

Polynômes à valeurs entières ainsi que leurs dérivées en caractéristique p

par

DAVID ADAM (Tahiti)

1. Introduction. Soit D un anneau intègre de corps des fractions K et S un sous-ensemble de D . On note $\text{Int}(S, D)$ (ou plus simplement $\text{Int}(D)$ si $S = D$) le D -module des polynômes à valeurs entières sur S relativement à D :

$$\text{Int}(S, D) = \{P \in K[X] \mid P(S) \subset D\}.$$

Il est bien connu (voir [3]) que les polynômes binomiaux

$$\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}$$

forment une base de $\text{Int}(\mathbb{Z})$. De même, on note $\text{Int}^{(\infty)}(S, D)$ (ou plus simplement $\text{Int}^{(\infty)}(D)$ si $S = D$) le D -module des polynômes à valeurs entières sur S relativement à D ainsi que toutes leurs dérivées :

$$\text{Int}^{(\infty)}(S, D) = \{P \in K[X] \mid \forall \sigma \in \mathbb{N} P^{(\sigma)}(S) \subset D\}.$$

En 1951, Straus a décrit une base de $\text{Int}^{(\infty)}(\mathbb{Z})$:

THÉORÈME 1.1 ([11]). *Les polynômes*

$$\prod_{p \text{ premier}} p^{[n/p]} \binom{X}{n} \quad (n \in \mathbb{N})$$

forment une base de $\text{Int}^{(\infty)}(\mathbb{Z})$.

En 1998, Laohakosol s'est intéressé au cas $D = \mathbb{F}_q[T]$. Dans la suite, on note $D^* = D \setminus \{0\}$. Soient $h \in D^*$ et $f \in K[X]$. On appelle *première différence finie de f par rapport à h* le polynôme

$$\Delta_h(f)(X) = \frac{f(X+h) - f(X)}{h}.$$

2010 *Mathematics Subject Classification*: Primary 13F20.

Key words and phrases: integer-valued polynomials.

Par récurrence, pour $h_1, \dots, h_k \in D^*$, on définit la *différence finie d'ordre k de f par rapport à h_1, \dots, h_k* :

$$\Delta_{h_1, \dots, h_k}(f)(X) = \Delta_{h_k}(\Delta_{h_{k-1}, \dots, h_1}(f))(X).$$

L'ensemble des polynômes à valeurs entières sur D ainsi que toutes leurs différences finies est noté $\text{Int}^{[\infty]}(D)$:

$$\text{Int}^{[\infty]}(D) = \{P \in \text{Int}(D) \mid \forall k \in \mathbb{N}^* \forall h_1, \dots, h_k \in D^* \Delta_{h_1, \dots, h_k}(P)(D) \subset D\}.$$

Dans [10, Theorem 5], Laohakosol formule l'égalité

$$(1.1) \quad \text{Int}^{(\infty)}(\mathbb{F}_q[T]) = \text{Int}^{[\infty]}(\mathbb{F}_q[T]).$$

Connaissant une base de $\text{Int}^{[\infty]}(\mathbb{F}_q[T])$ (voir [12] ou [1]), il en déduit une base de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$ [10, Corollary 4]. Cependant, l'égalité (1.1) est fautive. Dans la Section 2, on donnera l'exemple d'un polynôme appartenant à $\text{Int}^{[\infty]}(\mathbb{F}_q[T])$ mais non à $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$. Plus fondamentalement, Chabert a caractérisé dans [6] les anneaux noethériens intègres D pour lesquels on a l'égalité $\text{Int}^{[\infty]}(D) = \text{Int}^{(\infty)}(D)$. En particulier, un tel anneau est de caractéristique 0. Par conséquent, une base de $\text{Int}^{[\infty]}(\mathbb{F}_q[T])$ n'est pas une base de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$.

DÉFINITION 1.2.

(1) Soit B un anneau tel que $D[X] \subset B \subset K[X]$. Pour tout $n \in \mathbb{N}$, on appelle *n -ième idéal caractéristique de B* l'idéal

$$J_n(B) = \{0\} \cup \{\alpha \in K \mid \exists f \in B \text{ avec } f = \alpha X^n + \alpha_{n-1} X^{n-1} + \dots\}.$$

(2) Quand B est un D -module libre, une base $(P_n(X))_{n \in \mathbb{N}}$ de B est une *base régulière de B* si, pour tout $n \in \mathbb{N}$, $\text{deg } P_n = n$.

Dorénavant, nous supposons que D est un anneau de Dedekind de caractéristique $p > 0$ à corps résiduel fini. Dans la Section 2, nous décrivons les idéaux caractéristiques de $\text{Int}^{(\infty)}(S, D)$. Dans le cas où $\text{Int}(S, D)$ admet une base régulière, nous construisons une base régulière de $\text{Int}^{(\infty)}(S, D)$. Comme application, nous obtenons une base régulière de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$, corrigeant ainsi l'énoncé de [10, Corollary 4]. Dans la Section 3, nous supposons que D contient $\mathbb{F}_q[T]$ et nous considérons une autre sorte de dérivée : à chaque $a \in \mathbb{F}_q[T]$, on associe un opérateur "dérivée a -ième" δ_a sur $K[X]$. On note $\text{Int}^{(\infty)}(S, D)$ (ou plus simplement $\text{Int}^{(\infty)}(D)$ si $S = D$) l'ensemble

$$\text{Int}^{(\infty)}(S, D) = \{P \in K[X] \mid \forall a \in \mathbb{F}_q[T] (\delta_a(P))(S) \subset D\}.$$

Dans les cas où $S = \mathbb{F}_q$ ou $S = \mathbb{F}_q[T]$, une base régulière de $\text{Int}^{(\infty)}(S, \mathbb{F}_q[T])$ est explicitée, donnant alors un résultat très analogue au théorème 1.1.

2. Bases de $\text{Int}^{(\infty)}(S, D)$

NOTATIONS

- (1) Rappelons que D est un anneau de Dedekind à corps résiduel fini de caractéristique $p > 0$, de corps de fractions K , et S est un sous-ensemble de D .
- (2) Pour tout $i, j \in \mathbb{N} \times \mathbb{N} \cup \{+\infty\}$, on note $\llbracket i, j \rrbracket$ (resp. $\llbracket i, j \llbracket$) l'ensemble des entiers compris entre i et j (resp. compris entre i et j et strictement plus petits que j).

