Polynomials over $GF(q, x)$ with Integral-valued Differences

For my father, Carl T. Wagner, in the year of his sixty-fifth birthday

By

Carl G. Wagner

1. Introduction. Let D be an integral domain with quotient field K and let $f(t) \in K[t]$. For each $m \in D^*$ let

$$\Delta_m f(t) = \frac{f(t+m) - f(t)}{m},$$

and for each sequence $m_1, m_2, \ldots, m_r$ of nonzero elements of D, let the rth difference $\Delta_{m_1, m_2, \ldots, m_r} f(t)$ be defined inductively by

$$\Delta_{m_1, m_2, \ldots, m_r} f(t) = \Delta_{m_r}(\Delta_{m_1, m_2, \ldots, m_{r-1}} f(t)).$$

Let $I_0(D) = \{f(t) \in K[t] : f(d) \in D \text{ for all } d \in D\}$ and for each $r \geqq 1$ let $I_r(D) = \{f(t) \in K[t] : \Delta_{m_1, \ldots, m_r} f(t) \in I_0(D)$ for *every* sequence $m_1, \ldots, m_r$ of nonzero elements of $D\}$. Finally, let $\bar{I}_r(D) = I_0(D) \cap I_1(D) \cap \cdots \cap I_r(D)$. It is clear that $D[t] \subseteqq \bar{I}_r(D)$ for each $r \geqq 0$, and that in many cases this inclusion will be strict.

The $\bar{I}_r(D)$ are of interest both as D-modules and as subrings of $K[t]$. In the first case one wishes to know, for example, whether $\bar{I}_r(D)$ is free over D; in the second, questions about unique factorization and about the ideal structure of $\bar{I}_r(D)$ are natural. In this paper we shall investigate the D-modules $\bar{I}_r(D)$, where $D = GF[q, x]$, the ring of polynomials over the finite field $GF(q)$. Carlitz [5] has proved (by constructing an explicit basis) that $I_0(GF[q, x])$ is free over $GF[q, x]$ and since $GF[q, x]$ is a p.i.d., it follows immediately [8, p. 27, Th. 5.1] that each of the submodules $\bar{I}_r(GF[q, x])$ is free over $GF[q, x]$. Our purpose here is to construct explicit bases for these modules. The bases constructed may be used to prove that none of the rings $\bar{I}_r(GF[q, x])$ is a u.f.d.

We conclude this section with a brief survey of past work in this area. That $I_0(Z)$ is free over Z with basis $(\binom{t}{n})_{n \geqq 0}$ is a classical result. In 1919 Polya [10] and Ostrowski [9] investigated the module $I_0(D)$, where D is the ring of integers of an algebraic number field; and Cahen [3] has recently studied this module when D is any Dedekind domain. $\bar{I}_1(Z)$ has been treated by de Bruijn [6] and Hall [7], and the present author [13] has investigated the submodule of $\bar{I}_1(GF[q, x])$ consisting of linear polynomials. Carlitz [4] has studied the modules $\bar{I}_r(Z)$, constructing explicit bases, and Barsky [2] has generalized some of Carlitz's results to number fields, using as a tool Amice's interpolation series for local rings [1].

2. Preliminaries. Let $GF[q, x]$ denote the ring of polynomials over the finite field $GF(q)$ of characteristic p, and let $GF(q, x)$ denote the quotient field of $GF[q, x]$. A polynomial $f(t)$ over $GF(q, x)$ is called *integral-valued* if $f(m) \in GF[q, x]$ for all $m \in GF[q, x]$. The set of all integral-valued polynomials is denoted, as was indicated in section 1, by $I_0(GF[q, x])$.

