

Multiplicity estimates for certain pairs of functions involving Drinfeld modular forms

by

VINCENT BOSSER (Caen)

1. Introduction. Zero and multiplicity estimates play a crucial role in the classical theory of transcendence and algebraic independence. The use of such estimates is often unavoidable to get *quantitative* transcendence (or algebraic independence) results, and they are often essential to prove qualitative results as well: a striking example is the multiplicity estimate established by Nesterenko in [Ne], which was the crucial tool in the proof of his famous result about the algebraic independence of values of Eisenstein series.

There is also a rich theory of transcendence and algebraic independence in the framework of function fields in positive characteristic, and multiplicity estimates play an important role here too. But quite curiously, although most of the classical transcendence and algebraic independence results have now a known analogue in positive characteristic, no multiplicity estimates for modular functions are known (in contrast to the classical case, see e.g. [Ph], [Ne], [Pe]). One reason is possibly that the methods used in characteristic zero do not apply in characteristic p . In this paper, we will introduce a new method which works in characteristic p (and, by the way, also in characteristic zero), and using it we will show how one can prove multiplicity estimates for certain pairs of functions involving Drinfeld modular forms. The results obtained here can be applied [Bo2] to get quantitative versions of known transcendence results.

To state precisely the results, we need some notations which we now introduce. Let $A = \mathbb{F}_q[T]$ be the polynomial ring in the indeterminate T with coefficients in the finite field \mathbb{F}_q (whose characteristic will be denoted by p), let $K = \mathbb{F}_q(T)$ be its quotient field, let $K_\infty = \mathbb{F}_q((1/T))$ be its completion for the infinite place, and let C be the completion of an algebraic closure of K_∞ . The absolute value of an element z of C will be denoted by $|z|$ and normalized by the condition $|a| = q^{\deg a}$ for $a \in A$.

2000 *Mathematics Subject Classification*: 11J93, 11F52.

Key words and phrases: Drinfeld modular forms, multiplicity estimates.

We will denote by $\tau : C \rightarrow C$ the Frobenius map, i.e. $\tau(z) = z^q$, and by $\varrho : A \rightarrow C\{\tau\}$ the Carlitz module, defined by $\varrho(T) = \varrho_T = T\tau^0 + \tau$ (here $C\{\tau\}$ denotes as usual the ring of Ore polynomials). The lattice of periods of the Carlitz module has the form $L = \tilde{\pi}A$, where $\tilde{\pi}$ is an element of C , defined up to an element of \mathbb{F}_q^* . We will choose once for all such a $\tilde{\pi}$. We will further denote by $e : C \rightarrow C$ the Carlitz exponential.

Let $\Omega = C \setminus K_\infty$ be the Drinfeld upper half-plane. We will denote by $|z|_i$ the imaginary part of $z \in C$, i.e.

$$|z|_i = \inf_{x \in K_\infty} |z - x|.$$

Let $t(z) = 1/e(\tilde{\pi}z)$ be the parameter at infinity. Then every A -periodic function $f : \Omega \rightarrow C$ (that is, a function f such that $f(z + a) = f(z)$ for all $z \in \Omega$ and all $a \in A$) defines a unique function $\hat{f} : t(\Omega) \rightarrow C$ such that $f(z) = \hat{f}(t(z))$ ($z \in \Omega$). For instance, every modular function f for the group $\mathrm{GL}_2(A)$ defines such a function \hat{f} .

If $F(t)$ is a non-zero function having in a neighborhood of 0 an expansion of the form

$$(1) \quad F(t) = \sum_{n \geq n_0} a_n t^n,$$

with $n_0 \in \mathbb{Z}$, $a_n \in C$, $a_{n_0} \neq 0$, then we define as usual $\mathrm{ord}_0 F(t) := n_0$. If F is the zero function, then we put $\mathrm{ord}_0 F(t) := \infty$. For example, $\mathrm{ord}_0 \hat{f}$ is well defined for a modular function f .

We will denote by j the Drinfeld modular invariant, and by g, h the usual Drinfeld modular forms defined in [Ge]. We recall that these functions g, h generate all the modular forms (with type) for the full group $\mathrm{GL}_2(A)$ [Ge], exactly as the Eisenstein series E_4, E_6 do in the classical case (that is, every modular form of weight k and type m for $\mathrm{GL}_2(A)$ is an isobaric polynomial in g and h , the weights of g and h being $q - 1$ and $q + 1$, respectively).

Finally, if $P \in C[X, Y]$ is a polynomial, we denote for convenience (but in a quite unusual way) $\deg_X^\dagger P := \max\{\deg_X P, 1\}$, where $\deg_X P$ is the degree of P with respect to X , and we define similarly $\deg_Y^\dagger P$.

The two main theorems which we will prove in this paper are the following.

THEOREM 1. *Let $P \in C[X, Y]$ be a non-zero polynomial. Then*

$$\mathrm{ord}_0 P(t, \hat{j}(t)) \leq c_1 \deg_X P \deg_Y^\dagger P,$$

where $c_1 = c_1(q)$ is a positive real number depending only on q .

Here we can take for instance $c_1 = 2q(q + 1)$, as follows from the proof below (but we did not try to find the best constant). This theorem is an analogue of Philibert's multiplicity estimate [Ph] and is used in [Bo 2] to get a quantitative version of the transcendence result of [ADR].

THEOREM 2. *Let $P \in C[X, Y]$ be a non-zero polynomial, and let $\varphi : \Omega \rightarrow C$ be the function defined by $\varphi(z) = h(Tz)/h(z)$. Then*

$$\text{ord}_0 P(\hat{h}(t), \hat{\varphi}(t)) \leq c_2 \deg_X^+ P (\deg_X P + \deg_Y P),$$

where $c_2 = c_2(q) > 0$ depends only on q .

Here we can take $c_2 = 2q^2(q^2 + q)$ (see Section 4 below).

It is not difficult to deduce from Theorem 2 the following corollary (see Section 5).

COROLLARY 3. *Let $P \in C[X, Y]$ be a non-zero polynomial. Then*

$$\text{ord}_0 P(\hat{h}(t), \hat{j}(t)) \leq c_3 \deg_X P (\deg_X P + \deg_Y P),$$

where $c_3 = c_3(q) > 0$ depends only on q .

Because of the formula [Ge] $\Delta = -h^{q-1}$, where Δ is the Drinfeld discriminant function, it is straightforward to derive from Corollary 3 a multiplicity estimate for the two functions Δ and j . This estimate can be used [Bo 2] to get a quantitative version of the transcendence result of [Di].

We can deduce from Corollary 3 the following two corollaries.

COROLLARY 4. *Let $f : \Omega \rightarrow C$ be a non-constant modular form for $\text{GL}_2(A)$. There exists a real number $c_4 > 0$ (depending on q and f) such that for every non-zero polynomial $P \in C[X, Y]$,*

$$\text{ord}_0 P(\hat{f}(t), \hat{j}(t)) \leq c_4 \deg_X P (\deg_X P + \deg_Y P).$$

COROLLARY 5. *Let $f_1 : \Omega \rightarrow C$ and $f_2 : \Omega \rightarrow C$ be two algebraically independent modular forms for $\text{GL}_2(A)$. There exists a real number $c_5 > 0$ (depending on q , f_1 and f_2) such that for every non-zero polynomial $P \in C[X, Y]$,*

$$\text{ord}_0 P(\hat{f}_1(t), \hat{f}_2(t)) \leq c_5 (\deg_X P + \deg_Y P)^2.$$

The paper is organized as follows. In Section 2, we explain the idea of proofs of Theorems 1 and 2. In Section 3, we prove Theorem 1. In Section 4, we prove Theorem 2. Finally, we give the proofs of the corollaries in Section 5.

2. Idea of the proofs. A quite general method for proving multiplicity estimates, which is frequently used in the literature and on which our method is also based, is the following one. Suppose that you are given two C -algebraically independent functions $F_1, F_2 : U \rightarrow C$ having a t -expansion (1) in a neighborhood U of zero, and suppose that you want to prove a multiplicity estimate of the form

$$\text{ord}_0 P(F_1(t), F_2(t)) \leq c \deg_X^+ P \deg_Y^+ P$$

(where $c > 0$ depends only on q , F_1 and F_2). For simplicity we will assume that F_1 , F_2 are analytic on U , but the same kind of arguments can be used even if F_1 or F_2 has a pole at zero (as in Theorem 1).

First note that without loss of generality we may assume that the polynomial P is irreducible, and that $\deg_X P \geq 1$, $\deg_Y P \geq 1$. The main idea is then to construct from P a polynomial $Q \in \mathbb{C}[X, Y]$ satisfying the following three conditions (C_1 , C_2 , C_3 and C_4 denote here real numbers depending on q , F_1 and F_2):

- (a) $\deg_X Q \leq C_1 \deg_X P$ and $\deg_Y Q \leq C_1 \deg_Y P$, where $C_1 > 0$.
- (b) $\text{ord}_0 Q(F_1(t), F_2(t)) \geq C_2 \text{ord}_0 P(F_1(t), F_2(t)) - C_3 \deg_X P \deg_Y P$, where $C_2 > 0$ and $C_3 \geq 0$.
- (c) $P \nmid Q$.

