Rend. Sem. Mat. Univ. Padova (Online first)
DOI 10.4171/RSMUP/142

Published by EMS Press

On the Moore determinant

Jean Fresnel (*) – Michel Matignon (**)

Abstract – The existence of certain $\mathbb{F}_q$-spaces of differential forms of the projective line over a field K containing $\mathbb{F}_q$ leads us to prove an identity linking the determinant of the Moore matrix of n indeterminates with the determinant of the Moore matrix of the cofactors of its first row. These same spaces give an interpretation of Elkies pairing in terms of residues of differential forms. This pairing puts in duality the $\mathbb{F}_q$-vector space of the roots of an $\mathbb{F}_q$-linear polynomial and that of the roots of its reversed polynomial.

Mathematics Subject Classification (2020) – Primary 12E10; Secondary 13B40, 15A24.

Keywords – Moore matrix, Moore determinant, $\mathbb{F}_q$-linear polynomial, reversed polynomial, Elkies pairing, $\mathbb{F}_q$-space of differential forms, residue, K-étale algebra.

To Marco Garuti,
a friend too soon lost

1. Introduction

Marco Garuti was rapporteur for Guillaume Pagot's thesis [9, 10] and the origin of this note is the following remark [9, p. 68].

Let K be a field with characteristic $p > 0$, $n \geq 2$ and $W \subset K[X]$ be an n-dimensional $\mathbb{F}_p$-subspace in $K[X]$ whose non-zero elements have the same degree d, and let P be a non-zero polynomial which is a common multiple of the polynomials

(*) *Indirizzo dell'A.*: Université Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, 33400 Talence, France; jean.fresnel@math.u-bordeaux.fr

(**) *Indirizzo dell'A.*: Université Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, 33400 Talence, France; michel.matignon@math.u-bordeaux.fr

in W. Let $(P_1, P_2, \dots, P_n)$ be an $\mathbb{F}_p$-basis of W such that for $1 \le i \le n$ each differential form $\omega_i := \frac{P_i}{P}\, dX$ is a logarithmic differential. Then (Proposition 4.1) there is $\gamma \in K^\star$ such that

$$\Delta_n(P_1, P_2, \dots, P_n) = \gamma P^{1+p+p^2+\cdots+p^{n-2}}, \tag{1.1}$$

where $\Delta_n(P_1, P_2, \dots, P_n)$ is the Moore determinant of the polynomials $P_1, P_2, \dots, P_n$ (Definition 2.1).

In Proposition 3.1, we adapt the method of [4,9], where such an $\mathbb{F}_p$-space W for $n \ge 2$ was built, in order to build some $\mathbb{F}_q$-space of differential forms in $\Omega^1_K(K(X))$ that we call an $L^q_{\mu+1,n}$-space.

In Section 3.2 we give a first application to a construction of Elkies pairing [2, §4.35]. Elkies takes up and extends the results of Ore. For an $\mathbb{F}_q$-linear polynomial $P := c_0 X + c_1 X^q + \cdots + c_n X^{q^n}$ with $c_0 c_n \neq 0$, his pairing induces a duality between the $\mathbb{F}_q$-space of roots of P and that of its reversed polynomial. In our construction, the role of the $\mathbb{F}_q$-vector space of the roots of the reversed polynomial is played by an $L^q_{\mu+1,n}$-space of differential forms and the pairing is expressed by the residue of these forms evaluated at the roots of the polynomial P.

The rest of the note deals with the evaluation of the constant γ in (1.1) when we apply it to $L^q_{\mu+1,n}$-subspaces of $L^q_{\mu+1,n+m}$-spaces constructed in Proposition 3.1.

Thus, formula (1.1) takes the following form (Corollary 4.1):

Corollary 4.1. *Let $(\underline{Y}) := (Y_1, Y_2, \dots, Y_n)$ and $(\underline{X}) := (X_1, X_2, \dots, X_m)$ be $n+m$ indeterminates over $\mathbb{F}_q$ with $n \ge 2$, $m \ge 0$ and the convention that $\underline{X} = \emptyset$ and $\Delta_m(\underline{X}) = 1$ for $m = 0$. We write $(\widehat{\underline{Y}_i}) := (Y_1, \dots, Y_{i-1}, Y_{i+1}, \dots, Y_n)$ for $1 \le i \le n$. Then we have the following equality in $\mathbb{F}_q(\underline{Y}, \underline{X})$:*

$$\frac{\Delta_n(\Delta_{n-1+m}(\widehat{\underline{Y}_1}, \underline{X}), \dots, (-1)^{i+1}\Delta_{n-1+m}(\widehat{\underline{Y}_i}, \underline{X}), \dots, (-1)^{n+1}\Delta_{n-1+m}(\widehat{\underline{Y}_n}, \underline{X}))}{\Delta_m(\underline{X})^{q^{n-1}}\,\Delta_{n+m}(\underline{Y}, \underline{X})^{1+q+\cdots+q^{n-2}}}$$
$$= \frac{\Delta_n\big(\Delta_{n-1}(\widehat{\underline{Y}_1}), \dots, (-1)^{i+1}\Delta_{n-1}(\widehat{\underline{Y}_i}), \dots, (-1)^{n+1}\Delta_{n-1}(\widehat{\underline{Y}_n})\big)}{\Delta_n(\underline{Y})^{1+q+\cdots+q^{n-2}}} =: \gamma$$

Thanks to the work of Ore and Elkies (cf. Proposition 2.5) we know that $\gamma \in \mathbb{F}_q^\star$.

We show (Theorem 4.1) that $\gamma = 1$. We give three proofs. The first one shows it for $m = 1$ and by induction on n. It is a technical exercise in computing determinants. The second proof is a matrix equality which is in itself original and which translates a relation between a generic Moore matrix and the Moore matrix of the cofactors of its first row (see the theorem below), a relation analogous to the classical relation between a square matrix and its comatrix. The $m = 0$ case of Theorem 4.1 is immediately deduced.

THEOREM 4.2. *Let $Y_1, Y_2, \dots, Y_n$ be n indeterminates over $\mathbb{F}_q$, and let $\mathcal{M}_n(\Delta_n(\widehat{\underline{Y}_1}), \dots, (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i}), \dots, (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n}))$ be the Moore matrix of the cofactors $(\Delta_n(\widehat{\underline{Y}_1}), \dots, (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i}), \dots, (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n}))$ of the first row of $\mathcal{M}_n(\underline{Y})$, where for $1 \le i \le n$, we write $(\widehat{\underline{Y}_i}) := (Y_1, \dots, Y_{i-1}, Y_{i+1}, \dots, Y_n)$. Then we have*

$$\mathcal{M}_n\left(\Delta_n(\widehat{\underline{Y}_1}), \dots, (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i}), \dots, (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n})\right) {}^t\mathcal{M}_n(\underline{Y})$$

$$= \begin{pmatrix} 0 & . & . & \cdots & . & 0 & (-1)^{n-1}\Delta_n(\underline{Y}) \\ \Delta_n(\underline{Y}) & 0 & . & \cdots & . & 0 & 0 \\ \alpha_1 & \Delta_n(\underline{Y})^q & 0 & \cdots & . & 0 & 0 \\ \alpha_2 & \alpha_1^q & \Delta_n(\underline{Y})^{q^2} & \cdots & . & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & . & \vdots & \vdots \\ \alpha_{n-2} & \alpha_{n-3}^q & . & \cdots & \alpha_1^{q^{n-3}} & \Delta_n(\underline{Y})^{q^{n-2}} & 0 \end{pmatrix}$$

where

$$\alpha_k := \Delta_n(\widehat{\underline{Y}_1})^{q^{k+1}} Y_1 + \cdots + (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i})^{q^{k+1}} Y_i + \cdots + (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n})^{q^{k+1}} Y_n.$$

The third proof is a generalization of the above theorem, which gives a matrix equality (Theorem 4.3) from which we deduce Theorem 4.1 without invoking Corollary 4.1.

In Section 5, we offer two illustrations of the Moore determinant. In the first one we study the application $(a_1, \dots, a_n) \in K^n \to (\Delta_{n-1}(\hat{\underline{a}_i}))_{1 \le i \le n} \in K^n$ and in the second we study a K-étale algebra defined by n Artin–Schreier equations. In this context we express a group action in terms of an appropriate Elkies pairing.

2. Generalities and motivations

2.1 – *Notation*

In this note all rings are commutative and unitary and A (resp. K) denotes a ring (resp. a field) of characteristic $p > 0$ containing the field $\mathbb{F}_q$, where $q := p^s$. Finally, $F: A \to A$, with $F(a) = a^q$, denotes the Frobenius endomorphism.

We denote by K^{alg} a K algebraic closure. We adopt the following notation when the context is not ambiguous.

- Let $n \ge 1, m \ge 0$ be integers.
- Let $(\underline{a}) := (a_1, a_2, \dots, a_n)$, with $a_i \in A$ and $n \ge 1$.

- Let $(\underline{X}) := (X_1, X_2, \ldots, X_m)$ be indeterminates over A and let $m \geq 0$ with the convention $\underline{X} = \emptyset$ if $m = 0$. The integer m is determined by the context.
- Let $(\underline{\hat{a}_i}, \underline{X}) := (a_1, \ldots, \hat{a}_i, \ldots, a_n, \underline{X})$, i.e. we omit a_i and $\underline{X}$ may be empty. The integers n and m are determined by the context.

Definition 2.1. Let A be a commutative ring containing the finite field $\mathbb{F}_q$. Let $m, n \geq 1$ be integers and $\underline{a} := (a_1, \ldots, a_n) \in A^n$. We call the matrix of $M_{m,n}(A)$, denoted by $\mathcal{M}_{m,n}(\underline{a})$ ($\mathcal{M}_n(\underline{a})$ if $n = m$), where

$$\mathcal{M}_{m,n}(\underline{a}) := \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1^q & a_2^q & \cdots & a_n^q \\ \vdots & \vdots & \cdots & \vdots \\ a_1^{q^{m-1}} & a_2^{q^{m-1}} & \cdots & a_n^{q^{m-1}} \end{pmatrix},$$

the *Moore matrix* of size m, n associated to $\underline{a}$, and we call the determinant of $\mathcal{M}_n(\underline{a})$, denoted by $\Delta_n(\underline{a})$, the *Moore determinant* associated to $\underline{a}$.

2.2 – *Additive polynomials and Moore determinants*

Definition 2.2. Let K be a field containing $\mathbb{F}_q$. We call a polynomial of the form $c_n X^{q^n} + c_{n-1} X^{q^{n-1}} + \cdots + c_i X^{q^i} + \cdots + c_0 X \in K[X]$ an $\mathbb{F}_q$*-linear polynomial*.

It is easy to see that a polynomial $P \in K[X]$ is an $\mathbb{F}_q$-linear polynomial if and only if it satisfies the following two conditions:

(1) $P(X + Y) = P(X) + P(Y)$ in the polynomials ring $K[X, Y]$;

(2) $P(\lambda X) = \lambda P(X)$ for all $\lambda \in \mathbb{F}_q$.

A polynomial is *additive* if it satisfies condition (1). An additive polynomial is said to be *reduced* if it is separable. If it is non-zero, this means that the coefficient of X is non-zero.

Let $P \in K[X]$ be an $\mathbb{F}_q$-linear polynomial, let $\operatorname{Ker} P := \{x \in K^{\text{alg}} \mid P(x) = 0\}$ be the set of roots of P; it is an $\mathbb{F}_q$-subspace of K^{alg}.

The application $x \in K \to P(x) \in K$ is an $\mathbb{F}_q$-linear endomorphism of K. Thus we can consider the $\mathbb{F}_q$-subspace of K which is the *kernel* of this endomorphism. It coincides with $\operatorname{Ker} P$ when $\operatorname{Ker} P \subset K$.

Proposition 2.1 ([6, 8] and [2, Prop. 1, p. 80]). *Let A be an integral commutative ring containing $\mathbb{F}_q$. The n elements $a_1, a_2, \ldots, a_n$ of A are $\mathbb{F}_q$-linearly independent if and only if $\Delta_n(\underline{a}) \neq 0$. In other words, the n elements $a_1, a_2, \ldots, a_n$ of A are $\mathbb{F}_q$-linearly independent if and only if the n vectors $\underline{a}, F(\underline{a}), \ldots, F^{n-1}(\underline{a})$ of A^n are $\mathbb{F}_q$-linearly independent.*

This proposition is a consequence of Moore's identity [2, formula (3.4), p. 80; formula (3.6), p. 81], which says that if $a_1, a_2, \ldots, a_n$ are elements of A, then

$$\Delta_n(\underline{a}) = \prod_{1\le i\le n} \prod_{\varepsilon_{i-1}\in\mathbb{F}_q} \cdots \prod_{\varepsilon_1\in\mathbb{F}_q} (a_i + \varepsilon_{i-1}a_{i-1} + \cdots + \varepsilon_1 a_1). \tag{2.1}$$

Proposition 2.2. *Let K be a field containing $\mathbb{F}_q$ and W an $\mathbb{F}_q$-vector subspace of K with $\dim_{\mathbb{F}_q} W = n$. Then there exists a unique unit polynomial of degree q^n, denoted P_W, with $W = \{x \in K \mid P_W(x) = 0\}$. Moreover, P_W is an $\mathbb{F}_q$-linear polynomial which is reduced and if $\underline{w} := (w_1, \ldots, w_n) \in K^n$ is an $\mathbb{F}_q$-basis of W then*

$$\begin{aligned} P_W(X) &= \prod_{w\in W} (X - w) \\ &= \frac{\Delta_{n+1}(\underline{w}, X)}{\Delta_n(\underline{w})} = X^{q^n} + \cdots + (-1)^n \Delta_n(\underline{w})^{q-1} X. \end{aligned} \tag{2.2}$$

The following proposition is the version adapted to hyperplanes in Proposition 2.2.