REMARQUE 2.1. Soit $P \in K[X]$. Pour tout $\sigma \in \llbracket p, +\infty \llbracket$ on a $P^{(\sigma)} = 0$ et donc $P \in \text{Int}^{(\infty)}(S, D)$ si et seulement si pour tout $\sigma \in \llbracket 0, p - 1 \llbracket$ on a $P^{(\sigma)}(S) \subset D$. De plus, pour tout $(Q, \sigma) \in K[X] \times \mathbb{N}$, on a

$$(2.1) \quad (P^p Q)^{(\sigma)}(X) = P(X)^p Q^{(\sigma)}(X).$$

Par suite, si $P \in \text{Int}(S, D)$ et $Q \in \text{Int}^{(\infty)}(S, D)$, alors $P^p Q \in \text{Int}^{(\infty)}(S, D)$.

NOTATIONS. Soit $L \in \mathbb{N}$. On pose

- (1) $K_L[X] = \{f \in K[X] \mid \deg f < L\}$,
- (2) $\text{Int}_L(S, D) = \text{Int}(S, D) \cap K_L[X]$,
- (3) $\text{Int}_L^{(\infty)}(S, D) = \text{Int}^{(\infty)}(S, D) \cap K_L[X]$.

2.1. Cas où D est un anneau de valuation discrète. Comme dans [3, Theorem IX.3.5], on montre que $\text{Int}^{(\infty)}(S, D)$ se comporte bien par localisation : pour tout $\mathfrak{m} \in \text{Max}(D)$,

$$\text{Int}^{(\infty)}(S, D)_{\mathfrak{m}} = \text{Int}^{(\infty)}(S, D_{\mathfrak{m}}).$$

On peut donc se restreindre au cas $D = V$, l'anneau d'une valuation discrète v . On note t un paramètre local de V . Pour décrire des bases régulières de $\text{Int}(S, V)$, la notion de suite v -ordonnée introduite par Bhargava est très utile.

DÉFINITION 2.2 ([2]). Soit $(u_n)_{n \in \mathbb{N}}$ une suite d'éléments distincts de S .

- (1) Soit $L \in \mathbb{N}$. La suite $(u_n)_{n \in \mathbb{N}}$ est une *suite v -ordonnée de S de longueur L* si

$$\forall j \in \llbracket 0, L \llbracket \forall x \in V \quad v\left(\prod_{k=0}^{j-1} (u_j - u_k)\right) \leq v\left(\prod_{k=0}^{j-1} (x - u_k)\right).$$

- (2) La suite $(u_n)_{n \in \mathbb{N}}$ est une *suite v -ordonnée de S* si elle est v -ordonnée de longueur L pour tout $L \in \mathbb{N}$.

REMARQUE 2.3. Si S est infini, il existe toujours des suites v -ordonnées de S . Si S est fini de cardinal s , il n'existe des suites v -ordonnées de S que de longueur au plus s .

PROPOSITION 2.4 ([2]). Soient $(u_n)_{n \in \mathbb{N}}$ une suite d'éléments de S et $L \in \mathbb{N}$. La suite $(u_n)_{n \in \mathbb{N}}$ est une suite v -ordonnée de longueur L de S si et seulement si les polynômes

$$H_n(X) := \prod_{j=0}^{n-1} \frac{X - u_j}{u_n - u_j} \quad (0 \leq n < L)$$

forment une base régulière de $\text{Int}_L(S, V)$.

On déduit de la proposition 2.4 que si $(u_n)_{0 \leq n < L}$ est une suite v -ordonnée de S de longueur L , alors pour tout $n \in \llbracket 0, L \rrbracket$, la quantité

$$v\left(\prod_{j=0}^{n-1} (u_n - u_j)\right)$$

ne dépend pas du choix de la suite v -ordonnée considérée.

DÉFINITION 2.5. Soit $(u_n)_{0 \leq n < L}$ une suite v -ordonnée de S de longueur L . On appelle suite caractéristique de S la suite $(w_S(n))_{0 \leq n < L}$ définie par

$$\forall n \in \llbracket 0, L \rrbracket \quad w_S(n) = v\left(\prod_{j=0}^{n-1} (u_n - u_j)\right).$$

Pour tout $n \in \llbracket 0, L - 1 \rrbracket$ on a

$$J_n(\text{Int}(S, V)) = t^{-w_S(n)}V.$$

THÉORÈME 2.6. Soit $(u_n)_{0 \leq n < L}$ une suite v -ordonnée de S de longueur L . À chaque $n \in \llbracket 0, p(L + 1) \rrbracket$ écrit sous la forme $n = ps + r$ ($r, s \in \mathbb{N}$, $r < p$) on associe le polynôme

$$P_n(X) = H_s(X)^p (X - u_s)^r \quad \text{où} \quad H_s(X) = \prod_{j=0}^{s-1} \frac{X - u_j}{u_s - u_j}.$$

Alors, les P_n forment une base régulière de $\text{Int}_{(L+1)p}^{(\infty)}(S, D)$.