If (a), (b) and (c) are satisfied, one easily derives the multiplicity estimate as follows. Consider the resultant with respect to Y (say) $R(X) = \text{res}_Y(P, Q)$. Because of (c) we have $R(X) \neq 0$, and thus $(^1) \text{ord}_0 R(F_1(t)) \ll \deg R$ (here and in the following the symbol \ll means that the upper bound involves a constant depending on q , F_1 and F_2). Using (a) we derive

$$(2) \quad \begin{aligned} \text{ord}_0 R(F_1(t)) &\ll \deg R \ll \deg_X P \deg_Y Q + \deg_Y P \deg_X Q \\ &\ll \deg_X P \deg_Y P. \end{aligned}$$

Since now there exist polynomials U and V satisfying $UP + VQ = R$, we see, using (b), that

$$(3) \quad \begin{aligned} \text{ord}_0 R(F_1(t)) &\geq \min\{\text{ord}_0 P(F_1(t), F_2(t)), \text{ord}_0 Q(F_1(t), F_2(t))\} \\ &\geq C_4 \text{ord}_0 P(F_1(t), F_2(t)) - C_3 \deg_X P \deg_Y P. \end{aligned}$$

Combining (2) and (3) gives the desired estimate (naturally, the same method works even if we cannot separate the partial degrees, but it leads to a less precise result, as for instance in Theorem 2).

When the method described above applies, we usually find quite easily a natural candidate for Q which satisfies almost immediately the conditions (a) and (b), and the difficult part is to verify (c). This was for instance the case in the proof of Philibert's multiplicity estimate [Ph], and it will also be the case for us.

In order to explain the idea of the proof of Theorem 1, let us briefly sketch Philibert's proof of the complex analogue. So in this paragraph $j(z) = J(q)$ denotes the usual elliptic modular invariant, and $q = e^{2\pi iz}$. Using the modular equation of level 2 for j , Philibert takes for Q the unique polynomial of $\mathbb{C}[X, Y]$ such that

$$(4) \quad Q(X, j(z)) = P(X^2, j(2z))P(X^2, j(z/2))P(X^2, j((z+1)/2)).$$

(¹) To see this it suffices to decompose R as a product of linear factors.

It is not difficult to show that this polynomial satisfies conditions (a) and (b). Thus, it remains to verify (c). To do this, denote by \mathcal{K} the algebraic closure of the field $\mathbb{C}((q))$ of Laurent series in q , and suppose that P divides Q . Philibert's idea consists in showing that in this case there exist infinitely many roots in \mathcal{K} of the non-zero polynomial $f(X) = P(X, J(q)) \in \mathbb{C}((q))[X]$, which is a contradiction. The argument is as follows. Since the field \mathcal{K} is here the field $\bigcup_{e \geq 1} \mathbb{C}((q^{1/e}))$ of Puiseux series, we can find a first root $x_0 = x_0(q) \in \mathcal{K}$ of the polynomial f . Since $P \mid Q$, we also have $Q(x_0(q), J(q)) = 0$. Thus, the right-hand side of (4) vanishes when we substitute $x_0(q)$ to X , and it is easily seen that it leads to a new equality of the form $P(x_1(q), J(q)) = 0$. Repeating the argument, we get a sequence x_0, x_1, x_2, \dots of elements of \mathcal{K} which are roots of the polynomial f . Since it can be shown that these elements are pairwise distinct by a careful study of their q -expansion, we get the desired contradiction.

Let us now return to the Drinfeld case. One can define an analogue of the polynomial Q above (which would be the polynomial given by the formula (8) for $r = 0$ below). As in the complex case, only condition (c) is not trivial. However, we cannot mimic Philibert's proof here, because in characteristic p the existence of a Puiseux series $x_0(t)$ satisfying $P(x_0(t), \hat{j}(t)) = 0$ as above is not guaranteed.

To overcome this problem, the basic remark is that we can still construct such a root $x_0(t)$, which lies even in $C[[t]]$, if Newton's method to approximate the roots of a polynomial in non-archimedean, complete fields (Hensel lemma) is convergent. More precisely, set $f(X) = P(X, \hat{j}(t)) \in C((t))[X]$, and consider as starting point (first approximation of the root of f) $a_0 = t$. If Newton's method is convergent (first case to consider), we will find a root $x_0 \in C[[t]]$ and we will be able to apply Philibert's method sketched above. The standard sufficient condition to ensure convergence reads here ⁽²⁾

$$(5) \quad 2 \operatorname{ord}_0 \frac{\partial P}{\partial X}(t, \hat{j}(t)) < \operatorname{ord}_0 P(t, \hat{j}(t)) - (q - 1) \deg_Y P.$$

However, it can happen that (5) does not hold. But then it turns out that the condition obtained is exactly of the form (b) in the general method described above with now $Q = \partial P / \partial X$. Since in this case (a) is trivial, we see that we will be able to apply the general method with $Q = \partial P / \partial X$ provided (c) holds, i.e. if $\partial P / \partial X \neq 0$ (second case). It still remains to treat the case $\partial P / \partial X = 0$ (last case). In this case, we can write $P(X, Y) = S(X^{p^f}, Y)$ with $f \geq 1$, $\partial S / \partial X \neq 0$, and $\deg_X S < \deg_X P$. The idea is now to argue by induction on the partial degree $\deg_X P$. However, since $\operatorname{ord}_0 P(t, \hat{j}(t)) = \operatorname{ord}_0 S(t^{p^f}, \hat{j}(t))$, we see that in order to apply the induction hypothesis to S

⁽²⁾ In fact, for technical (computational) reasons (see §3.2), we will be able to apply Philibert's method only under a stronger condition than this standard one.

we now need a multiplicity estimate for the two functions t^{p^f} and $\hat{j}(t)$, and not only for t and $\hat{j}(t)$. Fortunately, all the arguments just described above also work *mutatis mutandis* with t^{p^f} instead of t , and therefore an inductive argument is possible.

Summing up, what we will prove is in fact the following apparently more general result: *For every irreducible polynomial $P \in C[X, Y]$ and every integer $r \geq 0$,*

$$\text{ord}_0 P(t^{p^r}, \hat{j}(t)) \leq c_1(q)p^r \deg_X P \deg_Y^+ P.$$

This will be proved in the next section by induction on $\deg_X P$, by distinguishing the three cases above. Theorem 2 will then be proved in Section 4 by the same method. Let us also mention that in the proof of Theorem 1, even in the case when Philibert's method applies, the problem of proving that the roots x_0, x_1, \dots are all distinct is, contrary to the complex case, not at all an easy one, and it requires quite involved computations (see Section 3.2).

3. Proof of Theorem 1. As already mentioned, it suffices to prove Theorem 1 when the polynomial P is irreducible. Indeed, the multiplicity estimate is plainly true if P is constant, and if it is true for two polynomials P_1 and P_2 , then it is true for their product $P_1 P_2$ by simply adding the inequalities.

As explained in the previous section, we will prove the following lemma, from which Theorem 1 will immediately follow by putting $r = 0$.

LEMMA 6. *For every irreducible polynomial $P \in C[X, Y]$ and every integer $r \geq 0$,*

$$\text{ord}_0 P(t^{p^r}, \hat{j}(t)) \leq c_1 p^r \deg_X P \deg_Y^+ P,$$

where $c_1 = c_1(q) > 0$ depends only on q .

Here the constant c_1 is the same as in Theorem 1. We can take for instance $c_1 = 2q(q + 1)$.

The proof of Lemma 6 will occupy the whole Section 3. It is divided into two parts. In the first one (Section 3.1), we prove the lemma, assuming that a certain resultant is not zero. In the second (technical) part (Section 3.2), we prove that this resultant is indeed not zero.

3.1. Proof of Lemma 6, assuming the non-vanishing of a resultant. Let P be an irreducible polynomial in $C[X, Y]$. If $\deg_X P = 0$ Lemma 6 is true because in this case the inequality $\text{ord}_0 P(t^{p^r}, \hat{j}(t)) \leq 0$ trivially holds for every r . Arguing by induction on $\deg_X P$, we now suppose that $\deg_X P \geq 1$ and that Lemma 6 is true for all polynomials whose partial degree with respect to X is strictly less than $\deg_X P$. Let $r \geq 0$ be an integer. Since Lemma 6 is clear if $\deg_Y P = 0$ or if $\text{ord}_0 P(t^{p^r}, \hat{j}(t)) < 0$, we may assume

in what follows that $\deg_Y P \geq 1$ and that $\text{ord}_0 P(t^{p^r}, \hat{j}(t)) \geq 0$. We now distinguish three cases.

First case: $\partial P/\partial X = 0$. In this case we write $P(X, Y) = S(X^{p^f}, Y)$, with $S \in C[X, Y]$ and $f \geq 1$ maximal (it is possible because $\deg_X P \geq 1$). Then $\deg_X P = p^f \deg_X S$ and $\deg_Y P = \deg_Y S$. We have in particular $\deg_X S < \deg_X P$ and thus we can apply the induction hypothesis to S (which is also irreducible), which gives

$$\begin{aligned} \text{ord}_0 P(t^{p^r}, \hat{j}(t)) &= \text{ord}_0 S(t^{p^{r+f}}, \hat{j}(t)) \\ &\leq c_1 p^{r+f} \deg_X S \deg_Y S = c_1 p^r \deg_X P \deg_Y P \end{aligned}$$

as desired.

