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 $\alpha, \beta \leqq \nu/2$),

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

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

$$L(\nu) = F_0(\nu); \tag{2}$$

the product of all the polynomials of degree ν is

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

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.

are not divisible by the ρth power of any polynomial (except 1), then

$$(4)\qquad Q_\rho(h\rho + k) = \frac{F(h\rho + k)}{F^{p_0}(h\rho - \rho + k)}\left\{\frac{F_\rho^{p_0}(h-1)}{F_\rho(h)}\right\}^{\rho p_0^k},$$

where it is assumed that $0 \leqq k < \rho$.

2. *Notation.* Polynomials will be denoted by large italic letters, ordinary integers by small Greek and italic letters. We write deg E for the degree of the polynomial E;

$$|E| = p^{n\nu} = p_0^\nu,$$

where $\nu = \deg E$. If s is a real quantity > 1, then

$$\zeta(s) = \sum_E |E|^{-s},$$

summed over all E in $\mathfrak{D}$, is the zeta-function of $\mathfrak{D}$; and it is immediately verified that

$$(5)\qquad \zeta(s) = (1 - p_0^{1-s})^{-1}, \qquad p_0 = p^n.$$

3. *The τ-Functions.* We define

$$\sigma_t(E) = \sum_{A|E} |A|^t,$$

the summation being taken over all the divisors of E. Then we may verify without any difficulty the following $\mathfrak{D}$ analog of a well known Ramanujan identity:*

$$(6)\qquad \sum_E \frac{\sigma_t(E)\sigma_u(E)}{|E|^s} = \frac{\zeta(s)\zeta(s-t)\zeta(s-u)\zeta(s-t-u)}{\zeta(2s-t-u)}.$$

Now it is evident from the definition of $\tau^{(\alpha)}(E)$ and $\sigma_t(E)$ that

$$\sigma_t(E) = \sum_\alpha \tau^{(\alpha)}(E)p_0^{\alpha t}$$

so that the left member of (1) is the coefficient of $p_0^{\alpha t+\beta u-\nu s}$ in the right member of (6). But, using (5), the product of zetas in (6) is equal to

---

* Messenger of Mathematics, vol. 45 (1916), pp. 81–84, or Collected Papers, 1927, pp. 133–135, formula (15).

$$(7)\qquad \frac{1 - p_0^{1+t+u-2s}}{(1 - p_0^{1-s})(1 - p_0^{1+t-s})(1 - p_0^{1+u-s})(1 - p_0^{1+t+u-s})}.$$

To determine the coefficient in question, we note first that, for $t, u < 0, s > 1$,

$$\frac{1}{(1 - p_0^{1+t-s})(1 - p_0^{1+u-s})(1 - p_0^{1+t+u-s})} = \sum_{\alpha,\beta,\nu} p_0^{\alpha t+\beta u+\nu-\nu s},$$

where the sum on the right is extended over all $\alpha, \beta, \nu \geqq 0$, such that $\alpha, \beta \leqq \nu$, $\alpha+\beta \geqq \nu$. Then the denominator in (7) is

$$\sum_{\nu \geqq \alpha+\beta} \min\,(\alpha + 1, \beta + 1) p_0^{\alpha t+\beta u+\nu-\nu s} + \sum_{\nu < \alpha+\beta};$$

clearly the second sum contributes nothing to the coefficient of $p_0^{\alpha t+\beta u-\nu s}$ in (7) when $\nu \geqq \alpha+\beta$, and so may be ignored. The coefficient in question is therefore

$$\begin{cases} (\gamma + 1)p_0^{\nu} - \gamma p_0^{\nu-1} & \text{for } \nu \geqq 2, \\ (\gamma + 1)p_0^{\nu} & \text{for } \nu < 2, \end{cases}$$

where $\gamma = \min\,(\alpha, \beta)$, thus completing the proof of (1).