Démonstration. Les polynômes $P_n(X)$ ($n \in \llbracket 0, p(L + 1) \rrbracket$) forment une base de $K_{p(L+1)}[X]$. D'après la remarque 2.1, ils sont dans $\text{Int}^{(\infty)}(S, V)$. Soit $P \in \text{Int}_{p(L+1)}^{(\infty)}(S, V)$, écrivons

$$P(X) = \sum_{k=0}^{\deg P} a_k P_k(X) \quad \text{avec } a_k \in K \text{ pour tout } k \in \llbracket 0, \deg P \rrbracket.$$

On a $P(u_0) = a_0 \in V$. Montrons par récurrence que les $a_k \in V$. Soit $k \in \llbracket 0, \deg P \rrbracket$ écrit sous la forme $k = ps + r$ ($r, s \in \mathbb{N}$, $r < p$). Alors

$$P^{(r)}(u_s) = \sum_{j=0}^{k-1} a_j P_j^{(r)}(u_s) + r! a_k H_s(u_s)^p.$$

Comme $H_s(u_s) = 1$, $r!$ est inversible dans V et $\sum_{j=0}^{k-1} a_j P_j^{(r)}(u_s) \in V$, on en déduit que $a_k \in V$. ■

COROLLAIRE 2.7. *Si $\text{Card } S \geq L$, alors pour tout $n < p(L + 1)$, on a*

$$J_n(\text{Int}^{(\infty)}(S, V)) = t^{-ws([n/p])}V.$$

PROPOSITION 2.8. *Supposons que S est de cardinal fini s . Alors*

$$\text{Int}^{(\infty)}(S, V) = \text{Int}_{ps}^{(\infty)}(S, V) \oplus H_s(X)^p K[X],$$

et pour tout $n \in \llbracket ps, +\infty \llbracket$,

$$J_n(\text{Int}^{(\infty)}(S, V)) = K.$$

Démonstration. Soit $P \in K[X]$,

$$P(X) = H_s(X)^p Q(X) + R(X) \quad \text{avec } Q, R \in K[X] \text{ et } \text{deg } R < ps.$$

Pour tout $(c, \sigma) \in S \times \mathbb{N}$ on a $(H_s^p)^{(\sigma)}(c) = 0$. Par conséquent, $P \in \text{Int}^{(\infty)}(S, V)$ si et seulement si $R \in \text{Int}^{(\infty)}(S, V)$. La deuxième partie de la proposition est une conséquence immédiate de la première. ■

2.2. Globalisation. Maintenant, D est un anneau de Dedekind et pour tout idéal maximal \mathfrak{m} de D , on note $w_{S,\mathfrak{m}}$ la suite caractéristique de S considérée comme un sous-ensemble de l'anneau de valuation discrète $D_{\mathfrak{m}}$. On commence par le cas où S est fini, de cardinal s .

THÉORÈME 2.9. *Soit D un anneau de Dedekind de caractéristique $p > 0$ et S un sous-ensemble de D de cardinal s .*

(1) *On a*

$$\text{Int}^{(\infty)}(S, D) = \text{Int}_{ps}^{(\infty)}(S, D) \oplus \prod_{c \in S} (X - c)^p K[X].$$

(2) *Pour tout $n \in \mathbb{N}$ le n -ième idéal caractéristique de $\text{Int}^{(\infty)}(S, D)$ est*

$$J_n(\text{Int}^{(\infty)}(S, D)) = \begin{cases} \prod_{\mathfrak{m} \in \text{Max}(D)} \mathfrak{m}^{w_{S,\mathfrak{m}}([n/p])} & \text{si } n < ps, \\ K & \text{si } n \geq ps. \end{cases}$$

(3) *Les polynômes*

$$V_{c,j}(X) = \left(\prod_{\substack{a \in S \\ a \neq c}} \frac{X - a}{c - a} \right)^p X^j, \quad \text{où } c \in S \text{ et } j \in \llbracket 0, p - 1 \llbracket,$$

forment une base de $\text{Int}_{ps}^{(\infty)}(S, D)$.

Démonstration. Les deux premières assertions sont des conséquences immédiates du corollaire 2.7 et de la proposition 2.8. Montrons que les polynômes $V_{c,j}$ ($c \in S$, $j \in \llbracket 0, p \llbracket$) forment une base de K_{ps} . Il suffit de

prouver que ces polynômes forment une famille libre. Soit $(a_{c,m})_{c \in S, 0 \leq m < p}$ une famille d'éléments de K telle que

$$f(X) := \sum_{\substack{c \in S \\ 0 \leq m < p}} a_{c,m} V_{c,m}(X) = 0.$$

Pour tout $c \in S$ on a $f^{(p-1)}(c) = (p-1)!a_{c,p-1} = 0$. Donc, pour tout $c \in S$, on voit que $a_{c,p-1} = 0$. Par récurrence descendante sur m , on obtient $a_{c,m} = 0$ pour tout $c \in S$ et tout $m \in \llbracket 0, p \llbracket$. Soient $P \in \text{Int}_{ps}^{(\infty)}(S, D)$ et $(a_{c,m})_{c \in S, 0 \leq m < p}$ une famille d'éléments de K telle que

$$P(X) = \sum_{\substack{c \in S \\ 0 \leq m < p}} a_{c,m} V_{c,m}(X).$$

Alors $P^{(p-1)}(c) = (p-1)!a_{c,p-1}$ pour tout $c \in S$. Donc, pour tout $c \in S$, on a $a_{c,p-1} \in D$. Par récurrence descendante sur m , on obtient $a_{c,m} \in D$ pour tout $c \in S$ et tout $m \in \llbracket 0, p \llbracket$. ■

On s'intéresse maintenant au cas où S est de cardinal infini. Le corollaire 2.7 donne immédiatement la

PROPOSITION 2.10. *Si S est infini, alors pour tout $n \in \mathbb{N}$, le n -ième idéal caractéristique de $\text{Int}^{(\infty)}(S, D)$ est*

$$J_n(\text{Int}^{(\infty)}(S, D)) = \prod_{\mathfrak{m} \in \text{Max}(D)} \mathfrak{m}^{ws, \mathfrak{m}([n/p])}.$$

THÉORÈME 2.11. *Si S est un sous-ensemble infini d'un anneau de Dedekind D tel que $\text{Int}(S, D)$ admet une base régulière $(f_n(X))_{n \in \mathbb{N}}$, alors les polynômes*

$$F_{n,j}(X) = f_n(X)^p X^j \quad (n \in \mathbb{N}, j \in \llbracket 0, p-1 \llbracket)$$

forment une base régulière de $\text{Int}^{(\infty)}(S, D)$.

Rappelons que pour que $\text{Int}(S, D)$ admette une base régulière, il faut et il suffit que pour tout $n \in \mathbb{N}$, $J_n(\text{Int}(S, D))$ soit principal (voir [3]).