Proposition 2.3. *Let W be an $\mathbb{F}_q$-subspace of K with $\dim_{\mathbb{F}_q} W = n$. Let $\underline{w} := (w_1, w_2, \ldots, w_n)$ be an $\mathbb{F}_q$-basis of W and $\underline{w^\star}$: $(w_1^\star, \ldots, w_n^\star)$ its dual basis. Let φ be a non-zero $\mathbb{F}_q$-linear form on W and $\operatorname{Ker}\varphi$ the hyperplane of W kernel of φ. Let $\underline{\alpha} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n - \{(0, \ldots, 0)\}$ be such that $\varphi = \sum_{1\le i\le n} \alpha_i w_i^\star$ and*

$$\Delta_\varphi(\underline{w}, X) = \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n & 0 \\ w_1 & w_2 & \cdots & w_n & X \\ w_1^q & w_2^q & \cdots & w_n^q & X^q \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ w_1^{q^{n-1}} & w_2^{q^{n-1}} & \cdots & w_n^{q^{n-1}} & X^{q^{n-1}} \end{vmatrix},$$

$$\delta_\varphi(\underline{w}) := \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ w_1 & w_2 & \cdots & w_n \\ w_1^q & w_2^q & \cdots & w_n^q \\ \vdots & \vdots & \cdots & \vdots \\ w_1^{q^{n-2}} & w_2^{q^{n-2}} & \cdots & w_n^{q^{n-2}} \end{vmatrix}.$$

Then $\delta_\varphi(\underline{w}) \neq 0$ and like in (2.2) we can write

$$\begin{aligned} P_{\operatorname{Ker}\varphi} &= \prod_{w\in\operatorname{Ker}\varphi} (X - w) \\ &= \frac{\Delta_\varphi(\underline{w}, X)}{\delta_\varphi(\underline{w})} = X^{q^{n-1}} + \cdots + (-1)^{n+1} \delta_\varphi(\underline{w})^{q-1} X, \end{aligned} \tag{2.3}$$

which is an $\mathbb{F}_q$-linear polynomial of degree q^{n-1} that is reduced. Moreover, we have for $1 \leq i \leq n$,

$$\begin{aligned}
\Delta_{w_i^\star}(\underline{w}, X) &= (-1)^{i-1}\Delta_n(\underline{\widehat{w}_i}, X),\\
\Delta_\varphi(\underline{w}, X) &= \sum_{1\leq i\leq n} \alpha_i \Delta_{w_i^\star}(\underline{w}, X) = \sum_{1\leq i\leq n} \alpha_i (-1)^{i-1}\Delta_n(\underline{\widehat{w}_i}, X),\\
\delta_\varphi(\underline{w}) &= \sum_{1\leq i\leq n} (-1)^{i-1}\alpha_i \Delta_{n-1}(\underline{\widehat{w}_i}).
\end{aligned}$$

Proof. First we show that $\Delta_\varphi(\underline{w}, X)$ is not the null polynomial. Let us assume the opposite. Since $\underline{w}, F(\underline{w}), \ldots, F^{n-1}(\underline{w})$ are $\mathbb{F}_q$-linearly independent and since for $j \in \{0, \ldots, n-1\}$ the coefficient of X^{q^j} is zero, we get $\underline{\alpha} \in \sum_{i\in\{0,\ldots,n-1\}, i\neq j} \mathbb{F}_q F^i(\underline{w})$; thus its $(j+1)$th coordinate in the $\mathbb{F}_q$-basis $\underline{w}, F(\underline{w}), \ldots, F^{n-1}(\underline{w})$ is zero, which contradicts the non-nullity of $\underline{\alpha}$.

The polynomial $\Delta_\varphi(\underline{w}, X)$ is thus an $\mathbb{F}_q$-linear polynomial of degree $\leq q^{n-1}$. We check that it is zero on the hyperplane $\operatorname{Ker}\varphi$; thus its degree is equal to q^{n-1}. Hence the proposition. ∎

Corollary 2.1. *Let K be a field containing $\mathbb{F}_q$, $\underline{w} := (w_1, w_2, \ldots, w_n) \in K^n$ and for $1 \leq i \leq n$, $\Delta_{n-1}(\underline{\widehat{w}_i}) := \Delta_{n-1}(w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_n)$. Then $\Delta_n(\underline{w}) \neq 0$ if and only if $\Delta_n(\underline{\Delta_{n-1}(\widehat{w}_i)}) := \Delta_n(\Delta_{n-1}(\underline{\widehat{w}_1}), \Delta_{n-1}(\underline{\widehat{w}_2}), \ldots, \Delta_{n-1}(\underline{\widehat{w}_n})) \neq 0$.*

Proof. Let us assume that $\Delta_n(\underline{w}) \neq 0$. Then, by Propositions 2.1 and 2.3, $\delta_{\underline{\varphi}}(\underline{w}) = \sum_{1\leq i\leq n} \alpha_i \Delta_{n-1}(\underline{\widehat{w}_i}) \neq 0$ for all $\underline{\alpha} := (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n - \{(0, \ldots, 0)\}$, where $\varphi = \sum_{1\leq i\leq n} \alpha_i w_i^\star$. It follows from Proposition 2.1 that $\Delta_n(\underline{\Delta_{n-1}(\widehat{w}_i)}) \neq 0$.

Let us assume that $\Delta_n(\underline{w}) = 0$. Then, by Proposition 2.1, there is $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \in \mathbb{F}_q^n - \{(0, \ldots, 0)\}$ with $\sum_{1\leq i\leq n} \varepsilon_i w_i = 0$. Let f be the $\mathbb{F}_q$-linear form over $\mathbb{F}_q^n$ such that $f((\alpha_1, \ldots, \alpha_n)) = \sum_{1\leq i\leq n} \varepsilon_i \alpha_i$ and $(\alpha_1, \ldots, \alpha_n) \in \operatorname{Ker} f - \{0\}$. Then

$$\begin{vmatrix}
\alpha_1 & \alpha_2 & \cdots & \alpha_n\\
w_1 & w_2 & \cdots & w_n\\
w_1^q & w_2^q & \cdots & w_n^q\\
\vdots & \vdots & \cdots & \vdots\\
w_1^{q^{n-2}} & w_2^{q^{n-2}} & \cdots & w_n^{q^{n-2}}
\end{vmatrix} = 0,$$

so $\sum_{1\leq i\leq n}(-1)^{i-1}\alpha_i \Delta_{n-1}(\underline{\widehat{w}_i}) = 0$. Thus, $\Delta_n(\underline{\Delta_{n-1}(\widehat{w}_i)}) = 0$. ∎

Definition 2.3. Let $P(X) := c_n X^{q^n} + c_{n-1} X^{q^{n-1}} + \cdots + c_0 X \in K[X]$ be a reduced $\mathbb{F}_q$-linear polynomial (i.e. $c_0 \neq 0$) of degree q^n (i.e. $c_n \neq 0$). With Ore we

consider the *reversed polynomial* ρP of the polynomial P, where

$$(\rho P)(X) := \sum_{0\le m\le n} c_{n-m}^{q^m} X^{q^m},$$

which is a reduced $\mathbb{F}_q$-linear polynomial of degree q^n.

Ore shows the following result (see [2, Theorem 5, p. 88]).

Proposition 2.4. *Let K be a field containing $\mathbb{F}_q$. Let $P = \sum_{0\le i\le n} c_i X^{q^i} \in K[X]$ be a reduced $\mathbb{F}_q$-linear polynomial of degree q^n, ρP its reversed polynomial (Definition 2.3). We assume that the roots of P are in K. Let $W := \operatorname{Ker} P \subset K$ (Definition 2.2) and $\underline{w} := (w_1, w_2, \dots, w_n) \in K^n$ be an $\mathbb{F}_q$-basis of W. Let $\widehat{W} \subset K$, the $\mathbb{F}_q$-subspace of K spanned by the n minors $\Delta_{n-1}(\underline{\widehat{w}_i})$, $1 \le i \le n$. Then, if $U := \operatorname{Ker} \rho P$, we have $U = c_n^{-1}(\frac{\widehat{W}}{\Delta_n(\underline{w})})^q$; this is an $\mathbb{F}_q$-subspace of K of dimension n.*

Remark 2.1. It follows from Proposition 2.4 (see also [3, Corollary 1.7.14, p. 18]) that if the n elements $w_1, \dots, w_n$ in K are $\mathbb{F}_q$-independent, so are the n elements $\Delta_{n-1}(\underline{\widehat{w}_i})$, $1 \le i \le n$. Although not explicitly written, Ore [8] and Elkies [2] show the following result

Proposition 2.5. *Let K be a field containing $\mathbb{F}_q$, $\underline{w} := (w_1, w_2, \dots, w_n) \in K^n$ and for $1 \le i \le n$, $\Delta_{n-1}(\underline{\widehat{w}_i}) := \Delta_{n-1}(w_1, \dots, w_{i-1}, w_{i+1}, \dots, w_n)$. Let us assume that $\Delta_n(\underline{w}) \neq 0$. Then*

$$(\Delta_n(\underline{\Delta_{n-1}(\underline{\widehat{w}_i})}))^{q-1} = \Delta_n(\underline{w})^{q^{n-1}-1}. \tag{2.4}$$

Thus,

$$\frac{\Delta_n(\underline{\Delta_{n-1}(\underline{\widehat{w}_i})})}{\Delta_n(\underline{w})^{1+q+\cdots+q^{n-2}}} \in \mathbb{F}_q^\star. \tag{2.5}$$

Proof. Let $W \subset K$ be the $\mathbb{F}_q$-vector space $\bigoplus_{1\le i\le n} \mathbb{F}_q w_i$ and P_W the polynomial associated to W by Proposition 2.2. Let $\widehat{W} := \bigoplus_{1\le i\le n} \mathbb{F}_q \Delta_{n-1}(\underline{\widehat{w}_i}) \subset K$. With (2.2) we have $P_W(X) := \frac{\Delta_{n+1}(\underline{w},X)}{\Delta_n(\underline{w})}$ and if $\Delta[i](\underline{w}) := \det(\underline{w}, F(\underline{w}), \dots, \widehat{F^i}(\underline{w}), \dots, F^n(\underline{w}))$ (i.e. the line $F^i(\underline{w})$ is left out), then

$$P_W(X) = \sum_{0\le m\le n} (-1)^{n-m} \frac{\Delta[m](\underline{w})}{\Delta_n(\underline{w})} X^{q^m},$$

thus

$$P_W(X) = \sum_{0\le m\le n} c_m X^{q^m} \quad \text{with } c_m = (-1)^{n-m} \frac{\Delta[m](\underline{w})}{\Delta_n(\underline{w})}.$$

Applying the above to the family $\underline{\Delta_{n-1}(\widehat{w}_i)}$ and the polynomial

$$P_{\widehat{W}}(X) := \frac{\Delta_{n+1}(\underline{\Delta_{n-1}(\widehat{w}_i)}, X)}{\Delta_n(\underline{\Delta_{n-1}(\widehat{w}_i)})} =: \sum_{0\le m\le n} \hat{c}_m X^{q^m},$$

we obtain the following identities for $0 \le m \le n$:

$$\hat{c}_m = (-1)^{n-m} \frac{\Delta[m](\underline{\Delta_{n-1}(\widehat{w}_i)})}{\Delta_n(\underline{\Delta_{n-1}(\widehat{w}_i)})}.$$

In particular $\hat{c}_0 = (-1)^n(\Delta_n(\underline{\Delta_{n-1}(\widehat{w}_i)}))^{q-1}$.

Elkies [2, formula (4.28)] shows, following Ore, that

$$P_{\widehat{W}}(X) = X^{q^n} + (-1)^n\left(\sum_{1\le m\le n-1} c_{n-m}^{q^{m-1}} \Delta_n(\underline{w})^{q^{n-1}-q^m} X^{q^m} + \Delta_n(\underline{w})^{q^{n-1}-1} X\right).$$

Thus, (2.4) is fulfilled.

In the case where $1 \le m \le n-1$ we obtain the equality

$$\hat{c}_m = (-1)^{n-m} \frac{\Delta[m](\underline{\Delta_{n-1}(\widehat{w}_i)})}{\Delta_n(\underline{\Delta_{n-1}(\widehat{w}_i)})} = (-1)^n c_{n-m}^{q^{m-1}} \Delta_n(\underline{w})^{q^{n-1}-q^m},$$

which taking into account (2.4) gives

$$(\Delta[m](\underline{\Delta_{n-1}(\widehat{w}_i)}))^{q-1} = \Delta_n(\underline{w})^{q^n-q^{m+1}+q^{m-1}-1}(\Delta[n-m](\underline{w}))^{q^{m-1}(q-1)}. \tag{2.6}$$

■

Remark 2.2. If we take into account Theorem 4.1, we can specify the equalities (2.5) and (2.6). Thus we have

$$\frac{\Delta_n(\underline{\Delta_{n-1}(\widehat{w}_i)})}{\Delta_n(\underline{w})^{1+q+\cdots+q^{n-2}}} = (-1)^{\lfloor \frac{n}{2} \rfloor},$$

where $\lfloor \frac{n}{2} \rfloor$ is the lower integer part of $\frac{n}{2}$, and

$$\Delta[m](\underline{\Delta_{n-1}(\widehat{w}_i)}) = (-1)^{\lfloor \frac{n}{2} \rfloor} \Delta_n(\underline{w})^{\frac{q^n-1}{q-1}-q^{m-1}-q^m} \Delta[n-m](\underline{w})^{q^{m-1}}.$$

The next proposition takes up results of Ore and Elkies [2, Proposition 3] which specify the link between composition of two $\mathbb{F}_q$-linear polynomials and the geometry of sets of roots.

Proposition 2.6. *Let K be a field which contains $\mathbb{F}_q$. Let W be an $\mathbb{F}_q$-vector space of K with $\dim_{\mathbb{F}_q} W = n$, W_1 be an $\mathbb{F}_q$-subvector space of W and $P_W(X) := \prod_{x\in W}(X-x)$ (resp. $P_{W_1}(X) := \prod_{x\in W_1}(X-x)$). Let $P_{W_1}(W) := \{P_{W_1}(x) \mid x \in W\}$, which is a finite-dimensional $\mathbb{F}_q$-subspace of K and*

$$P_W(X) = P_{P_{W_1}(W)}(P_{W_1}(X)). \tag{2.7}$$

Conversely, if Q is a monic $\mathbb{F}_q$-linear polynomial such that $P_W(X) = Q(P_{W_1}(X))$, we have $Q = P_{P_{W_1}(W)}$.

Proof. Let us assume that $\dim_{\mathbb{F}_q} W_1 = m$. Then $\deg P_{W_1} = q^m$. Since $x \in W \to P_{W_1}(x) \in K$ is an $\mathbb{F}_q$-linear map whose kernel is W_1, it follows that $P_{W_1}(W)$ is an $\mathbb{F}_q$-subspace of K of dimension $n-m$; thus the polynomial $P_{P_{W_1}(W)}(P_{W_1}(X))$ is a monic $\mathbb{F}_q$-linear polynomial of degree $q^{n-m}q^m = q^n$. Since it is by construction zero on W, it follows that $P_W(X)$ divides $P_{P_{W_1}(W)}(P_{W_1}(X))$ in $K[X]$, hence the equality.

For the reciprocal we remark that $(Q - P_{P_{W_1}(W)})(P_{W_1}(X))$ is the null polynomial in $K[X]$ and that $P_{W_1}(X)$ is transcendental over K. ∎

Finally, the following corollary specifies Proposition 2.3.

Corollary 2.2. *Let K be a field which contains $\mathbb{F}_q$. Let $W \subset K$ be an $\mathbb{F}_q$-vector space with $\dim_{\mathbb{F}_q} W = n$, $\underline{w} := (w_1, w_2, \ldots, w_n) \in K^n$ an $\mathbb{F}_q$-basis of W and $(w_1^\star, w_2^\star, \ldots, w_n^\star)$ its dual basis. Let φ be a non-zero $\mathbb{F}_q$-linear form on W and $\operatorname{Ker}\varphi$ be the hyperplane of the W kernel of φ. Let $\underline{\alpha} := (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n - \{(0,0,\ldots,0)\}$ and be such that*

$$\begin{aligned}
\varphi &= \sum_{1\le i\le n} \alpha_i w_i^\star,\\
\Delta_\varphi(\underline{w}, X) &= \sum_{1\le i\le n} \alpha_i (-1)^{i-1} \Delta_n(\underline{\widehat{w}_i}, X),\\
\delta_\varphi(\underline{w}) &= \sum_{1\le i\le n} \alpha_i (-1)^{i-1} \Delta_{n-1}(\underline{\widehat{w}_i}).
\end{aligned}$$

Let $P_W \in K[X]$ (resp. $P_{\operatorname{Ker}\varphi} \in K[X]$) be the monic (resp. reduced) polynomial whose set of roots is W (resp. $\operatorname{Ker}\varphi$).