By means of the Ramanujan identity (6) we may evidently evaluate

$$(8)\qquad \sum_{\deg E=\nu} \sigma_t(F)\sigma_u(F),$$

but for general t, u, the result is rather complicated. For certain special values of t, u, the sum in (8) is fairly simple. Thus, for $u = 2t$, it may be verified that

$$(9)\qquad \sum_{\deg E=\nu} \sigma_t(E)\sigma_{2t}(E) = p_0^{\nu}\begin{bmatrix} \nu + 3 \\ 3 \end{bmatrix} - p_0^{\nu-1+3t}\begin{bmatrix} \nu + 1 \\ 3 \end{bmatrix},$$

where

$$\begin{bmatrix} \nu + 3 \\ 3 \end{bmatrix} = \frac{(p_0^{(\nu+3)t} - 1)(p_0^{(\nu+2)t} - 1)(p_0^{(\nu+1)t} - 1)}{(p_0^{3t} - 1)(p_0^{2t} - 1)(p_0^{t} - 1)}.$$

Again, for $s = t = 0$, if we put

$$\sigma_0(E) = \tau(E) = \sum_{A|E} 1 = \sum_{\alpha} \tau^{(\alpha)}(E).$$

then it is obvious that (7) implies

$$\sum_{\deg E=\nu} \tau^2(E) = p^\nu \begin{bmatrix} \nu+3 \\ 3 \end{bmatrix} - p^{\nu-1} \begin{bmatrix} \nu+1 \\ 3 \end{bmatrix},$$

which is indeed a particular case of (9).

4. *Totient Functions.* Let $\phi(M; \alpha_1, \cdots, \alpha_k)$ denote the number of sets of (ordered) polynomials $A_1, \cdots, A_k$, such that

$$\deg A_i = \alpha_i, \qquad (A_1, \cdots, A_k, M) = 1.$$

Using this definition, we have evidently

$$\text{(10)} \qquad \begin{aligned} &\sum_{(A_1, \cdots, A_k, M)=1} |A_1|^{-s_1} \cdots |A_k|^{-s_k} \\ &= \sum_{\alpha_i=0}^{\infty} \phi(M; \alpha_1, \cdots, \alpha_k) p_0^{-\alpha_1 s_1 - \cdots - \alpha_k s_k}, \end{aligned}$$

where the s_i are real and each >1. By means of this identity it is easy to express the general ϕ-function in simple terms. Let $f(s)$ denote the left member of (10); then since

$$\begin{aligned} &\sum_{\text{all} A_i} |A_1|^{-s_1} \cdots |A_k|^{-s_k} \\ &= \prod_{P|M} \{1 + |P|^{-(s_1+\cdots+s_k)}\}^{-1} \sum_{(A_1, \cdots, A_k, M)=1} |A_1|^{-s_1} \cdots |A_k|^{-s_k} \end{aligned}$$

it follows that

$$f(s) = \zeta(s_1) \cdots \zeta(s_k) \prod_{P|M} \{1 - |P|^{-(s_1+\cdots+s_k)}\},$$

where P runs through the irreducible divisors of M. Therefore, by (10) and (5),

$$\text{(11)} \qquad \phi(M; \alpha_1, \cdots, \alpha_k) = p_0^{\alpha_1+\cdots+\alpha_k} \sum_{A|M}{}' \mu(A) |A|^{-k},\text{*}$$

the sum being taken over A, dividing M, and of degree $\leqq$ min $(\alpha_1, \cdots, \alpha_k)$. If all the quadratfrei divisors of M satisfy this condition, (11) may be written in the form

$$\text{(11)}' \qquad \phi(M; \alpha_1, \cdots, \alpha_k) = p_0^{\alpha_1+\cdots+\alpha_k} \prod_{P|M} (1 - |P|^{-k}).$$

In particular, let $\alpha_1 = \cdots = \alpha_k = \nu$, the degree of M. We now write $\phi_k(M)$ in place of $\phi(M; \nu, \cdots, \nu)$, and (11) becomes

* $\mu(A)$ is the Möbius μ-function for $\mathfrak{D}$; see A.P., §4.

$$(12)\quad \phi_k(M) = |M|^k \prod_{P|M}(1 - |P|^{-k}) = \sum_{M=AB} \mu(A)|B|^k$$

(where now all the terms in both sum and product are included). It is clear either from the definition or from (12) that $\phi_k(M)$ is the $\mathfrak{D}$-analog of the Jordan ϕ-function of higher order.

