Linear Pseudo-Polynomials over $GF[q, x]$

By

Carl G. Wagner *)

1. Introduction. A *pseudo-polynomial over the ring* $\mathbb{Z}$ of rational integers is a function f from the nonnegative integers to $\mathbb{Z}$ satisfying $f(n+k) \equiv f(n) \pmod{k}$ for all nonnegative n and k. In [4] R. R. Hall proved that the pseudo-polynomials over $\mathbb{Z}$ are precisely the functions f given by an interpolation series

$$f(x) = \sum_{n=0}^{\infty} A_n \binom{x}{n}, \tag{1.1}$$

where $A_n \in \mathbb{Z}$ and A_n is divisible by the l. c. m. of the numbers $1, 2, \ldots, n$. He also showed that the integral domain of pseudo-polynomials over $\mathbb{Z}$ (with pointwise multiplication of functions) is not a unique factorization domain.

Let $GF[q, x]$ denote the ring of polynomials over the finite field $GF(q)$. Following Hall, we say that a function $f\colon GF[q, x] \to GF[q, x]$ is a *pseudo-polynomial over* $GF[q, x]$ if $f(M+K) \equiv f(M) \pmod{K}$ for all $M, K \in GF[q, x]$. If, in addition, f is a linear operator on the $GF(q)$-vector space $GF[q, x]$ (in which case the aforementioned congruence reduces to $f(K) \equiv 0 \pmod{K}$) we say that f is a *linear pseudo-polynomial over* $GF[q, x]$. In this paper we present a characterization of such operators which is analogous to Hall's. We also show that the linear pseudo-polynomials constitute a non-commutative ring L (with operator composition as the ring multiplication) which is free of zero divisers. We conclude by showing that each operator in L may be extended uniquely to a continuous (though not necessarily differentiable) linear operator on the vector space of formal power series over $GF(q)$, equipped with an x-adic absolute value.

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 $GF[q, x]$. Following Carlitz [2], we define a sequence of polynomials $\psi_r(t)$ over $GF[q, x]$ by

$$\psi_r(t) = \prod_{\deg M < r} (t - M), \quad \psi_0(t) = t \tag{2.1}$$

where the product in (2.1) extends over all $M \in GF[q, x]$ (including 0) of degree $< r$. It follows [2] that

*) This work was supported by the University of Tennessee Faculty Research Fund.

$$\psi_r(t) = \sum_{i=0}^{r} (-1)^{r-i} \begin{bmatrix} r \\ i \end{bmatrix} t^{q^i}, \tag{2.2}$$

where

$$\begin{bmatrix} r \\ i \end{bmatrix} = \frac{F_r}{F_i L_{r-i}^{q^i}}, \quad \begin{bmatrix} r \\ 0 \end{bmatrix} = \frac{F_r}{L_r}, \quad \begin{bmatrix} r \\ r \end{bmatrix} = 1 \tag{2.3}$$

and

$$\begin{aligned} F_r &= \langle r \rangle \langle r-1 \rangle^q \cdots \langle 1 \rangle^{q^{r-1}}, \qquad F_0 = 1, \\ L_r &= \langle r \rangle \langle r-1 \rangle \cdots \langle 1 \rangle, \qquad L_0 = 1, \\ \langle r \rangle &= x^{q^r} - x. \end{aligned} \tag{2.4}$$

We remark that $\psi_r(x^r) = \psi_r(M) = F_r$ for M monic of degree r, so that F_r is the product of all monic polynomials in $GF[q, x]$ of degree r [2]. On the other hand, L_r may be seen to be the l. c. m. of all polynomials in $GF[q, x]$ of degree r [1].

A polynomial $f(t)$ over $GF(q, x)$ is called *integral valued* if $f(M) \in GF[q, x]$ for all $M \in GF[q, x]$; $f(t)$ is called *linear* if the polynomial function which it induces is a linear operator on the $GF(q)$-vector space $GF(q, x)$. It is proved in [2] and [3] that the sequence $(\psi_r(t)/F_r)$ is an ordered basis of the $GF[q, x]$-module of linear integral valued polynomials over $GF(q, x)$. Indeed, given any linear polynomial

$$f(t) = \sum_{i=0}^{n} \alpha_i t^{q^i} \qquad (\alpha_i \in GF(q, x)),$$

we have [2]

$$f(t) = \sum_{i=0}^{n} \Delta^i f(1) \frac{\psi_i(t)}{F_i}, \tag{2.5}$$

where the operators Δ^i are defined recursively by

$$\begin{aligned} \Delta^0 f(t) &= f(t), \\ \Delta^1 f(t) &= \Delta f(t) = f(xt) - x f(t), \\ \Delta^{i+1} f(t) &= \Delta^i f(xt) - x^{q^i} \Delta^i f(t). \end{aligned} \tag{2.6}$$

