Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2023) 47: 1073 – 1086
© TÜBİTAK
doi:10.55730/1300-0098.3413

Polynomials taking integer values on primes in a function field

Tuangrat CHAICHANA[1], **Vichian LAOHAKOSOL**[2], **Rattiya MEESA**[1,*], **Boonrod YUTTANAN**[3]

[1]Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand
[2]Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok, Thailand
[3]Division of Computational Science, Faculty of Science, Prince of Songkla University, Songkhla, Thailand

Received: 30.09.2022 • **Accepted/Published Online:** 13.01.2023 • **Final Version:** 16.05.2023

Abstract: Let $\mathbb{F}_q[x]$ be the ring of polynomials over a finite field $\mathbb{F}_q$ and $\mathbb{F}_q(x)$ its quotient field. Let $\mathbb{P}$ be the set of primes in $\mathbb{F}_q[x]$, and let $\mathcal{I}$ be the set of all polynomials f over $\mathbb{F}_q(x)$ for which $f(\mathbb{P}) \subseteq \mathbb{F}_q[x]$. The existence of a basis for $\mathcal{I}$ is established using the notion of characteristic ideal; this shows that $\mathcal{I}$ is a free $\mathbb{F}_q[x]$-module. Through localization, explicit shapes of certain bases for the localization of $\mathcal{I}$ are derived, and a well-known procedure is described as to how to obtain explicit forms of some bases of $\mathcal{I}$.

Key words: Integer-valued polynomial, polynomial over finite field, prime, localization

1. Introduction

Let D be an integral domain and K its quotient field. Let E be a subset of D. Denote the set of all integer-valued polynomials on E by

$$\operatorname{Int}(E, D) := \{f(t) \in K[t] \mid f(E) \subseteq D\}.$$

If $E = D$, write $\operatorname{Int}(D)$ instead of $\operatorname{Int}(D, D)$. In the classical case where D is the ring of rational integers $\mathbb{Z}$, it is well-known that $\operatorname{Int}(\mathbb{Z})$ is a free $\mathbb{Z}$-module. Indeed, for a number field K with the ring of integers $\mathcal{O}_K$, one can show that $\operatorname{Int}(\mathcal{O}_K)$ is a free $\mathcal{O}_K$-module [3, Chapter II, Section 3]. In 1997, Chabert et al. [5] proved that the set $\operatorname{Int}(P, \mathbb{Z})$ is a free $\mathbb{Z}$-module, where $P \subseteq \mathbb{Z}$ is the set of all primes, and described an algorithm which constructs such a free basis. There is a recent work in [6] which gives an interesting application of $\operatorname{Int}(P, \mathbb{Z})$.

Our objective here is to prove results analogous to those in [5] in the function field case. Throughout, we take the domain D to be $\mathbb{F}_q[x]$, the ring of all polynomials over $\mathbb{F}_q$, a finite field of q elements, so that its quotient field K is $\mathbb{F}_q(x)$. In [4, Section 3], it is shown that any polynomial in $\mathbb{F}_q[x]$ is uniquely expressible with respect to a certain basis, and, consequently in [4, Theorem 9-10], any element in $\operatorname{Int}(\mathbb{F}_q[x])$ is uniquely expressible with respect to such basis with suitably chosen coefficients, and so $\operatorname{Int}(\mathbb{F}_q[x])$ is a free $\mathbb{F}_q[x]$-module. Let $\mathbb{P}$ be the set of all monic irreducible polynomials, i.e., primes, in $\mathbb{F}_q[x]$. Using the idea of characteristic ideal, we prove in the next section that the set $\mathcal{I} := \operatorname{Int}(\mathbb{P}, \mathbb{F}_q[x])$ is a free $\mathbb{F}_q[x]$-module. In the third section,

*Correspondence: rattiya3328@gmail.com

2010 *AMS Mathematics Subject Classification:* 13F20, 11R58

This work is licensed under a Creative Commons Attribution 4.0 International License.

we establish certain properties of the module $\mathcal{I}$. In the fourth section, the localization $\mathcal{I}_{(p)}$ ($p \in \mathbb{P}$) of $\mathcal{I}$ is investigated, and employing the notion of p-ordering in [2], a basis for the module $\mathcal{I}_{(p)}$ is derived. Globalizing the localized bases, a procedure to compute explicit bases of the module $\mathcal{I}$ is described in the last section.

2. Existence of a basis

We first introduce the notion of characteristic ideal, [3, Chapter II, Section 1]. For brevity, let $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

Definition 2.1 *Let B be a domain such that $\mathbb{F}_q[x][t] \subseteq B \subseteq \mathbb{F}_q(x)[t]$. For $n \in \mathbb{N}_0$, we define the set $I_B(n)$ to be the union of the element $0 \in \mathbb{F}_q$ and the set of leading coefficients of all polynomials in B of degree n:*

$$I_B(n) = \{0\} \cup \left\{ A \in \mathbb{F}_q(x) \setminus \{0\} \mid \exists f \in B \text{ such that } f = At^n + A_{n-1}t^{n-1} + \cdots + A_0 \right\}.$$

One can show that if $B \subseteq \mathrm{Int}(\mathbb{F}_q[x])$, then $I_B(n)$ is a fractional ideal of $\mathbb{F}_q[x]$, [3, Proposition II.1.1], so that there exists $d(x) \in \mathbb{F}_q[x] \setminus \{0\}$ such that $d(x)I_B(n) \subseteq \mathbb{F}_q[x]$. We call $I_B(n)$ the n-th characteristic ideal of B.

To prove the existence of a basis for $\mathcal{I}$, we make use of the following result, [3, Proposition II.1.4].

For a domain B such that $\mathbb{F}_q[x][t] \subseteq B \subseteq \mathbb{F}_q(x)[t]$, we note that, [3, Definition II.1.3], a basis $\{f_n\}_{n\geq 0}$ of the $\mathbb{F}_q[x]$-module B is said to be a regular basis if, for each n, the polynomial f_n has degree n.

Proposition 2.2 *Let B be a domain such that $\mathbb{F}_q[x][t] \subseteq B \subseteq \mathbb{F}_q(x)[t]$. A sequence $\{f_n\}_{n\geq 0} \subseteq B$ is a regular basis of B if and only if, for each $n \in \mathbb{N}_0$, the polynomial f_n is of degree n whose leading coefficient generates $I_B(n)$ as an $\mathbb{F}_q[x]$-module.*

Taking B to be $\mathcal{I} = \mathrm{Int}(\mathbb{P}, \mathbb{F}_q[x])$ which is easily checked to be a domain, the set $I_{\mathcal{I}}(n)$ has a simple structure.