5. *Sets of Relatively Prime Polynomials.* Let $\psi(\alpha_1, \cdots, \alpha_k)$ denote the number of sets of (ordered) polynomials $A_1, \cdots, A_k$, such that $\deg A_i = \alpha_i$, $(A_1, \cdots, A_k) = 1$. Then, clearly,

$$\sum_{\alpha_i=0}^{\infty} \psi(\alpha_1, \cdots, \alpha_k) p_0^{-(\alpha_1 s_1 + \cdots + \alpha_k s_k)} = \sum_{(A_1, \cdots, A_k)=1} |A_1|^{-s_1} \cdots |A_k|^{-s_k}$$

$$= \frac{\zeta(s_1) \cdots \zeta(s_k)}{\zeta(s_1 + \cdots + s_k)} = \frac{1 - p_0^{1-(s_1+\cdots+s_k)}}{(1 - p_0^{1-s_1}) \cdots (1 - p_0^{1-s_k})};$$

and therefore

$$(13)\ \psi(\alpha_1, \cdots, \alpha_k) = \begin{cases} p_0^{\alpha_1+\cdots+\alpha_k}(1 - p_0^{1-k}) & \text{for } \alpha_1 \cdots \alpha_k \neq 0, \\ p_0^{\alpha_1+\cdots+\alpha_k} & \text{otherwise.} \end{cases}$$

As might be expected, the ϕ and ψ functions are closely related. Indeed, from the definition, $\psi(\alpha_1, \cdots, \alpha_k, \nu)$ is the number of sets of polynomials $A_1, \cdots, A_k, M$, such that

$$\deg A_i = \alpha_i,\ \deg M = \nu,\ (A_1, \cdots, A_k, M) = 1;$$

and therefore

$$(14)\qquad \psi(\alpha_1, \cdots, \alpha_k, \nu) = \sum_{\deg M=\nu} \phi(M; \alpha_1, \cdots, \alpha_k).$$

From (13) and (14) we have

$$(15)\qquad \sum_{\deg M=\nu} \phi(M; \alpha_1, \cdots, \alpha_k) = \begin{cases} p_0^{\alpha_1+\cdots+\alpha_k+\nu}(1 - p_0^{-k}) \\ \qquad \text{for } \alpha_1 \cdots \alpha_k \nu \neq 0, \\ p_0^{\alpha_1+\cdots+\alpha_k+\nu} \text{ otherwise.} \end{cases}$$

In particular, if $\alpha_1 = \cdots = \alpha_k = \nu$, we get for the ϕ-function in (12)

$$\sum_{\deg M=\nu} \phi_k(M) = \begin{cases} p_0^{(k+1)\nu} - p_0^{k(\nu-1)+\nu} & \text{for } \nu > 0, \\ 1 & \text{for } \nu = 0. \end{cases}$$

6. *A Modification of the ϕ-Functions.* Let us now denote by

$\phi'(M; \alpha_1, \cdots, \alpha_k)$ the number of sets of *quadratfrei* polynomials $A_1, \cdots, A_k$, such that $\deg A_i = \alpha_i$, $(A_1, \cdots, A_k, M) = 1$. Then, as in §4, we show that

$$\sum \phi'(M; \alpha_1, \cdots, \alpha_k) p_0^{-(\alpha_1 s_1 + \cdots + \alpha_k s_k)} = \sum{}' |A_1|^{-s_1} \cdots |A_k|^{-s_k},$$

the sum on the right being taken over all *quadratfrei* A_i such that $(A_1, \cdots, A_k, M) = 1$; but this sum is equal to

$$\frac{\zeta(s_1) \cdots \zeta(s_k)}{\zeta(2s_1) \cdots \zeta(2s_k)} \prod_{P|M} (1 + |P|^{-(s_1 + \cdots + s_k)})^{-1}.$$

Therefore, if $\lambda(B)$ is the $\mathfrak{D}$-analog of the Liouville λ-function,* and if $q(\nu)$ is defined by the relation†

$$\frac{\zeta(s)}{\zeta(2s)} = \sum_{\nu=0}^{\infty} \frac{q(\nu)}{p_0^{\nu s}},$$

we have in place of (11)

$$(16) \qquad \phi'(M; \alpha_1, \cdots, \alpha_k) = \sum_B \lambda(B) q(\alpha_1 - \beta) \cdots q(\alpha_k - \beta),$$

the sum extending over all B whose irreducible divisors are divisors of M, and such that $\deg B = \beta \leqq \min(\alpha_1, \cdots, \alpha_k)$. As for the function of §5, let us define $\psi'(\alpha_1, \cdots, \alpha_k)$ to be the number of sets of *quadratfrei* polynomials $A_1, \cdots, A_k$, such that $\deg A_i = \alpha_i$, $(A_1, \cdots, A_k) = 1$. Then

$$\sum \frac{\psi'(\alpha_1, \cdots, \alpha_k)}{p_0^{\alpha_1 s_1 + \cdots + \alpha_k s_k}} = \frac{\zeta(s_1) \cdots \zeta(s_k)}{\zeta(2s_1) \cdots \zeta(2s_k)} \frac{\zeta(2s_1 + \cdots + 2s_k)}{\zeta(s_1 + \cdots + s_k)},$$

so that

$$(17) \quad \psi'(\alpha_1, \cdots, \alpha_k) = \sum_\beta (-1)^\beta p_0^{\beta'} q(\alpha_1 - \beta) \cdots q(\alpha_k - \beta),$$

the sum being taken over all β, $0 \leqq \beta \leqq \min(\alpha_1, \cdots, \alpha_k)$; and β' is the greatest integer $\leqq (\beta + 1)/2$.