Then (2.7) is satisfied with $W_1 := \operatorname{Ker}\varphi$, and

$$\begin{aligned}
P_{\operatorname{Ker}\varphi}(X) &= \frac{\Delta_\varphi(\underline{w}, X)}{\delta_\varphi(\underline{w})},\\
P_{P_{\operatorname{Ker}\varphi}(W)}(X) &= X^q - \Big(\frac{\Delta_n(\underline{w})}{\delta_\varphi(\underline{w})}\Big)^{q-1} X,
\end{aligned}$$

thus

$$\frac{P_{\operatorname{Ker}\varphi}(X)}{P_W(X)} = \frac{\Delta_n(\underline{w})}{\delta_\varphi(\underline{w})}\frac{\Delta_\varphi(\underline{w},X)}{\Delta_{n+1}(\underline{w},X)} = \frac{1}{P_{\operatorname{Ker}\varphi}(X)^{q-1} - \left(\frac{\Delta_n(\underline{w})}{\delta_\varphi(\underline{w})}\right)^{q-1}}.$$

Proof. Since $\operatorname{Ker}\varphi$ is a hyperplane of W, it follows that $P_{P_{\operatorname{Ker}\varphi}(W)}(X) = X^q - c_\varphi X \in K[X]$. Thus, with (2.7) we have $P_W(X) = P_{W_1}(X)^q - c_\varphi P_{W_1}(X)$. Since $\operatorname{coeff}_X P_W = (-1)^n \Delta_n(\underline{w})^{q-1}$ (cf. (2.2) and (2.3)), $\operatorname{coeff}_X P_{W_1} = (-1)^{n+1}\delta_\varphi(\underline{w})^{q-1}$, the corollary follows. ∎

3. Vector spaces of differentials and Moore determinants

3.1 – *The $L^q_{\mu+1,n}$ spaces*

Definition 3.1. Let K be a field of characteristic $p > 0$. Let $\mu \in \mathbb{N}$ with $\mu \geq 2$ prime to p and $n \geq 1$. We call an $L_{\mu+1,n}$ space an $\mathbb{F}_p$-vector space of dimension n of logarithmic differential forms in $\Omega^1_K(K(X))$, whose non-zero elements have $(\mu-1)\infty$ as zero divisor and their poles are in K (such a form has $\mu+1$ poles and they are simple).

One can show [9, Lemme 6, p. 63] that if such a space exists then p^{n-1} divides $\mu + 1$.

Such $\mathbb{F}_p$-vector spaces have been constructed for $n \geq 1$ in [4] in order in particular to lift in null characteristic certain $(\mathbb{Z}/p\mathbb{Z})^n$-coverings of the projective line $\mathbb{P}^1_K$ into Galoisian coverings of the group $(\mathbb{Z}/p\mathbb{Z})^n$. See [7] for a presentation of recent contributions on the subject.

The $L_{\mu+1,n}$ spaces have been defined and studied by Pagot in his thesis ([10, p. 19]), a part of which is published in [9]. See also [5] for complements.

We will consider a generalization to the case where $\mathbb{F}_p$ is replaced by the field $\mathbb{F}_q$ with $q = p^s$.

Definition 3.2. Let K be a field which contains $\mathbb{F}_q$. Let $\mu \in \mathbb{N}$ with $\mu \geq 2$ prime to p and $n \geq 1$. We call an $L^q_{\mu+1,n}$ space an $\mathbb{F}_q$-vector space of dimension n of logarithmic differential forms in $\Omega^1_K(K(X))$ whose non-zero elements have $(\mu-1)\infty$ as zero divisor, such that their poles are simple and in K (so there are $\mu+1$ poles) and such that their residues are in $\mathbb{F}_q$.

Proposition 3.1. *Let K be a field containing $\mathbb{F}_q$, W an $\mathbb{F}_q$-subspace of K with $\dim_{\mathbb{F}_q} W = n$, $\underline{w} := (w_1, \ldots, w_n) \in K^n$ an $\mathbb{F}_q$-basis of W and $\underline{w^\star} := (w_1^\star, \ldots, w_n^\star)$*

its dual basis. For $j \in \{1, \dots, n\}$, *we note that*

$$\omega_j := \sum_{(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \mathbb{F}_q^n} \frac{\varepsilon_j}{X - \sum_{i=1}^n \varepsilon_i w_i} \, dX.$$

Let $\underline{\alpha} := (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n - \{(0, \dots, 0)\}$, $\varphi = \sum_{1 \le i \le n} \alpha_i w_i^\star$ *and*

$$\omega_\varphi := \sum_{1 \le j \le n} \alpha_j \omega_j = \sum_{(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \mathbb{F}_q^n} \frac{\sum_{1 \le j \le n} \alpha_j \varepsilon_j}{X - \sum_{i=1}^n \varepsilon_i w_i} \, dX.$$

Then

$$\omega_\varphi = -\Delta_n(\underline{w})^{q-1} \frac{\Delta_\varphi(\underline{w}, X)}{\Delta_{n+1}(\underline{w}, X)} \, dX$$

and $\Delta_\varphi(\underline{w}, X) \mid \Delta_{n+1}(\underline{w}, X)$ *(cf. Proposition 2.3).*

Thus, $\Omega_W := \sum_{1 \le j \le n} \mathbb{F}_q \omega_j \subset \Omega_K^1(K(X))$ *is* $L_{\mu+1,n}^q$ *with* $\mu + 1 := q^{n-1}(q-1)$.

Proof. Let $\omega \in \Omega_W$ and $\underline{\alpha} := (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_q^n - \{(0, 0, \dots, 0)\}$ with $\omega = \sum_{1 \le j \le n} \alpha_j \omega_j$. Then

$$\omega = \sum_{(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \mathbb{F}_q^n} \frac{\sum_{1 \le j \le n} \alpha_j \varepsilon_j}{X - \sum_{i=1}^n \varepsilon_i w_i} \, dX.$$

It follows that the poles of ω are the elements of W deprived of the zeros of the $\mathbb{F}_q$-linear form $\varphi = \sum_{1 \le i \le n} \alpha_i w_i^\star$, so they are of cardinal $q^n - q^{n-1} =: \mu + 1$ and they are simple. The residues by construction are in $\mathbb{F}_q$. In particular, $\omega \neq 0$ and therefore Ω_W is an $\mathbb{F}_q$-vector space of dimension n.

It remains to see that the zero divisor of ω is $(\mu - 1)\infty$. For that we consider the fraction

$$F(X) := -\Delta_n(\underline{w})^{q-1} \frac{\Delta_\varphi(\underline{w}, X)}{\Delta_{n+1}(\underline{w}, X)}.$$

The poles of F are the elements of $W - \operatorname{Ker} \varphi$ and they are simple (Corollary 2.2).

Let $w \in W$ with $\varphi(w) \neq 0$. Then

$$\operatorname{res}_w F(X) = -\Delta_n(\underline{w})^{q-1} \frac{\Delta_\varphi(\underline{w}, w)}{\Delta_{n+1}(\underline{w}, X)'(w)}.$$

We have $w = \sum_{i=1}^n \varepsilon_i(w) w_i$ with $\varepsilon_i(w) \in \mathbb{F}_q$; thus (cf. Proposition 2.3)

$$\begin{aligned} \Delta_\varphi(\underline{w}, w) &= \sum_{1 \le i \le n} \alpha_i (-1)^{i-1} \Delta_n(\widehat{\underline{w}_i}, w) \\ &= \sum_{1 \le i \le n} \alpha_i (-1)^{i-1} \varepsilon_i(w) \Delta_n(\widehat{\underline{w}_i}, w_i) \end{aligned}$$

$$= \sum_{1\le i\le n} \alpha_i (-1)^{i-1} \varepsilon_i(w)(-1)^{n-i}\Delta_n(\underline{w})$$
$$= (-1)^{n-1}\Big(\sum_{1\le i\le n} \alpha_i\varepsilon_i(w)\Big)\Delta_n(\underline{w}).$$

Finally (cf. Proposition 2.2), $\Delta_{n+1}(\underline{w}, X)'(w) = (-1)^n \Delta_n(\underline{w})^q$.
Thus,

$$\operatorname{res}_w F(X) = -\Delta_n(\underline{w})^{q-1}\frac{(-1)^{n-1}(\sum_{1\le i\le n}\alpha_i\varepsilon_i(w))\Delta_n(\underline{w})}{(-1)^n\Delta_n(\underline{w})^q} = \sum_{1\le i\le n}\alpha_i\varepsilon_i(w),$$

and so $\omega = \omega_\varphi$. It follows that the zeros of ω are concentrated at infinity (Corollary 2.2).

■

Remark 3.1. In [10, Remark 4, p. 29], Pagot remarks that if K is algebraically closed then the pullback by a morphism $\Phi\colon \mathbb{P}^1_K \to \mathbb{P}^1_K$ with $\Phi(X) = \alpha X + X^p P(X^p)$, where $\alpha \in K^\star$ and $P \in K[X]$, of an $L_{\mu+1,n}$ space is an $L_{(\mu+1)\deg\Phi,n}$ space. Similarly an exercise shows that the pullback of an $L^q_{\mu+1,n}$ space is an $L^q_{(\mu+1)\deg\Phi,n}$ space. We can thus construct new $L^q_{\mu+1,n}$ spaces, for example from Proposition 3.1.

3.2 – $L^q_{\mu+1,n}$ *spaces and Elkies pairing*

In this section, K denotes a field that contains $\mathbb{F}_q$, W is an $\mathbb{F}_q$-vector space of K with $\dim_{\mathbb{F}_q} W = n$, $\underline{w} := (w_1, \dots, w_n) \in K^n$, an $\mathbb{F}_q$-basis of W and $\underline{w^\star} := (w_1^\star, \dots, w_n^\star)$ its dual basis. Finally, let $\widehat{W} := \bigoplus_{1\le i\le n} \mathbb{F}_q \Delta_{n-1}(\underline{\widehat{w}_i})$ and $U := (\frac{\widehat{W}}{\Delta_n(\underline{w})})^q$. Recall that $U = \operatorname{Ker}\rho P_W$, where ρP_W is the reversed polynomial of the polynomial P_W (cf. Proposition 2.2, Definition 2.3, Proposition 2.4).

We will recall the construction of an Elkies pairing attached to the monic $\mathbb{F}_q$-linear polynomial P_W. It puts in duality the two $\mathbb{F}_q$-subvector spaces of K, which are W and U, and we will give a differential interpretation of it using the $L^q_{\mu+1,n}$ spaces defined in Proposition 3.1.

(A) Elkies pairing. Elkies [2, §4.35] defines an $\mathbb{F}_q$-perfect pairing $E\colon W \times U \to \mathbb{F}_q$ as follows. He first observes that if $(w,u) \in W \times U$ then $0 = w((\rho P_W)(u))^{q^{-n}} - uP_W(w) = E(w,u) - E(w,u)^q$, where

$$E(w,u) := \sum_{1\le m\le n}\ \sum_{0\le j\le m-1} ((c_m u)^{q^{-m}} w)^{q^j}, \quad P_W(X) = \sum_{0\le m\le n} c_m X^{q^m}$$

and $c_n = 1$. It follows that $E(w,u) \in \mathbb{F}_q$.

(B) The pairing $f : W \times U \to \mathbb{F}_q$. We will see that Proposition 3.1 allows us to define an $\mathbb{F}_q$-pairing $f : W \times U \to \mathbb{F}_q$ given by the residue of differential forms.

To be precise, if $w \in W$ and $u \in U$ are different from 0, we can write $w = \sum_{i=1}^{n} \varepsilon_i(\underline{w}, w) w_i$ in the basis $\underline{w}$ of W where $(\varepsilon_1(\underline{w}, w), \ldots, \varepsilon_n(\underline{w}, w)) \in \mathbb{F}_q^n - \{0\}$ and by definition of U we can write

$$u = \left(\frac{\sum_{1 \le i \le n} \alpha_i (-1)^{i-1} \Delta_{n-1}(\widehat{\underline{w}_i})}{\Delta_n(\underline{w})} \right)^q,$$

where $\underline{\alpha} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n - \{(0, \ldots, 0)\}$. Let $\varphi := \sum_{1 \le i \le n} \alpha_i w_i^\star$. Then (cf. Proposition 2.3)

$$u = \left(\frac{\delta_\varphi(\underline{w})}{\Delta_n(\underline{w})} \right)^q \quad \text{with } \delta_\varphi(\underline{w}) = \sum_{1 \le i \le n} \alpha_i (-1)^{i-1} \Delta_{n-1}(\widehat{\underline{w}_i}). \tag{3.1}$$

Let $\Omega_{\widehat{W}} := \sum_{1 \le j \le n} \mathbb{F}_q \omega_j \subset \Omega^1_K(K(X))$ be the $L^q_{\mu+1,n}$ space with $\mu + 1 := q^{n-1}(q-1)$ as defined in Proposition 3.1 and let

$$\omega_\varphi := \sum_j \alpha_j \omega_j = \sum_{(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \in \mathbb{F}_q^n} \frac{\sum_{1 \le j \le n} \alpha_j \varepsilon_j}{X - \sum_{i=1}^n \varepsilon_i w_i} \, dX \in \Omega_{\widehat{W}} - \{0\}.$$

Then we define

$$f(w, u) := (-1)^{n-1} \operatorname{res}_w \omega_\varphi = (-1)^{n-1} \sum_{1 \le j \le n} \alpha_j \varepsilon_j(\underline{w}, w) \in \mathbb{F}_q.$$

Lemma 3.1. *The pairing f is perfect.*

Proof. Let $u \in U$ and let us assume that $f(w, u) = 0$ for all $w \in W$. It follows from (3.1) that

$$u = \left(\frac{\delta_\varphi(\underline{w})}{\Delta_n(\underline{w})} \right)^q \quad \text{with } \delta_\varphi(\underline{w}) = \sum_{1 \le i \le n} \alpha_i (-1)^{i-1} \Delta_{n-1}(\widehat{\underline{w}_i}),$$

where $\underline{\alpha} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$ and $\varphi = \sum_{1 \le i \le n} \alpha_i w_i^\star$.

Thus, for any $w \in W$, the residue at w of the differential form $\omega_\alpha = \sum \alpha_i \omega_i$ is zero and since the poles of ω_α are simple, this form is the null form. Thus, $\alpha_i = 0$ for $1 \le i \le n$; it follows that $\delta_\varphi(\underline{w})$ and thus u are zero.

Now let $w \in W$, and let us assume that $f(w, u) = 0$ for all u in $\widehat{W}$. It follows from Proposition 3.1 that 0 is the only element of W which is not a pole of one of the ω_i forms, so $w = 0$. ∎

(C) Comparison of the two pairings E and f.

Proposition 3.2. *The two pairings E and f are equal.*

Proof. Let $w_1, w_2, \dots, w_n$ be a basis of W, $w \in W - \{0\}$ and $u \in U - \{0\}$. It follows from (3.1) that $u = (\frac{\delta_\varphi(w)}{\Delta_n(\underline{w})})^q$ where $\underline{\alpha} := (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n - \{(0, \dots, 0)\}$ and $\varphi = \sum_{1 \le i \le n} \alpha_i w_i^\star$.

As from Proposition 3.1 we have $\omega_\varphi = -\Delta_n(\underline{w})^{q-1} \frac{\Delta_\varphi(\underline{w}, X)}{\Delta_{n+1}(\underline{w}, X)}\, dX$, it follows from (2.3) and Corollary 2.2 that

$$f(w,u) = (-1)^{n-1} \operatorname{res}_w \omega_\varphi = (-1)^n \Delta_n(\underline{w})^{q-1} \frac{\delta_\varphi(\underline{w}) P_{\operatorname{Ker}\varphi}(w)}{(-1)^n \Delta_n(\underline{w}) \Delta_n(\underline{w})^{q-1}}$$
$$= u^{1/q} P_{\operatorname{Ker}\varphi}(w),$$

where $P_{\operatorname{Ker}\varphi}(X)$ is a monic polynomial of degree q^{n-1} (cf. (2.3)). On the other hand, $E(w,u) = u^{1/q} P_u(w)$, where $P_u(X)$ is a monic $\mathbb{F}_q$-linear polynomial of degree q^{n-1} [2, Lemma, p. 92, proof].