Second case: $\partial P/\partial X \neq 0$ and the following condition holds:

$$2 \text{ord}_0 \frac{\partial P}{\partial X}(t^{p^r}, \hat{j}(t)) \geq \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - (q-1) \deg_Y P - 2p^r.$$

In this case, we introduce the resultant $R = R(Y) = \text{res}_X(P, \partial P/\partial X) \in C[Y]$. Since $P \nmid \frac{\partial P}{\partial X}$ we have $R \neq 0$. Moreover, by a well-known property of the resultant there exist two polynomials $U, V \in C[X, Y]$ such that

$$R = UP + V \frac{\partial P}{\partial X},$$

and whose degrees in Y satisfy

$$\deg_Y U \leq \deg_X \left(\frac{\partial P}{\partial X} \right) \deg_Y P + \deg_X P \deg_Y \left(\frac{\partial P}{\partial X} \right) \leq 2 \deg_X P \deg_Y P$$

and analogously

$$\deg_Y V \leq 2 \deg_X P \deg_Y P.$$

Now, recall that the function $\hat{j}(t)$ has an expansion for $|t|$ small of the form

$$\hat{j}(t) = -\frac{1}{t^{q-1}} + T^q - T + \text{higher order terms.}$$

Hence, since $\hat{j}(t)$ has a pole of order $q-1$ at zero, we deduce

$$\text{ord}_0 U(t^{p^r}, \hat{j}(t)) \geq -(q-1) \deg_Y U \geq -2(q-1) \deg_X P \deg_Y P$$

and

$$\text{ord}_0 V(t^{p^r}, \hat{j}(t)) \geq -(q-1) \deg_Y V \geq -2(q-1) \deg_X P \deg_Y P.$$

From this we derive on one hand

$$\text{ord}_0(UP)(t^{p^r}, \hat{j}(t)) \geq \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - 2(q-1) \deg_X P \deg_Y P,$$

and on the other hand

$$\begin{aligned} \text{ord}_0 \left(V \frac{\partial P}{\partial X} \right) (t^{p^r}, \hat{j}(t)) &\geq \frac{1}{2} \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - \frac{1}{2} (q-1) \deg_Y P - p^r \\ &\quad - 2(q-1) \deg_X P \deg_Y P \\ &\geq \frac{1}{2} \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - \frac{5}{2} p^r q \deg_X P \deg_Y P. \end{aligned}$$

Thus, we obtain

$$\begin{aligned} \text{ord}_0 R(\hat{j}(t)) &\geq \min \left\{ \text{ord}_0(UP)(t^{p^r}, \hat{j}(t)); \text{ord}_0 \left(V \frac{\partial P}{\partial X} \right) (t^{p^r}, \hat{j}(t)) \right\} \\ &\geq \frac{1}{2} \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - \frac{5}{2} p^r q \deg_X P \deg_Y P. \end{aligned}$$

Since now $R \neq 0$ we have the trivial estimate $\text{ord}_0 R(\hat{j}(t)) \leq 0$, from which the conclusion of Lemma 6 follows (it suffices to take $c_1 \geq 5q$).

Third case: $\partial P/\partial X \neq 0$ and the following condition holds:

$$2 \text{ord}_0 \frac{\partial P}{\partial X} (t^{p^r}, \hat{j}(t)) < \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - (q-1) \deg_Y P - 2p^r.$$

In this case, we will construct a polynomial Q analogous to that constructed by Philibert and then apply the method using Newton approximations sketched in the previous section.

Denote by \mathcal{M} the set of matrices γ of $\text{GL}_2(A)$ of the form $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, where a, b, d are coprime, a is monic, $ad = T$ and $\deg b < \deg a$. We have explicitly

$$\mathcal{M} = \left\{ \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & T \end{pmatrix} \mid \lambda \in \mathbb{F}_q \right\}.$$

As in the classical case, there exists a modular polynomial $\Phi_T \in A[X, Y]$ which satisfies

$$\Phi_T(X, j(z)) = \prod_{\gamma \in \mathcal{M}} (X - j(\gamma z)) \quad (z \in \Omega)$$

(the notation γz means of course $(az + b)/d$). It follows in particular that every symmetrical polynomial in the functions $j(\gamma z)$ is in fact a polynomial in the function j .

Next, we note that

$$t(Tz) = \frac{1}{e(\tilde{\pi}Tz)} = \frac{1}{Te(\tilde{\pi}z) + e(\tilde{\pi}z)^q} = \frac{t(z)^q}{1 + Tt(z)^{q-1}}.$$

Thus, if we denote by s and s_r the rational functions defined by

$$(6) \quad s(X) = \frac{X^q}{1 + TX^{q-1}} \quad \text{and} \quad s_r(X) = \frac{X^q}{1 + T^{p^r} X^{q-1}},$$

we have the identities

$$(7) \quad t(Tz) = s(t(z)) \quad \text{and} \quad t(Tz)^{p^r} = s_r(t(z)^{p^r}).$$

Following the idea of Philibert, we now define the polynomial Q as the unique polynomial in $C[X, Y]$ satisfying the equality ($z \in \Omega$)

$$(8) \quad Q(X, j(z)) = \prod_{\gamma \in \mathcal{M}} [P(s_r(X), j(\gamma z))(1 + T^{p^r} X^{q-1})^{\deg_X P}].$$

Such a polynomial exists since the right hand side of (8) is a polynomial in X whose coefficients are symmetrical polynomials in the functions $j(\gamma z)$ (and it is plainly unique).

The next step consists now in estimating from above the partial degrees $\deg_X Q$ and $\deg_Y Q$ in terms of $\deg_X P$ and $\deg_Y P$. It is easy to see that each factor of the product (8) is a polynomial in X with coefficients in the field of meromorphic functions in Ω of degree at most $q \deg_X P$, so that

$$(9) \quad \deg_X Q \leq q(q+1) \deg_X P.$$

To find an upper bound for $\deg_Y Q$, we will estimate the order of the pole at infinity of each coefficient of the polynomial $Q(X, j(\gamma z))$. We will adopt the following convenient notation: If Π is any non-zero polynomial in X whose coefficients are meromorphic functions in Ω having a t -expansion at infinity, we will denote by $\text{ord}_0 \Pi$ the minimum of the orders at $t = 0$ of each coefficient of Π . With this notation we thus have $\text{ord}_0 Q(X, j(z)) = -(q-1) \deg_Y Q$. Now, since the individual factors of the product (8) do not necessarily have a t -expansion (although the product has one), we will merely consider the polynomial $Q(X, j(Tz))$, whose factors now have an expansion in $t(z)$. More precisely, if $\gamma = \begin{pmatrix} 1 & \lambda \\ 0 & T \end{pmatrix}$ ($\lambda \in \mathbb{F}_q$), then (for $|z|_i$ large)

$$j(\gamma(Tz)) = j(z + \lambda/T) = -\frac{1}{t(z + \lambda/T)^{q-1}} + \cdots = -\frac{1}{t^{q-1}} + \cdots,$$

where we have set $t = t(z)$ (we have also used the fact that $t(z + \lambda/T) = t/(1 + te(\tilde{\pi}\lambda/T))$). Thus $\text{ord}_0 P(s_r(X), j(\gamma(Tz)))(1 + T^{p^r} X^{q-1})^{\deg_X P} = -(q-1) \deg_Y P$ in this case. Similarly, if $\gamma = \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix}$, then

$$j(\gamma(Tz)) = j(T^2 z) = -\frac{1}{t(T^2 z)^{q-1}} + \cdots = -\frac{1}{t^{q^2(q-1)}} + \cdots,$$

since $t(T^2 z) = t^{q^2} + \cdots$ by (6) and (7). We have therefore

$$\text{ord}_0 P(s_r(X), j(\gamma(Tz)))(1 + T^{p^r} X^{q-1})^{\deg_X P} = -q^2(q-1) \deg_Y P.$$

It follows from these considerations and the formula (8) that

$$\text{ord}_0 Q(X, j(Tz)) = -(q^3 - q) \deg_Y P,$$

and thus, since $t(Tz) = t^q + \dots$,

$$\text{ord}_0 Q(X, j(z)) = \frac{1}{q} \text{ord}_0 Q(X, j(Tz)) = -(q^2 - 1) \deg_Y P.$$

Hence we have obtained

$$(10) \quad \deg_Y Q = (q + 1) \deg_Y P.$$

We now estimate $\text{ord}_0 Q(t^{p^r}, \hat{j}(t))$ from below. Using (8) and (7), we first have

$$(11) \quad Q(t(z)^{p^r}, j(z)) = (1 + T^{p^r} t(z)^{p^r(q-1)})^{\deg_X P} P(t(Tz)^{p^r}, j(Tz)) \cdot \prod_{\lambda \in \mathbb{F}_q} f_\lambda(z),$$

where

$$f_\lambda(z) = (1 + T^{p^r} t(z)^{p^r(q-1)})^{\deg_X P} P\left(s_r(t(z)^{p^r}), j\left(\frac{z + \lambda}{T}\right)\right).$$

Now, each function $z \mapsto f_\lambda(Tz)$ has an expansion in $t(z)$, and since $\hat{j}(t)$ has a pole of order $q - 1$ at $t = 0$, we find, in a similar way as above,

$$\text{ord}_0 f_\lambda(Tz) = \text{ord}_0 P(s_r(t(Tz)^{p^r}), j(z + \lambda/T)) \geq -(q - 1) \deg_Y P,$$

from which we derive

$$(12) \quad \text{ord}_0 \left(\prod_{\lambda \in \mathbb{F}_q} f_\lambda(z) \right) = \frac{1}{q} \text{ord}_0 \left(\prod_{\lambda \in \mathbb{F}_q} f_\lambda(Tz) \right) \geq -(q - 1) \deg_Y P.$$

Since $\text{ord}_0 P(t(Tz)^{p^r}, j(Tz)) = q \text{ord}_0 P(t(z)^{p^r}, j(z))$, it follows from (11) and (12) that

$$(13) \quad \text{ord}_0 Q(t^{p^r}, \hat{j}(t)) \geq q \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - (q - 1) \deg_Y P,$$

which is condition (b) of Section 2.