In [5] Carlitz constructed an ordered basis $(C_n(t))_{n \geqq 0}$ for the $GF[q, x]$-module $I_0(GF[q, x])$ as follows. Let $\psi_0(t) = t$ and for $n \geqq 1$ let

$$\psi_n(t) = \prod (t - m), \quad m \in GF[q, x], \quad \deg m < n .$$

Then [5]

$$\psi_n(t) = \sum_{i=0}^{n} (-1)^{n-i} \begin{bmatrix} n \\ i \end{bmatrix} t^{q^i}, \tag{2.1}$$

where

$$\begin{bmatrix} n \\ i \end{bmatrix} = \frac{f_n}{f_i \, l_{n-i}^{q^i}}$$

and

$$\begin{aligned} f_n &= \langle n \rangle \langle n-1 \rangle^{q} \cdots \langle 1 \rangle^{q^{n-1}}, \quad & f_0 &= 1, \\ l_n &= \langle n \rangle \langle n-1 \rangle \cdots \langle 1 \rangle, & l_0 &= 1, \\ \langle r \rangle &= x^{q^r} - x . \end{aligned} \tag{2.2}$$

We remark that f_n is the product of all monic polynomials in $GF[q, x]$ of degree n, and that l_n is the l.c.m. of all polynomials in $GF[q, x]$ of degree n [5].

Now set $G_0(t) = 1$ and if $n \geqq 1$ and $n = n_0 + n_1 q + \cdots + n_s q^s$ is the q-adic expansion of n, let

$$G_n(t) = \prod_{i=0}^{s} \psi_i^{n_i}(t) .$$

The polynomial $G_n(t)$ has degree n, and serves as an analogue over $GF[q, x]$ of the factorial polynomial $t(t-1) \ldots (t-n+1)$ over Z.

To complete the construction of $C_n(t)$ one requires a polynomial analogue of $n!$. Set $g_0 = 1$ and for $1 \leqq n = n_0 + n_1 q + \cdots + n_s q^s$ as above, let

$$g_n = \prod_{i=1}^{s} f_i^{n_i},$$

where f_i is defined by (2.2). The polynomial g_n is the desired analogue of $n!$, and the polynomials $C_n(t) = G_n(t)/g_n$ furnish an ordered basis for $I_0(GF[q, x])$ over $GF[q, x]$ [5, Th. 9]. We list below some essential properties of the above polynomials.

Theorem 2.1. $G_n(t+u) = \sum_{k=0}^{n} \binom{n}{k} G_k(t) \, G_{n-k}(u)$.

Proof. [5, (2.3)].

Theorem 2.2. $C_n(t+u) = \sum_{k=0}^{n} \binom{n}{k} C_k(t) \, C_{n-k}(u)$.

Proof. Use Theorem 2.1 and [11, Prop. 1].

Theorem 2.3. *For all* $n \geqq 1$

$$\frac{g_{n-1}}{g_n} = \frac{1}{l_{e(n)}},$$

where $e(n) = \max\{k : q^k \mid n\}$, *and* l_n *is defined by* (2.2).

Proof. [11, Prop. 4].

Theorem 2.4. *Let* $H_0(t) = 1$ *and for* $n \geqq 1$ *let*

$$(2.3) \qquad H_n(t) = \frac{G_{n+1}(t)}{t\, g_n}.$$

Then $(H_n(t))$ *is also an ordered basis of the* $GF[q, x]$*-module* $I_0(GF[q, x])$.

Proof. [12, Lemma 3.1]. Remark. The polynomial $H_{n-1}(t)$ bears the same relationship to $C_n(t)$ as the polynomial $\binom{t-1}{n-1}$ does to $\binom{t}{n}$ (see [4]).

We may now proceed to construct a basis for $\bar{I}_1(GF[q, x])$.

3. A Basis for $\bar{I}_1(GF[q, x])$. Let $f(t) \in I_0(GF[q, x])$ have degree n. By [5, Th. 9], we may write

$$(3.1) \qquad f(t) = \sum_{j=0}^{n} a_j C_j(t),$$

where the a_j are uniquely determined elements of $GF[q, x]$. The following theorem gives necessary and sufficient conditions for $f(t)$ to belong to $\bar{I}_1(GF[q, x])$.

Theorem 3.1. *Let* $f(t) \in I_0(GF[q, x])$ *be as in* (3.1). *Then* $f(t) \in \bar{I}_1(GF[q, x])$ *if and only if, for all* $j \geqq 1$, $l_{e^*(j)} \mid a_j$, *where* $e^*(j) = \max\{e(i) : 1 \leqq i \leqq j\}$, $e(i) = \max\{k : q^k \mid i\}$, *and* l_r *is defined by* (2.2).

Remark. $e^*(j) = [\log j / \log q]$.