Démonstration. Par la remarque 2.1, pour tout $n \in \mathbb{N}$ et tout $j \in \llbracket 0, p \llbracket$, on a $F_{n,j} \in \text{Int}^{(\infty)}(S, D)$, et par la proposition 2.10, le coefficient dominant de $F_{n,j}$ est un générateur de $J_{np+j}(\text{Int}(S, D))$. Par [3, Proposition II.1.4], $F_{n,j}$ peut être pris comme le $np+j$ -ième élément d'une base de $\text{Int}^{(\infty)}(S, D)$. ■

EXEMPLE. Soit $r \in D^*$ qui n'est pas une racine de l'unité et $S = \{r^n \mid n \in \mathbb{N}\}$. On sait (voir [2]) que la suite $(r^n)_{n \in \mathbb{N}}$ est une suite ordonnée de S pour tout idéal maximal de D . Par conséquent, la famille des polynômes

$$F_{n,j}(X) = \left(\prod_{k=0}^{n-1} \frac{X - r^k}{r^n - r^k} \right)^p X^j \quad (n \in \mathbb{N}, j \in \llbracket 0, p-1 \llbracket)$$

est une base régulière de $\text{Int}^{(\infty)}(S, D)$.

2.3. Le module $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$. Soit $q = p^f$ ($f \in \mathbb{N}^*$). Dans ce paragraphe, nous décrivons des bases régulières de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$.

Dans [4], Car définit une bijection $(c_n)_{n \in \mathbb{N}}$ de \mathbb{N} sur $\mathbb{F}_q[T]$ de manière suivante :

DÉFINITION 2.12. On pose $\mathbb{F}_q = \{c_0 = 0, \dots, c_{q-1}\}$. À tout $n \in \mathbb{N}$ de développement q -adique $n = n_0 + n_1q + \dots + n_sq^s$ on associe

$$c_n = c_{n_0} + c_{n_1}T + \dots + c_{n_s}T^s.$$

Une telle suite est appelée *suite de Car*.

Une suite de Car est une suite ordonnée de $\mathbb{F}_q[T]$ pour tout idéal maximal de $\mathbb{F}_q[T]$ (voir [2], [13] ou [7]). On en déduit que la suite $(\prod_{j=0}^{n-1} \frac{X-c_j}{c_n-c_j})_{n \in \mathbb{N}}$ est une base régulière de $\text{Int}(\mathbb{F}_q[T])$. En conséquence, on a le

THÉORÈME 2.13. Soit $(c_n)_{n \in \mathbb{N}}$ une suite de Car. L'ensemble des polynômes

$$\left(\prod_{k=0}^{n-1} \frac{X - c_k}{c_n - c_k} \right)^p X^j \quad (n \in \mathbb{N}, j \in \llbracket 0, p - 1 \rrbracket)$$

est une base régulière de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$.

Dans [5], Carlitz décrit une autre base de $\text{Int}(\mathbb{F}_q[T])$: pour tout $n \in \mathbb{N}$, soit

$$(2.2) \quad \Psi_n(X) = \prod_{\substack{h \in \mathbb{F}_q[T] \\ \deg h < n}} \frac{X - h}{T^n - h}.$$

À tout $n \in \mathbb{N}$ de développement q -adique $n = n_0 + n_1q + \dots + n_sq^s$ on associe le polynôme

$$(2.3) \quad G_n(X) = \prod_{i=0}^s \Psi_i(X)^{n_i}.$$

PROPOSITION 2.14 ([5]). Les polynômes $G_n(X)$ ($n \in \mathbb{N}$) forment une base régulière de $\text{Int}(\mathbb{F}_q[T])$.

On a donc le

THÉORÈME 2.15. Les polynômes $G_n(X)^p X^j$ ($n \in \mathbb{N}, j \in \llbracket 0, p - 1 \rrbracket$) forment une base régulière de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$.

On peut donner une description explicite des idéaux caractéristiques de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$: pour tout $n \in \mathbb{N}$, on pose

$$D_n = \prod_{\substack{h \in \mathbb{F}_q[T] \\ \deg h < n}} (T^n + h).$$

PROPOSITION 2.16. Soit $n \in \mathbb{N}$ de développement q -adique $n = n_0 + n_1q + \dots + n_sq^s$. Alors

$$J_n(\text{Int}^{(\infty)}(\mathbb{F}_q[T])) = \prod_{j=0}^s C_j^{-m_j} \mathbb{F}_q[T],$$

où

$$C_j = \begin{cases} D_j & \text{si } n_j \geq p, \\ D_{j-1} & \text{sinon,} \end{cases} \quad m_j = \begin{cases} [n_j/p] & \text{si } n_j \geq p, \\ n_j p^{j-1} & \text{sinon.} \end{cases}$$

Démonstration. Par la proposition 2.14, pour tout $n \in \mathbb{N}$ on a

$$J_n(\text{Int}(\mathbb{F}_q[T])) = \prod_{j=0}^s D_j^{-n_j} \mathbb{F}_q[T],$$

et par la proposition 2.10, on a

$$J_n(\text{Int}^{(\infty)}(\mathbb{F}_q[T])) = J_{[n/p]}(\text{Int}(\mathbb{F}_q[T])). \blacksquare$$

Donnons maintenant un contre-exemple à [10, Theorem 5] :

$$\Psi_1(X) = \frac{X^q - X}{D_1}$$

est un polynôme \mathbb{F}_q -linéaire. Ainsi, $\Psi_1(X)^p$ est un polynôme linéaire. On a donc

$$\Delta_T(\Psi_1^p)(T) = \frac{\Psi_1^p(T)}{T} = \frac{1}{T} \notin \mathbb{F}_q[T].$$

Clairement, $\Psi_1^p \in \text{Int}^{(\infty)}(\mathbb{F}_q[T])$, donc $\text{Int}^{[\infty]}(\mathbb{F}_q[T]) \neq \text{Int}^{(\infty)}(\mathbb{F}_q[T])$. On peut montrer (voir [3]) que $\text{Int}^{[\infty]}(\mathbb{F}_q[T]) \subset \text{Int}^{(\infty)}(\mathbb{F}_q[T])$. Donc :

PROPOSITION 2.17 ([3, Chapter IX] ou [6]). On a l'inclusion stricte

$$\text{Int}^{[\infty]}(\mathbb{F}_q[T]) \subsetneq \text{Int}^{(\infty)}(\mathbb{F}_q[T]).$$

3. Bases de $\text{Int}^{(\infty)}(S, D)$

3.1. Dérivée a -ième. Rappelons que D est un anneau de Dedekind de caractéristique $p > 0$ et de corps des fractions K . On suppose de plus que $\mathbb{F}_q[T] \subset D$. Nous considérons ici une nouvelle sorte de dérivée et puisque toute suite de Car forme une bijection de N sur $\mathbb{F}_q[T]$, au lieu de la suite des dérivées n -ièmes, nous considérons la suite des dérivées a -ièmes, où a est un élément de $\mathbb{F}_q[T]$.