Consider now the resultant (with respect to Y) $R(X) = \text{res}_Y(P, Q) \in C[X]$. There exist polynomials $U, V \in C[X, Y]$ satisfying

$$(14) \quad R(X) = UP + VQ$$

and such that, by (10),

$$\begin{aligned} \deg_Y U &\leq \deg_Y Q - 1 \leq (q + 1) \deg_Y P, \\ \deg_Y V &\leq \deg_Y P - 1 \leq \deg_Y P. \end{aligned}$$

It follows that

$$(15) \quad \begin{aligned} \text{ord}_0((UP)(t^{p^r}, \hat{j}(t))) &\geq \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - (q - 1) \deg_Y U \\ &\geq \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - (q^2 - 1) \deg_Y P \end{aligned}$$

and similarly, using (13),

$$(16) \quad \text{ord}_0((VQ)(t^{p^r}, \hat{j}(t))) \geq q \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - (q^2 - 1) \deg_Y P.$$

From (14)–(16) we deduce readily

$$(17) \quad \text{ord}_0 R(t^{p^r}) \geq \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - (q^2 - 1) \deg_Y P.$$

Now, suppose that we have shown that $R(X) \neq 0$. This fact is not trivial and will be proved in the next section. Assuming this, Lemma 6 becomes straightforward, because then we have, thanks to (9) and (10),

$$\begin{aligned} \text{ord}_0 R(t^{p^r}) &\leq p^r \deg R \leq p^r (\deg_X P \deg_Y Q + \deg_X Q \deg_Y P) \\ &\leq p^r (q + 1)^2 \deg_X P \deg_Y P. \end{aligned}$$

Combining this last inequality with (17) yields the lemma with $c_1 = 2q(q+1)$ (note that the previously required condition $c_1 \geq 5q$ is satisfied). ■

3.2. Non-vanishing of $R(X)$. To complete the proof of Lemma 6 (and thus of Theorem 1), it remains to show that the resultant $R(X)$ defined at the end of the previous section is not zero (which was assumed without proof). We state the result in the following proposition:

PROPOSITION 7. *Let $P \in C[X, Y]$ be an irreducible polynomial such that $\deg_Y P \geq 1$, $\partial P / \partial X \neq 0$ and*

$$(18) \quad 2 \text{ord}_0 \frac{\partial P}{\partial X}(t^{p^r}, \hat{j}(t)) < \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - (q - 1) \deg_Y P - 2p^r.$$

Let $Q \in C[X, Y]$ be the polynomial defined by the identity (8), and set $R(X) = \text{res}_Y(P, Q) \in C[X]$. Then $R(X) \neq 0$.

To prove the proposition it will be useful to introduce, for every $\alpha \in C$, the formal series $\sigma_\alpha \in C[[t]]$ defined by

$$(19) \quad \sigma_\alpha(t) = \frac{t}{1 + \alpha t}.$$

If α has the form $\alpha = e(\tilde{\pi}\gamma)$ with $\gamma \in K_\infty$, then a straightforward computation shows that for all $z \in \Omega$ we have

$$(20) \quad t(z + \gamma) = \sigma_\alpha(t(z)).$$

We will also need the formal series $s, s_r \in C[[t]]$ defined in the previous section by (see (6))

$$(21) \quad s = s(t) = \frac{t^q}{1 + Tt^{q-1}}, \quad s_r = s_r(t) = \frac{t^q}{1 + Tp^r t^{q-1}}.$$

If f and g are elements of $C((t))$ such that $\text{ord}_0 g \geq 1$, then the composition $f \circ g$ is well defined and will often be denoted just by fg in what follows. Thus, s^n stands for instance for $s \circ \dots \circ s$ (n times). We also note that $\sigma_\alpha \sigma_\beta = \sigma_{\alpha+\beta}$ and that σ_α is invertible for the composition, with inverse $\sigma_\alpha^{-1} = \sigma_{-\alpha}$. Finally, we observe that we may cancel from the right in $C((t))$ (but not from the left), that is: If f, g, h are elements in $C((t))$ with $h \neq 0$ and $\text{ord}_0 h \geq 1$, then the equality $f \circ h = g \circ h$ implies $f = g$. This property will often be used in what follows.

We first prove the following lemma involving the formal series σ_α and s :

LEMMA 8. *Let $a \in K_\infty$, $m \in \mathbb{Z}$ and $\alpha := e(\tilde{\pi}a/T^m)$.*

- (i) *For every $n \geq 0$ we have $\sigma_\alpha s^n = s^n \sigma_\beta$, where $\beta = e(\tilde{\pi}a/T^{m+n})$.*
- (ii) *If $a \in A$ and n is an integer with $n \geq m$, then $s^n \sigma_\alpha = s^n$.*

Proof. Let us first prove (i). For every $z \in \Omega$ we have, by (20) and (7),

$$\begin{aligned} \sigma_\alpha s^n(t(z)) &= \sigma_\alpha(t(T^n z)) = t(T^n z + a/T^m) = t(T^n(z + a/T^{m+n})) \\ &= s^n(t(z + a/T^{m+n})) = s^n \sigma_\beta(t(z)). \end{aligned}$$

This being true for all $z \in \Omega$, this gives rise to the desired equality in the field $C((t))$.

In the case (ii) we have similarly, for all $z \in \Omega$ (note that we have here $aT^{n-m} \in A$),

$$s^n \sigma_\alpha(t(z)) = t(T^n(z + a/T^m)) = t(T^n z + aT^{n-m}) = t(T^n z) = s^n(t(z)).$$

This being true for all $z \in \Omega$, we get the identity (ii). ■

We now want to argue as sketched in Section 2, using Newton approximations in complete, non-archimedean fields. For convenience for the reader, we recall below the ‘‘Hensel lemma’’ that we will use, which is taken from [La, Chapter XII, Proposition 7.6].

LEMMA 9. *Let \mathfrak{K} be a complete field under a non-archimedean absolute value $|\cdot|$. Let \mathfrak{D} be the valuation ring and let $f \in \mathfrak{D}[X]$ be a polynomial. Let $a_0 \in \mathfrak{D}$ be such that*

$$(22) \quad |f(a_0)| < |f'(a_0)|^2.$$

Then the sequence $(a_n)_{n \geq 0}$ defined by $a_{n+1} = a_n - f(a_n)/f'(a_n)$ converges to a root $a \in \mathfrak{D}$ of f , and moreover we have

$$(23) \quad |a - a_0| \leq \left| \frac{f(a_0)}{f'(a_0)^2} \right|.$$

With the help of this lemma, we prove:

LEMMA 10. *Let $P \in C[X, Y]$ be a polynomial satisfying the conditions of Proposition 7. There exists a power series $x = x(t) \in C[[t]]$ such that $P(x(t), \hat{j}(t)) = 0$ identically and*

$$(24) \quad x(t) = t^{p^r} + a_m t^m + \dots,$$

where $a_m \neq 0$, $m > 2p^r$, and where the dots stand for the terms of order $> m$.

Proof. Let $\mathfrak{K} = C((t))$. The field \mathfrak{K} is complete with respect to the non-archimedean absolute value given by $|x| = q^{-\text{ord}_0 x}$, and its valuation ring is $\mathfrak{D} = C[[t]]$. Set $f(X) := t^{(q-1)\deg_Y P} P(X, \hat{j}(t)) \in \mathfrak{D}[X]$ and $a_0 := t^{p^r}$. We have $f'(a_0) = t^{(q-1)\deg_Y P} \frac{\partial P}{\partial X}(t^{p^r}, \hat{j}(t))$, and the hypothesis (18) easily

implies that condition (22) is satisfied. Thus, there exists a formal power series $x \in C[[t]]$ such that $P(x(t), \hat{j}(t)) = 0$ identically. Moreover, (23) gives the following error estimate:

$$\begin{aligned} \text{ord}_0(x(t) - t^{p^r}) &\geq \text{ord}_0 P(t^{p^r}, \hat{j}(t)) - 2 \text{ord}_0 \frac{\partial P}{\partial X}(t^{p^r}, \hat{j}(t)) \\ &\quad - (q-1) \deg_Y P > 2p^r. \end{aligned}$$

To complete the proof it now remains to note that the series $\hat{j}(t)$ and t are algebraically independent over C (see [ADR]) and thus we cannot have $x(t) = t^{p^r}$. ■

We now begin the proof of Proposition 7. Let P be a polynomial satisfying the conditions of the proposition. Arguing by contradiction, we assume furthermore that $R(X) = 0$. Under this assumption we first prove:

LEMMA 11. *There exists a sequence $(x_i)_{i \geq 0}$ of elements of $C[[t]]$ satisfying the following conditions:*

- (i) $x_0 = x$.
- (ii) $\text{ord}_0 x_i \geq 1$ for all $i \geq 0$.
- (iii) For all $i \geq 1$, we have either $x_i = s_r x_{i-1}$ or $x_i = s_r x_{i-1} \sigma_\alpha s^2$, where $\alpha \in C$ is of the form $\alpha = e(\tilde{\pi} \lambda / T^{i-1})$ for some $\lambda \in \mathbb{F}_q$.
- (iv) For all $i \geq 0$, we have $P(x_i, \hat{j} \circ s^i) = 0$.