Proposition 2.3 *The set $I_{\mathcal{I}}(n)$ is a principal fractional ideal of $\mathbb{F}_q[x]$.*

Proof By [3, Proposition II.1.1], the set $I_{\mathcal{I}}(n)$ is a fractional ideal of $\mathbb{F}_q[x]$. To check that it is principal, let

$$f(t) = A_0 + A_1 t + \cdots + A_n t^n \in \mathcal{I}, \quad A_n \neq 0.$$

For $p_i \in \mathbb{P}$ with $\deg p_i = i$ $(1 \leq i \leq n+1)$, we have

$$\mathcal{A}_n \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_n \end{bmatrix} = \begin{bmatrix} f(p_1) \\ f(p_2) \\ \vdots \\ f(p_{n+1}) \end{bmatrix}, \quad \text{where} \quad \mathcal{A}_n := \begin{bmatrix} 1 & p_1 & \cdots & p_1^n \\ 1 & p_2 & \cdots & p_2^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & p_{n+1} & \cdots & p_{n+1}^n \end{bmatrix}.$$

Since $\mathcal{A}_n$ is a Vandermonde matrix, we have $\det \mathcal{A}_n = \prod_{1\leq i<j\leq n+1}(p_j - p_i) \in \mathbb{F}_q[x] \setminus \{0\}$ yielding

$$A_n \det \mathcal{A}_n = \begin{vmatrix} 1 & p_1 & \cdots & p_1^{n-1} & f(p_1) \\ 1 & p_2 & \cdots & p_2^{n-1} & f(p_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & p_{n+1} & \cdots & p_{n+1}^{n-1} & f(p_{n+1}) \end{vmatrix} \in \mathbb{F}_q[x],$$

and so $I_{\mathcal{I}}(n) \det \mathcal{A}_n \subseteq \mathbb{F}_q[x]$. Next, it is easily checked that $I_{\mathcal{I}}(n) \det \mathcal{A}_n$ is an ideal of $\mathbb{F}_q[x]$. Since $\mathbb{F}_q[x]$ is a principal ideal domain, $I_{\mathcal{I}}(n) \det \mathcal{A}_n$ is a principal ideal implying that $I_{\mathcal{I}}(n)$ is a principal fractional ideal. □

Remarks. In passing, we make some observations about the shape of each $I_{\mathcal{I}}(n)$. Clearly, the sequence $\{I_{\mathcal{I}}(n)\}_{n\geq 0}$ is increasing with respect to set inclusion. For degree 0, the set of all polynomials of degree 0 in $\mathcal{I}$ is $\mathbb{F}_q[x]$. For degree 1, consider $f(t) = A_0 + A_1 t \in \mathcal{I}$; its leading coefficient is $A_1 = f(x+1) - f(x) \in \mathbb{F}_q[x]$. So, $I_{\mathcal{I}}(0) = I_{\mathcal{I}}(1) = \mathbb{F}_q[x]$. In general, for degree $n \geq 2$, the set $I_{\mathcal{I}}(n)$ depends on q, the cardinality of $\mathbb{F}_q$. For example, if $q = 2$, we have $1/x \in I_{\mathcal{I}}(2)$ because $f(t) = t(t-1)/x \in \operatorname{Int}(\mathbb{P}, \mathbb{F}_2[x])$, but if $q > 2$, it is checked that $1/x \notin I_{\mathcal{I}}(2)$; for otherwise, $1/x \in I_{\mathcal{I}}(2)$. Then there exists

$$f(t) = \frac{1}{x}t^2 + \frac{a(x)}{b(x)}t + \frac{c(x)}{d(x)} \in \mathcal{I} \quad (a(x), b(x), c(x), d(x) \in \mathbb{F}_q[x] \text{ and } b(x), d(x) \neq 0).$$

Substituting $t = x,\ x+1,\ x+\alpha \in \mathbb{P}$ with $\alpha \in \mathbb{F}_q \setminus \{0,1\}$, we have $f(x),\ f(x+1),\ f(x+\alpha) \in \mathbb{F}_q[x]$. It follows that $\frac{\alpha(\alpha-1)}{x} = f(x+\alpha) - \alpha f(x+1) + (\alpha-1)f(x) \in \mathbb{F}_q[x]$, which is a contradiction.

From Proposition 2.3, we know that $I_{\mathcal{I}}(n)$ is a principal fractional ideal so that for each $n \in \mathbb{N}_0$, there is $a_n(x)/b_n(x) \in \mathbb{F}_q(x) \setminus \{0\}$ such that $I_{\mathcal{I}}(n) = \frac{a_n(x)}{b_n(x)}\mathbb{F}_q[x]$. Thus, $\frac{b_n(x)}{a_n(x)} I_{\mathcal{I}}(n) = \mathbb{F}_q[x] = I_{\mathcal{I}}(0) \subseteq I_{\mathcal{I}}(n)$ showing that $b_n(x)/a_n(x) \in \mathbb{F}_q[x]$, and so there exists $d_n \in \mathbb{F}_q[x]$ such that

$$I_{\mathcal{I}}(n) = d_n^{-1}\mathbb{F}_q[x]. \tag{2.1}$$

We are now ready for our first main theorem.

Theorem 2.4 *The set $\mathcal{I}$ is a free $\mathbb{F}_q[x]$-module with a regular basis.*

Proof From (2.1), let $I_{\mathcal{I}}(n) = d_n^{-1}\mathbb{F}_q[x]$ $(n \in \mathbb{N}_0)$. Let $\mathcal{B} = \{f_n(t)\}_{n\in\mathbb{N}_0} \subseteq \mathcal{I}$ be a sequence of polynomials such that $\deg f_n(t) = n$ and the leading coefficient of $f_n(t)$ is $1/d_n$. By Proposition 2.2, the set $\mathcal{B}$ forms a regular basis of $\mathcal{I}$. □

3. Auxiliary results

We shall make use of the following function field analogue of Dirichlet's theorem taken from [9, Theorem 4.8].

Lemma 3.1 *For $a(x), b(x) \in \mathbb{F}_q[x]$, if $\gcd(a(x), b(x)) = 1$, then there exists $c(x) \in \mathbb{F}_q[x]$ such that $a(x) + b(x)c(x) \in \mathbb{P}$ has degree n for a sufficiently large $n \in \mathbb{N}$.*

We next describe a classical algorithm to construct a basis for $\operatorname{Int}(\mathbb{F}_q[x])$.

Set $\mathbb{F}_q := \{a_0 = 0,\ a_1, \ldots, a_{q-1}\}$. For $n \in \mathbb{N},\ n \geq q$, with its unique base-$q$ representation being

$$n = n_0 + n_1 q + \cdots + n_s q^s \quad (0 \leq n_i < q,\ n_s \neq 0),$$

define

$$a_n = a_{n_0} + a_{n_1}x + \cdots + a_{n_s}x^s.$$

The sequence $\{a_n\}_{n\geq 0}$ so defined is referred to as a polynomial ordering with respect to the base x. From the sequence $\{a_n\}_{n\geq 0}$, define the Lagrange type interpolation polynomials $\{C_n(t)\}_{n\geq 0}$ by

$$C_0(t) = 1, \quad C_n(t) = \prod_{i=0}^{n-1} \frac{t - a_i}{a_n - a_i} \quad (n \geq 1). \tag{3.1}$$

The sequence $\{C_n(t)\}_{n\geq 0}$ forms a basis for $\mathrm{Int}(\mathbb{F}_q[x])$ as a $\mathbb{F}_q[x]$-module, [3, Chapter II, Section 2].