DÉFINITION 3.1. Soit $c := (c_n)_{n \in \mathbb{N}}$ suite de Car. Pour tout $a \in \mathbb{F}_q[T]$, on appelle *factorielle a* (par rapport à la suite c) et on note $a!_c$ le polynôme de $\mathbb{F}_q[T]$ donné par

$$a!_c = \prod_{j=0}^{n_a-1} (c_{n_a} - c_j),$$

où n_a dénote l'unique entier tel que $c_{n_a} = a$.

Dans tout ce qui suit, la suite $(c_n)_{n \in \mathbb{N}}$ sera supposée fixée. On omettra donc toutes les références à cette suite. Rappelons la notion de dérivée de Hasse (voir [9]). Pour tout $n, m \in \mathbb{N}$ ($m > n$), on pose $\binom{n}{m} = 0$.

DÉFINITION 3.2 ([9]). Soit $P \in K[X]$,

$$P(X) = \sum_{k=0}^{\deg P} a_k X^k \quad (a_k \in K \text{ pour tout } k \in \llbracket 0, \deg P \rrbracket).$$

Pour tout $n \in \mathbb{N}$, on appelle n -ième dérivée de Hasse de P et on note $\mathcal{D}^n(P)$ le polynôme

$$\mathcal{D}^n(P)(X) = \sum_{k=0}^{\deg P} a_k \binom{k}{n} X^{k-n}.$$

DÉFINITION 3.3. Soient $P \in K[X]$, $a \in \mathbb{F}_q[T]$ et n_a l'unique entier naturel tel que $a = c_{n_a}$. On appelle a -ième dérivée de P et on note $\delta_a(P)$ le polynôme

$$\delta_a(P) = a! \mathcal{D}^{n_a}(P).$$

REMARQUE 3.4. Dans le cas où $a_j = j$ pour tout $j \in \llbracket 0, p \rrbracket$ (condition qui sera toujours supposée), on obtient la dérivée k -ième classique pour $k < p$: $\delta_k(P) = P^{(k)}$.

NOTATION. Soient $a, b_1, \dots, b_s \in \mathbb{F}_q[T]$ tels que $\sum_{j=1}^s n_{b_j} = n_a$. On pose

$$\binom{a}{b_1, \dots, b_s} = \frac{a!}{b_1! \cdots b_s!}.$$

Par [2], on a $\binom{a}{b_1, \dots, b_s} \in \mathbb{F}_q[T]$.

PROPOSITION 3.5. Soient $P_1, \dots, P_s \in K[X]$. Pour tout $a \in \mathbb{F}_q[T]$, on a

$$(3.1) \quad \delta_a \left(\prod_{i=1}^s P_i \right) = \sum_{\substack{b_1, \dots, b_s \in \mathbb{F}_q[T] \\ n_{b_1} + \dots + n_{b_s} = n_a}} \binom{a}{b_1, \dots, b_s} \prod_{j=1}^s \delta_{b_j}(P_j).$$

Démonstration. C'est une conséquence immédiate de l'égalité (voir [9, Lemma 5.72]), pour tout $n \in \mathbb{N}$,

$$\mathcal{D}^n(P_1 \cdots P_s) = \sum_{\substack{i_1 \geq 0, \dots, i_s \geq 0 \\ i_1 + \dots + i_s = n}} \mathcal{D}^{i_1}(P_1) \cdots \mathcal{D}^{i_s}(P_s). \quad \blacksquare$$

NOTATION. Rappelons que $\text{Int}^{(\infty)}(S, D)$ (ou plus simplement $\text{Int}^{(\infty)}(D)$ si $S = D$) est l'ensemble des polynômes à valeurs entières sur S relativement à D ainsi que toutes leurs dérivées :

$$\text{Int}^{(\infty)}(S, D) = \{P \in K[X] \mid \forall a \in \mathbb{F}_q[T] \ (\delta_a(P))(S) \subset D\}.$$

Clairement, $\text{Int}^{(\infty)}(S, D)$ est un D -module.

3.2. Cas local. Reprenant mots pour mots la preuve de [3, Proposition IX.1.5], on montre que $\text{Int}^{(\infty)}(S, D)$ se comporte bien par localisation : pour tout idéal maximal \mathfrak{m} de D , on a

$$\text{Int}^{(\infty)}(S, D)_{\mathfrak{m}} = \text{Int}^{(\infty)}(S, D_{\mathfrak{m}}).$$

NOTATION. On suppose donc que $D = V$ est l'anneau d'une valuation discrète v contenant $\mathbb{F}_q[T]$ d'idéal maximal \mathfrak{m} . On note e l'indice de ramification de \mathfrak{m} sur $\mathfrak{m} \cap \mathbb{F}_q[T]$ et r_0 le cardinal de $\mathbb{F}_q[T]/(\mathfrak{m} \cap \mathbb{F}_q[T])$.