Now, from the definition of ϕ' and ψ', it is clear that

$$(18) \qquad \psi'(\alpha_1, \cdots, \alpha_k, \nu) = \sum_{\deg M = \nu} \mu^2(M) \phi'(M; \alpha_1, \cdots, \alpha_k),$$

* That is, if $B = P_1^{e_1} P_2^{e_2} \cdots$, $\lambda(B) = (-1)^{e_1 + e_2 + \cdots}$; see A.P., §3.

† It is evident that $q(\nu) = p_0^\nu - p_0^{\nu-1}$ for $\nu \geqq 2$ and that $q(\nu) = p_0^\nu$ otherwise.

and therefore the sum

$$\sum_{\deg M=\nu}{}' \phi'(M; \alpha_1, \cdots, \alpha_k),$$

taken over quadratfrei M only, is equal to the right member of (17).

7. *The L.C.M. of Polynomials of Degree ν.* We recall the well known result that

$$x^{p_0^\nu} - x = \prod_{\alpha | \nu} \Theta(\alpha), \tag{19}$$

where $\Theta(\alpha)$ is the product of the irreducible polynomials of degree α. If now $L(\nu)$ is the L.C.M. of the polynomials of degree ν, it is evident, to begin with, that if P is irreducible of degree δ, then the exponent of the highest power of P dividing $L(\nu)$ is precisely $[\nu/\delta]$, the greatest integer $\leqq \nu/\delta$. Therefore

$$\begin{aligned} L(\nu) &= \prod_{\deg P \leqq \nu} P^{[\nu/\deg P]} \\ &= \prod_{\delta=1}^{\nu} \left\{ \prod_{\deg P=\delta} P \right\}^{[\nu/\delta]} = \prod_{\delta=1}^{\nu} \{\Theta(\delta)\}^{[\nu/\delta]}. \end{aligned} \tag{20}$$

On the other hand, by (19),

$$F_0(\nu) = \prod_{\alpha=1}^{\nu} (x^{p_0^\alpha} - x) = \prod_{\alpha=1}^{\nu} \prod_{\delta | \alpha} \Theta(\delta) = \prod_{\delta=1}^{\nu} \{\Theta(\delta)\}^{[\nu/\delta]}.$$

Comparison with the right member of (20) shows at once that

$$L(\nu) = F_0(\nu). \tag{2}$$

8. *The Product of Polynomials of Degree ν.* Formula (3) may be proved very quickly if we make use of the following theorem due to E. H. Moore:*

If G run through the linear forms $G = \alpha_0 x_0 + \cdots + \alpha_\nu x_\nu$, where the coefficients α_i lie in $GF(p^n)$, and the α_i of lowest subscript $\neq 0$ is taken $=1$, then

$$\prod G = \left| x_i^{p_0^j} \right|, \qquad (i, j = 0, \cdots, \nu). \tag{21}$$

Suppose that in this theorem $x_i = x^{\nu - i}$ $(i = 0, \cdots, \nu)$; then the left hand member of (21) has the value

* This Bulletin, vol. 2 (1896), p. 189.

$$\prod_{\alpha=0}^{\nu} \prod_{\deg E=\alpha} E = \prod_{\alpha=1}^{\nu} \prod_{\deg E=\alpha} E; \tag{22}$$

the right member of (21) is a familiar determinant, and is easily seen to be equal to

$$\prod_{\alpha=0}^{\nu-1}(x^{p_0^{\nu-\alpha}} - x)^{1+p_0+\cdots+p_0^{\alpha}}. \tag{23}$$

Therefore, comparing (22) and (23), we have at once the formula to be proved:

$$\prod_{\deg E=\nu} E = \prod_{\alpha=0}^{\nu-1}(x^{p_0^{\nu-\alpha}} - x)^{p_0^{\alpha}} = F(\nu). \tag{3}$$

