ON POLYNOMIALS IN A GALOIS FIELD*

BY LEONARD CARLITZ†

1. Introduction. Let $p$ be an arbitrary prime, $n$ an integer $\geq 1$, $GF(p^n)$ the Galois field of order $p^n$; let $\mathcal{D}(x, p^n)$ 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 $\mathcal{D}$. 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 $\alpha$, then, for $\alpha \leq \beta$ and $\alpha + \beta \leq \nu$, $\nu$ the degree of $E$ (we may evidently assume without any loss in generality that $\alpha, \beta \leq \nu/2$),

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

the summation on the left being taken over all polynomials $E$ of degree $\nu$. 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

$$ F_p(\nu) = \prod_{\alpha=1}^{\nu} (x^{p_0^\alpha} - x)^{p_{\nu}(p-\alpha)}, F(\nu) = F_1(\nu). $$

Then we show that the least common multiple of the polynomials of degree $\nu$ is

$$ L(\nu) = F_p(\nu); $$

the product of all the polynomials of degree $\nu$ is

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

if $Q_p(\nu)$ denote the product of those polynomials of degree $\nu$ that

---

* Presented to the Society, August 31, 1932.
† International Research Fellow.
are not divisible by the \( \rho \)th power of any polynomial (except 1), then

\[
Q_k(h^\rho + k) = \frac{F(h^\rho + k)}{F(h^\rho - \rho + k)} \left\{ \frac{F_{\rho^n}(h - 1)}{F_{\rho}(h)} \right\}^{\rho n k},
\]

where it is assumed that \( 0 \leq k < \rho \).

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 \( E \);

\[
|E| = \rho^n \nu,
\]

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

\[
\zeta(s) = \sum_{E} |E|^{-s},
\]

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

\[
\zeta(s) = (1 - \rho_0 s^{-1})^{-1}, \quad \rho_0 = \rho^n.
\]

3. The \( \tau \)-Functions. We define

\[
\sigma_t(E) = \sum_{A \mid E} |A|^t,
\]

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

\[
\sum_{E} \sigma_t(E)\sigma_u(E) |E|^{-s} = \frac{\zeta(s)\zeta(s - t)\zeta(s - u)\zeta(s - t - u)}{\zeta(2s - t - u)}.
\]

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

\[
\sigma_t(E) = \sum_{\alpha} \tau^{(\alpha)}(E) \rho_0^{\alpha t},
\]

so that the left member of (1) is the coefficient of \( \rho_0^{\alpha t + \beta u - \rho s} \) in the right member of (6). But, using (5), the product of zetas in (6) is equal to

---

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

\[
\frac{1 - p_0^{1+t+u-3s}}{(1 - p_0^{1-t-e})(1 - p_0^{1+u-e})(1 - p_0^{1+t+u-e})} = \sum_{a, b, r} p_0^{a+b+u+v-r-s},
\]

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

\[
\sum_{\nu \leq \alpha + \beta} \min (\alpha + 1, \beta + 1) \cdot \sum \frac{p_0^{a+b+u+v-r-s}}{\nu < \alpha + \beta};
\]

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

\[
\begin{cases} 
(\gamma + 1)p_0^s - \gamma p_0^{s-1} & \text{for } \nu \geq 2, \\
(\gamma + 1)p_0^s & \text{for } \nu < 2,
\end{cases}
\]

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

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

\[
\sum_{\deg E = \nu} \sigma_t(F)\sigma_u(F),
\]

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

\[
\sum_{\deg E = \nu} \sigma_t(E)\sigma_{2t}(E) = p_0^s \left[ \frac{\nu + 3}{3} \right] - p_0^{s-1+3t}\left[ \frac{\nu + 1}{3} \right],
\]

where

\[
\left[ \frac{\nu + 3}{3} \right] = \frac{(p_0^{3+3t} - 1)(p_0^{3+2t} - 1)(p_0^{3+t} - 1)}{(p_0^{3t} - 1)(p_0^{3t} - 1)(p_0^{3t} - 1)}.
\]