We conclude this section with some valuation theoretic remarks. Let $P \in GF[q, x]$ be irreducible. Each nonzero $\alpha \in GF(q, x)$ may be written, in essentially unique fashion, as $\alpha = P^e M/N$, where $M, N \in GF[q, x]$ are prime to P and to each other, and $e \in \mathbb{Z}$. Setting $v_P(\alpha) = e$ yields an integer-valued valuation on $GF(q, x)$. The valuation v_P induces a discrete non-archimedean absolute value $|\ |_P$ on $GF(q, x)$ by $|0|_P = 0$ and $|\alpha|_P = b^{v_P(\alpha)}$ (for some fixed b such that $0 < b < 1$) if $\alpha \neq 0$. As is familiar, $GF(q, x)$ may be embedded as a dense subfield in an essentially unique complete field. When $P = x$ this complete field is simply the field of formal power series

$$\alpha = \sum_{i=-\infty}^{\infty} a_i x^i, \tag{2.7}$$

where $a_i \in GF(q)$ and all but a finite number of the a_i's vanish for $i < 0$ (if n is the least integer such that $a_n \neq 0$, we have the extended valuation $v_x(\alpha) = n$). We denote this field by $GF((q, x))$. Its valuation ring, denoted $GF[[q, x]]$, consists of all formal power series of the form

$$\alpha = \sum_{i=0}^{\infty} a_i x^i .$$

Obviously, $GF[q, x]$ is a dense subring of the compact ring $GF[[q, x]]$.

3. Linear pseudo-polynomials over $GF[q, x]$. We recall from the Introduction that a linear pseudo-polynomial over $GF[q, x]$ is a linear operator f on the $GF(q)$-vector space $GF[q, x]$ such that $f(K) \equiv 0 \pmod{K}$ for all $K \in GF[q, x]$. Obviously, each linear polynomial $f(t)$ with coefficients in $GF[q, x]$ gives rise to a linear pseudo-polynomial over $GF[q, x]$. The same is true for some (but not all) linear, integral valued polynomials over $GF(q, x)$ (see Theorem 3.2). We denote the set of all linear pseudo-polynomials over $GF[q, x]$ by L. For $f, g \in L$ set $f + g(M) = f(M) + g(M)$ and $f \circ g(M) = f(g(M))$ for all $M \in GF[q, x]$. Clearly, $(L, +, \circ)$ is a noncommutative ring with identity. It follows from the next theorem that L is free of zero-divisors.

Theorem 3.1. *Let f be a nonzero linear operator in L. Then the null space of f is finite dimensional and the range of f is infinite dimensional.*

Proof. Suppose that the null space of f is infinite dimensional. Then there is an infinite sequence $M_1, M_2, \ldots$ of polynomials in $GF[q, x]$ such that for all i,

$$\deg M_i < \deg M_{i+1} \quad \text{and} \quad f(M_i) = 0 .$$

Now let $K \in GF[q, x]$ be arbitrary. Then $f(M_i + K) = f(K)$ for all i. But since f is a pseudo-polynomial, $M_i + K$ divides $f(K)$ for all i. Since the degree of $M_i + K$ ultimately exceeds that of $f(K)$, it follows that $f(K) = 0$. This contradicts the hypothesis that f is not the zero operator.

It follows immediately that the range of f is infinite dimensional, for it is well known that the null space and range of a linear operator on an infinite dimensional vector space (in this case the $GF(q)$-vector space $GF[q, x]$) cannot both be finite dimensional.

Corollary. *L contains no zero diviso s.*

Proof. Let $f, g \in L$, where g is not the zero operator. If $f \circ g$ is the zero operator, then the (infinite dimensional) range of g is contained in the null space of f. Hence, by the previous theorem, f is the zero operator.