For each $\ell \in \mathbb{P}$, define the ℓ-adic ordinal $\nu_\ell : \mathbb{F}_q[x] \longrightarrow \mathbb{R} \cup \{\infty\}$ by

$$\nu_\ell(0) = \infty, \quad \nu_\ell(a) = \alpha \quad \text{for } a = \ell^\alpha \cdot f \ (\alpha \in \mathbb{N},\ f \in \mathbb{F}_q[x],\ \ell \nmid f),$$

and extend it to $\mathbb{F}_q(x)$ in the usual manner. Connecting the sequence $\{C_n(t)\}_{n\geq 0}$ with Lemma 3.1, we get:

Proposition 3.2 *Let $\{C_n(t)\}_{n\geq 0}$ be a sequence of polynomials as defined in (3.1), and for a given $n \in \mathbb{N}_0$, let $A_n \in \mathbb{F}_q(x)$ be such that $A_n C_n(t) \in \mathcal{I}$. If $n \not\equiv -1 \pmod q$ then, $A_n \in \mathbb{F}_q[x]$.*

Proof Note that if

$$C_n(t) = \frac{u_n(x)}{v_n(x)} t^n + \frac{u_{n-1}(x)}{v_{n-1}(x)} t^{n-1} + \cdots + \frac{u_0(x)}{v_0(x)},$$

where $u_i(x), v_i(x) \in \mathbb{F}_q[x]$, then $\mathrm{LCM}(v_n, \ldots, v_0) C_n(t) \in \mathbb{F}_q[x][t]$, which assures the existence of A_n. Let $\ell \in \mathbb{P}$. Set $r = 1 + \sup_{0\leq i<n} \{\nu_\ell(a_n - a_i)\}$. If $\ell \nmid a_n$, then, by Lemma 3.1, there exists $p = a_k \ell^r + a_n \in \mathbb{P}$ for some $a_k \in \mathbb{F}_q[x]$. Then,

$$C_n(p) = \prod_{i=0}^{n-1} \frac{p - a_i}{a_n - a_i} = \prod_{i=0}^{n-1} \frac{a_k \ell^r + a_n - a_i}{a_n - a_i}.$$

Since $\nu_\ell(a_k \ell^r) > \nu_\ell(a_n - a_i)$, we have $\nu_\ell(a_k \ell^r + a_n - a_i) = \nu_\ell(a_n - a_i)$ for $0 \leq i < n$, and so $\nu_\ell(C_n(p)) = 0$. On the other hand, if $\ell \mid a_n$, let $a'_n = a_n - a_{n_0} + a_{q-1}$ where n_0 is first digit in the q-adic expansion of $n = n_0 + n_1 q + \cdots + n_s q^s$. Let

$$r' = 1 + \sup_{0\leq i<n} \{\nu_\ell(a'_n - a_i)\}.$$

Since $-a_{n_0} + a_{q-1} \in \mathbb{F}_q$, we have $\ell \nmid a'_n$. By Lemma 3.1, there exists $p = a_{k'} \ell^{r'} + a'_n \in \mathbb{P}$ for some $a_{k'} \in \mathbb{F}_q[x]$. If $n/q > 1$, then for $0 \leq j < \lfloor n/q \rfloor$ we have

$$\prod_{i=jq}^{(j+1)q-1} (a_n - a_i) = \prod_{i=jq}^{(j+1)q-1} (a'_n - a_i); \tag{3.2}$$

because a_n and a'_n differ only by a constant term and both products in (3.2) run over a complete residue class modulo x. Since $n \not\equiv -1 \pmod q$, $a'_n - a_{n_0} + a_{q-1} \neq a_i$ for all $0 \leq i < n$. Note that $a'_n - a_i \neq 0$. As $\nu_\ell(a_k \ell^{r'}) > \nu_\ell(a'_n - a_i)$ for all $0 \leq i < n$,

$$\nu_\ell\left(\prod_{i=jq}^{(j+1)q-1} (a_k \ell^{r'} + a'_n - a_i)\right) = \nu_\ell\left(\prod_{i=jq}^{(j+1)q-1} (a'_n - a_i)\right) = \nu_\ell\left(\prod_{i=jq}^{(j+1)q-1} (a_n - a_i)\right).$$

Moreover, $a_n - a_i$ and $a'_n - a_i$ are elements in $\mathbb{F}_q \setminus \{0\}$ for all $n - n_0 \leq i < n$. This implies that

$$\nu_\ell\left(\prod_{i=n-n_0}^{n-1} (a_k \ell^{r'} + a'_n - a_i)\right) = \nu_\ell\left(\prod_{i=n-n_0}^{n-1} (a'_n - a_i)\right) = 0 = \nu_\ell\left(\prod_{i=n-n_0}^{n-1} (a_n - a_i)\right).$$

Thus,

$$\nu_\ell(C_n(p)) = \nu_\ell\left(\prod_{i=0}^{n-1} \frac{a_k\ell^{r'} + a'_n - a_i}{a_n - a_i}\right) = 0.$$

Since $\nu_\ell(A_nC_n(p)) \geq 0$, we conclude that $\nu_\ell(A_n) \geq 0$ for all $\ell \in \mathbb{P}$. □

Since Proposition 3.2 indicates that the sequence $\{C_n(t)\}_{n\geq 0}$ is a basis of $\mathcal{I}$ over $\mathbb{F}_q[x]$, and since the coefficients of each $C_n(t)$ are of certain special kind, it is then natural to ask for properties that the coefficients of any basis element must have, and this is answered in the next proposition.

Proposition 3.3 *Let $n \in \mathbb{N}$ and $\{m_1, m_2, \ldots, m_n\} \subseteq \mathbb{F}_q[x]$. If $A \in \mathbb{F}_q(x)$ is such that $A\prod_{i=1}^{n}(t - m_i(x)) \in \mathcal{I}$, then for all $\ell \in \mathbb{P}$ with $\deg \ell > \log_q n$, we have $\nu_\ell(A) \geq 0$.*

Proof Let $\ell \in \mathbb{P}$ be such that $\deg \ell > \log_q n$. We consider two possible cases.
Case 1: $\nu_\ell(m_i) = 0$ for all $1 \leq i \leq n$. Then $\nu_\ell(A) = \nu_\ell(A(\ell - m_1)\cdots(\ell - m_n)) \geq 0$.
Case 2: there exists m_j for some $1 \leq j \leq n$ such that $\nu_\ell(m_j) \geq 1$. Since the number of elements in $\mathbb{F}_q[x]/(\ell)$ is $q^{\deg \ell} > n$, there exists $s \in \mathbb{F}_q[x]$ such that $\nu_\ell(s - m_i) = 0 \quad (1 \leq i \leq n)$. As $\nu_\ell(m_j) \geq 1$ and $\nu_\ell(s - m_j) = 0$, we obtain that $\nu_\ell(s) = 0$. By Lemma 3.1, there exists $p = k\ell + s \in \mathbb{P}$ for some $k \in \mathbb{F}_q[x]$. So,

$$0 \leq \nu_\ell(A(p - m_1)\cdots(p - m_n)) = \nu_\ell(A(k_0\ell + s - m_1)\cdots(k_0\ell + s - m_n)) = \nu_\ell(A).$$

□

4. Localization

For each $p \in \mathbb{P}$, set

- $X_p = (\mathbb{F}_q[x] \setminus p\mathbb{F}_q[x]) \cup \{p\}$
- $\mathbb{F}_q[x]_{(p)} = \{a/b \in \mathbb{F}_q(x) \mid a \in \mathbb{F}_q[x] \text{ and } b \in \mathbb{F}_q[x] \setminus p\mathbb{F}_q[x]\}$
- $\text{Int}(X_p, \mathbb{F}_q[x]_{(p)}) = \left\{f(t) \in \mathbb{F}_q(x)[t] \mid f(X_p) \subseteq \mathbb{F}_q[x]_{(p)}\right\}$.

The set $\mathbb{F}_q[x]_{(p)}$ is called the localization of $\mathbb{F}_q[x]$ at the prime p. The next proposition gives a basic result connecting $\mathcal{I}$ with $\mathbb{F}_q[x]_{(p)}$.