LEMME 3.6. *On suppose $e < r_0$. Pour tout $a, b \in \mathbb{F}_q[T]$, tels que les r_0 -chiffres de n_b soient tous plus petits que les r_0 -chiffres de n_a , on a*

$$v(a!) - v(b!) \leq n_a - n_b.$$

Démonstration. Soient

$$n_a = n_{a,0} + n_{a,1}r_0 + \dots + n_{a,g}r_0^g, \quad n_b = n_{b,0} + n_{b,1}r_0 + \dots + n_{b,g}r_0^g$$

les développements r_0 -adiques de n_a et n_b . D'après [3, Chapter II], on a

$$v(a!) = e \frac{n_a - (n_{a,0} + \dots + n_{a,g})}{r_0 - 1}, \quad v(b!) = e \frac{n_b - (n_{b,0} + \dots + n_{b,g})}{r_0 - 1}.$$

Par conséquent, puisque $e < r_0$, on obtient

$$v(a!) - v(b!) \leq \frac{e}{r_0 - 1}(n_a - n_b) \leq n_a - n_b. \blacksquare$$

Soit $\bar{S} = \{c_0, \dots, c_{s-1}\}$ un système complet de représentants de S/\mathfrak{m} inclus dans S . À tout $n \in \mathbb{N}$, écrit sous la forme $n = us + w$ avec $w \in \llbracket 0, s-1 \rrbracket$, on associe le polynôme

$$f_n(X) = \prod_{c \in \bar{S}} (X - c)^u \prod_{j=0}^{w-1} (X - c_j).$$

PROPOSITION 3.7. *On suppose $\text{Card } S = \text{Card } \bar{S}$ ou $e < r_0$. Alors, pour tout $n \in \mathbb{N}$, on a*

$$\min_{\substack{x \in S \\ a \in \mathbb{F}_q[T]}} \{v(\delta_a(f_n)(x))\} = e \sum_{l \geq 1} \left\lfloor \frac{n}{sr_0^l} \right\rfloor.$$

Démonstration. Pour tout $n \in \mathbb{N}$ ($n = us + w$, $u, w \in \mathbb{N}$ et $w < s$), on a

$$f_n(X) = \prod_{k=0}^{w-1} (X - c_k)^{u+1} \prod_{k=w}^{s-1} (X - c_k)^u.$$

D'après la proposition 3.5, pour tout $a \in \mathbb{F}_q[T]$,

$$\delta_a(f_n)(X) = \sum_{\substack{b_0, \dots, b_{s-1} \in \mathbb{F}_q[T] \\ n_{b_0} + \dots + n_{b_{s-1}} = n_a}} \binom{a}{b_0, \dots, b_{s-1}} \times \delta_{b_0}((X - c_0)^{u+1}) \cdots \delta_{b_{s-1}}((X - c_{s-1})^u).$$

Pour tout $d \in V$, tout $j \in \mathbb{N}$ et tout $b \in \mathbb{F}_q[T]$, on a (voir [9] ou la proposition 3.5)

$$\delta_b((X - d)^j) = \binom{j}{n_b} b! (X - d)^{j-n_b}.$$

Soient $c \in \overline{S}$, k l'exposant de $X - c$ dans f_n et $x \in S$. On a

$$\delta_b(v((x - c)^k)) = \begin{cases} +\infty & \text{si } n_b > k \text{ ou } x = c \text{ ou } p \mid \binom{k}{n_b}, \\ (k - n_b)v(x - c) + v(b!) & \text{sinon.} \end{cases}$$

Pour $x = c \pmod{\mathfrak{m}}$, par le lemme 3.6, on obtient

$$\delta_b(v((x - c)^k)) \geq v(a_k!).$$

Par conséquent, pour tout $(x, a) \in S \times \mathbb{F}_q[T]$,

$$v(\delta_a(f_n)(x)) \geq v(a_u!) = v(a_{[n/s]!}) = \sum_{l \geq 1} \left\lfloor \frac{n}{s^l r_0} \right\rfloor.$$

De plus,

$$\delta_{a_u}(f_n)(c_w) = a_u! \prod_{k=0}^{w-1} (c_w - c_k)^{u+1} \prod_{k=w+1}^{s-1} (c_w - c_k)^u$$

et finalement

$$v(\delta_{a_u}(f_n)(c_w)) = v(a_u!) = e \sum_{l \geq 1} \left\lfloor \frac{n}{s^l r_0} \right\rfloor. \blacksquare$$

PROPOSITION 3.8. Pour tout $n \in \mathbb{N}$, soit

$$w_S^{\langle \infty \rangle}(n) = e \sum_{l \geq 1} \left\lfloor \frac{n}{s^l r_0} \right\rfloor.$$

Si $\text{Card } S = \text{Card } \overline{S}$ ou $e < r_0$, alors les polynômes $t^{-w_S^{\langle \infty \rangle}(n)} f_n(X)$ ($n \in \mathbb{N}$) forment une base régulière de $\text{Int}^{[\infty]}(S, V)$.

Démonstration. D'après la proposition précédente, les polynômes ci-dessus appartiennent à $\text{Int}^{\langle \infty \rangle}(S, V)$. De plus, ils forment une base de $K[X]$. Soit $P \in \text{Int}^{\langle \infty \rangle}(S, D)$,

$$P(X) = \sum_{j=0}^{\deg P} a_j t^{-w_S^{\langle \infty \rangle}(j)} f_j(X) \quad (\forall k \in [0, \deg P] \ a_k \in K).$$

On a $P(c_0) = a_0 \in V$. Montrons par récurrence que les $a_k \in V$. Soit $k \in \mathbb{N}$, $k = us + w$ avec $u, w \in \mathbb{N}$ et $w < u$. On a, par la preuve de la proposition précédente,

$$\delta_{a_u}(P)(c_w) = \sum_{j=0}^{k-1} a_j t^{-w} s^{(\infty)(j)} \delta_{a_u}(f_j)(c_w) + a_k \times \xi,$$

avec $\xi \in V^\times$. Puisque $\delta_{a_u}(P)(c_w)$ et $\sum_{j=0}^{k-1} a_j t^{-w} s^{(\infty)(j)} \delta_{a_u}(f_j)(c_w)$ appartiennent à V , on obtient $a_k \in V$. ■

3.3. Cas $D = \mathbb{F}_q[T]$. Dans toute la suite, on note l'ensemble des polynômes unitaires irréductibles de $\mathbb{F}_q[T]$ par \mathbb{P} . En globalisant, la proposition 3.8 donne la

PROPOSITION 3.9. *Pour tout $n \in \mathbb{N}$, on a*

$$J_n(\text{Int}^{(\infty)}(S, \mathbb{F}_q[T])) = \prod_{P \in \mathbb{P}} P^{-\sum_{l \geq 1} \lfloor n/s_P q^l \deg P \rfloor} \mathbb{F}_q[T],$$

où $s_P = \text{Card}(S/P\mathbb{F}_q[T])$.