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

\[
\sigma_0(E) = \tau(E) = \sum_{\Delta \mid E} 1 = \sum_{\alpha} \tau^{(\alpha)}(E).
\]

then it is obvious that (7) implies
\[
\sum_{\deg R = \nu} \tau^3(E) = p^\nu \left[ \frac{\nu + 3}{3} \right] - p^{\nu - 1} \left[ \frac{\nu + 1}{3} \right],
\]
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
\[
\deg A_i = \alpha_i, \quad (A_1, \cdots, A_k, M) = 1.
\]
Using this definition, we have evidently
\[
\sum_{(A_1, \cdots, A_k, M) = 1} \prod_{i=1}^{k} |A_i|^{-\alpha_i} \prod_{j=1}^{k} |A_j|^{-s_j}
\]
(10)
\[
= \sum_{\alpha_1, \cdots, \alpha_k} \phi(M; \alpha_1, \cdots, \alpha_k) p_{\alpha_1^{\alpha_1} \cdots \alpha_k^{\alpha_k}},
\]
where the \( s_i \) are real and each \( > 1 \). By means of this identity it is easy to express the general \( \phi \)-function in simple terms. Let \( f(s) \) denote the left member of (10); then since
\[
\sum_{\alpha_1, \cdots, \alpha_k} \phi(M; \alpha_1, \cdots, \alpha_k) p_{\alpha_1^{\alpha_1} \cdots \alpha_k^{\alpha_k}}
\]
(11)
\[
< \prod_{P \mid M} (1 + |P|^{-s_1+\cdots+s_k}) \prod_{A \mid M} \left( 1 - |A|^{-s_1+\cdots+s_k} \right),
\]
where \( P \) runs through the irreducible divisors of \( M \). Therefore, by (10) and (5),
\[
(11') \quad \phi(M; \alpha_1, \cdots, \alpha_k) = p_{\alpha_1^{\alpha_1} \cdots \alpha_k^{\alpha_k}} \sum_{A \mid M} \mu(A) |A|^{-s_1+\cdots+s_k},
\]
the sum being taken over \( A \), dividing \( M \), and of degree \( \leq \min (\alpha_1, \cdots, \alpha_k) \). If all the quadratfrei divisors of \( M \) satisfy this condition, (11) may be written in the form
\[
(11) \quad \phi(M; \alpha_1, \cdots, \alpha_k) = p_{\alpha_1^{\alpha_1} \cdots \alpha_k^{\alpha_k}} \prod_{P \mid M} \left( 1 - |P|^{-s_1+\cdots+s_k} \right).
\]
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) \text{ is the Möbius \( \mu \)-function for } \mathbb{D}; \text{ see A.P., §4.}
(12) $\phi_k(M) = \left| M \right|^k \prod_{P \mid M} (1 - \left| P \right|^{-k}) = \sum_{M = AB} \mu(A) \left| B \right|^k$

(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 $\mathcal{D}$-analog of the Jordan $\phi$-function of higher order.

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

$$\sum_{\alpha_i = 0}^{\alpha_k} \psi(\alpha_1, \ldots, \alpha_k) p_0^{-(\alpha_1 + \cdots + \alpha_k)} = \sum_{\alpha_1, \ldots, \alpha_k = 1} \left| A_1 \right|^{-\alpha_1} \cdots \left| A_k \right|^{-\alpha_k}$$

$$= \frac{\xi(s_1) \cdots \xi(s_k)}{\xi(s_1 + \cdots + s_k)} = \frac{1 - p_0^{1-(\alpha_1 + \cdots + \alpha_k)}}{(1 - p_0^{1-\alpha_1}) \cdots (1 - p_0^{1-\alpha_k})},$$

and therefore

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

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

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

and therefore

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

From (13) and (14) we have

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

In particular, if $\alpha_1 = \cdots = \alpha_k = \nu$, we get for the $\phi$-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 $\phi$-Functions. Let us now denote by
\[ \sum \phi'(M; \alpha_1, \ldots, \alpha_k) p_0^{-(\alpha_1 + \cdots + \alpha_k)} = \sum' |A_1|^{-s_1} \cdots |A_k|^{-s_k}, \]

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

\[ \frac{\zeta(s_1) \cdots \zeta(s_k)}{\zeta(2s_1) \cdots \zeta(2s_k)} \prod_{P \mid M} (1 + |P|^{-(\alpha_1 + \cdots + \alpha_k)})^{-1}. \]