Proposition 4.1 *Let $f(t) \in \mathcal{I}$, $p \in \mathbb{P}$ and $h \in \mathbb{F}_q[x]$. If $p \nmid h$, then $f(h) \in \mathbb{F}_q[x]_{(p)}$.*

Proof Let $d \in \mathbb{F}_q[x] \setminus \{0\}$ be such that $df(t) \in \mathbb{F}_q[x][t]$. Then, $d = p^{\nu_p(d)}e$ where $p \nmid e$. Assume that $p \nmid h$. By Lemma 3.1, there exists $r = kp^{\nu_p(d)} + h \in \mathbb{P}$ for some $k \in \mathbb{F}_q[x]$. Since $df(t) \in \mathbb{F}_q[x][t]$, we can write $df(t) = u_nt^n + u_{n-1}t^{n-1} + \cdots + u_0 \quad (u_i \in \mathbb{F}_q[x])$. Thus,

$$d(f(r) - f(h)) = u_n(r^n - h^n) + u_{n-1}(r^{n-1} - h^{n-1}) + \cdots + u_1(r - h) \in (r - h)\mathbb{F}_q[x],$$

and so $ep^{\nu_p(d)}(f(r) - f(h)) \in kp^{\nu_p(d)}\mathbb{F}_q[x]$. This implies that $f(r) - f(h) \in e^{-1}\mathbb{F}_q[x]$. Since $e \notin p\mathbb{F}_q[x]$, we have $f(r) - f(h) \in \mathbb{F}_q[x]_{(p)}$. As $f(r) \in \mathbb{F}_q[x] \subseteq \mathbb{F}_q[x]_{(p)}$, the desired result follows. □

Proposition 4.2 *Let* $p := p(x) \in \mathbb{P}$ *and define*

$$\mathcal{I}_{(p)} := \operatorname{Int}(\mathbb{P}, \mathbb{F}_q[x])_{(p)} = \{f(t)/b(x) \in \mathbb{F}_q(x)[t] \mid f(t) \in \mathcal{I},\ b(x) \in X_p \setminus \{p\}\}. \tag{4.1}$$

Then $\mathcal{I}_{(p)} = \operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)})$.

Proof We first show that $\mathcal{I} \subseteq \operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)})$. Let $f(t) \in \mathcal{I}$. Then $f(p) \in \mathbb{F}_q[x] \subseteq \mathbb{F}_q[x]_{(p)}$, and by Proposition 4.1, $f(h) \in \mathbb{F}_q[x]_{(p)}$ for all $h \in \mathbb{F}_q[x] \setminus p\mathbb{F}_q[x]$. Thus, $\mathcal{I} \subseteq \operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)})$. This inclusion and [3, Proposition I.2.7] show that $\mathcal{I}_{(p)} \subseteq \operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)})_{(p)} = \operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)})$.

Since $\mathbb{P} \subseteq X_p$, we have $\operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)}) \subseteq \operatorname{Int}(\mathbb{P}, \mathbb{F}_q[x]_{(p)})$. By [3, Proposition I.2.7] again, we obtain $\operatorname{Int}(\mathbb{P}, \mathbb{F}_q[x]_{(p)}) = \mathcal{I}_{(p)}$. Thus, $\operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)}) \subseteq \mathcal{I}_{(p)}$. □

4.1. Localized bases

Throughout this subsection, let $p := p(x)$ be a prime of degree d. Let

$$\{c_0^{(p)} = 0, c_1^{(p)}, \ldots, c_{q^d-1}^{(p)}\}$$

be a complete set of residue classes of $\mathbb{F}_q[x]$ modulo p. Define the sequence $\{c_n^{(p)}\}_{n \geq q^d}$ by

$$c_n^{(p)} = c_{n_0}^{(p)} + c_{n_1}^{(p)} p + \cdots + c_{n_s}^{(p)} p^{n_s},$$

where $n = n_0 + n_1 q^d + \cdots + n_s q^{ds} \geq q^d$ is the base-q^d representation of n. Define a corresponding sequence $\{b_n^{(p)}\}_{n \geq 0} \subseteq \mathbb{F}_q[x]$ by

$$b_0^{(p)} = p, \quad b_n^{(p)} = c^{(p)}_{n + \left\lfloor \frac{n-1}{q^d-1} \right\rfloor} \qquad (n \geq 1). \tag{4.2}$$

For brevity, throughout this section, since p is fixed, we replace $c_n^{(p)}$ by c_n and $b_n^{(p)}$ by b_n. For ease of comprehension, we list all the elements in the sequence $\{c_n\}_{n \geq 0}$ in the following ordering manner.

$$\begin{array}{cccc}
0 & c_1 & \cdots & c_{q^d-1} \\
\hline
c_{q^d} = c_1 p & c_{q^d+1} = c_1 p + c_1 & \cdots & c_{2q^d-1} = c_1 p + c_{q^d-1} \\
c_{2q^d} = c_2 p & c_{2q^d+1} = c_2 p + c_1 & \cdots & c_{3q^d-1} = c_2 p + c_{q^d-1} \\
\vdots & \vdots & \ddots & \vdots \\
c_{(q^d-1)q^d} = c_{q^d-1} p & c_{(q^d-1)q^d+1} = c_{q^d-1} p + c_1 & \cdots & c_{q^{2d}-1} = c_{q^d-1} p + c_{q^d-1} \\
\hline
c_{q^{2d}} = c_1 p^2 & c_{q^{2d}+1} = c_1 p^2 + c_1 & \cdots & c_{q^{2d}+q^d-1} = c_1 p^2 + c_{q^d-1} \\
c_{q^{2d}+q^d} = c_1 p^2 + c_1 p & c_{q^{2d}+q^d+1} = c_1 p^2 + c_1 p + c_1 & \cdots & c_{q^{2d}+2q^d-1} = c_1 p^2 + c_1 p + c_{q^d-1} \\
c_{q^{2d}+2q^d} = c_1 p^2 + c_2 p & c_{q^{2d}+2q^d+1} = c_1 p^2 + c_2 p + c_1 & \cdots & c_{q^{2d}+3q^d-1} = c_1 p^2 + c_2 p + c_{q^d-1} \\
\vdots & \vdots & \ddots & \vdots \\
c_{(q^d-1)q^{2d}+(q^d-1)q^d} & c_{(q^d-1)q^{2d}+(q^d-1)q^d+1} & \cdots & c_{q^{3d}-1} \\
= c_{q^d-1} p^2 + c_{q^d-1} p & = c_{q^d-1} p^2 + c_{q^d-1} p + c_1 & \cdots & = c_{q^d-1} p^2 + c_{q^d-1} p + c_{q^d-1} \\
\hline
\vdots & & &
\end{array}$$

From the array, the first line contains all complete residue classes modulo p, while the second and third parts separated by the following two lines contain all complete residue classes modulo p^2 and p^3, respectively.

Observe that when we delete the first column of the array, the remaining entries give an ordering of the sequence $\{b_n\}_{n\geq 1}$.

