GROUPE DE TRAVAIL
D'ANALYSE ULTRAMÉTRIQUE

ALFRED J. VAN DER POORTEN

Hadamard operations on rational functions

Groupe de travail d'analyse ultramétrique, tome 10, nº 1 (1982-1983), exp. nº 4, p. 1-11
<http://www.numdam.org/item?id=GAU_1982-1983__10_1_A3_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
10e année, 1982/83, n° 4, 11 p.

15 novembre 1982

HADAMARD OPERATIONS ON RATIONAL FUNCTIONS

by Alfred J. VAN DER POORTEN (*)

If $\sum_{h\geq 0} a_h X^h$, $\sum b_h X^h$ are rational functions then so is their Hadamard product $\sum c_h X^h$, $a_h b_h = c_h$, $h \geq 0$ and equally simply if f is a polynomial then also $\sum f(a_h) X^h$ is rational. In a talk at Budapest, in july 1981 [13], I announced, and at this séminaire I presented, purported proofs of best possible converse results in characteristic zero. Throughout, $\underset{\sim}{K}$ denotes a field of characteristic zero, and R is a finitely generated subring of $\underset{\sim}{K}$. In the algebraic case, when we suppose $\underset{\sim}{K}$ of degree d over $\underset{\sim}{Q}$, the ring R is then a ring of S-integers of $\underset{\sim}{K}$ with S some finite set of valuations of $\underset{\sim}{K}$ including all its archimedean valuations.

THEOREM A (Hadamard quotient theorem). - Suppose $\sum c_h X^h$, $\sum b_h X^h$ are Taylor expansions of functions rational over $\underset{\sim}{K}$ and that there is a sequence (a'_h) of elements of R so that $a'_h b_h = c_h$, $h \geq 0$. Then there is a rational function $\sum a_h X^h$ with $a_h b_h = c_h$, $h \geq 0$.

THEOREM B. - Suppose b is a possibly degenerate exponential polynomial and (a'_h) a sequence of elements of R so that $\sum b(a'_h) X^h$ is rational. Then there is a rational function $\sum a_h X^h$ with $b(a_h) = b(a'_h)$, $h \geq 0$. In particular, if b is a nondegenerate exponential polynomial and a an arbitrary permutation of $\underset{\sim}{N} = \{0 , 1 , 2 , 3 , \ldots \}$ then $\sum b_{a(h)} X^h$ rational implies there is an integer $d > 0$ so that for each r , $0 \leq r < d$, the function $a(hd + r)$ is linear in h for all sufficiently large h .

In 1979, POURCHET [8], outlined a proof of theorem A. It seems fair to remark that [8] was generally viewed as consisting entirely of wellknown or evident propositions that did not appear to contribute materially to a proof of theorem A. I shared this view, vide [13], until the writing of the present report (april 1983). Though it may have taken me some years to decipher Pourchet's intent, and though my proof arose more or less independently, the proof below precisely follows the programme proposed in [8]. Just as it is improper to claim that a sequence of uninterpretable hints contitutes a proof, so it is immoral to suggest that a proof acting upon such hints is independent. I do not suggest this. The proof below is, d'après POURCHET,

(*) Alfred J. VAN DER POORTEN, School of Mathematics and Physics, Macquarie University NORTH RYDE, NSW 2113 (Australie).

I do not provide a proof of theorem B but restrict myself to the improper expedient of giving some easily understandable hints.

1. Rappels.

If $\sum_{h\geq 0} a_h X^h = r(X)/s(X)$ with r , s polynomials then we may set over $\underset{\sim}{K}$:

$$s(X) = 1 - \sum_{j=1}^{n} s_j X_j = \prod_{i=1}^{m} (1 - \alpha_i X)^{n(i)} , \quad s_n \neq 0 .$$

From a partial fraction expansion we then obtain

$$a_h = \sum_{i=1}^{m} \sum_{k=1}^{n(i)} A_{ik} \binom{h + k - 1}{k - 1} \alpha_i^h = \sum A_i(h) \alpha_i^h ,$$

with the A_i in $\underset{\sim}{K}[X]$ and $\deg A_i = n_i - 1$. Thus the a_h are generalised power sums or equivalently are given by an exponential polynomial a evaluated at the non-negative integers. The distinct quantities $\alpha_1 , \dots , \alpha_m$ are the characteristic roots of the exponential polynomial a ; each appears with multiplicity, respectively n_i . We also have a linear homogeneous recurrence relation

$$a_{h+n} = s_1 a_{h+n-1} + \dots + s_n a_h .$$

So (a_h) is a so-called recurrence sequence of order n . Its initial values $a_0 , a_1 , \dots , a_{n-1} , \dots$ are determined by the numerator $r(X)$. If $\deg r(X) = r \geq n$ then the exponential polynomial and the recurrence relation, yields a_h only for $h > r - n$.