Therefore, if \( \lambda(B) \) is the \( \mathfrak{D} \)-analogue of the Liouville \( \lambda \)-function,*

and if \( q(\nu) \) is defined by the relation†

\[ \frac{\zeta(s)}{\zeta(2s)} = \sum_{r=0}^{\infty} \frac{q(\nu)}{R_0^{s^2}}, \]

we have in place of (11)

\[ \phi'(M; \alpha_1, \ldots, \alpha_k) = \sum_B \lambda(B) q(\alpha_1 - \beta) \cdots q(\alpha_k - \beta), \]

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

\[ \sum \psi'(\alpha_1, \ldots, \alpha_k) p_0^{\sigma_1 + \cdots + \alpha_k} = \frac{\zeta(s_1) \cdots \zeta(s_k)}{\zeta(2s_1) \cdots \zeta(2s_k)} \frac{\zeta(2s_1 + \cdots + 2s_k)}{\zeta(s_1 + \cdots + s_k)}, \]

so that

\[ \psi'(\alpha_1, \ldots, \alpha_k) = \sum_{\beta} (-1)^{\beta} p_0^{\beta'} q(\alpha_1 - \beta) \cdots q(\alpha_k - \beta), \]

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

Now, from the definition of \( \phi' \) and \( \psi' \), it is clear that

\[ \psi'(\alpha_1, \ldots, \alpha_k, \nu) = \sum_{\deg M = \nu} \mu^2(M) \phi'(M; \alpha_1, \ldots, \alpha_k), \]

\[ * \text{That is, if } B = P_1^{\alpha_1} P_2^{\alpha_2} \cdots, \lambda(B) = (-1)^{e_1 + e_2 + \cdots}; \text{see A.P., } \S3. \]

† It is evident that \( q(\nu) = p_0^{\nu} - p_0^{\nu-1} \) for \( \nu \geq 2 \) and that \( q(\nu) = p_0^{\nu} \) otherwise.
and therefore the sum
\[ \sum_{\deg M = v}^{\prime} \phi'(M; \alpha_1, \ldots, \alpha_k), \]
taken over quadratfrei \( M \) only, is equal to the right member of (17).

7. The L.C.M. of Polynomials of Degree \( v \). We recall the well known result that
\[ x^{p^v} - x = \prod_{\alpha \not{\mid} p} \Theta(\alpha), \]
where \( \Theta(\alpha) \) is the product of the irreducible polynomials of degree \( \alpha \). If now \( L(v) \) is the L.C.M. of the polynomials of degree \( v \), it is evident, to begin with, that if \( P \) is irreducible of degree \( \delta \), then the exponent of the highest power of \( P \) dividing \( L(v) \) is precisely \( \lfloor v/\delta \rfloor \), the greatest integer \( \leq v/\delta \). Therefore
\[ L(v) = \prod_{\deg P \leq v} P^{[v/\deg P]} \]
(20)
\[ = \prod_{\delta = 1}^{v} \left\{ \prod_{\deg P = \delta} P \right\}^{[v/\delta]} = \prod_{\delta = 1}^{v} \left\{ \Theta(\delta) \right\}^{[v/\delta]}. \]

On the other hand, by (19),
\[ F_0(v) = \prod_{\alpha = 1}^{v}(x^{p^\alpha} - x) = \prod_{\alpha = 1}^{v} \prod_{\delta | \alpha} \Theta(\delta) = \prod_{\delta = 1}^{v} \left\{ \Theta(\delta) \right\}^{[v/\delta]}. \]
Comparison with the right member of (20) shows at once that
\[ L(v) = F_0(v). \]

8. The Product of Polynomials of Degree \( v \). 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 \( G = \alpha_0x_0 + \cdots + \alpha_vx_v \), where the coefficients \( \alpha_i \) lie in \( GF(p^n) \), and the \( \alpha_i \) of lowest subscript \( \neq 0 \) is taken \( = 1 \), then
\[ \prod G = |x_i^{p^j}|, \quad (i, j = 0, \ldots, v). \]
(21)

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

(22) \[ \prod_{\alpha=0}^{v} \prod_{\deg E=\alpha} E = \prod_{\alpha=1}^{v} \prod_{\deg E=\alpha} E; \]

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

(23) \[ \prod_{\alpha=0}^{v-1} (x_{\rho}^{\alpha} - x)^{1+p_{\alpha} + \cdots + p_{\alpha}^{\alpha}}. \]