The sequence $\{b_n\}_{n\geq 1}$ contains all polynomials which are relatively prime to p. To see this, assume that there exists $n \in \mathbb{N}$ such that $b_n = c_{n+\lfloor (n-1)/(q^d-1)\rfloor}$ is a multiple of p. This implies that the subscript belongs to the first column of the array, i.e. $n + \lfloor (n-1)/(q^d-1)\rfloor = q^d \cdot m$ for some $m \in \mathbb{N}$. If $q^d - 1 \mid n$, then $n = (q^d-1)\ell$ for some $\ell \in \mathbb{N}$. We then have $\ell - 1 = \lfloor (n-1)/(q^d-1)\rfloor = q^d m - (q^d-1)\ell$, and so $q^d\ell = q^d m + 1$, a contradiction. If $q^d - 1 \nmid n$, then $n = (q^d-1)\ell' + r$ for some $\ell' \in \mathbb{N}$ and $r \in \{1, 2, \ldots, q^d - 2\}$. Thus, $\ell' = \lfloor (n-1)/(q^d-1)\rfloor = q^d m - (q^d-1)\ell' - r$, and so $q^d\ell' = q^d m - r$, a contradiction.

A useful characterization of the sequence $\{b_n\}_{n\geq 0}$ is given in the next proposition. To do so, define

$$w_p(0) = 0, \quad w_p(n) = \sum_{i\geq 0} \left\lfloor \frac{n-1}{q^{di}(q^d-1)} \right\rfloor \quad (n \geq 1). \tag{4.3}$$

Proposition 4.3 *For each $n > 0$, we have $\nu_p\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) = w_p(n)$.*

Proof Since $b_n \not\equiv b_0 = p \pmod{p}$, we have $\nu_p(b_n - b_0) = 0$. This implies that

$$\nu_p\left(\prod_{i=0}^{n-1}(b_n - b_i)\right) = \nu_p\left(\prod_{i=1}^{n-1}(b_n - b_i)\right). \tag{4.4}$$

Note that the sequence $\{b_i\}_{1\leq i\leq q^d-1}$ contains all residue classes modulo p except the class 0. Moreover, for each $i \in \{1, \ldots, q^d - 1\}$, we have

$$b_i = c_i \equiv c_{i+rq^d} = b_{i+r(q^d-1)} \pmod{p} \quad (r \in \mathbb{N}_0).$$

This implies that the $\{b_i\}_{1+r(q^d-1)\leq i\leq (r+1)(q^d-1)}$ also contains all residue classes modulo p except the class 0. Thus, the number of factors $(b_n - b_i)$ in (4.4) satisfying $\nu_p(b_n - b_i) \geq 1$ $(1 \leq i \leq n-1)$ is $\lfloor (n-1)/(q^d-1)\rfloor$. In general, consider the case of the modulo p^m $(m \in \mathbb{N})$. We first observe that $\{c_i\}_{0\leq i\leq q^{md}-1}$ is a complete set of residue classes modulo p^m. Since $\{c_0, c_{q^d}, \ldots, c_{(q^{(m-1)d}-1)q^d}\}$ is the set of all elements in $\{c_i\}_{0\leq i\leq q^{md}-1}$ each of which is a multiple of p, we deduce that there are $q^{md} - q^{(m-1)d} = q^{(m-1)d}(q^d-1)$ elements in $\{c_i\}_{0\leq i\leq q^{md}-1}$ that are relatively prime to p which in turn shows that $\{b_i\}_{1\leq i\leq q^{(m-1)d}(q^d-1)}$ contains all residue classes which are relatively prime to p modulo p^m. Note also that, for each $i \in \{1, 2, \ldots, q^{d(m-1)}(q^d-1)\}$ and $r \in \mathbb{N}$, modulo p^m we have

$$\begin{aligned} b_i = c_{i+\left\lfloor \frac{i-1}{q^d-1}\right\rfloor} &\equiv c_{i+\left\lfloor \frac{i-1}{q^d-1}\right\rfloor + rq^{md}} = c_{i+rq^{(m-1)d}(q^d-1)+\left\lfloor \frac{i-1}{q^d-1}\right\rfloor + \frac{rq^{(m-1)d}(q^d-1)}{q^d-1}} \\ &= c_{i+rq^{(m-1)d}(q^d-1)+\left\lfloor \frac{i+rq^{(m-1)d}(q^d-1)-1}{q^d-1}\right\rfloor} = b_{i+rq^{(m-1)d}(q^d-1)}. \end{aligned}$$

It follows that $\{b_i\}_{1+rq^{(m-1)d}(q^d-1)\leq i\leq (r+1)q^{(m-1)d}(q^d-1)}$ contains all residue classes relatively prime to p modulo p^m. Thus, the number of factors $(b_n - b_i)$ in (4.4) such that $\nu_p(b_n - b_i) \geq m$ $(1 \leq i \leq n-1)$ for all $m \in \mathbb{N}$ is equal to $\lfloor (n-1)/q^{(m-1)d}(q^d-1) \rfloor$, and so

$$\nu_p\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) = \sum_{k\geq 0}\left\lfloor \frac{n-1}{q^{dk}(q^d-1)} \right\rfloor = w_p(n).$$

□

Now, we recall the notion of p-ordering due to Bhargava and one of its important consequences, [1], [2], [7], [8].

Definition 4.4 *A sequence $\{s_n\}_{n\geq 0}$ of elements of X_p is a p-ordering of X_p, if for all $a \in X_p$, one has*

$$\nu_p\left(\prod_{i=0}^{n-1}(s_n - s_i)\right) \leq \nu_p\left(\prod_{i=0}^{n-1}(a - s_i)\right) \quad (n \geq 1), \tag{4.5}$$

and s_0 can be chosen arbitrarily in X_p.

Proposition 4.5 *[7, Section 4.1, Obs 1] Let $p \in \mathbb{P}$. Any two p-orderings $\{s_n\}_{n\geq 0}$ and $\{s'_n\}_{n\geq 0}$ of X_p result in the same minimal condition:*

$$\nu_p\left(\prod_{i=0}^{n-1}(s_n - s_i)\right) = \nu_p\left(\prod_{i=0}^{n-1}(s'_n - s'_i)\right) \quad (n \geq 1).$$

Our sequence $\{b_n\}_{n\geq 0}$ so constructed in (4.2) above is indeed a p-ordering as we now verify.

Proposition 4.6 *The sequence $\{b_n\}_{n\geq 0}$ is a p-ordering of X_p.*

Proof Let $a \in X_p$. Since $\{b_n\}_{n\geq 0}$ contains the prime p and all polynomials which are relatively prime to p and $X_p = (\mathbb{F}_q[x] \setminus p\mathbb{F}_q[x]) \cup \{p\}$, we have $a = b_m$ for some $m \geq 0$. Let $n \in \mathbb{N}$. There are three possible cases.
Case 1: $m < n$. Then $\prod_{i=0}^{n-1}(a - b_i) = 0$ and so $\nu_p\left(\prod_{i=0}^{n-1}(b_n - b_i)\right) < \nu_p\left(\prod_{i=0}^{n-1}(a - b_i)\right)$.
Case 2: $m = n$. Then $\prod_{i=0}^{n-1}(a - b_i) = \prod_{i=0}^{n-1}(b_n - b_i)$.
Case 3: $m > n$. Since the elements $b_0, b_1, \ldots, b_{n-1}$ precede the element $a = b_m$ in the above array, we deduce that the number of i such that $\nu_p(b_n - b_i) \geq r$ $(1 \leq i \leq n-1)$ is not more than the number of j such that $\nu_p(a - b_j) \geq r$ $(1 \leq j \leq n-1)$, and so $\nu_p\left(\prod_{i=0}^{n-1}(b_n - b_i)\right) \leq \nu_p\left(\prod_{i=0}^{n-1}(a - b_i)\right)$ and the result follows from Definition 4.4. □