Proof. We define inductively the sequence $(x_i)_{i \geq 0}$ as follows. Put $x_0 := x$, and suppose we have already constructed, for some $i \geq 0$, power series x_0, \dots, x_i satisfying conditions (i) to (iv) (for $i = 0$ these conditions follow from Lemma 10). Since $R(X) = 0$, we have $P|Q$ and thus (iv) implies $Q(x_i, \hat{j} s^i) = 0$. It follows *a fortiori* that $Q(x_i s, \hat{j} s^{i+1}) = 0$. Note now that $1 + T^{p^r} (x_i s)^{q-1} \neq 0$ (here $(x_i s)^{q-1}$ means $x_i \circ s$ to the exponent $q-1$), because otherwise we would have $\text{ord}_0(x_i \circ s) = 0$, which contradicts condition (ii). Using this remark and the formula (8), we find that either $P(s_r x_i s, \hat{j} s^{i+2}) = 0$ or $P(s_r x_i s, \hat{j} \sigma_{\alpha'} s^i) = 0$ with $\alpha' = e(\tilde{\pi} \lambda / T)$ for some $\lambda \in \mathbb{F}_q$. In the first case, putting $x_{i+1} := s_r x_i$ gives $P(x_{i+1}, \hat{j} s^{i+1}) = 0$. Hence conditions (ii), (iii) and (iv) hold for x_{i+1} in this case (note that $\text{ord}_0 x_{i+1} = q \text{ord}_0 x_i \geq q$). In the second case, we first write, thanks to Lemma 8, $\sigma_{\alpha'} s^i = s^i \sigma_\beta$ with $\beta = e(\tilde{\pi} \lambda / T^{i+1})$. Composing the relation $P(s_r x_i s, \hat{j} s^i \sigma_\beta) = 0$ from the right with $\sigma_\beta^{-1} s$, we get $P(s_r x_i s \sigma_{-\beta} s, \hat{j} s^{i+1}) = 0$. Now, Lemma 8 again gives $s \sigma_{-\beta} = \sigma_\alpha s$, where $\alpha = e(-\tilde{\pi} \lambda / T^i)$. It follows that $P(s_r x_i \sigma_\alpha s^2, \hat{j} s^{i+1}) = 0$, and thus conditions (ii), (iii) and (iv) are also satisfied in this case by putting $x_{i+1} = s_r x_i \sigma_\alpha s^2$. ■

We now define

$$n := \deg_X P \quad \text{and} \quad y_i = x_i s^{n-i}, \quad 0 \leq i \leq n.$$

It follows from the previous lemma that $P(y_i, \hat{j} \circ s^n) = 0$ for $i = 0, \dots, n$. As already explained in Section 2, we now want to prove that these y_i 's are pairwise distinct. We will need three more lemmas.

LEMMA 12. *Suppose $y_i = y_{i+k}$ for some integers i, k with $0 \leq i \leq i+k \leq n$. Then $s_r^k x_i = x_i s^k$.*

Proof. It follows from Lemma 11(iii) that $\text{ord}_0 x_{j+1} = q \text{ord}_0 x_j$ if $x_{j+1} = s_r x_j$, and that $\text{ord}_0 x_{j+1} = q^3 \text{ord}_0 x_j$ in the other case (all $j \geq 0$). Thus, $\text{ord}_0 y_{j+1} = \text{ord}_0 y_j$ if $x_{j+1} = s_r x_j$ and $\text{ord}_0 y_{j+1} = q^2 \text{ord}_0 y_j > \text{ord}_0 y_j$ otherwise. We deduce from this that if $y_i = y_{i+k}$, then we must have

$$\text{ord}_0 y_{j+1} = \text{ord}_0 y_j, \quad j = i, \dots, k-1$$

and therefore $x_{j+1} = s_r x_j$, $j = i, \dots, k-1$. Hence we get

$$y_{i+k} = x_{i+k} s^{n-i-k} = s_r^k x_i s^{n-i-k} = y_i = x_i s^{n-i},$$

and Lemma 12 follows. ■

LEMMA 13. *Suppose that $y_i = y_{i+k}$ for some indices i, k with $0 \leq i \leq i+k \leq n$. Then there exists $a \in A$ with $\deg a < i-1$ such that if we set $\alpha = e(\tilde{\pi}a/T^{i-1})$, then*

$$s_r^{k+i} x_0 \sigma_\alpha = s_r^i x_0 \sigma_\alpha s^k.$$

Proof. Let i, k be integers such that $0 \leq i \leq i+k \leq n$ and suppose that $y_i = y_{i+k}$. We will prove by induction that for all l , $0 \leq l \leq i$, there is $a_l \in A$ with $\deg a_l < i-1$ such that if we set $\alpha_l = e(\tilde{\pi}a_l/T^{i-1})$, then

$$(25) \quad s_r^{k+l} x_{i-l} \sigma_{\alpha_l} = s_r^l x_{i-l} \sigma_{\alpha_l} s^k.$$

For $l = 0$, this assertion is true by Lemma 12 and by choosing $a_0 := 0$. Suppose now it has been proved for l , where $0 \leq l \leq i-1$. If $x_{i-l} = s_r x_{i-l-1}$ (see Lemma 11(iii)), then (25) immediately gives the corresponding formula for $l+1$ by choosing $a_{l+1} = a_l$. If not, we have $x_{i-l} = s_r x_{i-l-1} \sigma_\alpha s^2$ with $\alpha = e(\tilde{\pi}\lambda/T^{i-l-1})$ and some $\lambda \in \mathbb{F}_q$. Substituting in the formula (25) yields

$$s_r^{k+l+1} x_{i-l-1} \sigma_\alpha s^2 \sigma_{\alpha_l} = s_r^{l+1} x_{i-l-1} \sigma_\alpha s^2 \sigma_{\alpha_l} s^k.$$

Now, Lemma 8(i) allows us to write $\sigma_\alpha s^2 \sigma_{\alpha_l} = \sigma_{\alpha_{l+1}} s^2$, where

$$\alpha_{l+1} = \alpha + e\left(\frac{\tilde{\pi}a_l}{T^{i-3}}\right) = e\left(\frac{\tilde{\pi}\lambda T^l + \tilde{\pi}a_l T^2}{T^{i-1}}\right).$$

The division of $\lambda T^l + a_l T^2$ by T^{i-1} shows that we can even write $\alpha_{l+1} = e(\tilde{\pi}a_{l+1}/T^{i-1})$ with $a_{l+1} \in A$ and $\deg a_{l+1} < i-1$. We thus obtain

$$s_r^{k+l+1} x_{i-l-1} \sigma_{\alpha_{l+1}} s^2 = s_r^{l+1} x_{i-l-1} \sigma_{\alpha_{l+1}} s^{k+2}.$$

Cancelling from the right by s^2 leads to the formula (25) for $l+1$, and this completes the proof of (25) for all l . Choosing now $l = i$ gives the lemma. ■

LEMMA 14. *Let $k \geq 0$ and $i \geq 0$ be integers, let a be an element of A such that $\deg a < i - 1$, and set $\alpha = e(\tilde{\pi}a/T^{i-1})$. Then*

$$(26) \quad s_r^{k+i}x_0\sigma_\alpha(t) - s_r^{i+k}(\sigma_\alpha(t)^{p^r}) = a_m T^{ip^r} t^{2p^r q^k (q^i - 1) + mq^k} + \dots$$

and

$$(27) \quad s_r^i x_0 \sigma_\alpha s^k(t) - s_r^{i+k}(\sigma_\alpha(t)^{p^r}) = a_m T^{(k+i)p^r} t^{2p^r (q^{k+i} - 1) + m} + \dots,$$

where the dots stand for the terms of higher order.

Proof. It is a simple but busy calculation. Recall that $\varrho : A \rightarrow C\{\tau\}$ denotes the Carlitz module. For $l \in \mathbb{N}_0$, write

$$\varrho_{T^l} = \varrho(T^l) = \sum_{j=0}^l \varrho_{l,j} \tau^j,$$

where $\varrho_{l,j} \in A$. We have $\varrho_{ll} = 1$ and $\varrho_{l0} = T^l$. Using this notation, we have, for all $z \in \Omega$ and by setting $t := t(z)$,

$$(28) \quad s^l(t) = t(T^l z) = \frac{t^{q^l}}{f_{T^l}(t)},$$

where $f_{T^l}(t) := t^{q^l} \varrho_{T^l}(t^{-1}) = \sum_{j=0}^l \varrho_{l,j} t^{q^l - q^j}$. The formula (28) being true for all $z \in \Omega$, it gives rise to an identity in $C[[t]]$. Recalling next that $s_r^l(t^{p^r}) = (s^l(t))^{p^r}$, we also derive from (28) that

$$(29) \quad s_r^l(t) = \frac{t^{q^l}}{g_{T^l}(t)}, \quad \text{where} \quad g_{T^l}(t) = \sum_{j=0}^l \varrho_{l,j}^{p^r} t^{q^l - q^j}.$$

In order to prove (27), let us now compute the first non-zero term of the formal series $s_r^i x_0 \sigma_\alpha s^k(t) - s_r^{i+k}(\sigma_\alpha(t)^{p^r})$. From the equation (24) of Lemma 10 and since $\sigma_\alpha s^k(t) = t^{q^k} + \dots$, we first have

$$(30) \quad x_0 \sigma_\alpha s^k(t) = (\sigma_\alpha(s^k(t)))^{p^r} + a_m t^{mq^k} + \dots.$$

Next, for each j , $0 \leq j \leq i - 1$, we have

$$\begin{aligned} (x_0 \sigma_\alpha s^k(t))^{q^i - q^j} &= ((\sigma_\alpha s^k(t))^{p^r q^j} + a_m^{q^j} t^{mq^{k+j}} + \dots)^{q^i - q^j - 1} \\ &= (\sigma_\alpha s^k(t))^{p^r (q^i - q^j)} - a_m^{q^j} t^{p^r q^{i+k} + (m - 2p^r)q^{k+j}} + \dots. \end{aligned}$$

Hence we find, since $m - 2p^r > 0$,

$$g_{T^i}(x_0 \sigma_\alpha s^k(t)) = (f_{T^i}(\sigma_\alpha s^k(t)))^{p^r} - a_m T^{ip^r} t^{p^r q^{i+k} + (m - 2p^r)q^k} + \dots,$$

from which it easily follows that

$$\frac{1}{g_{T^i}(x_0 \sigma_\alpha s^k(t))} - \frac{1}{(f_{T^i}(\sigma_\alpha s^k(t)))^{p^r}} = a_m T^{ip^r} t^{p^r q^{i+k} + (m - 2p^r)q^k} + \dots.$$

Using now (29), we get

$$(31) \quad s_r^i x_0 \sigma_\alpha s^k(t) - \frac{(x_0 \sigma_\alpha s^k(t))^{q^i}}{(f_{T^i}(\sigma_\alpha s^k(t)))^{p^r}} = a_m T^{ip^r} t^{2p^r q^{i+k} + (m-2p^r)q^k} + \dots$$

Now, (30) yields

$$\begin{aligned} \frac{(x_0 \sigma_\alpha s^k(t))^{q^i}}{(f_{T^i}(\sigma_\alpha s^k(t)))^{p^r}} &= \left(\frac{(\sigma_\alpha s^k(t))^{q^i}}{f_{T^i}(\sigma_\alpha s^k(t))} \right)^{p^r} + a_m^{q^i} t^{mq^{i+k}} + \dots \\ &= (s^i \sigma_\alpha s^k(t))^{p^r} + a_m^{q^i} t^{mq^{i+k}} + \dots \end{aligned}$$

Combining this equality with (31) and since $m > 2p^r$, we get

$$(32) \quad s_r^i x_0 \sigma_\alpha s^k(t) - (s^i \sigma_\alpha s^k(t))^{p^r} = a_m T^{ip^r} t^{2p^r q^{i+k} + (m-2p^r)q^k} + \dots$$

Since we have $s^i \sigma_\alpha s^k = s^{i+k} = s^{i+k} \sigma_\alpha$ by Lemma 8(ii), (27) is proved.