It then remains to compare the two polynomials $P_u(X)$ and $P_{\operatorname{Ker}\varphi}(X)$.

As $P_u(X)$ and $P_{\operatorname{Ker}\varphi}(X)$ divide $P_W(X)$ in $K[X]$ and as $\operatorname{Ker} P_{\operatorname{Ker}\varphi}$ (resp. $\operatorname{Ker} P_u$) is a hyperplane in W, we have (Proposition 2.6) $P_W = Q_\varphi \circ P_{\operatorname{Ker}\varphi} = Q_u \circ P_u$ in $K[X]$, where $Q_\varphi(X) = X^q - q_\varphi X$ and $Q_u = X^q - q_u X$ with q_φ, q_u non-zero elements in K. In particular, $\operatorname{coeff}_X(P_W) = -q_\varphi \operatorname{coeff}_X(P_{\operatorname{Ker}\varphi}) = -q_u \operatorname{coeff}_X(P_u)$. We have $\operatorname{coeff}_X(P_u) = -(-1)^n \Delta_n(\underline{w})^{q-1} u^{\frac{q-1}{q}}$ [2, Lemma, p. 92, proof]. From Corollary 2.2 we know that

$$q_\varphi = (\frac{\Delta_n(\underline{w})}{\delta_\varphi(\underline{w})})^{q-1} \quad \text{and} \quad \operatorname{coeff}_X(P_W) = (-1)^n \Delta_n(\underline{w})^{q-1}$$

(cf. (2.2)) and so $\operatorname{coeff}_X(P_{\operatorname{Ker}\varphi}) = \operatorname{coeff}_X(P_u)$; hence $q_\varphi = q_u$.

The equality $Q_\varphi = Q_u$ then follows from the uniqueness of the decomposition in Proposition 2.6. ∎

4. A property of $L^q_{\mu+1,n}$ spaces

4.1 – *The property*

Proposition 4.1. *Let $n \ge 2$ and Ω be an $L^q_{\mu+1,n}$-space (Definition 3.2) and $\underline{\omega} := (\omega_1, \omega_2, \dots, \omega_n)$ an $\mathbb{F}_q$-basis. Let $\mathcal{P}(\Omega) \subset K$ be the set of poles of the differentials in Ω and $P(X) := \prod_{x \in \mathcal{P}(\Omega)} (X - x)$. Let $P_i \in K[X]$ with $\omega_i = \frac{P_i}{P}\, dX$ for $1 \le i \le n$. Then there is $\gamma \in K^\star$ with*

$$\Delta_n(P_1, \dots, P_n) = \gamma P^{1+q+\cdots+q^{n-2}}. \tag{4.1}$$

Proof. Thanks to (2.1) we can write

$$\Delta_n(P_1,\dots,P_n)=\prod_{1\le i\le n}\prod_{\varepsilon_{i-1}\in\mathbb{F}_q}\cdots\prod_{\varepsilon_1\in\mathbb{F}_q}(P_i+\varepsilon_{i-1}P_{i-1}+\cdots+\varepsilon_1P_1).$$

By hypothesis, each factor $P_i+\varepsilon_{i-1}P_{i-1}+\cdots+\varepsilon_1P_1$ divides P and factorizes into a product of distinct irreducible polynomials of degree 1. Thus, for $x\in\mathcal{P}(\Omega)$, we must show that x is a root of $1+q+\cdots+q^{n-2}$ polynomials $P_i+\varepsilon_{i-1}P_{i-1}+\cdots+\varepsilon_1P_1$ with $(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{i-1},1,0,0,\dots,0)\in\mathbb{F}_q^n$.

Let $x\in\mathcal{P}(\Omega)$. Since x is a pole of at least one of the ω_i forms, the tuple $(\operatorname{res}_x\omega_i)_{1\le i\le n}\in\mathbb{F}_q^n-\{(0,\dots,0)\}$. Let $\varphi_x\colon\Omega\to\mathbb{F}_q$ be the linear form with $\varphi_x(\omega)=\sum_{1\le i\le n}\alpha_i\operatorname{res}_x\omega_i$, where $\omega=\sum_{1\le i\le n}\alpha_i\omega_j$. Then φ_x is an $\mathbb{F}_q$-linear non-zero form. If $(\alpha_1:\alpha_2:\cdots:\alpha_n)\in\mathbb{P}^n(\mathbb{F}_q)$, then $\varphi_x(\omega)=\sum_{1\le i\le n}\alpha_i\operatorname{res}_x\omega_i=0$ if and only if $\sum_{1\le i\le n}\alpha_iP_i(x)=0$. Then, as $\{(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{i-1},1,0,0,\dots,0),1\le i\le n\}\in\mathbb{F}_q^n$ is a system of representatives of the elements of $\mathbb{P}^n(\mathbb{F}_q)$, the multiplicity of the zero x in $\Delta_n(P_1,\dots,P_n)$ is equal to the number of points of the hyperplane of $\mathbb{P}^n(\mathbb{F}_q)$ induced by $\operatorname{Ker}\varphi_x$, so it is equal to $1+q+\cdots+q^{n-2}$.

Finally, by Proposition 2.1, γ is not zero since the n fractions $\frac{P_i}{P}$ are $\mathbb{F}_q$-linearly independent. ∎

Remark 4.1. Proposition 4.1 is a remark in [9, p. 68] in the framework of $L_{\mu+1,n}$-spaces of logarithmic differentials (i.e. $q=p$).

4.2 – *An equality between Moore's determinants* (I)

Corollary 4.1. *Let* $(\underline{Y}):=(Y_1,Y_2,\dots,Y_n)$ *and* $(\underline{X}):=(X_1,X_2,\dots,X_m)$ *be* $n+m$ *indeterminates over* $\mathbb{F}_q$, *where* $n\ge2$, $m\ge0$ *and we apply the convention that* $\underline{X}=\emptyset$ *and* $\Delta_m(\underline{X})=1$ *if* $m=0$. *For* $1\le i\le n$, *we write* $(\widehat{\underline{Y}_i}):=(Y_1,\dots,Y_{i-1},Y_{i+1},\dots,Y_n)$. *Then we have the following equality in* $\mathbb{F}_q(\underline{Y},\underline{X})$:

$$\begin{aligned}&\frac{\Delta_n\big(\Delta_{n-1+m}(\widehat{\underline{Y}_1},\underline{X}),\dots,(-1)^{i+1}\Delta_{n-1+m}(\widehat{\underline{Y}_i},\underline{X}),\dots,(-1)^{n+1}\Delta_{n-1+m}(\widehat{\underline{Y}_n},\underline{X})\big)}{\Delta_m(\underline{X})^{q^{n-1}}\Delta_{n+m}(\underline{Y},\underline{X})^{1+q+\cdots+q^{n-2}}}\\&=\frac{\Delta_n(\Delta_{n-1}(\widehat{\underline{Y}_1}),\dots,(-1)^{i+1}\Delta_{n-1}(\widehat{\underline{Y}_i}),\dots,(-1)^{n+1}\Delta_{n-1}(\widehat{\underline{Y}_n})}{\Delta_n(\underline{Y})^{1+q+\cdots+q^{n-2}}}=:\gamma.\end{aligned}\tag{4.2}$$

Proof. Let $A:=\mathbb{F}_q[\underline{Y},\underline{X}]$ and K be its fraction field. For $j\in\{1,\dots,n+m\}$, we denote

$$\omega_j:=\sum_{(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{n+m})\in\mathbb{F}_q^{n+m}}\frac{\varepsilon_j\,dZ}{Z-\sum_{i=1}^n\varepsilon_iY_i-\sum_{i=1}^m\varepsilon_{n+i}X_i}.$$

Then $\Omega_{\underline{Y},\underline{X}} := \sum_{1\le j\le n+m} \mathbb{F}_q\omega_j \subset \Omega^1_K(K(Z))$ is an $L^q_{\mu+1,n+m}$-space, where $\mu + 1 := q^{n-1+m}(q-1)$ and $\Omega_{\underline{Y}} := \sum_{1\le j\le n} \mathbb{F}_q\omega_j \subset \Omega^1_K(K(Z))$ is an n-dimensional $\mathbb{F}_q$-subspace Ω of $\Omega_{\underline{Y},\underline{X}}$, hence it is an $L^q_{\mu+1,n}$-space.

We apply Proposition 3.1 to this last space Ω.

For $1 \le i \le n$, we have

$$\omega_i = -\Delta_{n+m}(\underline{Y},\underline{X})^{q-1}\frac{\Delta_{n+m}(\underline{\widehat{Y}_i},\underline{X},Z)}{\Delta_{n+m+1}(\underline{Y},\underline{X},Z)}\,dZ.$$

It follows that $\mathcal{P}(\Omega) = \{\sum_{i=1}^n \varepsilon_i Y_i + \sum_{i=1}^m \varepsilon_{n+i}X_i\}$ with $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{n+m}) \in \mathbb{F}_q^{n+m}$, $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n) \ne (0,\ldots,0)$ is the set of poles $\mathcal{P}(\Omega) \subset K$ of the elements of Ω .

Thus,

$$P(Z) := \prod_{z\in\mathcal{P}(\Omega)}(Z-z) = \frac{\Delta_m(\underline{X})}{\Delta_{n+m}(\underline{Y},\underline{X})}\frac{\Delta_{n+m+1}(\underline{Y},\underline{X},Z)}{\Delta_{m+1}(\underline{X},Z)}$$

(cf. (2.2)) and $\omega_i = \frac{P_i}{P}\,dZ$, where

$$\frac{P_i}{P} = -\Delta_{n+m}(\underline{Y},\underline{X})^{q-1}\frac{\Delta_{n+m}(\underline{\widehat{Y}_i},\underline{X},Z)}{\Delta_{n+m+1}(\underline{Y},\underline{X},Z)}.$$

Equality (4.1) in Proposition 4.1 then gives

$$\begin{aligned}&\Delta_n\big(\Delta_{n+m}(\underline{\widehat{Y}_1},\underline{X},Z),\ldots,(-1)^{i+1}\Delta_{n+m}(\underline{\widehat{Y}_i},\underline{X},Z),\ldots,\\ &\qquad(-1)^{n+1}\Delta_{n+m}(\underline{\widehat{Y}_n},\underline{X},Z)\big)\\ &\qquad= \gamma\Delta_{m+1}(\underline{X},Z)^{q^{n-1}}\Delta_{n+m+1}(\underline{Y},\underline{X},Z)^{1+q+\cdots+q^{n-2}},\end{aligned}\tag{4.3}$$

where $\gamma \in \mathbb{F}_q(\underline{Y},\underline{X})$.

Finally, the comparison in equality (4.3) of the coefficients of higher degree in Z gives the equality

$$\begin{aligned}&\Delta_n\big(\Delta_{n-1+m}(\underline{\widehat{Y}_1},\underline{X}),\ldots,(-1)^{i+1}\Delta_{n-1+m}(\underline{\widehat{Y}_i},\underline{X}),\ldots,(-1)^{n+1}\Delta_{n-1+m}(\underline{\widehat{Y}_n},\underline{X})\big)\\ &\quad= \gamma\Delta_m(\underline{X})^{q^{n-1}}\Delta_{n+m}(\underline{Y},\underline{X})^{1+q+\cdots+q^{n-2}}.\end{aligned}$$

By making X_m play the role played by Z in (4.3) we deduce that

$$\begin{aligned}&\Delta_n\big(\Delta_{n+m-2}(\underline{\widehat{Y}_1},X_1,\ldots,X_{m-1}),\ldots,(-1)^{i+1}\Delta_{n-1+m-1}(\underline{\widehat{Y}_i},X_1,\ldots,X_{m-1}),\ldots,\\ &\qquad(-1)^{n+1}\Delta_{n-1+m-1}(\underline{\widehat{Y}_n},X_1,\ldots,X_{m-1})\big)\\ &\quad= \gamma\Delta_{m-1}(X_1,\ldots,X_{m-1})^{q^{n-1}}\Delta_{n-1+m-1}(\underline{Y},X_1,\ldots,X_{m-1})^{1+q+\cdots+q^{n-2}}.\end{aligned}$$

By iterating the process we exhaust $\underline{X}$, hence

$$\begin{aligned}\Delta_n\big(\Delta_{n-1}(\underline{\widehat{Y}_1}),\dots,(-1)^{i+1}\Delta_{n-1}(\underline{\widehat{Y}_i}),\dots,(-1)^{n-1}\Delta_{n-1}(\underline{\widehat{Y}_n})\big)\\ =\gamma\Delta_n(\underline{Y})^{1+q+\cdots+q^{n-2}},\end{aligned}$$

as announced. ∎

4.3 – *An equality between Moore's determinants* (II)

We show in two different ways that the constant γ in (4.2) is equal to 1.
Thus we can state the theorem.