Combining Propositions 4.3, 4.5, and 4.6, we immediately obtain:

Proposition 4.7 *A sequence $\{s_n\}_{n\geq 0}$ of elements of X_p is a p-ordering if and only if*

$$w_p(n) = \nu_p\left(\prod_{i=0}^{n-1}(s_n - s_i)\right) \quad (n \geq 1).$$

We are now ready to construct explicit bases of the localized module $\mathcal{I}_{(p)}$ defined in (4.1). For each $p \in \mathbb{P}$, define the polynomials $C_n^p(t)$ and $G_n^p(t)$ by

$$C_0^p(t) = 1, \quad C_n^p(t) = \frac{1}{p^{w_p(n)}} \prod_{0 \le i < n} (t - b_i) \quad (n \ge 1), \tag{4.6}$$

and

$$G_0^p(t) = 1, \quad G_n^p(t) = \prod_{0 \le i < n} \frac{t - b_i}{b_n - b_i} \quad (n \ge 1). \tag{4.7}$$

Theorem 4.8 *The sequences $\{C_n^p(t)\}_{n \ge 0}$ and $\{G_n^p(t)\}_{n \ge 0}$ are two regular bases of the $\mathbb{F}_q[x]_{(p)}$-module $\mathcal{I}_{(p)}$.*

Proof By (4.6) and (4.7), $C_n^p(p) = 0 = G_n^p(p)$. By Proposition 4.3 and the inequality (4.5), $C_n^p(a)$ and $G_n^p(a)$ are in $\mathbb{F}_q[x]_{(p)}$ for all $a \in X_p$. It follows that $C_n^p(t)$ and $G_n^p(t)$ belong to $\operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)})$.

Let $f(t) \in \operatorname{Int}(X_p, \mathbb{F}_q[x]_{(p)})$ with degree n. Then, we can write

$$f(t) = \sum_{i=0}^{n} \alpha_i C_i^p(t) = \sum_{i=0}^{n} \gamma_i G_i^p(t) \quad (\alpha_i, \gamma_i \in \mathbb{F}_q(x)). \tag{4.8}$$

It remains to show that $\alpha_i, \gamma_i \in \mathbb{F}_q[x]_{(p)}$. To do so, consider $C_i^p(b_k)$ and $G_i^p(b_k)$. For fixed $i \in \{1, \ldots, n\}$, we have

$$C_i^p(b_k) = 0 = G_i^p(b_k) \quad (0 \le k < i).$$

Since $G_i^p(b_i) = 1$ and $\nu_p(C_i^p(b_i)) = 0$, we have $(G_i^p(b_i))^{-1}$ and $(C_i^p(b_i))^{-1} \in \mathbb{F}_q[x]_{(p)}$. Substituting $t = b_0, b_1, b_2, \ldots$, we get

$$\alpha_0 = f(b_0) \in \mathbb{F}_q[x]_{(p)}, \; \alpha_1 = (C_1^p(b_1))^{-1}(f(b_1) - \alpha_0) \in \mathbb{F}_q[x]_{(p)},$$

$$\alpha_2 = (C_2^p(b_2))^{-1}(f(b_2) - \alpha_0 - \alpha_1 C_1^p(b_2)) \in \mathbb{F}_q[x]_{(p)}.$$

Continuing this process, we obtain that $\alpha_i \in \mathbb{F}_q[x]_{(p)}$ for all i.

The proof for $\{G_i^p(t)\}_{i \ge 0}$ is similar. □

The next theorem provides a method of obtaining a new basis from an old one.

Theorem 4.9 *Let $p \in \mathbb{P}$, $n \in \mathbb{N}$, and let $\{b_i\}_{i \ge 0}$ be the sequence defined in (4.2). For fixed $j \in \mathbb{N}_0$ with $0 \le j < n$, define*

$$m = m(p, j, n) := \begin{cases} \max\{\nu_p(b_k - b_j) \mid 0 \le k \le n, \; k \ne j\}, & 0 < j < n \\ 0, & j = 0 \end{cases}.$$

Let $C_n^p(t)$ be the n-th polynomial as defined in (4.6) in the regular basis $\mathcal{B} = \{C_n^p(t)\}_{n \ge 0}$ of the $\mathbb{F}_q[x]_{(p)}$-module $\mathcal{I}_{(p)}$. If $\beta_j \in X_p$ satisfies $\nu_p(\beta_j - b_j) > m$, then the set

$$\mathcal{C} := \left(\mathcal{B} \setminus \{C_n^p(t)\}\right) \cup \left(\frac{t - \beta_j}{t - b_j} \cdot C_n^p(t)\right)$$

is also a regular basis of $\mathbb{F}_q[x]_{(p)}$-module $\mathcal{I}_{(p)}$.

Proof To show that $\mathcal{C}$ is a regular basis whose n-th polynomial is

$$C'_n := \frac{t-\beta_j}{t-b_j} \cdot C^p_n(t) = \frac{t-\beta_j}{p^{w_p(n)}} \prod_{\substack{0\le i<n \\ i\ne j}} (t-b_i),$$

by Proposition 2.2, we need to check two assertions (i) $C'_n(t) \in \mathcal{I}_{(p)}$ and (ii) the leading coefficient of the polynomial $C'_n(t)$ generates the the n-th characteristic ideal $I_{\mathcal{I}}(n)$.

As $\nu_p(b_i-\beta_j) > m$, we can write $\beta_j = b_j + ep^{m+1}$ for some $e \in \mathbb{F}_q[x]$. For each $0 \le k \le n$ and $j \ne k$, we get

$$\nu_p(b_k-\beta_j) = \nu_p(b_k-b_j-p^{m+1}e) = \min\{\nu_p(b_k-b_j), \nu_p(p^{m+1}e)\} = \nu_p(b_k-b_j). \tag{4.9}$$

Consider the sequence $\{b_0, b_1, \dots, b_{j-1}, \beta_j, b_{j+1}, \dots, b_n\}$. Since $\{b_0, b_1, \dots, b_{j-1}\}$ contains the first j elements of some p-ordering of X_p, it remains to show that $\{\beta_j, b_{j+1}, \dots, b_n\}$ is the set of succeeding elements in a p-ordering. By (4.9), we have

$$\nu_p\left(\prod_{0\le i\le j-1} (\beta_j - b_i)\right) = \nu_p\left(\prod_{0\le i\le j-1} (b_j - b_i)\right) = w_p(j),$$

and

$$\nu_p\left(\prod_{\substack{0\le i\le \ell-1 \\ i\ne j}} (b_\ell - b_i)\right) + \nu_p(b_\ell-\beta_j) = \nu_p\left(\prod_{0\le i\le \ell-1} (b_\ell - b_i)\right) = w_p(\ell) \quad (i<\ell\le n).$$

By Proposition 4.7, the set $\{b_0, b_1, \dots, b_{j-1}, \beta_j, b_{j+1}, \dots, b_n\}$ contains the first $n+1$ elements of some p-ordering on X_p possibly different from the previous one. This implies that

$$w_p(n) = \nu_p\left(\prod_{\substack{0\le i\le n-1 \\ i\ne j}} (b_n - b_i)\right) + \nu_p(b_n-\beta_j) \le \nu_p\left(\prod_{\substack{0\le i\le n-1 \\ i\ne j}} (a - b_i)\right) + \nu_p(a-\beta_j) \quad (a \in X_p).$$

Thus, $C'_n(t) \in \mathcal{I}_{(p)}$, which proves assertion (i).