To prove now (26), we note that the equality (32) above also holds for $k = 0$ and $i + k$ instead of i (same computations). Thus we have

$$s_r^{i+k} x_0 \sigma_\alpha - (s^{i+k}(\sigma_\alpha))^{p^r} = a_m T^{(i+k)p^r} t^{2p^r q^{i+k} + m - 2p^r} + \dots \quad \blacksquare$$

The proof of Proposition 7 is now straightforward.

Proof of Proposition 7. Suppose that $R(X) = 0$. We define $n = \deg_X P$ and $y_i, 0 \leq i \leq n$, as before. If two y_i 's were equal, say y_i and y_{i+k} with $k \geq 1$, then thanks to Lemma 13 there would exist an $a \in A$ with $\deg a < i - 1$ such that if we set $\alpha = e(\tilde{\pi}a/T^{i-1})$, then

$$s_r^i x_0 \sigma_\alpha s^k - s_r^{k+i} x_0 \sigma_\alpha = 0.$$

But this would contradict Lemma 14 since $a_m \neq 0$ and the exponents of t on the right-hand sides of (26) and (27) are distinct (because $m - 2p^r \neq 0$). Thus, the y_i 's are pairwise distinct. As they satisfy the equation $P(y_i, \hat{j} \circ s^n) = 0$, it follows that the polynomial $P(X, \hat{j} \circ s^n) \in C((t))[X]$ has at least $n + 1$ roots. But since this polynomial is non-zero of degree n (the \hat{j} function is transcendental over C , hence so is $\hat{j} \circ s^n$), this is impossible. Thus, $R(X) \neq 0$. \blacksquare

4. Proof of Theorem 2. The proof of Theorem 2 is similar to that of Theorem 1 (and in fact easier). But instead of arguing with the functions h and φ , it will be more convenient to work with the two functions $f(z) := h(Tz)$ and $\varphi(z)$. For these two functions we will prove the following result, from which Theorem 2 will easily follow:

PROPOSITION 15. *For every non-zero polynomial $P \in C[X, Y]$ and every integer $r \geq 0$,*

$$\text{ord}_0 P(\hat{f}^{p^r}(t), \hat{\varphi}(t)) \leq c_2' p^r \deg_X^+ P(p^r \deg_X P + \deg_Y P),$$

where $c_2' = q^2(q^2 + q)$.

Proof. First of all, we note that since $\hat{h}(t) = -t + \dots$, and since (see (6) and (7))

$$t(Tz) = \frac{t(z)^q}{1 + Tt(z)^{q-1}},$$

we have $\hat{f}(t) = -t^q + \dots$ and $\hat{\varphi}(t) = \hat{f}(t)/\hat{h}(t) = t^{q-1} + \dots$.

Let now $P \in C[X, Y]$ be a non-zero polynomial. As at the beginning of Section 3, in order to prove the proposition we may (and will) assume that P is irreducible. If $\deg_X P = 0$, then P has the form $P = a_1 Y + a_0$ with $a_1 \neq 0$, whence

$$\text{ord}_0 P(\hat{f}^{p^r}(t), \hat{\varphi}(t)) \leq q - 1.$$

Thus, the multiplicity estimate of Proposition 15 is true when $\deg_X P = 0$ with $c'_2 \geq q - 1$.

We assume from now on that $\deg_X P \geq 1$ and that Proposition 15 is true for all irreducible polynomials S with $\deg_X S < \deg_X P$. Let $r \geq 0$ be an integer. If $\deg_Y P = 0$, then we easily see, in the same way as before, that

$$\text{ord}_0 P(\hat{f}^{p^r}(t), \hat{\varphi}(t)) \leq qp^r,$$

so the inequality of Proposition 15 is true (with $c'_2 \geq q$). We will therefore assume in what follows that $\deg_Y P \geq 1$. We distinguish three cases.

First case: $\partial P / \partial X = 0$. In this case, we argue exactly as in the first case of Section 3.1 and we get the estimate of the proposition (recall that it is here that we need the induction hypothesis).

Second case: $\partial P / \partial X \neq 0$ and the following condition holds:

$$(33) \quad 2 \text{ord}_0 \frac{\partial P}{\partial X}(\hat{f}^{p^r}(t), \hat{\varphi}(t)) \geq \text{ord}_0 P(\hat{f}^{p^r}(t), \hat{\varphi}(t)) - qp^r.$$

In this case, consider the resultant $R = R(Y) = \text{res}_X(P, \partial P / \partial X) \in C[Y]$. As in Section 3.1 we have $R \neq 0$, and there exist two polynomials $U, V \in C[X, Y]$ such that $R = UP + V\partial P / \partial X$. Now, we trivially have

$$\text{ord}_0((UP)(\hat{f}^{p^r}(t), \hat{\varphi}(t))) \geq \text{ord}_0 P(\hat{f}^{p^r}(t), \hat{\varphi}(t))$$

and

$$\text{ord}_0 \left(\left(V \frac{\partial P}{\partial X} \right) (\hat{f}^{p^r}(t), \hat{\varphi}(t)) \right) \geq \text{ord}_0 \frac{\partial P}{\partial X}(\hat{f}^{p^r}(t), \hat{\varphi}(t)).$$

It follows from this, using the condition (33), that

$$(34) \quad \text{ord}_0 R(\hat{\varphi}(t)) \geq \frac{1}{2} \text{ord}_0 P(\hat{f}^{p^r}(t), \hat{\varphi}(t)) - \frac{1}{2} qp^r.$$

Now, since $R \neq 0$ and $\text{ord}_0 \hat{\varphi}(t) = q - 1$, it is easily seen that

$$\text{ord}_0 R(\hat{\varphi}(t)) \leq (q - 1) \deg R.$$

Combining this with (34) and using the fact that $\deg R \leq 2 \deg_X P \deg_Y P$, we get the estimate of the proposition (with e.g. $c'_2 \geq 4q - 4$).

Third case: $\partial P / \partial X \neq 0$ and the following condition holds:

$$(35) \quad 2 \operatorname{ord}_0 \frac{\partial P}{\partial X}(\hat{f}^{p^r}(t), \hat{\varphi}(t)) < \operatorname{ord}_0 P(\hat{f}^{p^r}(t), \hat{\varphi}(t)) - qp^r.$$

In this case, we will use the modular equation connecting the two functions $\varphi(z)$ and $\varphi(z/T)$. For $\lambda \in \mathbb{F}_q$ define $\psi_\lambda(z) := \varphi((z + \lambda)/T)$. We know (see e.g. [Bo 1, Lemma 5.1]) that there exists a polynomial $\Psi \in A[X, Y]$ such that

$$\Psi(X, \varphi) = \prod_{\lambda \in \mathbb{F}_q} (X - \psi_\lambda).$$

It follows in particular that every symmetrical polynomial in the functions ψ_λ is a polynomial in φ . Hence we can define Q as the polynomial $Q \in C[X, Y]$ such that

$$(36) \quad Q(X, \varphi) = \prod_{\lambda \in \mathbb{F}_q} \varphi^{p^r \deg_X P} P\left(\frac{X}{\varphi^{p^r}}, \psi_\lambda\right).$$

We clearly have

$$(37) \quad \deg_X Q = q \deg_X P.$$

In order to estimate $\deg_Y Q$, we introduce the elementary symmetrical functions $\sigma_1, \dots, \sigma_q$ of the ψ_λ 's. The right-hand side of (36) shows that each coefficient of the polynomial $Q(X, \varphi)$ (viewed as a polynomial in X) is a polynomial in φ and the σ_i 's, of degree at most $qp^r \deg_X P$ in φ and at most $q \deg_Y P$ in the σ_i 's (see e.g. [La, proof of Theorem 6.1 in Chapter IV]). But from [Bo 1, Lemma 5.1] we know that the σ_i 's are polynomials in φ of degree at most q . It follows that

$$(38) \quad \deg_Y Q \leq qp^r \deg_X P + q^2 \deg_Y P.$$

Next, we estimate $\operatorname{ord}_0 Q(\hat{f}^{q^r}(t), \hat{\varphi}(t))$ from below. Evaluating the formula (36) at Tz and then replacing X by $f(Tz)^{p^r}$, we get, for $|z|_i$ large,

$$(39) \quad Q(f(Tz)^{p^r}, \varphi(Tz)) = \varphi(Tz)^{qp^r \deg_X P} P(f(z)^{p^r}, \varphi(z)) \prod_{\lambda \in \mathbb{F}_q^*} g_\lambda(z),$$

where

$$g_\lambda(z) = P(f(z)^{p^r}, \varphi(z + \lambda/T)) \quad (\lambda \in \mathbb{F}_q^*).$$