THÉORÈME 3.10. *Les polynômes*

$$\prod_{P \in \mathbb{P}} P^{-\sum_{l \geq 1} \lfloor n/q^{1+l} \deg P \rfloor} (X^q - X)^{\lfloor n/q \rfloor} \prod_{j=0}^{n - \lfloor n/q \rfloor q} (X - a_j) \quad (n \in \mathbb{N})$$

forment une base régulière de $\text{Int}^{(\infty)}(\mathbb{F}_q, \mathbb{F}_q[T])$.

Démonstration. Pour tout $P \in \mathbb{P}$, \mathbb{F}_q est un système complet de représentants de $\mathbb{F}_q/P\mathbb{F}_q[T]$. On applique la proposition 3.8 en remarquant que $\prod_{j=0}^{q-1} (X - a_j) = X^q - X$. ■

On détermine maintenant des bases régulières de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$. On rappelle que pour tout $n \in \mathbb{N}$, G_n est le n -ième polynôme de Carlitz défini dans (2.3) et que toutes les dérivées sont prises par rapport à la suite de Car $(c_n)_{n \in \mathbb{N}}$.

THÉORÈME 3.11. *Les polynômes*

$$B_n(X) := \prod_{P \in \mathbb{P}} P^{\lfloor n/q^{\deg P} \rfloor} G_n(X) \quad (n \in \mathbb{N})$$

forment une base régulière de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$.

Démonstration. Pour tout $n \in \mathbb{N}$ de développement q -adique

$$n = n_0 + n_1 q + \dots + n_l q^l,$$

le n -ième idéal caractéristique de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$ est

$$\begin{aligned} J_n(\text{Int}^{(\infty)}(\mathbb{F}_q[T])) &= \prod_{P \in \mathbb{P}} P^{-\sum_{l \geq 1} \lfloor n/q^{(l+1)\deg P} \rfloor} \mathbb{F}_q[T] \quad (\text{par la proposition 3.9}) \\ &= \prod_{P \in \mathbb{P}} P^{\lfloor n/q^{\deg P} \rfloor} \prod_{P \in \mathbb{P}} P^{-\sum_{l \geq 1} \lfloor n/q^{l \deg P} \rfloor} \mathbb{F}_q[T] \\ &= \prod_{P \in \mathbb{P}} P^{\lfloor n/q^{\deg P} \rfloor} J_n(\text{Int}(\mathbb{F}_q[T])) \quad (\text{par [3, Chapter II]}) \\ &= \prod_{P \in \mathbb{P}} P^{\lfloor n/q^{\deg P} \rfloor} \left(\prod_{j=0}^s D_j^{n_j} \right)^{-1} \mathbb{F}_q[T] \quad (\text{par le théorème 2.15}). \end{aligned}$$

Par conséquent, le coefficient dominant de B_n engendre $J_n(\text{Int}^{(\infty)}(\mathbb{F}_q[T]))$. Montrons que $B_n \in \text{Int}^{(\infty)}(\mathbb{F}_q[T])$. Comme on a

$$B_n(X) = \prod_{j=0}^l \left(\prod_{P \in \mathbb{P}} P^{\lfloor q^j/q^{\deg P} \rfloor} G_{q^j} \right)^{n_j},$$

d'après la formule (3.1), il suffit de montrer que pour tout $j \in \mathbb{N}$,

$$\prod_{P \in \mathbb{P}} P^{\lfloor q^j/q^{\deg P} \rfloor} G_{q^j} \in \text{Int}^{(\infty)}(\mathbb{F}_q[T]).$$

On a (voir [8, Chapter 3]), pour tout $j \in \mathbb{N}$,

$$G_{q^j}(X) = \Psi_j(X) = \sum_{l=0}^j \frac{1}{D_l L_{j-l}^{q^l}} X^{q^l}, \quad \text{où } L_{j-l} = \underset{\substack{h \in \mathbb{F}_q[T] \text{ unitaire} \\ \deg h = j-l}}{\text{PPCM}} h.$$

Par conséquent, pour tout $n \notin \{1, \dots, q^j\}$,

$$\delta_{c_n}(\Psi_j)(X) = \sum_{l=0}^j \frac{1}{D_l L_{j-l}^{q^l}} \binom{q^l}{n} X^{q^l-n} = 0,$$

par le théorème de Lucas. Pour tout $l \in \llbracket 0, j \rrbracket$,

$$\delta_{c_{q^l}}(\Psi_j)(X) = c_{q^l}! \frac{1}{D_l L_{j-l}^{q^l}} = \frac{1}{L_{j-l}^{q^l}}.$$

On en déduit que pour tout $l \in \llbracket 0, j \rrbracket$,

$$\delta_{c_{q^l}} \left(\prod_{P \in \mathbb{P}} P^{\lfloor q^j/q^{\deg P} \rfloor} \Psi_j(X) \right) = \prod_{\substack{P \in \mathbb{P} \\ \deg P \leq j}} P^{\lfloor q^j/q^{\deg P} \rfloor} \frac{1}{L_{j-l}^{q^l}}.$$

Comme $L_{j-l} = \prod_{P \in \mathbb{P}, \deg P \leq j-l} P^{\lfloor (j-l)/\deg P \rfloor}$, on obtient

$$\delta_{c_{q^l}} \left(\prod_{P \in \mathbb{P}} P^{[q^j/q^{\deg P}]} \Psi_j(X) \right) = \prod_{\substack{P \in \mathbb{P} \\ \deg P \leq j}} P^{q^{j-\deg P}} \prod_{\substack{P \in \mathbb{P} \\ \deg P \leq j-l}} P^{-q^l[(j-l)/\deg P]}.$$