Proof. Let $m \in GF[q, x] - \{0\}$. Then by (3.1) and Theorem 2.2,

$$f(t + m) = \sum_{i=0}^{n} a_i \sum_{k=0}^{i} \binom{i}{k} C_k(t)\, C_{i-k}(m) =$$

$$= \sum_{k=0}^{n} C_k(t) \sum_{i=k}^{n} \binom{i}{k} a_i\, C_{i-k}(m).$$

Hence,

$$f(t + m) - f(t) = \sum_{k=0}^{n-1} C_k(t) \sum_{i=k+1}^{n} \binom{i}{k} a_i\, C_{i-k}(m) =$$

$$= \sum_{k=0}^{n-1} C_k(t) \sum_{i=1}^{n-k} \binom{i+k}{k} a_{i+k}\, C_i(m),$$

and so by (2.3), Theorem 2.3, and the fact that $C_i(m) = G_i(m)/g_i$,

$$\Delta_m f(t) = \frac{f(t+m) - f(t)}{m} = \tag{3.2}$$

$$= \sum_{k=0}^{n-1} C_k(t) \sum_{i=1}^{n-k} \binom{i+k}{k} \frac{a_{i+k}}{l_{e(i)}} H_{i-1}(m).$$

Since the $C_k(t)$ are a basis over $GF[q, x]$ of $I_0(GF[q, x])$, it follows that $\Delta_m f(t)$ is integral-valued for all nonzero m if and only if

$$\sum_{i=1}^{n-k} \binom{i+k}{k} \frac{a_{i+k}}{l_{e(i)}} H_{i-1}(m) \in GF[q, x] \tag{3.3}$$

for all nonzero m, i.e., if and only if

$$\sum_{i=1}^{n-k} \binom{i+k}{k} \frac{a_{i+k}}{l_{e(i)}} H_{i-1}(t)$$

is integral-valued. By Theorem 2.4, this is equivalent to the condition

$$\binom{i+k}{k} \frac{a_{i+k}}{l_{e(i)}} \in GF[q, x]$$

for all i, k such that $0 \leqq k \leqq n-1$ and $1 \leqq i \leqq n-k$. Hence, $f(t) \in \bar{I}_1(GF[q, x])$ if and only if

$$\binom{j}{i} \frac{a_j}{l_{e(i)}} \in GF[q, x] \tag{3.4}$$

for all i, j such that $1 \leqq i \leqq j \leqq n$. Now if $r \leqq s$, then $l_r \mid l_s$ [5,(1.4)], and so the condition $l_{e^*(j)} \mid a_j$ is sufficient for (3.4). To see that it is also necessary, write $j = j_0 + j_1 q + \cdots + j_s q^s$, where $0 \leqq j_i < q$ and $j_s \neq 0$. Clearly $e^*(j) = s$, and if (3.4) holds, it holds in particular for $i = j_s q^s$. But by a well known congruence for binomial coefficients, we have

$$\binom{j}{j_s q^s} \equiv \binom{j_0}{0} \binom{j_1}{0} \cdots \binom{j_s}{j_s} \equiv 1 \pmod{p}$$

and so $l_{e(j_s q^s)} = l_s = l_{e^*(j)}$ divides a_j in $GF[q, x]$.

It follows from the preceding theorem that the sequence

$$\left(1, l_{e^*(1)} \frac{G_1(t)}{g_1}, \ldots, l_{e^*(j)} \frac{G_j(t)}{g_j}, \ldots\right) \tag{3.3}$$

furnishes a basis for $\bar{I}_1(GF[q, x])$ over $GF[q, x]$. (Compare [6, Theorem 1].) Note that when $j = q^n$

$$l_{e^*(j)} \frac{G_j(t)}{g_j} = l_n \frac{\psi_n(t)}{f_n}.$$

Thus the above theorem contains as a special case the author's earlier characterization [13, Th. 3.2] of the submodule of $\bar{I}_1(GF[q, x])$ consisting of linear polynomials (i.e., polynomials in which each exponent of t is a power of q).