Now, each function g_λ clearly has a t -expansion \hat{g}_λ for $|z|_i$ large with $\operatorname{ord}_0 \hat{g}_\lambda(t) \geq 0$. So (39) implies

$$\operatorname{ord}_0(Q(\hat{f}(t(Tz)))^{p^r}, \hat{\varphi}(t(Tz))) \geq \operatorname{ord}_0 P(\hat{f}(t)^{p^r}, \hat{\varphi}(t)),$$

and therefore

$$(40) \quad \text{ord}_0(Q(\hat{f}(t))^{p^r}, \hat{\varphi}(t)) \geq \frac{1}{q} \text{ord}_0 P(\hat{f}(t)^{p^r}, \hat{\varphi}(t)).$$

The end of the proof is now very similar to that of Theorem 1. Define $R(X) = \text{res}_Y(P, Q)$. There exist $U, V \in C[X, Y]$ such that $R = UP + VQ$. From this and (40) we deduce at once

$$(41) \quad \text{ord}_0 R(\hat{f}(t)^{p^r}) \geq \frac{1}{q} \text{ord}_0 P(\hat{f}(t)^{p^r}, \hat{\varphi}(t)).$$

Assume for a moment that we have shown that $R \neq 0$ (this will be done in Lemma 16 hereafter). Then, since $\text{ord}_0 \hat{f}(t) = q$, we have

$$\text{ord}_0 R(\hat{f}(t)^{p^r}) \leq qp^r \deg R \leq qp^r (\deg_X P \deg_Y Q + \deg_X Q \deg_Y P).$$

This last inequality together with (41), (37) and (38) give again the multiplicity estimate, as soon as $c'_2 \geq q^2(q^2 + q)$. Gathering all the cases, we see that Proposition 15 is true with $c'_2 = q^2(q^2 + q)$. ■

It remains to prove that the resultant just introduced above is not zero, which we state in the following lemma:

LEMMA 16. *Let $P \in C[X, Y]$ be an irreducible polynomial such that $\deg_Y P \geq 1$, $\partial P / \partial X \neq 0$ and the inequality (35) holds. Let $Q \in C[X, Y]$ be the polynomial defined by (36), and set $R(X) = \text{res}_Y(P, Q) \in C[X]$. Then $R(X) \neq 0$.*

Proof. Suppose that $R(X) = 0$. We want to derive a contradiction. We will argue as in Section 3.2, using Newton's approximation method (but the proof will fortunately be much easier). Here again, we will use the formal series $\sigma_\alpha \in C[[t]]$ and $s \in C[[t]]$ introduced in Section 3.2 (see (19) and (21)). We will also write $\mathfrak{K} = C((t))$.

We first show that there exists a sequence $(x_i)_{i \geq 0}$ of elements of \mathfrak{K} satisfying the following three conditions:

- (i) $x_0(t) = \hat{f}^{p^r}(t) + a_m t^m + \dots$, where $a_m \neq 0$ and $m > qp^r$ (the dots stand for terms of degree $> m$).
- (ii) $P(x_i(t), \hat{\varphi}(t)) = 0$ for all $i \geq 0$.
- (iii) For all $i \geq 1$, we have

$$x_i = \frac{x_{i-1} \circ s}{(\hat{\varphi} \circ s)^{p^r}}.$$

We construct the sequence (x_i) by induction. For $i = 0$ we only have to find x_0 satisfying (i) and (ii). To this end, we define $f(X) = P(X, \hat{\varphi}(t)) \in \mathfrak{D}[X]$, where $\mathfrak{D} = C[[t]]$, and we set $a_0 := \hat{f}^{p^r} \in \mathfrak{D}$. Arguing now as in the proof of Lemma 10, we apply Lemma 9 (Hensel's lemma) and we get the existence of $x_0 \in C[[t]]$ satisfying $P(x_0(t), \hat{\varphi}(t)) = 0$ and $\text{ord}_0(x_0 - \hat{f}^{p^r}) > qp^r$. Now, we claim that $x_0 \neq \hat{f}^{p^r}$. Indeed, otherwise the functions f and

φ would be algebraically dependent over C and thus, since $C(\varphi)$ is a finite extension of $C(j)$ (see e.g. [Bo1]), the two functions $h = f/\varphi$ and j would also be algebraically dependent over C . But this is a contradiction, since $j = -g^{q+1}/h^{q-1}$ and the functions g, h are algebraically independent over C ([Ge]). So, $x_0 \neq \hat{f}^{p^r}$ as claimed and thus (i) and (ii) hold.

Suppose now that we have already constructed x_i satisfying the conditions (ii) and (iii), where $i \geq 0$. Since $R(X) = 0$ we have $P \mid Q$, and thus (ii) implies

$$(42) \quad Q(x_i \circ s, \hat{\varphi} \circ s) = 0.$$

Using the formula (36) at the point Tz , and noticing that (for $|z|_i$ large) $\varphi(Tz) = \hat{\varphi}(s(t(z)))$ and, for every $\lambda \in \mathbb{F}_q$,

$$\psi_\lambda(Tz) = \varphi(z + \lambda/T) = \hat{\varphi}(t(z + \lambda/T)) = \hat{\varphi}(\sigma_{\alpha_\lambda}(t(z))) \quad \text{with } \alpha_\lambda = e(\tilde{\pi}\lambda/T),$$

we get the following equality (in the ring $\mathfrak{K}[X]$):

$$Q(X, \hat{\varphi} \circ s) = \prod_{\lambda \in \mathbb{F}_q} (\hat{\varphi} \circ s)^{p^r \deg_X P} P\left(\frac{X}{(\hat{\varphi} \circ s)^{p^r}}, \hat{\varphi} \circ \sigma_{\alpha_\lambda}\right).$$

It follows from this formula and from (42) that there is $\lambda \in \mathbb{F}_q$ such that

$$P\left(\frac{x_i \circ s}{(\hat{\varphi} \circ s)^{p^r}}, \hat{\varphi} \circ \sigma_{\alpha_\lambda}\right) = 0.$$

As $\sigma_{\alpha_\lambda} \circ \sigma_{-\alpha_\lambda} = t$, we see that if $x_{i+1} := (x_i \circ s \circ \sigma_{-\alpha_\lambda})/(\hat{\varphi} \circ s \circ \sigma_{-\alpha_\lambda})^{p^r}$, then $P(x_{i+1}, \hat{\varphi}) = 0$. Since by Lemma 8(ii) we have $s \circ \sigma_{-\alpha_\lambda} = s$, we have constructed x_{i+1} satisfying (ii) and (iii).

We now show that the x_i 's are pairwise distinct. First of all, a straightforward induction using (iii) and the fact that $\hat{\varphi} \circ s = (\hat{f} \circ s)/\hat{f}$ yields, for all $i \geq 0$,

$$(43) \quad x_i = \frac{x_0 \circ s^i}{\left(\frac{\hat{f} \circ s^i}{\hat{f}}\right)^{p^r}}.$$

Suppose that there exist $i \geq 0$ and $k \geq 1$ such that $x_i = x_{i+k}$. Then, by (43), we get ⁽³⁾

$$x_0 \circ s^{i+k} = \left(\frac{\hat{f} \circ s^{i+k}}{\hat{f} \circ s^i}\right)^{p^r} x_0 \circ s^i,$$

that is, cancelling from the right by s^i ,

$$(44) \quad x_0 \circ s^k = \left(\frac{\hat{f} \circ s^k}{\hat{f}}\right)^{p^r} x_0.$$

⁽³⁾ The right-hand side of this equality is the *product* of $\left(\frac{\hat{f} \circ s^{i+k}}{\hat{f} \circ s^i}\right)^{p^r}$ and $x_0 \circ s^i$, *not* the composition.

Now, by condition (i) we have $x_0/\hat{f}^{p^r} = 1 - a_m t^{m-qp^r} + \dots$, so

$$(45) \quad \left(\frac{\hat{f} \circ s^k}{\hat{f}} \right)^{p^r} x_0 = (\hat{f} \circ s^k)^{p^r} + a_m t^{m-qp^r+q^{k+1}p^r} + \dots$$

On the other hand, we have, using again (i),

$$(46) \quad x_0 \circ s^k = (\hat{f} \circ s^k)^{p^r} + a_m t^{mq^k} + \dots$$

We see that the exponents of the “ a_m terms” in (45) and (46) are not equal since $m > qp^r$. It follows that (44) cannot hold, and therefore the x_i ’s are pairwise distinct, as announced.