The leading coefficients of both polynomials $C^p_n(t)$ and $C'_n(t)$ are equal to $1/p^{w_p(n)}$ which is a generator of $I_{\mathcal{I}}(n)$, i.e. assertion (ii) holds. □

The proof of Theorem 4.8 immediately yields the following result which provides a convenient checking whether a polynomial is an integer-valued polynomial.

Corollary 4.10 *Let $f(t) \in \mathbb{F}_q(x)[t]$ of degree n. Then f belongs to $\mathrm{Int}(\mathbb{P}, (\mathbb{F}_q[x])_{(p)}$ if and only if $f(b_i)$ belongs to $(\mathbb{F}_q[x])_{(p)}$ for all $i = 0, 1, \dots, n$.*

To illustrate the notation and concepts used in the last section, we work out two examples.

Example 4.11 *The following table lists all elements of the bases $C^p_n(t)$ of $\mathrm{Int}(X_p, \mathbb{F}_3[x]_{(p)})$ for $1 \le n \le 4$ and $p = x,\ x+1,\ x+2$.*

$p = x$	$p = x+1$	$p = x+2$
$C_1^p(t) = t - x$ $C_2^p(t) = (t-x)(t-1)$ $C_3^p(t) = \frac{(t-x)(t-1)(t-2)}{x}$ $C_4^p(t) = \frac{(t-x)(t-1)(t-2)(t-x-1)}{x}$	$C_1^p(t) = t - x - 1$ $C_2^p(t) = (t-x-1)(t-1)$ $C_3^p(t) = \frac{(t-x-1)(t-1)(t-2)}{x+1}$ $C_4^p(t) = \frac{(t-x-1)(t-1)(t-2)(t-x-2)}{x+1}$	$C_1^p(t) = t - x - 2$ $C_2^p(t) = (t-x-2)(t-1)$ $C_3^p(t) = \frac{(t-x-2)(t-1)(t-2)}{x+2}$ $C_4^p(t) = \frac{(t-x-2)(t-1)(t-2)(t-x)}{x+2}$

Example 4.12 *Keep the above notation and the polynomials in Example 4.11. Recall that $m(p,j,n)$ is defined as in Theorem 4.9.*

1. *For each $n \in \mathbb{N}, p \in \mathbb{P}$, since $m(p,0,n) = 0$, we can replace b_0 in the polynomial $C_n^p(t)$ by β_0 satisfying the relation*
$$\beta_0 \equiv b_0 = p \pmod{p^1}.$$
2. *Since $m(x,3,4) = 1$, we can replace b_3 in the polynomial $C_4^x(t)$ by β_3 satisfying the relation*
$$\beta_3 \equiv b_3 = x+1 \pmod{x^2}.$$
3. *Since $m(x+1,3,4) = 1$, we can replace b_3 in the polynomial $C_4^{x+1}(t)$ by β_3 satisfying the relation*
$$\beta_3 \equiv b_3 = x+2 \pmod{(x+1)^2}.$$
4. *Since $m(x+2,3,4) = 1$, we can replace b_3 in the polynomial $C_4^{x+2}(t)$ by β_3 satisfying the relation*
$$\beta_3 \equiv b_3 = x \pmod{(x+2)^2}.$$

5. Explicit bases

To characterize the characteristic ideal of the set $\mathcal{I}$, we need the following lemma.

Lemma 5.1 *For $p \in \mathbb{P}$, one has $I_{\mathcal{I}_{(p)}}(n) = (I_{\mathcal{I}}(n))_{(p)}$ where*
$$(I_{\mathcal{I}}(n))_{(p)} := \left\{ \frac{A}{b} \in \mathbb{F}_q(x) \,\middle|\, A \in I_{\mathcal{I}}(n),\ b \in \mathbb{F}_q[x] \setminus p\mathbb{F}_q[x] \right\}, \tag{5.1}$$
is the localization of the characteristic ideal $I_{\mathcal{I}}(n)$ at p.

Proof Since the characteristic ideal $I_{\mathcal{I}}(n)$ is the set of leading coefficients of all polynomials of degree n in $\mathcal{I}$ including 0, by (5.1), we get
$$(I_{\mathcal{I}}(n))_{(p)} = \{0\} \cup \left\{ \frac{A}{b} \in \mathbb{F}_q(x) \,\middle|\, \exists f \in \mathcal{I} \text{ such that } f = At^n + \cdots + A_0,\ b \in \mathbb{F}_q[x] \setminus p\mathbb{F}_q[x] \right\}$$
$$= \{0\} \cup \left\{ \frac{A}{b} \in \mathbb{F}_q(x) \,\middle|\, \exists \frac{f}{b} \in \mathcal{I}_{(p)} \text{ such that } f = At^n + \cdots + A_0,\ b \in \mathbb{F}_q[x] \setminus p\mathbb{F}_q[x] \right\} = I_{\mathcal{I}_{(p)}}(n).$$
□

Returning to the module $\mathcal{I}$, we now prove our final main result.

Theorem 5.2 *For $n \geq 0$, the set of leading coefficients of the polynomials in $\mathcal{I}$ with degree $\leq n$ is the fractional ideal*

$$I_{\mathcal{I}}(n) = \prod_{p} p^{-w_p(n)} \, \mathbb{F}_q[x],$$

where the product extends over all $p \in \mathbb{P}$ such that $q^{\deg p} \leq n$, and $w_p(n)$ is as defined in (4.3)

Proof By Theorem 4.8 and Proposition 2.2, the characteristic ideal of the localized module $\mathcal{I}_{(p)}$ is $I_{\mathcal{I}_{(p)}(n)} = p^{-w_p(n)}\mathbb{F}_q[x] \quad (n \geq 0)$, and so by Lemma (5.1), $(I_{\mathcal{I}}(n))_{(p)} = p^{-w_p(n)}\mathbb{F}_q[x]$. Since $I_{\mathcal{I}}(n)$ is generated by the product of the generators of $\mathcal{I}_{(p)}$ for all $p \in \mathbb{P}$, noting that $w_p(n) = 0$ when $q^{\deg p} > n$, the result follows. □

With the globalization result in Theorem 5.2, we show now how to construct an explicit basis of $\mathcal{I}$ by exhibiting an algorithm to inductively construct elements belonging to a basis of $\mathcal{I}$. Let n be a fixed integer ≥ 0, and let

$$S_n := \{p \in \mathbb{P} \mid q^{\deg p} \leq n\}.$$

For each $p \in S_n$, let

$$\mathcal{A}_n^{(p)} = \{b_0^{(p)}, b_1^{(p)}, \ldots, b_{n-1}^{(p)}\}$$

be the sequence of polynomials as defined in (4.2) (with $b_i^{(p)}$ in place of b_i as in Subsection 4.1) corresponding to the prime p, and let $C_n^p(t) = p^{-w_p(n)} \prod_{0 \leq i < n}(t - b_i^{(p)})$ be the n-th element, as defined in (4.6), in a basis of the localized module $\mathcal{I}_{(p)}$. The following algorithm determines the n-th element $\mathcal{C}_n(t)$ belonging to a regular basis of the globalized module $\mathcal{I}$.