Theorem 4.1. *Let* $(\underline{Y}) \coloneqq (Y_1, Y_2, \dots, Y_n)$ *and* $(\underline{X}) \coloneqq (X_1, X_2, \dots, X_m)$ *be* $n+m$ *indeterminates over* $\mathbb{F}_q$*, where* $n \geq 2$*,* $m \geq 0$ *and we apply the convention that* $\underline{X} = \emptyset$ *and* $\Delta_m(\underline{X}) = 1$ *for* $m = 0$*. We write* $(\underline{\widehat{Y}_i}) \coloneqq (Y_1, \dots, Y_{i-1}, Y_{i+1}, \dots, Y_n)$ *for* $1 \leq i \leq n$*.*

Then we have the following polynomial equalities in $\mathbb{F}_q[X, Y]$*:*

$$\begin{aligned}\widetilde{\Delta}_{n,m}(\underline{Y},\underline{X}) &\coloneqq \Delta_n\big(\Delta_{n-1+m}(\underline{\widehat{Y}_1},\underline{X}),\dots,(-1)^{i+1}\Delta_{n-1+m}(\underline{\widehat{Y}_i},\underline{X}),\dots,\\ &\qquad (-1)^{n+1}\Delta_{n-1+m}(\underline{\widehat{Y}_n},\underline{X})\big)\\ &= \Delta_m(\underline{X})^{q^{n-1}}\Delta_{n+m}(\underline{Y},\underline{X})^{1+q+\cdots+q^{n-2}},\end{aligned}\tag{4.4}$$

which is also (compare to (4.1)*)*

$$\begin{aligned}\Delta_n\Big(\frac{\Delta_{n-1+m}(\underline{\widehat{Y}_1},\underline{X})}{\Delta_m(\underline{X})},\dots,\frac{\Delta_{n-1+m}(\underline{\widehat{Y}_i},\underline{X})}{\Delta_m(\underline{X})},\dots,\frac{\Delta_{n-1+m}(\underline{\widehat{Y}_n},\underline{X})}{\Delta_m(\underline{X})}\Big)\\ =(-1)^{\lfloor\frac{n}{2}\rfloor}\Big(\frac{\Delta_{n+m}(\underline{Y},\underline{X})}{\Delta_m(\underline{X})}\Big)^{1+q+\cdots+q^{n-2}},\end{aligned}$$

where $\lfloor\frac{n}{2}\rfloor$ *is the lower integer part of* $\frac{n}{2}$*. We remark that* $\Delta_m(\underline{X})$ *divides* $\Delta_{n+m}(\underline{Y},\underline{X})$ *thanks to* (2.1)*.*

We deduce by specialization of formula (4.4) the following corollary:

Corollary 4.2. *Let* A *be a commutative ring containing* $\mathbb{F}_q$*. Let* $(\underline{a}) \coloneqq (a_1, a_2, \dots, a_n) \in A^n$ *and* $(\underline{b}) \coloneqq (b_1, b_2, \dots, b_m) \in A^m$*, where* $n \geq 2$*,* $m \geq 0$ *and we apply the convention that* $\underline{b} = \emptyset$ *and* $\Delta_m(\underline{b}) = 1$ *for* $m = 0$*. Then*

$$\begin{aligned}\Delta_n\big(\Delta_{n-1+m}(\underline{\hat{a}_1},\underline{b}),\dots,(-1)^{i+1}\Delta_{n-1+m}(\underline{\hat{a}_i},\underline{b}),\dots,(-1)^{n+1}\Delta_{n-1+m}(\underline{\hat{a}_n},\underline{b})\big)\\ =\Delta_m(\underline{b})^{q^{n-1}}\Delta_{n+m}(\underline{a},\underline{b})^{1+q+\cdots+q^{n-2}}.\end{aligned}$$

4.4 – *First proof of Theorem* 4.1. *The case* $m = 1$ *by induction on* n

(A) We check (4.4) for $(n, m) = (2, 1)$. i.e.

$$\Delta_2\Big(\frac{\Delta_2(Y_2, X)}{X}, -\frac{\Delta_2(Y_1, X)}{X}\Big) = \frac{\Delta_3(Y_1, Y_2, X)}{X}.$$

This is an equality between polynomials in the variable X of degree $q^2 - 1$. The terms of higher degree are equal as $\Delta_2(\Delta_1(Y_2X^{q-1}), -\Delta_1(Y_1X^{q-1})) = \Delta_2(Y_1, Y_2)X^{q^2-1}$. For $Y_{\underline{\alpha}} := \alpha_1Y_1 + \alpha_2Y_2$ with $\underline{\alpha} \in \mathbb{F}_q^2$, we have $\Delta_2(\Delta_2(Y_2, Y_{\underline{\alpha}}), \Delta_2(Y_1, Y_{\underline{\alpha}})) = 0$, thus the two polynomials have the same zeros (see (2.2)). Hence the equality.

(B) We assume that $m = 1$ and we proceed by induction on n. Let us assume that (4.4) is satisfied for $m = 1$ and up to rank n. We show it for $m = 1$ and $n + 1$.

(B1) We show the equality of the coefficients of highest degree in (4.4) for $m = 1$ and $n + 1$; it is also (4.4) for $m = 0$ and $n + 1$.

Let $(\underline{Y}) := (Y_1, Y_2, \dots, Y_{n+1})$ be $n + 1$ indeterminates over $\mathbb{F}_q$. Let j be such that $1 \le j \le n + 1$. We apply (4.4) to the n indeterminates $(Y_1, \dots, Y_{j-1}, \widehat{Y}_j, Y_{j+1}, \dots, Y_{n+1}) := \underline{\widehat{Y}_j}$ over $\mathbb{F}_q$ and we specialize X in Y_j. Thus,

$$\begin{aligned}
&\Delta_n\big(\Delta_n(\widehat{Y}_1, \dots, \widehat{Y}_j, \dots, Y_{n+1}, Y_j), \dots,\\
&\qquad \Delta_n(Y_1, \dots, \widehat{Y}_i, \dots, \widehat{Y}_j, \dots, Y_{n+1}, Y_j), \dots,\\
&\qquad \Delta_n(Y_1, \dots, \widehat{Y}_j, \dots, Y_n, \widehat{Y}_{n+1}, Y_j)\big)\\
&= (-1)^{\lfloor \frac{n}{2} \rfloor}\widetilde{\Delta}_{n,1}(\underline{\widehat{Y}_j}, Y_j) \qquad \text{(cf. (4.4))}\\
&= (-1)^{\lfloor \frac{n}{2} \rfloor}Y_j^{q^{n-1}}\Delta_{n+1}(Y_1, \dots, \widehat{Y}_j, \dots, Y_{n+1}, Y_j)^{1+q+\cdots+q^{n-2}}\\
&= (-1)^{\lfloor \frac{n}{2} \rfloor}Y_j^{q^{n-1}}((-1)^{n+1-j}\Delta_{n+1}(\underline{Y}))^{1+q+\cdots+q^{n-2}}\\
&= (-1)^{\lfloor \frac{n}{2} \rfloor}(-1)^{(n-1)(n+1-j)}Y_j^{q^{n-1}}\Delta_{n+1}(\underline{Y})^{1+q+\cdots+q^{n-2}}. \qquad (4.5)
\end{aligned}$$

Below, we use the following three identities:

- For $1 \le j < i \le n + 1$, we have

$$\begin{aligned}
&\Delta_n(Y_1, \dots, \widehat{Y}_j, \dots, Y_i, \dots, Y_{n+1})\\
&\qquad = (-1)^{n+1-i}\Delta_n(Y_1, \dots, \widehat{Y}_j, \dots, \widehat{Y}_i, \dots, Y_{n+1}, Y_i).
\end{aligned}$$

- For $1 \le i < j \le n + 1$, we have

$$\begin{aligned}
&\Delta_n(Y_1, \dots, Y_i, \dots, \widehat{Y}_j, \dots, Y_{n+1})\\
&\qquad = (-1)^{n-i}\Delta_n(Y_1, \dots, \widehat{Y}_i, \dots, \widehat{Y}_j, \dots, Y_{n+1}, Y_i).
\end{aligned}$$

- For $1 \le i \le n+1$, we have

$$\Delta_{n+1}(Y_1, \dots, \widehat{Y_i}, \dots, Y_{n+1}, Y_i) = (-1)^{n+1-i} \Delta_{n+1}(\underline{Y}).$$

Then it follows with (4.5) that for $1 \le i \le n+1$,

$$\begin{aligned}
&\Delta_n\big(\Delta_n(\underline{\widehat{Y}_1}), \Delta_n(\underline{\widehat{Y}_2}), \dots, \widehat{\Delta}_n(\underline{\widehat{Y}_i}), \dots, \Delta_n(\underline{\widehat{Y}_{n+1}})\big) \\
&\quad = \Delta_n\big(\Delta(\widehat{Y}_1, Y_2, \dots, Y_i, \dots, Y_{n+1}), \dots, \Delta_n(Y_1, \dots, \widehat{Y}_{i-1}, Y_i, \dots, Y_{n+1}), \\
&\qquad\quad \Delta_n(Y_1, \dots, Y_{i-1}, Y_i, \widehat{Y}_{i+1}, \dots, Y_{n+1}), \dots, \\
&\qquad\quad \Delta_n(Y_1, \dots, Y_i, \dots, \widehat{Y}_{n+1})\big) \\
&\quad = (-1)^{(n+1-i)(i-1)+(n-i)(n+1-i)} (-1)^{\lfloor \frac{n}{2} \rfloor} \widetilde{\Delta}_{n,1}(\underline{\widehat{Y}_i}, Y_i) \\
&\quad = (-1)^{(n+1-i)(i-1)+(n-i)(n+1-i)} (-1)^{\lfloor \frac{n}{2} \rfloor} (-1)^{(n-1)(n-i+1)} Y_i^{q^{n-1}} \\
&\qquad \times \Delta_{n+1}(\underline{Y})^{1+q+\cdots+q^{n-2}} \\
&\quad = (-1)^{\lfloor \frac{n}{2} \rfloor} Y_i^{q^{n-1}} \Delta_{n+1}(\underline{Y})^{1+q+\cdots+q^{n-2}}. \qquad (4.6)
\end{aligned}$$

Thus, by developing the determinant $\Delta_{n+1}(\Delta_n(\underline{\widehat{Y}_1}), \dots, \Delta_n(\underline{\widehat{Y}_i}), \dots, \Delta_n(\underline{\widehat{Y}_{n+1}}))$ along the first row, it follows that

$$\begin{aligned}
&\Delta_{n+1}\big(\Delta_n(\underline{\widehat{Y}_1}), \dots, \Delta_n(\underline{\widehat{Y}_i}), \dots, \Delta_n(\underline{\widehat{Y}_{n+1}})\big) \\
&\quad = \Delta_n(\underline{\widehat{Y}_1}) \Delta_n\big(\widehat{\Delta}_n(\underline{\widehat{Y}_1}), \Delta_n(\underline{\widehat{Y}_2}), \dots, \Delta_n(\underline{\widehat{Y}_i}), \dots, \Delta_n(\underline{\widehat{Y}_{n+1}})\big)^q \\
&\qquad - \Delta_n(\underline{\widehat{Y}_2}) \Delta_n\big(\Delta_n(\underline{\widehat{Y}_1}), \widehat{\Delta}_n(\underline{\widehat{Y}_2}), \dots, \Delta_n(\underline{\widehat{Y}_i}), \dots, \Delta_n(\underline{\widehat{Y}_{n+1}})\big)^q + \cdots \\
&\qquad + (-1)^{n+2} \Delta_n(\underline{\widehat{Y}_{n+1}}) \Delta_n\big(\Delta_n(\underline{\widehat{Y}_1}), \dots, \Delta_n(\underline{\widehat{Y}_i}), \dots, \Delta_n(\underline{\widehat{Y}_n}), \widehat{\Delta}_n(\underline{\widehat{Y}_{n+1}})\big)^q \\
&\quad = (-1)^{\lfloor \frac{n}{2} \rfloor} \Bigg(\sum_{1 \le i \le n+1} (-1)^{i+1} \Delta_n(\underline{\widehat{Y}_i}) Y_i^{q^n} \Bigg) \Delta_{n+1}(\underline{Y})^{q(1+q+\cdots+q^{n-2})} \\
&\quad = (-1)^{\lfloor \frac{n}{2} \rfloor} (-1)^n \Bigg(\sum_{1 \le i \le n+1} (-1)^{i+n+1} Y_i^{q^n} \Delta_n(\underline{\widehat{Y}_i}) \Bigg) \Delta_{n+1}(\underline{Y})^{q(1+q+\cdots+q^{n-2})} \\
&\quad = (-1)^{\lfloor \frac{n+1}{2} \rfloor} \Delta_{n+1}(\underline{Y})^{1+q+\cdots+q^{n-1}}.
\end{aligned}$$

This is (4.4) for $m = 0$ and $n+1$. This also shows the equality of the coefficients of higher degree in (4.4) for $m = 1$ and $n+1$.

(B2) We compare the zeros with multiplicity in the two members of (4.4) for $m = 1$ and $n+1$. We write

$$\begin{aligned}
G &:= \Delta_{n+1}\big(\Delta_{n+1}(\underline{\widehat{Y}_1}, X), \dots, (-1)^{i+1} \Delta_{n+1}(\underline{\widehat{Y}_i}, X), \dots, \\
&\qquad\qquad (-1)^{n+2} \Delta_{n+1}(\underline{\widehat{Y}_{n+1}}, X)\big), \\
D &:= X^{q^n} \Delta_{n+2}(\underline{Y}, X)^{1+q+\cdots+q^{n-1}}.
\end{aligned}$$

We are first interested in $X = 0$, for which we notice that

$$\frac{G}{X^{1+q+\cdots+q^n}} = \Delta_{n+1}\Big(\frac{\Delta_{n+1}(\underline{\widehat{Y}_1}, X)}{X}, \ldots, (-1)^{i+1}\frac{\Delta_{n+1}(\underline{\widehat{Y}_i}, X)}{X}, \ldots, (-1)^{n+2}\frac{\Delta_{n+1}(\underline{\widehat{Y}_{n+1}}, X)}{X}\Big),$$

whose constant term is

$$(-1)^{n(n+1)}\Delta_{n+1}\big(\Delta_n(\underline{\widehat{Y}_1}), \ldots, (-1)^{i+1}\Delta_n(\underline{\widehat{Y}_i}), \ldots, (-1)^{n+2}\Delta_n(\underline{\widehat{Y}_{n+1}})\big)^q.$$

On the other hand,

$$\frac{D}{X^{1+q+\cdots+q^n}} = \Big(\frac{\Delta_{n+2}(\underline{Y}, X)}{X}\Big)^{1+q+\cdots+q^{n-1}},$$

whose constant term is

$$(-1)^{(n+1)n}\Delta_{n+1}(\underline{Y})^{q(1+q+\cdots+q^{n-1})}.$$

Then we have equality and non-nullity of constant terms by (B1), which ensures in particular that the multiplicity of $X = 0$ is $1 + q + \cdots + q^n$ in G and in D.

Thanks to (2.2), we can handle the other zeros. Let $\underline{\varepsilon} := (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n+1}) \in \mathbb{F}_q^{n+1} - (0, \ldots, 0)$, and $x_{\underline{\varepsilon}} := \sum_{1\le j\le n+1}\varepsilon_j Y_j$. We need to show that $x_{\underline{\varepsilon}}$ is a root of G with multiplicity $1 + q + \cdots + q^{n-1}$.

With (2.1) we get

$$G = \prod_{1\le i\le n}\prod_{\alpha_{i-1}\in\mathbb{F}_q}\cdots\prod_{\alpha_1\in\mathbb{F}_q}\big(\Delta[i](\underline{Y}, X) + \alpha_{i-1}\Delta[i-1](\underline{Y}, X) + \cdots + \alpha_1\Delta[1](\underline{Y}, X)\big),$$

where $\Delta[i](\underline{Y}, X) := (-1)^{i+1}\Delta_{n+1}(\underline{\widehat{Y}_i}, X)$ and so with Proposition 2.3,

$$G = \prod_{1\le i\le n}\prod_{\alpha_{i-1}\in\mathbb{F}_q}\cdots\prod_{\alpha_1\in\mathbb{F}_q}\Delta_{(\alpha_1,\ldots,\alpha_{i-1},1,0,\ldots,0)}(\underline{Y}, X),$$

where $\Delta_{(\alpha_1,\ldots,\alpha_{i-1},1,0,\ldots,0)} = \Delta_{\varphi_i}$ with $\varphi_i = \alpha_1 Y_1^\star + \cdots + \alpha_{i-1}Y_i^\star + Y_i^\star$, and $(Y_i^\star)_{1\le i\le n}$ is the dual basis of $(Y_i)_{1\le i\le n}$. The roots of $\Delta_{(\alpha_1,\ldots,\alpha_{i-1},1,0,\ldots,0)}(\underline{Y}, X)$ seen as a polynomial in X and coefficients in $\mathbb{F}_q(\underline{Y})$ are simple (Proposition 2.3) and $\Delta_{(\alpha_1,\ldots,\alpha_{i-1},1,0,\ldots,0)}(x_{\underline{\varepsilon}}) = 0$ if and only if $\varepsilon_i + \alpha_{i-1}\varepsilon_{i-1} + \cdots + \alpha_1\varepsilon_1 = 0$. Thus, the multiplicity of $x_{\underline{\varepsilon}}$ in G is equal to the cardinality of the $(\alpha_1 : \alpha_2 : \cdots : \alpha_{n+1}) \in \mathbb{P}^n(\mathbb{F}_q)$ which belong to the hyperplane $\sum_{1\le i\le n+1}\varepsilon_i\alpha_i = 0$, i.e. $1 + q + \cdots + q^{n-1}$. Hence we get (4.4) for $m = 1$ and $n + 1$.