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

(3) \[ \prod_{\deg E=\nu} E = \prod_{\alpha=0}^{v-1} (x_{\rho}^{\alpha} - x)^{v_{\alpha}} = F(\nu). \]

9. The Formula for \( Q_{\rho}(\nu) \). Since any \( E \) may be written in the form \( E = GM', \ P^\nu \uparrow G \), it is evident that, for \( \nu = hp + k, \ 0 \leq k < \rho, \)

\[ F(\nu) = \prod_{\deg E=\nu} E \]

(24) \[ = \prod_{\alpha=0}^{h} \left\{ \prod_{\deg G_i=\nu - \alpha \rho} G_{\rho} \right\} \left\{ \prod_{\deg M_{\alpha}=\nu - \alpha \rho} M_{\rho} q_{\rho}(\nu - \alpha \rho) \right\} \]

\[ = \prod_{\alpha=0}^{h} q_{\rho}(\nu - \alpha \rho) \cdot \prod_{\alpha=0}^{h} F(\alpha) \cdot q_{\rho}(\nu - \alpha \rho), \]

where \( q_{\rho}(\nu) \) is the number of polynomials \( E \) of degree \( \nu \) such that \( P^\nu \uparrow E \) for any irreducible \( P \). It is known that* \( q_{\rho}(\nu) = \begin{cases} p_{\rho}^{\nu} - p_{\rho}^{\nu - \rho + 1} & \text{for } \nu \geq \rho, \\ p_{\rho}^{\nu} & \text{otherwise}; \end{cases} \)

so that

(25) \[ \sum_{\alpha=0}^{h} \rho^{\alpha} q_{\rho}(\nu - \alpha \rho) = p_{\rho}^{\nu - \beta}. \]

Then the product in (24) is equal to

\[ \prod_{\alpha=1}^{h} \left\{ \prod_{\beta=1}^{\alpha} (x_{\rho}^{\beta} - x)^{p_{\rho}^{\alpha - \beta}} \cdot q_{\rho}(\nu - \alpha \rho) \right\}; \]

* A.P., §6.
\[
= \prod_{\beta=1}^{h}(x^{\rho^\beta} - x)^{p_\beta}, \quad e_\beta = \sum_{a=\beta}^{h} p_\beta^{\sigma-a} q_\rho (\nu - \alpha_\rho),
\]
\[
= \prod_{\beta=1}^{h}(x^{\rho^\beta} - x)^{p_\rho^{\rho^\beta}} \quad \text{(by (25))}
\]
\[
= \left\{ \prod_{\beta=1}^{h}(x^{\rho^\beta} - x)^{p_\rho^{\rho^\beta}(h^\rho)} \right\}^{p_\rho h^\rho} = F_\rho^{\rho h^\rho}(h).
\]

By (24) and (26)
\[
F(\nu) = \prod_{a=0}^{h} Q_\rho^{p_\rho^a}(\nu - \alpha_\rho) \cdot F_\rho^{p_\rho^k}(h),
\]
or, writing \( h - \alpha \) for \( \alpha \),
\[
\prod_{a=0}^{h} Q_\rho^{p_\rho^{\alpha+a}}(\alpha_\rho + k) = F(h_\rho + k) F_\rho^{-p_\rho^k}(h)
\]
\[
= R_\rho(h_\rho + k), \quad \text{say}.
\]

It is now easy to evaluate \( Q_\rho \). Indeed, substituting \( h - 1 \) for \( h \) in (27), and raising both members of the resulting equation to the \( p_\sigma \)th power, we have
\[
\prod_{a=0}^{h-1} Q_\rho^{p_\rho^{\alpha+a}}(\alpha_\rho + k) = R_\rho(p_\rho - p_\rho^k)(\nu - \rho),
\]
and therefore
\[
Q_\rho(\nu) = R_\rho(\nu) R_\rho^{-p_\rho^k}(\nu - \rho).
\]

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 \( \rho \)th power of an irreducible polynomial, it is evident that
\[
Q_\rho(k) = F(k), \quad (0 \leq k < \rho):
\]
therefore, by (27), the expression
\[
F(h_\rho + k) F^{-p_\rho^k}(k) F_\rho^{-p_\rho^k}(h)
\]
is a polynomial provided that \( 0 \leq k < \rho \).

CAMBRIDGE, ENGLAND