u_0^{p^n} & \cdots & u_0^{p^{n_m}} \\ \cdots & \cdots & \cdots & \cdots \\ u_m & u_m^{p^n} & \cdots & u_m^{p^{n_m}} \end{vmatrix},$$

and $D(u_0, \dots, u_{m-1}, t)$ is defined by taking $u_m = t$. In the special case²

(1.4)
$$u_i = x^i$$
 $(i = 0, 1, 2, \cdots),$

where x is an indeterminate, the linear form

$$c_0 u_0 + c_1 u_1 + \cdots + c_{m-1} u_{m-1}$$
 $(c_j \text{ in } GF(p^n))$

reduces to $c_0 + c_1 x + \cdots + c_{m-1} x^{m-1}$, the general polynomial of degree < m, and $f_m(t)$ reduces to $\psi_m(t)$. We shall refer to (1.4) as the P-case. The chief object of the present paper is to extend certain properties of $\psi_m(t)$ to the more general $f_m(t)$. In particular we define an operator Ω^i for which

$$g(tw) = \sum \Omega^{i}g(w)f_{i}(t),$$

where g(t) is an arbitrary linear³ polynomial in t. Applications are made to the evaluation of certain power sums. The inverse of $f_m(t)$ and certain limiting cases are discussed briefly. Finally we define a polynomial $G_k(t)$ of degree k that reduces to $f_m(t)$ for $k = p^{nm}$.

Received May 8, 1940.

¹ Bulletin of the American Mathematical Society, vol. 2(1896), pp. 189-195. See also O. Ore, Transactions of the American Mathematical Society, vol. 35(1933), pp. 559-584; L. E. Dickson, Trans. Amer. Math. Soc., vol. 12(1911), p. 75.

² This Journal, vol. 1(1935), pp. 137-168. Cited as I.

³ That is, of the form $\sum \beta_i t^{p^{n_i}}$.