4.5 – *Second proof of Theorem 4.1 by a matrix interpretation in the case $m = 0$*

The following theorem is of interest independently of the rest. It gives indeed a relation between a generic Moore matrix and the Moore matrix of the cofactors of its first row, a relation analogous to the classical relation between a square matrix and its comatrix. The $m = 0$ case of Theorem 4.1 is then an immediate corollary by taking the determinants.

THEOREM 4.2. *Let $Y_1, Y_2, \dots, Y_n$ be n indeterminates over $\mathbb{F}_q$, and let $\mathcal{M}_n(\Delta_n(\widehat{\underline{Y}_1}), \dots, (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i}), \dots, (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n}))$ be the Moore matrix of the cofactors $(\Delta_n(\widehat{\underline{Y}_1}), \dots, (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i}), \dots, (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n}))$ of the first row of $\mathcal{M}_n(\underline{Y})$. Then one gets*

$$\mathcal{M}_n\big(\Delta_n(\widehat{\underline{Y}_1}), \dots, (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i}), \dots, (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n})\big)\ {}^t\mathcal{M}_n(\underline{Y})$$

(4.7)

$$= \begin{pmatrix} 0 & . & . & \cdots & . & 0 & (-1)^{n-1}\Delta_n(\underline{Y}) \\ \Delta_n(\underline{Y}) & 0 & . & \cdots & . & 0 & 0 \\ \alpha_1 & \Delta_n(\underline{Y})^q & 0 & \cdots & . & 0 & 0 \\ \alpha_2 & \alpha_1^q & \Delta_n(\underline{Y})^{q^2} & \cdots & . & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & . & \vdots & \vdots \\ \alpha_{n-2} & \alpha_{n-3}^q & . & \cdots & \alpha_1^{q^{n-3}} & \Delta_n(\underline{Y})^{q^{n-2}} & 0 \end{pmatrix},$$

where

$$\alpha_k := \Delta_n(\widehat{\underline{Y}_1})^{q^{k+1}} Y_1 + \cdots + (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i})^{q^{k+1}} Y_i + \cdots + (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n})^{q^{k+1}} Y_n.$$

PROOF. We write

$$\mathcal{M}_n\big(\Delta_n(\widehat{\underline{Y}_1}), \dots, (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i}), \dots, (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n})\big)\ {}^t\mathcal{M}_n(\underline{Y}) =: [m_{i,j}]_{1\le i,j\le n}.$$

Since $(-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i})^q$ is the cofactor of Y_i in the Moore matrix $\mathcal{M}_n(\underline{Y})$, we get the following formulas:

$$\Delta_n(\widehat{\underline{Y}_1})^q Y_1 + \cdots + (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i})^q Y_i + \cdots + (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n})^q Y_n = \Delta_n(\underline{Y}), \tag{4.8}$$

and for $1 \le k \le n-1$,

$$\Delta_n(\widehat{\underline{Y}_1})^q Y_1^{q^k} + \cdots + (-1)^{i-1}\Delta_n(\widehat{\underline{Y}_i})^q Y_i^{q^k} + \cdots + (-1)^{n-1}\Delta_n(\widehat{\underline{Y}_n})^q Y_n^{q^k} = 0. \tag{4.9}$$

Since $(-1)^{i-1}\Delta_n(\widehat{\underline{Y_i}})$ is the cofactor of $Y_i^{q^{n-1}}$, we get the following formulas:

$$\begin{aligned}&\Delta_n(\widehat{\underline{Y_1}})Y_1^{q^{n-1}}+\cdots+(-1)^{i-1}\Delta_n(\widehat{\underline{Y_i}})Y_i^{q^{n-1}}+\cdots+(-1)^{n-1}\Delta_n(\widehat{\underline{Y_n}})Y_n^{q^{n-1}}\\ &\quad=(-1)^{n-1}\Delta_n(\underline{Y}),\end{aligned}\tag{4.10}$$

and for $0\le k\le n-2$,

$$\begin{aligned}&\Delta_n(\widehat{\underline{Y_1}})Y_1^{q^k}+\cdots+(-1)^{i-1}\Delta_n(\widehat{\underline{Y_i}})Y_i^{q^k}+\cdots+(-1)^{n-1}\Delta_n(\widehat{\underline{Y_n}})Y_n^{q^k}\\ &\quad=0.\end{aligned}\tag{4.11}$$

It follows from relations (4.10) and (4.11) that $m_{1,j}=0$ for $1\le j\le n_1$ and that $m_{1,n}=(-1)^{n-1}\Delta_n(\underline{Y})$.

Now let $2\le i\le n$. Raising (4.8) and (4.9) to the power q^{i-1}, it follows that $m_{i,i-1}=\Delta_n(\underline{Y})^{q^{i-1}}$ and $m_{i,j}=0$ for $i\le j\le n$.

In conclusion, the matrix $[m_{i,j}]_{1\le i,j\le n}$ satisfies (4.7). ∎

By taking the determinant of the matrices in (4.7) we obtain that $\gamma=1$ in the case $m=0$ of Corollary 4.1; Theorem 4.1 follows.

4.6 – *A matrix interpretation of the general case* (n,m)

The following theorem is a generalization of Theorem 4.2 adapted to a matrix interpretation of the general case of Theorem 4.1. Theorem 4.2 corresponds to the case $m=0$, i.e. $\underline{X}=\emptyset$.

THEOREM 4.3. *For $n\ge 2$, $m\ge 1$ let $Y_1,Y_2,\dots,Y_n,X_1,X_2,\dots,X_m$ be $n+m$ indeterminates over $\mathbb{F}_q$, $\delta_i:=(-1)^{i-1}\Delta_{n+m-1}((\widehat{\underline{Y_i}}),(\underline{X}))$ for $1\le i\le n$, $\delta_i:=(-1)^{i-1}\Delta_{n+m-1}((\underline{Y}),(\widehat{\underline{X_i}}))$ for $n+1\le i\le n+m$.*

Let $A:=[a_{i,j}]_{1\le i,j\le n+m}$, where $a_{i,j}=(\delta_j)^{q^{i-1}}$ for $1\le i\le n$, $1\le j\le n+m$ and $a_{i,i-n}=1$ for $n+1\le i\le n+m$ and $a_{i,j}=0$ for $n+1\le i\le n+m$ and $j\ne n-i$.

Hence,

$$A=\begin{pmatrix}\mathcal{M}_n(\delta_1,\delta_2,\dots,\delta_n) & \mathcal{M}_{n,m}(\delta_{1+n},\delta_{2+n},\dots,\delta_{n+m})\\ 0\in M_{m,n}(\mathbb{F}_q[Y,X]) & \mathrm{Id}_m\end{pmatrix}.\tag{4.12}$$

Then

$$A\,{}^t\mathcal{M}_{n+m}(\underline{Y},\underline{X})=[m_{i,j}]_{1\le i,j\le n}=:M,\tag{4.13}$$

with

$$\begin{aligned}
m_{1,j} &= 0 && \text{for } 1 \le j \le n+m-1,\\
m_{1,n+m} &= (-1)^{n+m-1}\Delta_{n+m}(\underline{Y},\underline{X}),\\
m_{2,1} &= \Delta_{n+m}(\underline{Y},\underline{X}),\\
m_{2,j} &= 0 && \text{for } 2 \le j \le n+m,\\
m_{i,j} &= \alpha_{i-j-1}^{q^{j-1}} && \text{for } 3 \le i \le n,\ 1 \le j \le i-2,\\
m_{i,i-1} &= \Delta_{n+m}(\underline{Y},\underline{X})^{q^i},\ m_{i,j} = 0 && \text{for } i \le j \le n+m,
\end{aligned}$$

with

$$\alpha_k := \delta_1^{q^{k+1}} Y_1 + \cdots + \delta_n^{q^{k+1}} Y_n + \delta_{n+1}^{q^{k+1}} X_1 + \cdots + \delta_{n+m}^{q^{k+1}} X_m.$$

In matrix notation we have $M = \left(\begin{smallmatrix} M_1 & M_2 \\ M_3 & M_4 \end{smallmatrix}\right)$, *where*

$$M_1 := \begin{pmatrix}
0 & . & . & \cdots & . & 0 & 0\\
\beta_0 & 0 & . & \cdots & . & 0 & 0\\
\alpha_1 & \beta_1 & 0 & \cdots & . & 0 & 0\\
\alpha_2 & \alpha_1^q & \beta_2 & \cdots & . & 0 & 0\\
\vdots & \vdots & \vdots & \cdots & . & \vdots & \vdots\\
\alpha_{n-2} & \alpha_{n-3}^q & . & \cdots & \alpha_1^{q^{n-3}} & \beta_{n-2} & 0
\end{pmatrix}$$

with $\beta_i := \Delta_{n+m}(\underline{Y},\underline{X})^{q^i}$,

$$M_2 := \begin{pmatrix}
0 & 0 & \cdots & (-1)^{m+n-1}\Delta_{n+m}(\underline{Y},\underline{X})\\
0 & 0 & \cdots & 0\\
. & . & \cdots & .\\
0 & 0 & \cdots & 0
\end{pmatrix},$$

$$\begin{aligned}
M_3 &= {}^t\mathcal{M}_{n,m}(X_1, X_2, \ldots, X_m),\\
M_4 &= {}^t\mathcal{M}_m(X_1^{q^n}, X_2^{q^n}, \ldots, X_m^{q^n}).
\end{aligned}$$

Proof. We can consider δ_i^q as the cofactor of Y_i or X_i in the Moore matrix $\mathcal{M}_n(\underline{Y},\underline{X})$, so we have the following formulas:

$$\begin{aligned}
&\delta_1^q Y_1 + \delta_2^q Y_2 + \cdots + \delta_n^q Y_n + \delta_{n+1}^q X_1 + \delta_{n+2}^q X_2 + \cdots + \delta_{n+m}^q X_m\\
&\qquad = \Delta_{n+m}(\underline{Y},\underline{X}), \qquad (4.14)\\
&\delta_1^q Y_1^{q^k} + \delta_2^q Y_2^{q^k} + \cdots + \delta_n^q Y_n^{q^k} + \delta_{n+1}^q X_1^{q^k} + \delta_{n+2}^q X_2^{q^k} + \cdots\\
&\qquad + \delta_{n+m}^q X_m^{q^k} = 0 \qquad (4.15)
\end{aligned}$$

for $1 \le k \le n+m-1$.

We can also consider δ_i as the cofactor of $Y_i^{q^{n+m-1}}$ or of $X_i^{q^{n+m-1}}$ in the Moore matrix $\mathcal{M}_n(\underline{Y}, \underline{X})$. We thus have the following formulas:

$$\delta_1 Y_1^{q^{n+m-1}} + \delta_2 Y_2^{q^{n+m-1}} + \cdots + \delta_n Y_n^{q^{n+m-1}} + \delta_{n+1} X_1^{q^{n+m-1}} + \cdots + \delta_{n+m} X_m^{q^{n+m-1}} = (-1)^{n+m-1} \Delta_{n+m}(\underline{Y}, \underline{X})$$

$$\delta_1 Y_1^{q^k} + \delta_2 Y_2^{q^k} + \cdots + \delta_n Y_n^{q^k} + \delta_{n+1} X_1^{q^k} + \delta_{n+2} X_2^{q^k} + \cdots + \delta_{n+m} X_m^{q^k} = 0$$

for $0 \leq k \leq n+m-2$.

It follows from the relations (4.12) and (4.13) that the first line of $A\,{}^t\mathcal{M}_n(\underline{Y}, \underline{X})$ is the same as the first line of $M = [m_{i,j}]_{1 \leq i,j \leq n}$.

Then, to show the equality between the lines of index i with $2 \leq i \leq n$, it is enough to raise relations (4.14) and (4.15) to the power q^{i-1} and to use the definition of α_k for $1 \leq k \leq n-2$.

The equality between the lines of index i with $n+1 \leq i \leq n+m$ is immediate. All this shows relation (4.13). ∎

Corollary 4.3. *Theorem 4.1 is a consequence of the matrix equality in Theorem 4.3.*

Proof. Expanding the determinant of M according to the first line, we have

$$\det M = \Delta_{n+m}(\underline{Y}, \underline{X}) \det N \tag{4.16}$$

with $N = \begin{pmatrix} N_1 & N_2 \\ N_3 & N_4 \end{pmatrix}$, where

$$N_1 = \begin{pmatrix} \beta_1 & 0 & . & \cdots & . & 0 \\ \alpha_0 & \beta_1 & 0 & \cdots & . & 0 \\ \alpha_2 & \alpha_1^q & \beta_2 & \cdots & . & 0 \\ \vdots & \vdots & \vdots & \cdots & . & \vdots \\ \alpha_{n-2} & \alpha_{n-3}^q & . & \cdots & \alpha_1^{q^{n-3}} & \beta_{n-2} \end{pmatrix}$$

with $\beta_i := \Delta_{n+m}(\underline{Y}, \underline{X})^{q^i}$,

N_2 is the zero matrix in $M_{n-1,m-1}(\mathbb{F}_q[\underline{Y}, \underline{X}])$,

$N_3 = {}^t\mathcal{M}_{n-1,m}(X_1, X_2, \ldots, X_m)$,

$N_4 = {}^t\mathcal{M}_m(X_1^{q^{n-1}}, X_2^{q^{n-1}}, \ldots, X_m^{q^{n-1}})$.

It is then clear that

$$\det N = \Delta_{n+m}(\underline{Y}, \underline{X})^{1+q+\cdots+q^{n-2}} \Delta_m(\underline{X})^{q^{n-1}}. \tag{4.17}$$

Thus, with (4.16) and (4.17), one gets

$$\det M = \Delta_{n+m}(\underline{Y}, \underline{X})\Delta_{n+m}(\underline{Y}, \underline{X})^{1+q+\cdots+q^{n-2}}\Delta_m(\underline{X})^{q^{n-1}}. \tag{4.18}$$

It follows from (4.13) that $\det M = \Delta_{n+m}(\underline{Y}, \underline{X}) \det A$ and from (2.6) that $\det A = \Delta_n(\delta_1, \delta_2, \ldots, \delta_n)$, thus

$$\det M = \Delta_{n+m}(\underline{Y}, \underline{X})\Delta_n(\delta_1, \delta_2, \ldots, \delta_n). \tag{4.19}$$

Since (cf. Proposition 2.1) $\Delta_{n+m}(\underline{Y}, \underline{X}) \neq 0$, and $\mathbb{F}_q[(\underline{Y}, \underline{X})]$ is an integral ring, equality (4.4) in Theorem 4.1 for $m \geq 1$ follows from (4.18) and (4.19).