It should be noted that the module $I_1(GF[q, x])$ is *not* free over $GF[q, x]$, for the fact that a polynomial $f(t)$ over $GF(q, x)$ belongs to $I_1(GF[q, x])$ places no constraint on the constant term of $f(t)$. Consequently, $I_1(GF[q, x])$ contains as a submodule an isomorphic copy of $GF(q, x)$ and since $GF(q, x)$ is not free over $GF[q, x]$, the same is true of $I_1(GF[q, x])$. Similarly, none of the modules $I_r(GF[q, x])$ is free over $GF[q, x]$.

4. Higher Differences. Let $f(t)$ be given by (3.1) and denote the polynomial of (3.3) by $a_k(m)$. Then (3.2) may be written

$$\Delta_m f(t) = \sum_{k=0}^{n-1} a_k(m)\, C_k(t)$$

and we may repeat the procedure of Section 3 to derive the formula

$$\Delta_{m_1 m_2} f(t) = \sum_{k=0}^{n-2} C_k(t) \sum_{\substack{i_1+i_2 \leqq n-k \\ i_1, i_2 > 0}} \frac{(i_1+i_2+k)!}{i_1!\, i_2!\, k!} \frac{a_{i_1+i_2+k}}{l_{e(i_1)}\, l_{e(i_2)}} H_{i_1-1}(m_1)\, H_{i_2-1}(m_2)\,.$$

It follows again from the fact that $(C_k(t))$ and $(H_k(t))$ are bases of $I_0(GF[q, x])$ that $f(t) \in I_2(GF[q, x])$ if and only if, for all $j \geqq 2$

$$\frac{a_j}{l_{e(i_1)}\, l_{e(i_2)}} \in GF[q, x]$$

whenever $i_1, i_2 > 0$, $i_1 + i_2 \leqq j$, and the multinomial coefficient $j!/i_1!\, i_2!\, (j - i_1 - i_2)!$ is prime to p, the characteristic of $GF(q)$. In the general case we have the following theorem.

Theorem 4.1. *Let $f(t)$ be given by* (3.1). *Then $f(t) \in I_r(GF[q, x])$ if and only if, for all $j \geqq r$*

$$\frac{a_j}{l_{e(i_1)}\, l_{e(i_2)} \cdots l_{e(i_r)}} \in GF[q, x]$$

whenever $i_1, i_2, \ldots, i_r > 0$, $i_1 + i_2 + \cdots + i_r \leqq j$, and the multinomial coefficient $j!/i_1!\, i_2! \cdots i_r!\, (j - i_1 - i_2 - \cdots - i_r)!$ is prime to p.

If $1 \leqq j < r$, let $L_j^{(r)} = 1$, and for $1 \leqq r \leqq j$, let

$$L_j^{(r)} = \text{l.c.m.}\, \{l_{e(i_1)} \ldots l_{e(i_r)} : i_1, \ldots, i_r > 0\,,\ i_1 + \cdots + i_r \leqq j, \text{ and } j!/i_1! \ldots i_r!\, (j - i_1 - \cdots - i_r)! \text{ is prime to } p\}. \tag{4.1}$$

Then if, for all $j, r \geqq 1$, we set

$$\bar{L}_j^{(r)} = \text{l.c.m.}\, \{L_j^{(s)} : 1 \leqq s \leqq r\}\,, \tag{4.2}$$

it is clear from Theorem 4.1 that the sequence

$$\left(1, \bar{L}_1^{(r)} \frac{G_1(t)}{g_1}, \ldots, \bar{L}_j^{(r)} \frac{G_j(t)}{g_j}, \ldots\right) \tag{4.3}$$

furnishes a basis for $\bar{I}_r(GF[q, x)]$ over $GF[q, x]$. This should be compared with [4, Theorem 4].

We recall that in Section 3 we were able to conclude that $\bar{L}_j^{(1)} = l_{e*(j)}$ by appealing to a well known congruence (mod p) for binomial coefficients. Analogous congruences for multinomial coefficients do not appear to contribute to a significant simplification of formulas (4.1) and (4.2).