We now present a concrete characterization of the operators of L. Let f be any linear operator on the $GF(q)$-vector space $GF[q, x]$. It follows easily from assertion (2.5) for linear polynomials that, for all $M \in GF[q, x]$,

$$f(M) = \sum_{i=0}^{\deg M} \Delta^i f(1) \frac{\psi_i(M)}{F_i}, \tag{3.1}$$

where the operators Δ^i are defined by (2.6). Since $\psi_i(M) = 0$ if $\deg M < i$, we may rewrite (3.1) as

$$f(t) = \sum_{i=0}^{\infty} \Delta^i f(1) \frac{\psi_i(t)}{F_i}, \tag{3.2}$$

where the variable t is understood to run through $GF[q, x]$. From (2.6) it is clear that $\Delta^i f(1) \in GF[q, x]$ for all i. Conversely, given any sequence (A_i) in $GF[q, x]$, since $\psi_i(t)/F_i$ is integral valued [3], it follows that

$$g(t) = \sum_{i=0}^{\infty} A_i \frac{\psi_i(t)}{F_i} \tag{3.3}$$

defines a linear operator g on $GF[q, x]$ for which $\Delta^i g(1) = A_i$. The following theorem specifies which of these linear operators are pseudo-polynomials over $GF[q, x]$.

Theorem 3.2. *Let the linear operator g on $GF[q, x]$ be given by the interpolation series (3.3). Then g is a pseudo-polynomial over $GF[q, x]$ if and only if A_i is divisible by L_i in $GF[q, x]$ for all i, where L_i is defined by* (2.4).

Sufficiency. It obviously suffices to show that

$$\frac{L_n \psi_n(K)}{F_n} \equiv 0 \pmod{K} \tag{3.4}$$

for all $K \in GF[q, x]$. If $\deg K < n$, then by (2.1) $\psi_n(K) = 0$. If $\deg K = n$ and the leading coefficient of K is c, then by the remark following (2.4) $L_n \psi_n(K)/F_n = = c L_n$, and since L_n is the l. c. m. of all polynomials of degree n, (3.4) follows.

Suppose then that $\deg K > n$. To establish (3.4) in this case it suffices to show that if P is a monic irreducible divisor of K such that P^e divides K but P^{e+1} does not divide K, then P^e divides $L_n \psi_n(K)/F_n$, i.e., $v_P(L_n \psi_n(K)/F_n) \geqq e$. Suppose that the P-adic expansion of K is

$$K = K_e P^e + \cdots + K_s P^s, \tag{3.5}$$

where $K_i \in GF[q, x]$, $K_e, K_s \neq 0$, and $\deg P = d$. Recall that P divides $\langle r \rangle$ (see 2.4) exactly once in $GF[q, x]$ if and only if d divides r. Hence by (2.4)

$$v_P(L_n) = \sum_{j=1}^{[n/d]} 1 = [n/d] \tag{3.6}$$

and

$$v_P(F_n) = \sum_{j=1}^{[n/d]} q^{n-jd}. \tag{3.7}$$

To evaluate $v_P(\psi_n(K))$, let $S_n = \{M \in GF[q, x] : \deg M < n\}$ and, for each $j \geqq 1$, let $a_j = \operatorname{card}\{M \in S_n : M \equiv K \pmod{P^j}\}$. Then by (2.2)

$$v_P(\psi_n(K)) = \sum_{M \in S_n} v_P(K - M) = \sum_{j=1}^{\infty} j(a_j - a_{j+1}) = \sum_{j=1}^{\infty} a_j, \tag{3.8}$$

where, in the last two sums of (3.8) all but a finite number of terms vanish. Indeed, it is clear from (3.5) and the fact that $\deg K > n$ that $a_j = 0$ when $j > s$. On the other hand, if $1 \leqq j \leqq [n/d]$, then since S_n contains precisely q^{n-jd} complete residue systems $(\bmod P^j)$, $a_j = q^{n-jd}$ for such j. For $[n/d] < j \leqq s$, however, $\alpha_j \leqq 1$, since in such cases S_n contains only a fragment of a complete residue system $(\bmod P^j)$. Along with (3.6), (3.7), and (3.8) the foregoing remarks yield the preliminary formula

$$v_P\left(\frac{L_n\,\psi_n(K)}{F_n}\right) = [n/d] + \sum_{j=[n/d]+1}^{s} a_j, \tag{3.9}$$

where $0 \leqq a_j \leqq 1$. If $[n/d] \geqq e$, the desired result follows immediately. Suppose then that $[n/d] = e - r$ for some $r > 1$. Since $0 \in S_n$ and $K \equiv 0 \pmod{P^j}$ for $j \leqq e$, we have $a_j = 1$ for $e - r + 1 \leqq j \leqq e$. Hence by (3.9)

$$v_P\left(\frac{L_n\,\psi_n(K)}{F_n}\right) = (e-r) + \sum_{j=e-r+1}^{s} a_j \geqq (e-r) + \sum_{j=e-r+1}^{e} 1 = e$$