Finally, the equality of the coefficients of highest degree in X_1 in formula (4.4) in Theorem 4.1 for $m = 1$ gives, as noticed in the first proof, formula (4.4) in Theorem 4.1 for $m = 0$. ∎

5. Two illustrations of the Moore determinant

5.1 – *The map* $(a_1, \ldots, a_n) \in K^n \to (\Delta_{n-1}(\hat{\underline{a}}_i))_{1\leq i\leq n} \in K^n$

Proposition 5.1. *Let K be an algebraically closed field with characteristic $p > 0$. Let us denote $V(\Delta_n) := \{(a_1, a_2, \ldots, a_n) := \underline{a} \in K^n \mid \Delta_n(\underline{a}) = 0\}$. The map $\varphi\colon \underline{a} := (a_1, a_2, \ldots, a_n) \in K^n \to (\Delta_{n-1}(\hat{\underline{a}}_i))_{1\leq i\leq n} \in K^n$ induces an onto map from $K^n - V(\Delta_n)$ to itself. Moreover, for $\underline{a}$ and $\underline{a}'$ in $K^n - V(\Delta_n)$, one has $\varphi(\underline{a}) = \varphi(\underline{a}')$ if and only if $\underline{a}' = \lambda\underline{a}$, where $\lambda^{1+q+\cdots+q^{n-2}} = 1$.*

Proof. Let $(a_1, a_2, \ldots, a_n) \in K^n - V(\Delta_n)$ and $b_i := \Delta_{n-1}(\hat{\underline{a}}_i)$ for $1 \leq i \leq n$. Since $\Delta_n(\underline{b}) = (-1)^{\lfloor \frac{n}{2} \rfloor}\Delta_n(\underline{a})^{1+q+\cdots+q^{n-2}}$ (we recognize (4.4) for $m = 0$), it follows that $\varphi(K^n - V(\Delta_n)) \subset K^n - V(\Delta_n)$. Then

$$\begin{aligned}\varphi^2(\underline{a}) &= (\Delta_{n-1}(\hat{\underline{b}}_i))_{1\leq i\leq n}\\ &= \big(\Delta_{n-1}\big(\Delta_{n-1}(\hat{\underline{a}}_1), \ldots, \Delta_{n-1}(\underline{\hat{a}_{i-1}}), \Delta_{n-1}(\underline{\hat{a}_{i+1}}), \ldots, \Delta_{n-1}(\hat{\underline{a}}_n)\big)\big)_{1\leq i\leq n}\\ &= ((-1)^{\lfloor \frac{n-1}{2} \rfloor}\Delta_n(\underline{a})^{1+q+\cdots+q^{n-3}}a_i^{q^{n-2}})_{1\leq i\leq n},\end{aligned}$$

as seen in equality (4.6) at rank n obtained in the first proof of Theorem 4.1. It follows that

$$\varphi^2(\underline{a}) = (-1)^{\lfloor \frac{n-1}{2} \rfloor}\Delta_n(\underline{a})^{1+q+\cdots+q^{n-3}}(\underline{a})^{q^{n-2}}.$$

Let $\lambda \in K - \{0\}$. Then

$$\varphi^2(\underline{\lambda a}) = \lambda^{(1+q+\cdots+q^{n-1})(1+q+\cdots+q^{n-3})+q^{n-2}}\varphi^2(\underline{a}).$$

Note that we have the equality $(1+q+\cdots+q^{n-1})(1+q+\cdots+q^{n-3})+q^{n-2}=(1+q+\cdots+q^{n-2})^2$ according to the fact that $\varphi(\underline{\lambda a})=\lambda^{1+q+\cdots+q^{n-2}}\varphi(\underline{a})$. Thus, by taking λ with $\lambda^{(1+q+\cdots+q^{n-1})^2}=\Delta_n(\underline{a})^{-(1+q+\cdots+q^{n-3})}$, one gets $\varphi^2(\underline{\lambda a})=(\underline{a})^{q^{n-2}}$. Hence the surjectivity of φ^2 and therefore of φ.

Let us now examine the injectivity defect of the map φ.

Let $\underline{a}$ and $\underline{a}'$ be in $K^n-V(\Delta_n)$ such that $\varphi(\underline{a})=\varphi(\underline{a}')$. Then $\varphi^2(\underline{a})=\varphi^2(\underline{a}')$ and so $\Delta_n(\underline{a})^{1+q+\cdots+q^{n-3}}a_i^{q^{n-2}}=\Delta_n(\underline{a}')^{1+q+\cdots+q^{n-3}}{a'_i}^{q^{n-2}}$. Thus, there is $\lambda\in K$ such that $\underline{a}'=\lambda\underline{a}$, hence $\lambda^{1+q+\cdots+q^{n-2}}\varphi(\underline{a})=\varphi(\underline{a})$ and so $\lambda^{1+q+\cdots+q^{n-2}}=1$. The converse is immediate. ∎

Remark 5.1. Proposition 5.1 works the same if we replace the map φ by the map φ_1 where $\varphi_1\colon\underline{a}:=(a_1,a_2,\ldots,a_n)\in K^n\to((-1)^{i-1}\Delta_{n-1}(\underline{\hat{a}_i}))_{1\le i\le n}\in K^n$ as $\varphi^2=(-1)^{\lfloor\frac{n}{2}\rfloor}\varphi_1^2$.

5.2 – *On K-étale algebras and Elkies pairing*

In this paragraph, unless expressly mentioned, K is a field of characteristic $p>0$, K^{alg} is an algebraic closure of K and F is the Frobenius automorphism defined by $F(x)=x^p$ for $x\in K^{\mathrm{alg}}$.

Let $\underline{f}:=(f_1,f_2,\ldots,f_n)\in K^n$ with $\Delta_n(\underline{f})\neq 0$, i.e. $f_1,f_2,\ldots,f_n$ are $\mathbb{F}_p$-free. We intend to study the K-algebra

$$A:=\frac{K[W_i,1\le i\le n]}{(W_i^p-W_i-f_i)_{1\le i\le n}},$$

in particular its group of K-automorphisms $\mathrm{Aut}_K A$, and to exhibit a special generator of the K-algebra A and a subgroup $(\mathbb{Z}/p\mathbb{Z})^n\subset\mathrm{Aut}_K A$ whose action on A is dictated by an associated Elkies pairing (Section 3.2 (A)).

Proposition 5.2. *Let $n\ge 1$ and $\underline{f}:=(f_1,f_2,\ldots,f_n)\in K^n$, where $\Delta_n(\underline{f})\neq 0$. Let V be the $\mathbb{F}_p$-vector space*

$$\frac{(\sum_{1\le i\le n}\mathbb{F}_p f_i)+(F-\mathrm{Id})(K)}{(F-\mathrm{Id})(K)}$$

of dimension $r\le n$ and $I\sqcup J$ be a partition of $\{1,2,\ldots,n\}$ such that f_i, $i\in I$ induces an $\mathbb{F}_p$-basis of the vector space V. Let A be the K-algebra $\frac{K[W_k,1\le k\le n]}{(P_k)_{1\le k\le n}}$, where $P_k:=W_k^p-W_k-f_k$. Then A is an étale K-algebra isomorphic to $L^{p^{n-r}}$, the cartesian product of p^{n-r} copies of L, where $L\subset K^{\mathrm{alg}}$ is a field which is a Galois extension of K of group $(\mathbb{Z}/p\mathbb{Z})^r$ and $L\simeq\frac{K[W_k,k\in I]}{(P_k)_{k\in I}}$.

The group of K-automorphisms $\mathrm{Aut}_K A$ *is then isomorphic to a semidirect product of the groups* $\mathfrak{S}_{p^{n-r}}$ *and* $((\mathbb{Z}/p\mathbb{Z})^r)^{p^{n-r}}$.

Moreover, if w_i denotes the canonical image of W_i in A and if

$$w := \delta_{\underline{w}}(\underline{f}) := \begin{vmatrix} w_1 & w_2 & \cdots & w_n \\ f_1 & f_2 & \cdots & f_n \\ f_1^p & f_2^p & \cdots & f_n^p \\ \vdots & \vdots & \cdots & \vdots \\ f_1^{p^{n-2}} & f_2^{p^{n-2}} & \cdots & f_n^{p^{n-2}} \end{vmatrix} \in K[w_1, w_2, \ldots, w_n],$$

then

$$w_i = \frac{\Delta_n\big(\Delta_{n-1}(\underline{\hat{f}_1}), \ldots, (-1)^{i-2}\Delta_{n-1}(\underline{\hat{f}_{i-1}}), w, (-1)^i\Delta_{n-1}(\underline{\hat{f}_{i+1}}), \ldots, (-1)^{n-1}\Delta_{n-1}(\underline{\hat{f}_n})\big)}{\Delta_n\big(\Delta_{n-1}(\underline{\hat{f}_1}), \ldots, (-1)^{j-1}\Delta_{n-1}(\underline{\hat{f}_j}), \ldots, (-1)^{n-1}\Delta_{n-1}(\underline{\hat{f}_n})\big)} - (f_i + f_i^p + \cdots + f_i^{p^{n-2}}) \in K[w],$$

where $\Delta_{n-1}(\underline{\hat{f}_i}) = \Delta_{n-1}(f_1, f_2, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n)$ *and*

$$A = K[w_1, w_2, \ldots, w_n] = K[w] \simeq \frac{K[W]}{(Q(W))} \tag{5.1}$$

where

$$\begin{aligned} Q(W) &= \frac{\Delta_{n+1}\big(\Delta_{n-1}(\underline{\hat{f}_1}), \ldots, \Delta_{n-1}(\underline{\hat{f}_n}), W\big)}{\Delta_n\big(\Delta_{n-1}(\underline{\hat{f}_1}), \ldots, \Delta_{n-1}(\underline{\hat{f}_n})\big)} - \Delta_n(\underline{f})^{p^{n-1}} \\ &= W^{p^n} + \left(\sum_{1\le i\le n-1} (-1)^{n-i}\Delta_n(\underline{f})^{p^{n-1}-p^{i-1}-p^i}(\Delta[n-i](\underline{f}))^{p^{i-1}} W^{p^{n-i}}\right) \\ &\quad + (-1)^n\Delta_n(\underline{f})^{p^{n-1}-1}W - \Delta_n(\underline{f})^{p^{n-1}}, \end{aligned}$$

$\Delta[i](\underline{f}) := \det(\underline{f}, F(\underline{f}), \ldots, \widehat{F^i}(\underline{f}), \ldots, F^n(\underline{f}))$ *and* $Q(w) = 0$.

Proof. (i) Let us show that A is isomorphic to the K-algebra $L^{p^{n-r}}$. By definition of I, we have

$$V = \frac{(\sum_{i\in I} \mathbb{F}_p f_i) + (F - \mathrm{Id})(K)}{(F - \mathrm{Id})(K)}.$$

Artin–Schreier theory [1, §11, Theorem 5, p. A V.88] says that

$$(F - \mathrm{Id})^{-1}\left(\sum_{i\in I} \mathbb{F}_p f_i + (F - \mathrm{Id})(K)\right) \subset K^{\mathrm{alg}}$$

is a Galois extension L/K of the group $\mathrm{Hom}(V,\mathbb{F}_p)\simeq(\mathbb{Z}/p\mathbb{Z})^r$ and that

$$L=\bigoplus_{\substack{0\le\alpha_i<p\\ i\in I}} K\prod_{i\in I}x_i^{\alpha_i},\quad \text{where } x_i\in K^{\mathrm{alg}} \text{ and } P_i(x_i)=0. \tag{5.2}$$

Let π be the K-algebra homomorphism of $K[W_i, i\in I]$ onto L mapping $\pi(W_i)$ to x_i. It follows from (5.2) that π induces a K-algebra homomorphism

$$\pi'\colon \frac{K[W_i,i\in I]}{(P_i)_{i\in I}}=K[w_i,i\in I]\to L,$$

which is surjective, and as

$$K[w_i,i\in I]=\sum_{\substack{0\le\alpha_i<p\\ i\in I}} K\prod_{i\in I}w_i^{\alpha_i},$$

we get a K-algebra isomorphism

$$\frac{K[W_i,i\in I]}{(P_i)_{i\in I}}\simeq L. \tag{5.3}$$

On the other hand, we have for $j\in J$, $f_j=\sum_{i\in I}\lambda_{j,i}f_i+g_j^p-g_j$ with $\lambda_{j,i}\in\mathbb{F}_p$ and $g_j\in K$. Thus, for $j\in J$, and if $W_j':=W_j+\sum_{i\in I}\lambda_{j,i}W_i$, one gets $K[W_k,1\le k\le n]=K[W_i,i\in I,W_j',j\in J]$ and for $j\in J$ one has $W_j'^p-W_j'-(g_j^p-g_j)=W_j{}^p-W_j-f_j+\sum_{i\in I}\lambda_{j,i}(W_i{}^p-W_i-f_i)$ and so if $P_j'(W_j'):=W_j'^p-W_j'-(g_j^p-g_j)$ we have

$$A\simeq\frac{K[W_i,i\in I,W_j',j\in J]}{(P_i,i\in I,P_j',j\in J)}.$$

Now we can apply the following general lemma:

Lemma 5.1. *Let K be any field (no condition on the characteristic) and K^{alg} an algebraic closure.*

Let $n\ge1$ and for $1\le k\le n$, $P_k\in K[W_k]$ be a non-constant polynomial. Let A be the K-algebra

$$\frac{K[W_k,1\le k\le n]}{(P_k)_{1\le k\le n}}=K[w_k,1\le k\le n],$$

where w_k is the canonical image of W_k.

Let $I\sqcup J$ be a partition of $\{1,2,\dots,n\}$ and B be the K-algebra $B:=\frac{K[W_k,k\in I]}{(P_k)_{k\in I}}$. Let $u\colon K[W_k,k\in I]\to A$ be the K-homomorphism with $u(W_k)=w_k$ for $k\in I$. Then $\mathrm{Ker}\,u=\sum_{i\in I}P_iK[W_k,k\in I]$ and u induces on one side an isomorphism between the two K-algebras B and $K[w_k,k\in I]\subset A$ and on the other side an isomorphism between the two K-algebras $\frac{B[W_k,k\in J]}{(P_k)_{k\in J}}$ and A.

PROOF. We have

$$\operatorname{Ker} u := \{P \in K[W_k, k \in I] \mid P = \textstyle\sum_{1\le k\le n} Q_k P_k\},$$

where $Q_k \in K[W_k, 1 \le k \le n]$. Let $z_k \in K^{\mathrm{alg}}$ with $P_k(z_k) = 0$. Let $\sigma\colon K[W_k, 1 \le k \le n] \to K^{\mathrm{alg}}[W_k, k \in I]$ such that $\sigma(a) = a$ for $a \in K$, $\sigma(W_k) = W_k$ for $k \in I$ and $\sigma(W_k) = z_k$ for $k \in J$. Then

$$P = \sigma(P) = \sum_{k\in I} \sigma(Q_k) P_k \quad \text{and} \quad \sigma(Q_k) \in K^{\mathrm{alg}}[W_k, k \in I]. \tag{5.4}$$

It follows that there is a finite field extension L/K inside K^{alg} with $\sigma(Q_k) \in L[W_k, k \in I]$. Let $\{e_0 = 1, e_1, \dots, e_m\}$ be a basis for L/K. Then $L[W_k, k \in I] = \bigoplus_{0\le s\le m} K[W_k, k \in I]e_s$. It follows from (5.4) that there is $R_k \in K[W_k, k \in I]$ with $P = \sum_{k\in I} R_k P_k$; thus $\operatorname{Ker} u = \sum_{i\in I} P_i K[W_k, k \in I]$.

Let $\pi\colon K[W_k, k \in I] \to B$ be the canonical K-homomorphism and let $v\colon B \to A$ be the unique K-homomorphism with $u = v \circ \pi$. Then v induces an isomorphism from B to $K[w_k, k \in I] \subset A$.

So we have the following commutative diagram:

$$\begin{array}{ccc} K[W_k, k \in I] & \xrightarrow{u} & A \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle v} & \\ B. & & \end{array}$$

It extends in the following commutative diagram:

$$\begin{array}{ccc} K[W_k, k \in I][W_k, k \in J] & \xrightarrow{\tilde{u}} & A \\ \downarrow{\scriptstyle \tilde{\pi}} & \nearrow{\scriptstyle \tilde{v}} & \\ B[W_k, k \in J], & & \end{array}$$

where $\tilde{u}(W_k) = w_k$, $\tilde{\pi}(W_k) = W_k$, $\tilde{v}(W_k) = w_k$ for $k \in J$.