Soient $P \in \mathbb{P}$ tel que $\deg P \leq j$ et ν la valuation de P dans l'anneau $\delta_{c_{q^l}}(\prod_{P \in \mathbb{P}} P^{[q^j/q^{\deg P}]} \Psi_j(X))$. Clairement, si $\deg P > j-l$, on a $\nu \geq 0$. Sinon,

$$\nu = q^{j-\deg P} - q^l \left\lfloor \frac{j-l}{\deg P} \right\rfloor.$$

Comme la fonction $u \rightarrow q^u/u$ est croissante sur \mathbb{N}^* , on en déduit que

$$q^{j-\deg P} \deg P - q^l(j-l) \geq 0,$$

et donc $\nu \geq 0$. Par conséquent, $\delta_{c_{q^l}}(\prod_{P \in \mathbb{P}} P^{[q^j/q^{\deg P}]} \Psi_j(X)) \in \text{Int}(\mathbb{F}_q[T])$ et ainsi $\prod_{P \in \mathbb{P}} P^{[q^j/q^{\deg P}]} \Psi_j \in \text{Int}^{(\infty)}(\mathbb{F}_q[T])$. ■

On en déduit le

THÉORÈME 3.12. *Soit $(f_n)_{n \in \mathbb{N}}$ une base régulière de $\text{Int}(\mathbb{F}_q[T])$. Alors, les polynômes*

$$C_n(X) = \prod_{P \in \mathbb{P}} P^{[n/q^{\deg P}]} f_n(X) \quad (n \in \mathbb{N})$$

forment une base régulière de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$.

Démonstration. Pour tout $n \in \mathbb{N}$, notons $e_n = \prod_{P \in \mathbb{P}} P^{[n/q^{\deg P}]}$. Clairement, pour tout $m \in \llbracket 0, n \rrbracket$, e_m divise e_n dans $\mathbb{F}_q[T]$, et ainsi, il existe $m_j \in \mathbb{F}_q[T]$ tel que $e_n = m_j e_j$. Le coefficient dominant de C_n est, à un élément de \mathbb{F}_q^* près, celui de B_n . Par conséquent, il engendre $J_n(\text{Int}^{(\infty)}(\mathbb{F}_q[T]))$. Il reste à montrer que $e_n f_n \in \text{Int}^{(\infty)}(\mathbb{F}_q[T])$. Comme la suite $(G_n)_{n \in \mathbb{N}}$ est une base de $\text{Int}(\mathbb{F}_q[T])$ et que $f_n \in \text{Int}(\mathbb{F}_q[T])$, on peut écrire

$$f_n(X) = \sum_{j=0}^n l_j G_j(X) \quad \text{avec } l_j \in \mathbb{F}_q[T] \text{ pour tout } j \in \llbracket 0, n \rrbracket,$$

c'est-à-dire

$$e_n f_n(x) = \sum_{j=0}^n l_j m_j e_j G_j(X).$$

La famille $(e_n G_n)_{n \in \mathbb{N}}$ formant une base de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$, on en déduit que $e_n f_n \in \text{Int}^{(\infty)}(\mathbb{F}_q[T])$. ■

COROLLAIRE 3.13. *Soit $(a_n)_{n \in \mathbb{N}}$ une suite de Car. Les polynômes*

$$\prod_{P \in \mathbb{P}} P^{[n/q^{\deg P}]} \prod_{j=0}^{n-1} \frac{X - a_j}{a_n - a_j} \quad (n \in \mathbb{N})$$

forment une base régulière de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$.

REMARQUE 3.14. L'analogie entre $\text{Int}^{(\infty)}(\mathbb{Z})$ et $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$ peut être renforcée si on remarque que la base régulière de Straus de $\text{Int}^{(\infty)}(\mathbb{Z})$ peut s'écrire sous la forme

$$\prod_{p \text{ premier}} p^{[n/\text{Norme}(\mathbb{Z}/p\mathbb{Z})]} \prod_{j=0}^{n-1} \frac{X-j}{n-j} \quad (n \in \mathbb{N}),$$

et celle de $\text{Int}^{(\infty)}(\mathbb{F}_q[T])$ sous la forme

$$\prod_{P \in \mathbb{P}} P^{[n/\text{Norme}(\mathbb{F}_q[T]/P\mathbb{F}_q[T])]} \prod_{j=0}^{n-1} \frac{X-a_j}{a_n-a_j} \quad (n \in \mathbb{N}).$$

Références

- [1] D. Adam, *Finite differences in finite characteristic*, J. Algebra 296 (2006), 285–300.
- [2] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. Reine Angew. Math. 490 (1997), 101–127.
- [3] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Math. Surveys Monogr. 48, Amer. Math. Soc., Providence, RI, 1997.
- [4] M. Car, *Répartition modulo 1 dans un corps de séries formelles sur un corps fini*, Acta Arith. 69 (1995), 229–242.
- [5] L. Carlitz, *A set of polynomials*, Duke Math. J. 6 (1940), 486–504.
- [6] J.-L. Chabert, *Dérivées et différences divisées à valeurs entières*, Acta Arith. 63 (1993), 143–156.
- [7] S. Evrard and Y. Fares, *p-adic subsets whose factorials satisfy a generalized Legendre formula*, Bull. London Math. Soc. 40 (2008), 37–50.
- [8] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergeb. Math. Grenzgeb. 35, Springer, Berlin, 1996.
- [9] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Ser. Appl. Math., Princeton Univ. Press, Princeton, NJ, 2008.
- [10] V. Laohakosol, *Bases for integer-valued polynomials in a Galois field*, Acta Arith. 87 (1998), 13–26.
- [11] E. G. Straus, *On the polynomials whose derivatives have integral values at the integers*, Proc. Amer. Math. Soc. 2 (1951), 24–27.
- [12] C. G. Wagner, *Polynomials over $\text{GF}(q, x)$ with integer-valued differences*, Arch. Math. (Basel) 27 (1976), 495–501.
- [13] J. Yeramian, *Anneaux de Bhargava*, Comm. Algebra 32 (2004), 3043–3069.

David Adam

Géométrie Algébrique et Applications à la Théorie de l'Information

Université de la Polynésie Française

BP 6570

98702 Faa'a, Tahiti, Polynésie Française

E-mail: david.adam@upf.pf

Reçu le 5.2.2010
et révisé le 22.10.2010

(6281)