9. *The Formula for $Q_\rho(\nu)$*. Since any E may be written in the form $E = GM^\rho$, $P^\rho \dagger G$, it is evident that, for $\nu = h\rho + k$, $0 \leqq k < \rho$,

$$\begin{aligned} F(\nu) &= \prod_{\deg E=\nu} E \\ &= \prod_{\alpha=0}^{h} \left\{ \prod_{\deg G=\nu-\alpha\rho} G^{p_0^{\alpha}} \right\} \left\{ \prod_{\deg M=\alpha} M^{\rho q_\rho(\nu-\alpha\rho)} \right\} \\ &= \prod_{\alpha=0}^{h} Q_\rho^{p_0^{\alpha}}(\nu - \alpha\rho) \cdot \prod_{\alpha=0}^{h} \{F(\alpha)\}^{\rho q_\rho(\nu-\alpha\rho)}, \end{aligned} \tag{24}$$

where $q_\rho(\nu)$ is the number of polynomials E of degree ν such that $P^\rho \dagger E$ for any irreducible P. It is known that*

$$q_\rho(\nu) = \begin{cases} p_0^{\nu} - p_0^{\nu-\rho+1} & \text{for } \nu \geqq \rho, \\ p_0^{\nu} & \text{otherwise}; \end{cases}$$

so that

$$\sum_{\alpha=\beta}^{h} p_0^{\alpha-\beta} q_\rho(\nu - \alpha\rho) = p_0^{\nu-\beta\rho}. \tag{25}$$

Then the product in (24) is equal to

$$\begin{aligned} &\prod_{\alpha=1}^{h} \{F(\alpha)\}^{\rho q_\rho(\nu-\alpha\rho)} \\ &= \prod_{\alpha=1}^{h} \prod_{\beta=1}^{\alpha} (x^{p_0^{\beta}} - x)^{p^{\alpha-\beta} \cdot \rho q_\rho(\nu-\alpha\rho)} \end{aligned}$$

---

* A.P., §6.

$$= \prod_{\beta=1}^{h}(x^{p_0^\beta} - x)^{\rho e_\beta}, \qquad e_\beta = \sum_{\alpha=\beta}^{h} p_0^{\alpha-\beta} q_\rho(\nu - \alpha\rho),$$

$$= \prod_{\beta=1}^{h}(x^{p_0^\beta} - x)^{\rho p_0^{\nu-\beta\rho}} \quad \text{(by (25))}$$

$$(26) \qquad = \left\{ \prod_{\beta=1}^{h}(x^{p_0^\beta} - x)^{p_0^{(h-\beta)\rho}} \right\}^{\rho p_0^k} = F_\rho^{\rho p_0^k}(h^0).$$

By (24) and (26)

$$F(\nu) = \prod_{\alpha=0}^{h} Q_\rho^{p_0^\alpha}(\nu - \alpha\rho) \cdot F_\rho^{\rho p_0^k}(h),$$

or, writing $h-\alpha$ for α,

$$(27) \qquad \begin{aligned} \prod_{\alpha=0}^{h} Q_\rho^{p_0^{h-\alpha}}(\alpha\rho + k) &= F(h\rho + k)F_\rho^{-\rho p_0^k}(h) \\ &= R_\rho(h\rho + k), \text{ say.} \end{aligned}$$

It is now easy to evaluate Q_ρ. Indeed, substituting $h-1$ for h in (27), and raising both members of the resulting equation to the p_0th power, we have

$$\prod_{\alpha=0}^{h-1} Q_\rho^{p_0^{h-\alpha}}(\alpha\rho + k) = R_\rho^{p_0}(\nu - \rho),$$

and therefore

$$(4) \qquad Q_\rho(\nu) = R_\rho(\nu) R_\rho^{-p_0}(\nu - \rho).$$

It will be remarked that by (27) $R_\rho(\nu)$ is a polynomial, so that by (4), $Q_\rho(\nu)$ is expressed as the ratio of two polynomials.

From (27) we may deduce another result of some interest. Since no polynomial of degree $<\rho$ is divisible by the ρth power of an irreducible polynomial, it is evident that

$$Q_\rho(k) = F(k), \qquad (0 \leqq k < \rho):$$

therefore, by (27), the expression

$$F(h\rho + k)F^{-p_0^h}(k)F_\rho^{-\rho p_0^k}(h)$$

is a polynomial provided that $0 \leqq k < \rho$.

CAMBRIDGE, ENGLAND