We claim that $\operatorname{Ker} \tilde{v} = \sum_{k\in J} P_k B[W_k, k \in J]$.

Let $Q \in \operatorname{Ker} \tilde{v}$ and $\tilde{Q} \in K[W_k, k \in I][W_k, k \in J]$ such that $Q = \tilde{\pi}(\tilde{Q})$. Then $\tilde{u}(\tilde{Q}) = \tilde{v}\tilde{\pi}(\tilde{Q}) = 0$ and so $\tilde{Q} \in \sum_{1\le k\le n} K[W_t, 1 \le t \le n] P_k$ and

$$Q \in \tilde{\pi}\Big(\sum_{1\le k\le n} P_k K[W_t, 1 \le t \le n]\Big) = \sum_{k\in J} P_k B[W_k, k \in J]. \qquad \blacksquare$$

As

$$A \simeq \frac{K[W_i, i \in I, W'_j, j \in J]}{(P_i, i \in I, P'_j, j \in J)},$$

it follows from Lemma 5.1 that

$$A = \frac{K[w_i, i \in I][W'_j, j \in J]}{(P'_j, j \in J)}, \quad \text{where } K[w_i, i \in I] = \frac{K[W_i, i \in I]}{(P_i, i \in I)}.$$

Now with (5.3) we deduce that $A \simeq \frac{L[W'_j, j\in J]}{(P'_j)} \simeq L^{p^{n-r}}$. Moreover, A is a K-étale algebra since L/K is separable.

(ii) We show that the group $\mathrm{Aut}_K A$ is a semidirect product of the groups $\mathfrak{S}_{p^{n-r}}$ and $((\mathbb{Z}/p\mathbb{Z})^r)^{p^{n-r}}$. This follows from (i) and the following lemma:

Lemma 5.2. *Let K be a commutative field (no condition on the characteristic) and L/K be a finite Galois extension of group G. Let $t \geq 1$ and $A := L^t$ and $\mathrm{Aut}_K A$ be the group of K-automorphisms of A. Let $\rho\colon \mathfrak{S}_t \to \mathrm{Aut}_K A$, where $\rho(\sigma)(x_1, x_2, \ldots, x_t) := (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(t)})$ and $\varphi\colon G^t \to \mathrm{Aut}_K A$ such that*

$$\varphi(g_1, g_2, \ldots, g_t)(x_1, x_2, \ldots, x_t) := (g_1(x_1), g_2(x_2), \ldots, g_t(x_t)).$$

Then ρ and φ are two injective homomorphisms of groups with

$$\rho(\sigma)\varphi(g_1, g_2, \ldots, g_t)\rho(\sigma)^{-1} = \rho(g_{\sigma^{-1}(1)}, g_{\sigma^{-1}(2)}, \ldots, g_{\sigma^{-1}(t)})$$

and $\mathrm{Aut}_K A$ is the internal semidirect product of the groups $\rho(\mathfrak{S}_t) \simeq \mathfrak{S}_t$ and $\varphi(G^t) \simeq G^t$.

Proof. We can assume that $t \geq 2$ and we show the last assertion.

Let $\mathfrak{M}_i := \{(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_t)\}$ with $x_j \in L$ for $j \neq i$. Then $\mathfrak{M}_i$ is a maximal ideal of A and $\frac{A}{\mathfrak{M}_i} \simeq L$. Then $\{\mathfrak{M}_i, 1 \leq i \leq t\}$ is the set of maximal ideals $\mathrm{Spm}(A)$ of A.

Now, if $\Phi \in \mathrm{Aut}_K A$, Φ induces a bijection of $\mathrm{Spm}(A)$, so there is $\sigma \in \mathfrak{S}_t$ with $\Phi(\mathfrak{M}_i) = \mathfrak{M}_{\sigma^{-1}(i)}$ for $1 \leq i \leq t$, hence $\rho(\sigma^{-1})\Phi(\mathfrak{M}_i) = \mathfrak{M}_i$ for $1 \leq i \leq t$.

Let $\Psi := \rho(\sigma^{-1})\Phi$. We have $\Psi(\bigcap_{j\neq i} \mathfrak{M}_j) = \bigcap_{j\neq i} \mathfrak{M}_j = (0, 0, \ldots, L, 0, \ldots, 0)$ for $1 \leq i \leq t$, where only the ith component is not zero. Thus, Ψ induces a K-automorphism g_i of L. Thus we have $\Psi = \varphi(g_1, g_2, \ldots, g_t)$ and so $\Phi = \rho(\sigma)\varphi(g_1, g_2, \ldots, g_t)$. ∎

(iii) We show (5.1). Let $v_i := w_i + (f_i + f_i^p + \cdots + f_i^{p^{n-2}})$. Then $w = \delta_{\underline{w}}(\underline{f}) = \delta_{\underline{v}}(\underline{f})$ and $v_i^p = v_i + f_i^{p^{n-1}}$. It follows that $w^{p^j} = \delta_{\underline{v}}(\underline{f}^{p^j})$ for $0 \leq j \leq n-1$ and $w^{p^n} = \delta_{\underline{v}}(\underline{f}^{p^n}) + \Delta_n(\underline{f}^{p^{n-1}})$. Since $\delta_{\underline{v}}(\underline{f}^{p^j}) = \sum_{1\leq i\leq n}(-1)^{i-1}\Delta_{n-1}(\hat{f}_i)^{p^j} v_i$, for $1 \leq j \leq n$, we deduce from Cramer's formulas the announced formula for w_i as a

polynomial function of w. Finally, the previous formulas also give a non-trivial linear relation between the columns of the determinant

$$\begin{vmatrix} \Delta_{n-1}(\underline{\hat{f}_1}) & \cdots & \Delta_{n-1}(\underline{\hat{f}_n}) & w \\ \Delta_{n-1}(\underline{\hat{f}_1})^p & \cdots & \Delta_{n-1}(\underline{\hat{f}_n})^p & w^p \\ \vdots & \cdots & \vdots & \vdots \\ \Delta_{n-1}(\underline{\hat{f}_1})^{p^{n-1}} & \cdots & \Delta_{n-1}(\underline{\hat{f}_n})^{p^{n-1}} & w^{p^{n-1}} \\ \Delta_{n-1}(\underline{\hat{f}_1})^{p^n} & \cdots & \Delta_{n-1}(\underline{\hat{f}_n})^{p^n} & w^{p^n} - \Delta_n(\underline{f}^{p^{n-1}}) \end{vmatrix},$$

which is zero. We get (5.1), where

$$Q(W) := \frac{\Delta_{n+1}\big(\Delta_{n-1}(\underline{\hat{f}_1}), \ldots, \Delta_{n-1}(\underline{\hat{f}_n}), W\big)}{\Delta_n\big(\Delta_{n-1}(\underline{\hat{f}_1}), \ldots, \Delta_{n-1}(\underline{\hat{f}_n})\big)} - \Delta_n(\underline{f})^{p^{n-1}},$$

whose first term is the monic additive polynomial whose roots are the $\mathbb{F}_p$-space $\bigoplus_{1\le i\le n} \mathbb{F}_p \Delta_{n-1}(\underline{\hat{f}_i})$. Then the equality

$$\begin{aligned} Q(W) = W^{p^n} + \Bigg(\sum_{1\le i\le n-1} (-1)^{n-i} \Delta_n(\underline{f})^{p^{n-1}-p^{i-1}-p^i} (\Delta[n-i](\underline{f}))^{p^{i-1}} W^{p^{n-i}} \Bigg) \\ + (-1)^n \Delta_n(\underline{f})^{p^{n-1}-1} W - \Delta_n(\underline{f})^{p^{n-1}} \end{aligned}$$

follows from Elkies [2, formula (4.28)] and the proof of Proposition 2.5. ∎

Remark 5.2. (i) Since $\Delta_r(f_i, i \in I) \neq 0$, Proposition 5.2 applied to the K-algebra $L = \frac{K[W_k, k\in I]}{(P_k)_{k\in I}}$ gives a generator of the extension L/K.

(ii) One may consult [5] for an application in the case where $K = k((t))$ is a field of formal power series.

Corollary 5.1. *We keep the notation of the proposition.*

Let $F := \bigoplus_{1\le i\le n} \mathbb{F}_p f_i$, $Z := \bigoplus_{1\le i\le n} \mathbb{F}_p \Delta_{n-1}(\underline{\hat{f}_i})$ be two $\mathbb{F}_p$-subspaces of K associated to $\underline{f}$. Let $z \in Z$ and σ_z be the K-algebra automorphism of $K[W]$ such that $\sigma_z(W) := W + z$. Then σ_z induces a K-algebra automorphism of A that we still denote by σ_z. The map $z \in Z \to \sigma_z \in \mathrm{Aut}_K A$ is an injective group homomorphism and its image is a subgroup G of $\mathrm{Aut}_K A$ which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$. Let $U := (\frac{Z}{\Delta_n(\underline{f})})^p \subset K$ be the $\mathbb{F}_p$-space of roots of the reversed polynomial of

$$P_F(X) := \prod_{f\in F} (X - f) = \frac{\Delta_{n+1}(\underline{f}, X)}{\Delta_n(\underline{f})} = X^{p^n} + \cdots + (-1)^n \Delta_n(\underline{f})^{p-1} X$$

(cf. (2.2) and Section 3.2).

Let $z \in Z$. We can write $z = \Delta_n(\underline{f})u^{1/p}$ with $u \in U$ and for $\underline{\varepsilon} := (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \mathbb{F}_p^n - (0, 0, \dots, 0)$ let $w_{\underline{\varepsilon}} := \sum_{1 \le i \le n} \varepsilon_i w_i \in A$ (resp. $f_{\underline{\varepsilon}} := \sum_{1 \le i \le n} \varepsilon_i f_i \in K$). Then $w_{\underline{\varepsilon}}^p - w_{\underline{\varepsilon}} = f_{\underline{\varepsilon}}$ and $K[w_{\underline{\varepsilon}}] \subset A$ is isomorphic to the K-algebra

$$\frac{K[W_{\underline{\varepsilon}}]}{(W_{\underline{\varepsilon}}^p - W_{\underline{\varepsilon}} - f_{\underline{\varepsilon}})}$$

and so is a K-subalgebra of dimension p. Moreover, $\sigma_z(w_{\underline{\varepsilon}}) = w_{\underline{\varepsilon}} + (-1)^{n-1} E(f_{\underline{\varepsilon}}, u)$, where $E\colon F \times U \to \mathbb{F}_p$ is the Elkies pairing (see Section 3.2 (A)).

In particular when $r = n$, i.e. A is a field and the group G is the full group $\mathrm{Aut}_K A$, then the set $\{K[w_{\underline{\varepsilon}}] \mid \underline{\varepsilon} \in \mathcal{E}\}$, where $\mathcal{E}$ is a set of representatives of $\mathbb{P}^{n-1}(\mathbb{F}_p)$, is equal to the $\frac{p^n-1}{p-1}$, p-cyclic extensions of K inside A.

Proof. (i) We show the equality $\sigma_z(w_{\underline{\varepsilon}}) = w_{\underline{\varepsilon}} + (-1)^{n-1} E(f_{\underline{\varepsilon}}, u)$.
We have $z := \sum_{1 \le i \le n} \alpha_i (-1)^{i-1} \Delta_{n-1}(\underline{\hat{f}_i})$ with $(\alpha_1, \dots, \alpha_n) \in \mathbb{F}_p^n$. Thus,

$$\begin{aligned}
&\sigma_z(w_{\underline{\varepsilon}}) \\
&= \sum_{1 \le i \le n} \varepsilon_i \left(w_i + \frac{\Delta_n\big(\Delta_{n-1}(\underline{\hat{f}_1}), \dots, (-1)^{i-2}\Delta_{n-1}(\underline{\hat{f}_{i-1}}), z, (-1)^i \Delta_{n-1}(\underline{\hat{f}_{i+1}}), \dots, (-1)^{n-1}\Delta_{n-1}(\underline{\hat{f}_n})\big)}{\Delta_n\big(\Delta_{n-1}(\underline{\hat{f}_1}), \dots, (-1)^{j-1}\Delta_{n-1}(\underline{\hat{f}_j}), \dots, (-1)^{n-1}\Delta_{n-1}(\underline{\hat{f}_n})\big)} \right) \\
&= w_{\underline{\varepsilon}} + \sum_{1 \le i \le n} \varepsilon_i \alpha_i \\
&= w_{\underline{\varepsilon}} + (-1)^{n-1} E(f_{\underline{\varepsilon}}, u),
\end{aligned}$$

where $E\colon F \times U \to \mathbb{F}_p$ is the Elkies pairing (see Proposition 3.2 and Section 3.2 (B)).

(ii) We show that $K[w_{\underline{\varepsilon}}] \subset A$ is a K-subalgebra of dimension p. As the w_i, $0 \le i \le n$ are $\mathbb{F}_p$-linearly independent, after an $\mathbb{F}_p$-linear change of variables we can assume that $\varepsilon = (0, 0, \dots, n-1, 1)$. Then the result follows from Lemma 5.1.

The case $n = r$ in Corollary 5.1 then follows from Galois theory. ∎

References

[1] N. Bourbaki, *Éléments de mathématique. Algèbre. Chapitres 4 à 7*. Springer, Berlin Heidelberg, 2007. Zbl 1139.12001

[2] N. D. Elkies, Linearized algebra and finite groups of Lie type. I. Linear and symplectic groups. In *Applications of curves over finite fields (Seattle, WA, 1997)*, pp. 77–107, Contemp. Math. 245, American Mathematical Society, Providence, RI, 1999. Zbl 0976.20032 MR 1732230

[3] D. Goss, *Basic structures of function field arithmetic*. Ergeb. Math. Grenzgeb. (3) 35, Springer, Berlin, 1996. Zbl 0874.11004 MR 1423131

[4] M. Matignon, p-groupes abéliens de type $(p, \cdots, p)$ et disques ouverts p-adiques. *Manuscripta Math.* **99** (1999), no. 1, 93–109. Zbl 0953.12004 MR 1697205

[5] M. Matignon – G. Pagot – D. Turchetti. Work in progress.

[6] E. H. Moore, A two-fold generalization of Fermat's theorem. *Bull. Amer. Math. Soc.* **2** (1896), no. 7, 189–199. Zbl 27.0139.05 MR 1557441

[7] A. Obus, Lifting of curves with automorphisms. In *Open problems in arithmetic algebraic geometry*, pp. 9–59, Adv. Lect. Math. (ALM) 46, International Press, Somerville, MA, 2019. Zbl 1427.14061 MR 3971180

[8] O. Ore, On a special class of polynomials. *Trans. Amer. Math. Soc.* **35** (1933), no. 3, 559–584. Zbl 59.0130.05 MR 1501703

[9] G. Pagot, $\mathbb{F}_p$-espaces vectoriels de formes différentielles logarithmiques sur la droite projective. *J. Number Theory* **97** (2002), no. 1, 58–94. Zbl 1076.14504 MR 1939137

[10] G. Pagot, *Relèvement en caractéristique zéro d'actions de p-groupes abéliens de type $(p, p, \ldots, p)$*. Ph.D. thesis, Université Bordeaux 1, 2002, https://tel.archives-ouvertes.fr/tel-03514229, visited on 23 November 2023.

Manoscritto pervenuto in redazione il 23 aprile 2022.