5. Factorization in the Rings $\bar{I}_r(GF[q, x])$. It is easy to see that the ring $I_0(GF[q, x])$ of integral-valued polynomials over $GF(q, x)$ is not a u.f.d., for the sequence $C_n(t)$ of Carlitz polynomials (which furnishes a basis for the module $I_0(GF[q, x])$) has the properties (a) $C_n(t) = t^n$ if $0 \leqq n < q$ and (b) $C_q(t) = (t^q - t)/x^q - x$ [5, p. 486/87]. Hence $C_q(t)$ is irreducible, since by (a) all polynomials of degree less that q belonging to $I_0(GF[q, x])$ have integral coefficients. Thus the equation

$$\prod_{\lambda \in GF(q)} (x - \lambda)\, C_q(t) = \prod_{\lambda \in GF(q)} (t - \lambda)$$

shows that unique factorization fails in this ring. More generally, we have the following theorem.

Theorem 5.1. *For each $r \geqq 1$, unique factorization fails in the ring $\bar{I}_r(GF[q, x])$.*

Proof. It clearly suffices to exhibit a polynomial $F(t)$ which belongs to each of the rings $\bar{I}_r(GF[q, x])$ and (when written as a linear combination of powers of t) has at least one non-integral coefficient. For this will imply [by (4.3)] that for each $r \geqq 1$ there exists a smallest $j > 1$ such that $\bar{L}_j^{(r)} G_j(t)/g_j$ (when written as a linear combination of powers of t) has at least one non-integral coefficient. Hence $\bar{L}_j^{(r)} G_j(t)/g_j$ will be irreducible in $\bar{I}_r(GF[q, x])$, and we may argue as in the preceding paragraph. Thus we consider the polynomial

$$F(t) = l_2 C_{q^2}(t) = l_2 \frac{\psi_2(t)}{f_2} = \frac{\psi_2(t)}{(x^2 - x)^{q-1}}.$$

By (2.1) and (2.2), the leading coefficient of $F(t)$ is non-integral. By [5, Theorem 9], $F(t) \in I_0(GF[q, x])$ and by our Theorem 3.1, $F(t) \in \bar{I}_1(GF[q, x])$. Since $F(t)$ is linear by (2.1),

$$\Delta_{m_1} F(t) = \frac{F(m_1)}{m_1},$$

and so $\Delta_{m_1, \ldots, m_r} F(t) = 0$ for all $r \geqq 2$ and $F(t) \in \bar{I}_r(GF[q, x])$ for all $r \geqq 1$, but $F(t) \notin D[t]$ $(D = GF[q, x])$.

References

[1] Y. Amice, Interpolation p-adique. Bull. Soc. Math. France **92**, 117–180 (1964).
[2] D. Barsky, Fonctions k-Lipschitziennes sur un anneau local et polynômes à valeurs entières. Bull. Soc. Math. France **101**, 397–411 (1973).
[3] P. J. Cahen, Polynômes à valeurs entières. Canad. J. Math. **24**, 747–754 (1972).
[4] L. Carlitz, A note on integral-valued polynomials. Indag. Math. **21**, 294–299 (1959).
[5] L. Carlitz, A set of polynomials. Duke Math. J. **6**, 486–504 (1940).

[6] N. G. DE BRUIJN, Some classes of integer-valued functions. Indag. Math. **17**, 363–367 (1955).
[7] R. R. HALL, On pseudo-polynomials. Mathematika **18**, 71–77 (1971).
[8] P. HILTON and U. STAMMBACH, A Course in Homological Algebra. New York 1971.
[9] A. OSTROWSKI, Über ganzwertige Polynome in algebraischen Zahlkörpern. J. Reine Angew. Math. **149**, 117–124 (1919).
[10] G. POLYA, Über ganzwertige Polynome in algebraischen Zahlkörpern. J. Reine Angew. Math. **149**, 97–116 (1919).
[11] C. G. WAGNER, Interpolation series in local fields of prime characteristic. Duke Math. J. **39**, 203–210 (1972).
[12] C. G. WAGNER, Differentiability in local fields of prime characteristic. Duke Math. J. **41**, 285–290 (1974).
[13] C. G. WAGNER, Linear pseudo-polynomials over $GF[q, x]$. Arch. Math. **25**, 385–390 (1974).

Eingegangen am 17. 5. 1975

Anschrift des Autors:

C. G. Wagner
Mathematics Department
University of Tennessee
Knoxville, Tennessee 37916
U.S.A.