Necessity. We are given that K divides $g(K)$ for all $K \in GF[q, x]$. We show by induction on i that L_i divides A_i for all i. By (2.4), $L_0 = 1$ and so L_0 divides A_0. Suppose that L_i divides A_i for all $i < n$. Let $K \in GF[q, x]$ be an arbitrary monic polynomial of degree n. Then

$$g(K) = \sum_{i=0}^{n} A_i \frac{\psi_i(K)}{F_i} = \sum_{i=0}^{n-1} A_i \frac{\psi_i(K)}{F_i} + A_n.$$

Since L_i divides A_i for $i < n$, then by the preceding proof of sufficiency, K divides $A_i\psi_i(K)/F_i$ for $i < n$. Since K also divides $g(K)$, K divides A_n. Hence A_n is divisible by L_n, the l. c. m. of all polynomials in $GF[q, x]$ of degree n.

4. Extensions to $GF[[q, x]]$. In [4] Hall remarks that it would be of interest to find an interpolation formula for the function f given in (1.1) "which would extend its definition to all real or even complex values of x". While this would appear to be a task of some difficulty, it may be of interest to note that the aforementioned function f extends by the very same formula to a continuous function on the ring $\mathbb{Z}_p$ of p-adic integers for any prime p. Indeed, Mahler [5] has shown that a series of the form (1.1), where $A_n \in \mathbb{Z}_p$, represents a continuous function on $\mathbb{Z}_p$ precisely when $\lim_{n\to\infty} A_n = 0$ for the p-adic topology, and Hall's divisibility conditions on the A_n clearly insure that (A_n) is a p-adic null sequence. On the other hand, this extension of a pseudo-polynomial to $\mathbb{Z}_p$ may not yield a differentiable function, for Mahler [5] has proved, among other things, that the extended function f of (1.1) is differentiable at 0 if and only if (A_n/n) is a p-adic null sequence. Thus if we set $A_n = \text{l.c.m.}\ \{1, 2, \ldots, n\}$, f is not differentiable at 0 since the subsequence (A_{p^r}/p^r) is not a p-adic null sequence.

Analogously, the linear pseudo-polynomial g given by (3.3) extends by the very same formula to a continuous linear operator on the $GF(q)$-vector space $GF[[q, x]]$. For it is known [6] that a series of the form (3.3), where $A_i \in GF[[q, x]]$ represents a continuous linear operator on $GF[[q, x]]$ (for the x-adic topology) precisely when (A_i) is an x-adic null sequence, and the divisibility conditions on A_i insure this when g is an extension of a linear pseudo-polynomial. On the other hand, g is differentiable at 0 (hence everywhere) if and only if (A_i/L_i) is an x-adic null sequence [6]. Hence if we set $A_i = L_i$ in (3.3), this yields a linear pseudo-polynomial over $GF[q, x]$, the unique continuous extension of which to $GF[[q, x]]$ is nowhere differentiable.

References

[1] L. CARLITZ, On Polynomials in a Galois Field. Bull. Amer. Math. Soc. **38**, 736—744 (1932).
[2] L. CARLITZ, On Certain Functions Connected with Polynomials in a Galois Field. Duke Math. J. **1**, 137—168 (1935).
[3] L. CARLITZ, A Set of Polynomials. Duke Math. J. **6**, 486—504 (1940).
[4] R. R. HALL, On Pseudo-Polynomials. Mathematika **18**, 71—77 (1971).
[5] K. MAHLER, An interpolation series for continuous functions of a p-adic variable. J. Reine Angew. Math. **251**, 23—34 (1958).
[6] C. WAGNER, Linear operators in local fields of prime characteristic. J. Reine Angew. Math. **251**, 153—160 (1971).

Eingegangen am 11. 11. 1973

Anschrift des Autors:
Carl G. Wagner
Mathematics Department
University of Tennessee
Knoxville, Tennessee 37916, USA