ON POLYNOMIALS IN A GALOIS FIELD*

BY LEONARD CARLITZ†

1. *Introduction.* Let p be an arbitrary prime, n an integer $\geqq 1$, $GF(p^n)$ the Galois field of order p^n; let $\mathfrak{D}(x, p^n)$ denote the totality of *primary* polynomials in the indeterminate x, with coefficients in $GF(p^n)$, that is, of polynomials such that the coefficient of the highest power of x is unity. In this note we give a number of miscellaneous results concerning the elements of $\mathfrak{D}$. The results are of two kinds. The first involve generalizations of certain formulas treated by the writer in another paper.‡ Thus if we let $\tau^{(\alpha)}(E)$ denote the number of divisors of E of degree α, then, for $\alpha \leqq \beta$ and $\alpha+\beta \leqq \nu$, ν the degree of E (we may evidently assume without any loss in generality that $\alpha, \beta \leqq \nu/2$),

$$(1) \qquad \sum \tau^{(\alpha)}(E)\tau^{(\beta)}(E) = (\alpha + 1)p^{n\nu} - \alpha p^{n(\nu-1)},$$

the summation on the left being taken over all polynomials E of degree ν. The other results of this kind involve generalized totient functions, as defined in §4.

The second group of formulas are of a different nature. Let us write p_0 for p^n, and define

$$F_\rho(\nu) = \prod_{\alpha=1}^{\nu}(x^{p_0^\alpha} - x)^{p_0^{\rho(\nu-\alpha)}}, F(\nu) = F_1(\nu).$$

Then we show that the least common multiple of the polynomials of degree ν is

$$(2) \qquad L(\nu) = F_0(\nu);$$

the product of all the polynomials of degree ν is

$$(3) \qquad \prod_{\deg E=\nu} E = F(\nu) = F_1(\nu);$$

if $Q_\rho(\nu)$ denote the product of those polynomials of degree ν that

* Presented to the Society, August 31, 1932.

† International Research Fellow.

‡ *The arithmetic of polynomials in a Galois field,* American Journal of Mathematics, vol. 54 (1932), pp. 39–50. Cited as A.P.