Since the x_i ’s are distinct and by condition (ii) above they are all roots of the polynomial $P(X, \hat{\varphi}) \in \mathfrak{K}[X]$, which is non-zero since $\hat{\varphi}$ is transcendental over C , we have the desired contradiction. Hence Lemma 16, and thus Proposition 15, is proved. ■

Proof of Theorem 2. Let $P \in C[X, Y]$ be a non-zero polynomial. Define $Q \in C[X, Y]$ by

$$Q(X, Y) = P(X/Y, Y)Y^{\deg_X P}.$$

We have $Q \neq 0$ and $Q(\hat{f}(t), \hat{\varphi}(t)) = \hat{\varphi}(t)^{\deg_X P} P(\hat{h}(t), \hat{\varphi}(t))$. Using now Proposition 15 with $r = 0$ (and with Q instead of P), together with the facts that $\deg_X Q = \deg_X P$, $\deg_Y Q \leq \deg_X P + \deg_Y P$ and $\text{ord}_0 \hat{\varphi}(t) = q - 1$, one readily obtains Theorem 2 with $c_2 = 2c'_2$. ■

5. Proofs of the corollaries. The proof of the corollaries is based on Lemma 17 below. To state it more easily, we introduce the following definition. Let $\mathfrak{K} = C((t))$. Given $\alpha, \beta \in \{0, 1\}$, we will say that a pair (F, G) of elements of \mathfrak{K} satisfies a multiplicity hypothesis of type (α, β) if there exists a real number $c = c(F, G) > 0$ such that, for every non-zero polynomial $P \in C[X, Y]$,

$$(47) \quad \text{ord}_0 P(F(t), G(t)) \leq c(\deg_X^+ P + \alpha \deg_Y^+ P)(\deg_Y^+ P + \beta \deg_X^+ P).$$

Thus, for example, by Theorem 1 the pair $(t, \hat{j}(t))$ satisfies a multiplicity hypothesis of type $(0, 0)$ (and also of type (α, β) for all $\alpha, \beta \in \{0, 1\}$), whereas in Corollary 5 the pair (\hat{f}_1, \hat{f}_2) satisfies a multiplicity hypothesis of type $(1, 1)$. With this terminology we can state:

LEMMA 17. *Let $F_0, G \in \mathfrak{K}$, and suppose that (F_0, G) satisfies a multiplicity hypothesis of type (α, β) . Let F be a non-constant element of \mathfrak{K} such that F_0 and F are algebraically dependent over C . Then (F, G) also satisfies a multiplicity hypothesis of type (α, β) .*

Proof. In the following proof, the symbol \ll means that the implied constant (is positive and) depends only on F_0, F and G . Let $A \in C[X, Y]$ be an irreducible polynomial such that $A(F_0, F) = 0$. Since (F_0, G) satisfies

a multiplicity hypothesis, F_0 is in particular transcendental over C and thus we have $\deg_Y A \geq 1$. Let now $P \in C[X, Y]$ be a non-zero polynomial. We want to prove that (47) holds, so we may clearly assume that P is irreducible. If $\deg_Y P = 0$, then P has the form $P = aX + b$ with $a, b \in C$, $a \neq 0$, and since F is non-constant, we immediately get $\text{ord}_0 P(F(t), G(t)) \ll \deg_X P$ as desired. Hence we assume from now on that $\deg_Y P \geq 1$. We introduce in this case a new indeterminate Z and consider the resultant $R(X, Z) = \text{res}_Y(P(Y, Z), A(X, Y))$. There exist two polynomials $U(X, Y, Z)$ and $V(X, Y, Z)$ such that $R(X, Z) = U(X, Y, Z)P(Y, Z) + V(X, Y, Z)A(X, Y)$, so we have in particular $R(F_0, G) = U(F_0, F, G)P(F, G)$. We now note that $\deg_X A$ and $\deg_Y A$ depend only on F_0 and F , so they are constants. Also, $\text{ord}_0 F_0(t)$, $\text{ord}_0 F(t)$ and $\text{ord}_0 G(t)$ are constants. From this we deduce first that $\deg_X U \ll \deg_X P$, $\deg_Z U \ll \deg_Y P$, $\deg_Y U \ll 1$, and next that $U(F_0, F, G)$ has a pole at zero of order at most

$$\ll \deg_X P + \deg_Y P \ll (\deg_X^+ P + \alpha \deg_Y^+ P)(\deg_Y^+ P + \beta \deg_X^+ P).$$

Hence

$$\begin{aligned} \text{ord}_0 P(F(t), G(t)) &\leq \text{ord}_0 R(F_0(t), G(t)) \\ &\quad + c'(\deg_X^+ P + \alpha \deg_Y^+ P)(\deg_Y^+ P + \beta \deg_X^+ P), \end{aligned}$$

where c' is a constant. Now, since $\deg_Z P(Y, Z) = \deg_Y P \geq 1$ and $\deg_Z A(X, Y) = 0$, we trivially have $P(Y, Z) \nmid A(X, Y)$. The polynomial $P(Y, Z)$ being irreducible in $C[X, Y, Z]$, it follows that $R(X, Z) \neq 0$ and thus using the hypothesis on (F_0, G) we have an inequality of the form (47) with F and P replaced by F_0 and R . Using $\deg_X R \ll \deg_X P$ and $\deg_Z R \ll \deg_Y P$, we finally obtain

$$\text{ord}_0 P(F(t), G(t)) \ll (\deg_X^+ P + \alpha \deg_Y^+ P)(\deg_Y^+ P + \beta \deg_X^+ P)$$

as required. ■

Proof of Corollary 3. We know that the field $C(\varphi)$ is a finite extension of the field $C(j)$ of degree $q + 1$ (see for instance [Bo 1]), so $j \in C(\varphi)$. Theorem 2 and Lemma 17 then immediately give Corollary 3. If we want now to compute explicitly a possible constant c_3 , we can proceed as follows. The explicit formula relating j and φ is computed in [Bo 1] and reads $j = B(\varphi)$ with

$$B(X) = -1/X + T^q + T^{q^2} X^{q-1} - T^{q^2+q} X^q.$$

Let $P \in C[X, Y]$, $P \neq 0$. Then, by setting $Q(X, Y) = Y^{\deg_Y P} P(X, B(Y))$ and noticing that $\text{ord}_0 \hat{\varphi}(t) = q - 1$, we obtain, using Theorem 2,

$$\begin{aligned} \text{ord}_0 P(\hat{h}(t), \hat{j}(t)) &= \text{ord}_0 Q(\hat{h}(t), \hat{\varphi}(t)) - (q - 1) \deg_Y P \\ &\leq c_2 \deg_X^+ Q(\deg_X Q + \deg_Y Q). \end{aligned}$$

Using now $\deg_X Q = \deg_X P$ and $\deg_Y Q \leq (q + 1) \deg_Y P$ we get the corollary with the explicit constant $c_3 = (q + 1)c_2$. ■

Proof of Corollary 4. Let k be the weight of f . Then f^{q+1}/h^k is a meromorphic modular function of weight 0 and type 0, so $f^{q+1}/h^k \in C(j)$. But since the function f^{q+1}/h^k has no poles in Ω (recall that h does not vanish on Ω), we have in fact $f^{q+1}/h^k \in C[j]$. Thus, we can write $f^{q+1}/h^k = B(j)$ for a certain (non-zero) $B \in C[X]$. Let now $P \in C[X, Y]$ be a non-zero polynomial. Then $P(\hat{f}(t)^{q+1}, \hat{j}(t)) = Q(\hat{h}(t), \hat{j}(t))$, where $Q(X, Y) = P(X^k B(Y), Y)$. Since k and B depend on f only, we have furthermore $\deg_X Q \ll \deg_X P$ and $\deg_Y Q \ll \deg_X P + \deg_Y P$, where the constant involved depends on f only. Corollary 3 yields $\text{ord}_0 P(\hat{f}(t)^{q+1}, \hat{j}(t)) \ll \deg_X P(\deg_X P + \deg_Y P)$. Thus, with the above terminology, (\hat{f}^{q+1}, \hat{j}) satisfies a multiplicity hypothesis of type $(0, 1)$. Applying now Lemma 17 yields the corollary. ■

Proof of Corollary 5. The proof is similar to the previous one. Let k_1 and k_2 be the weights of f_1 and f_2 , respectively. As in the proof of Corollary 4 there exist polynomials $A_1, A_2 \in C[X]$ such that $f_i^{q+1} = h^{k_i} A_i(j)$, $i = 1, 2$. Let $P \in C[X, Y]$ be a non-zero polynomial, and define $Q(X, Y) = P(X^{k_1} A_1(Y), X^{k_2} A_2(Y))$. Then $P(\hat{f}_1(t)^{q+1}, \hat{f}_2(t)^{q+1}) = Q(\hat{h}(t), \hat{j}(t))$, $Q \neq 0$ (because of the latter relation and the fact that $\hat{f}_1^{q+1}, \hat{f}_2^{q+1}$ are algebraically independent), $\deg_X Q \ll \deg_X P + \deg_Y P$ and $\deg_Y Q \ll \deg_X P + \deg_Y P$, where the implied constants do not depend on P . From this and Corollary 3 we derive that $(\hat{f}_1^{q+1}, \hat{f}_2^{q+1})$ satisfies a multiplicity hypothesis of type $(1, 1)$. Applying now Lemma 17 twice yields Corollary 5. ■

Acknowledgements. This paper was written when I was working at the Institute of Mathematics of Basel. It is a great pleasure for me to thank this institute for their hospitality, and in particular to thank David Masser for his support during all the years I spent within his group.

References

- [ADR] M. Ably, L. Denis et F. Recher, *Transcendance de l'invariant modulaire en caractéristique finie*, Math. Z. 231 (1999), 75–89.
- [Bo 1] V. Bosser, *Congruence properties of the coefficients of the Drinfeld modular invariant*, Manuscripta Math. 109 (2002), 289–307.
- [Bo 2] —, *Approximation measures for transcendental values of certain Drinfeld modular functions*, in progress.
- [Di] S. Dion, *Un théorème de transcendance en caractéristique finie*, J. Théor. Nombres Bordeaux 15 (2003), 57–82.
- [Ge] E.-U. Gekeler, *On the coefficients of Drinfeld modular forms*, Invent. Math. 93 (1988), 667–700.
- [La] S. Lang, *Algebra*, rev. 3rd ed., Grad. Texts in Math. 211, Springer, 2002.

- [Ne] Yu. V. Nesterenko, *Modular functions and transcendence questions*, Sb. Math. 187 (1996), 1319–1348.
- [Pe] F. Pellarin, *Les nilradicaux différentiels d'anneaux associés aux groupes triangulaires de Riemann–Schwarz*, Rend. Sem. Mat. Univ. Padova 114 (2005), 213–239.
- [Ph] G. Philibert, *Un lemme de zéros modulaire*, J. Number Theory 66 (1997), 306–313.

LMNO-UMR 6139
Université de Caen
Boulevard Maréchal Juin
BP 5186
14032 Caen Cedex, France
E-mail: bosser@math.unicaen.fr

Received on 7.5.2007

(5442)