STEP 1: Let $\mathcal{A}_n := \bigcap_{p \in S_n} \mathcal{A}_n^{(p)}$. Note that for all $\gamma \in \mathcal{A}_n$, $t - \gamma$ is a factor of all the numerators of $C_n^p(t)$ $(p \in S_n)$. Therefore, the product $\prod_{\gamma \in \mathcal{A}_n}(t - \gamma)$ is the greatest common factor of the numerators of $C_n^p(t)$ for all $p \in S_n$.

STEP 2: If $\mathcal{A}_n^{(p)} \setminus \mathcal{A}_n \neq \emptyset$, let

$$\mathcal{A}_n^{(p)} \setminus \mathcal{A}_n := \{\delta_1^{(p)}, \delta_2^{(p)}, \ldots, \delta_{k_p}^{(p)}\},$$

and let the integer m be as defined in Theorem 4.9. For each $i \in \{1, \ldots, k_p\}$, by the Chinese remainder theorem, [9, Proposition 1.4], the system of congruences

$$\beta_i \equiv \delta_i^{(p)} \pmod{p^m} \qquad (i = 1, \ldots, k_p)$$

with the primes p running over the set S_n, is solvable for $\beta_i \in \mathbb{F}_q[x]$.

STEP 3: Set

$$\mathcal{C}_n(t) = \prod_{p \in S_n} p^{-w_p(n)} \prod_{\gamma \in \mathcal{A}_n} (t - \gamma) \prod_{i=1}^{k_p}(t - \beta_i),$$

where the last product is taken to be 1 if $\mathcal{A}_n^{(p)} \setminus \mathcal{A}_n = \emptyset$.

There remains to check that the so constructed elements $\mathcal{C}_n(t)$ form a regular basis of $\mathcal{I}$. By Theorem 4.9, we have $\mathcal{C}_n(t) \in \mathcal{I}_{(p)}$ for all $p \in S_n$. Since the denominator of $C_n^p(t)$ is not a multiple of any prime ℓ for all $\ell \in \mathbb{P} \setminus S_n$, it follows that $C_n^p(t)$ also belongs to $\mathcal{I}_{(\ell)}$ for all $\ell \in \mathbb{P} \setminus S_n$. Thus, $\mathcal{C}_n(t) \in \mathcal{I}_{(p)}$ for all $p \in \mathbb{P}$, and so $\mathcal{C}_n(t) \in \mathcal{I}$. Since the leading coefficient of $\mathcal{C}_n(t)$ is $\prod_{p \in S_n} p^{-w_p(n)}$, a generator of $I_{\mathcal{I}}(n)$, by Theorem 5.2, the polynomials $\mathcal{C}_n(t)$ $(n \geq 0)$ form a regular basis of $\mathcal{I}$.

We end this paper with an example illustrating our algorithm.

Example 5.3 *Keeping the notation of Example 4.11, for $n = 4$, we have*

$$S_4 = \{x,\ x+1,\ x+2\}.$$

Thus,

$$\mathcal{A}_4^{(x)} = \{x, 1, 2, x+1\},\ \mathcal{A}_4^{(x+1)} = \{x+1, 1, 2, x+2\},\ \mathcal{A}_4^{(x+2)} = \{x+2, 1, 2, x\}.$$

STEP 1: We have $\mathcal{A}_4 = \{1, 2\}$. The product $(t-1)(t-2)$ is the greatest common factor of the numerators of the polynomials $C_4^x(t)$, $C_4^{x+1}(t)$, $C_4^{x+2}(t)$ displayed in Example 4.11.

STEP 2: Since

$$\mathcal{A}_n^{(x)} \setminus \mathcal{A}_n = \{\delta_1^{(x)} = x,\ \delta_2^{(x)} = x+1\}$$
$$\mathcal{A}_n^{(x+1)} \setminus \mathcal{A}_n = \{\delta_1^{(x+1)} = x+1,\ \delta_2^{(x+1)} = x+2\}$$
$$\mathcal{A}_n^{(x+2)} \setminus \mathcal{A}_n = \{\delta_1^{(x+2)} = x+2,\ \delta_2^{(x+2)} = x\},$$

by Theorem 5.2, we have $I_{\mathcal{I}}(4) = (x(x+1)(x+2))^{-1}\mathbb{F}_3(x)$. Using the results in Example 4.12, the polynomial $\mathcal{C}_4(t)$ takes the form $\mathcal{C}_4(t) = \frac{(t-1)(t-2)(t-\beta_1)(t-\beta_2)}{x(x+1)(x+2)}$, where

$$\beta_1 \equiv x \pmod{x}, \quad \beta_1 \equiv x+1 \pmod{x+1}, \quad \beta_1 \equiv x+2 \pmod{x+2}$$
$$\beta_2 \equiv x+1 \pmod{x^2}, \quad \beta_2 \equiv x+2 \pmod{(x+1)^2}, \quad \beta_2 \equiv x \pmod{(x+2)^2}.$$

Solving for β_1 and β_2, we get $\beta_1 = 0$ and $\beta_2 = 2x^3 + x + 1$, and so

$$\mathcal{C}_4(t) = \frac{t(t-1)(t-2)(t-2x^3-x-1)}{x(x+1)(x+2)}.$$

Other globalized polynomials $\mathcal{C}_n(t) \in \operatorname{Int}(\mathbb{P}, \mathbb{F}_3[x])$ can be constructed in the same manner. For example, when $1 \leq n \leq 3$, we obtain

$$\mathcal{C}_1(t) = t,\ \mathcal{C}_2(t) = t(t-1),\ \mathcal{C}_3(t) = \frac{t(t-1)(t-2)}{x(x+1)(x+2)}.$$

Acknowledgment

The authors wish to thank the referee for his/her meticulous reading, comments, and suggestions.

References

[1] Adam D. Finite differences in finite characteristic. Journal of Algebra 2006; 296: 285-300. https://doi.org/10.1016/j.jalgebra.2005.05.036

[2] Bhargava M. P-orderings and polynomial functions on arbitrary subsets of Dedekind rings. Journal für die reine und angewandte Mathematik 1997; 490: 101-127. https://doi.org/10.1515/crll.1997.490.101

[3] Cahen P-J, Chabert J-L. Integer-valued Polynomials. American Mathematical Society Surveys and Monographs Providence, 1997.

[4] Carlitz L. A set of polynomials. Duke Mathematical Journal 1940; 6 (2): 486-504. https://doi.org/10.1215/S0012-7094-40-00639-1

[5] Chabert J-L, Chapman S and Smith W. A basis for the ring of polynomials integer-valued on prime numbers. Factorization in integral domains. Lecture Notes in Pure and Applied Mathematics. Dekker, New York, 1997, pp. 271-284.

[6] Chabert J-L. Integer-valued polynomials on prime numbers and logarithm of power expansion. European Journal of Combinatorics 2007; 28: 754-761. https://doi.org/10.1016/j.ejc.2005.12.009

[7] Chaichana T, Laohakosol V and Meesa R. Sequences of polynomials satisfying the Pascal property. Turkish Journal of Mathematics 2022; 46: 1565-1579. https://doi.org/10.55730/1300-0098.3180

[8] Meesa R, Laohakosol V, Chaichana T. Integer-valued polynomials satisfying Lucas property. Turkish Journal of Mathematics 2021; 45: 1459-1478. https://doi.org/10.3906/mat-2102-104

[9] Rosen M. Number Theory in Function Fields. Springer, New York, 2002.