To verify the rationality of $\sum a_h X^h$ one studies the Kronecker-Hankel determinants of the sequence (a_h) :

$$K_h a = |a_{i+j}|_{0\leq i, j\leq r} .$$

It is immediate that with (a_h) a recurrence sequence as above one has $K_h a = 0$ for $h \geq \max(r + 1 , n)$. The converse is true but some traditional proofs, for example [7] (chap. 3, p. 85-99), seem to me to be unnecessarily clever. Certainly a straight forward induction as given by SALEM [11], suffices and makes it easy to see more. For example, if $K_h a = 0$ for $H_0 \leq h \leq H$ then there is a recurrence sequence (a'_h) of order $H'_0 \leq H_0$ so that $a_h = a'_h$ for at least $H_0 - H'_0 \leq h \leq H + H_0$.

How might we go about showing that $K_h a = 0$? In the first instance, we will want to suppose that the field of definition of the roots and coefficients of the generalised power sum a_h is an algebraic number field $\underset{\sim}{K}$ of degree d over $\underset{\sim}{Q}$. Given a sequence (a_h) of elements of $\underset{\sim}{K}$, we write

$$d \log \sigma_h a = \sum_{\nu} \max_{0\leq k\leq h} \log |a_k|_{\nu}$$

and we then say that the sequence (a_h) has size at most ρ if

$$\lim\sup (\sigma_h\, a)^{1/h} \leq \rho .$$

Here the sum is over the usually normalised valuations ν of $\underset{\sim}{K}$: thus for $0 \neq x \in \underset{\sim}{K}$ one has the product formula $\sum_\nu \log |x|_\nu = 0$ and if y is an integer of $\underset{\sim}{K}$ the constant sequence $(y\ ,\ y\ ,\ \dots)$ has size $|N_y|^{1/d}$, where N is the norm from $\underset{\sim}{K}$ to $\underset{\sim}{Q}$. Since early values do not affect the size of (a_h) nor the rationality of $\sum a_h X^h$ we may if we wish always suppose $a_0 = 1$. A recurrence sequence certainly has finite size ; conversely a power series $\sum a_h X^h$, with (a_h) of finite size, is called a G-function (see BOMBIERI [1]).

Now turn to the sequence (K_h) of Kronecker determinants $K_h\, a$ of the sequence (a_h) .

Let T be a finite set of valuations of $\underset{\sim}{K}$. By the product formula : $K_h = 0$ or $\sum_\nu \log |K_h|_\nu = 0$ so

$$- \sum_{\nu \in T} \log |K_h|_\nu \leq \sum_\nu \max_{0 \leq k \leq h} |K_h|_\nu .$$

But a simple estimate yields

$$\sigma_h\, K \leq (h+1)!\, (\sigma_h\, a)^{h+1} .$$

Hence if

$$\prod_{\nu \in T} |K_h|_\nu^{-1/h^2} > \rho^d$$

for certain sufficiently large h then $K_h = 0$ for such h .

2. p-adification and specialisation

It is wellknown, and elegantly described by CASSELS [4], that any finitely generated field $\underset{\sim}{K}$ may be embedded in infinitely many fields $\underset{\sim}{Q}_p$ of p-adic rationals in such a way that any nominated finite set of nonzero elements of $\underset{\sim}{K}$ is mapped onto a set of p-adic units. The account in [4] is such that one sees that stopping partway yields a homomorphism of a finitely generated subring R of $\underset{\sim}{K}$ into an algebraic number field, say of degree d over $\underset{\sim}{Q}$; this latter mapping, which we call specialisation is such that any nominated finite set of nonzero elements of $\underset{\sim}{K}$ may be supposed to have been specialised to nonzero elements of the algebraic number field. For some details see the account in [14]. Though the point is not explicitly made in [4] it is clear that the density of the good, or regular primes that is those primes p for which one obtains an appropriate embedding of $\underset{\sim}{K}$ into $\underset{\sim}{Q}_p$, is $1/d$; for example note [5] (p. 78 and p. 163). More precisely,

$$\prod_{p \leq x} p^{1/p-1} = O(x^{1/d}) , \quad x \longrightarrow \infty$$

where the product is over regular primes only.

We apply these notions as follows : Given an exponential polynomial d over $\underset{\sim}{K}$

$$d(h) = \sum D_i(h)\ \delta_i^h$$

we may deem d to be defined over $\underset{\sim}{Q}_p$, p regular with respect to d , so that the roots δ_i be units of $\underset{\sim}{Q}_p$, so that no nonzero coefficient of the D_i vanishes as element of $\underset{\sim}{Q}_p$, and so that at most finitely many $d(h)$ not already zero in $\underset{\sim}{K}$ become zero as elements of $\underset{\sim}{Q}_p$. Only the last condition requires comment ; I refer the reader to the survey commencing [6] and to remarks of CANTOR [3]. In much the same way the exponential polynomial may be supposed to be defined over an algebraic number field without the sensible specialisation introducing any degeneracies.

Now consider the $p - 1$ p-adic power series

$$d(t(p-1)+r) = \sum D_i(t(p-1)+r)\ \delta_i^r \exp(t \log \delta_i^{p-1})\ , \quad 0 \leqslant r < p-1\ .$$

Because the δ_i are units of $\underset{\sim}{Q}_p$ we have

$$|\delta_i^{p-1} - 1|_p \leqslant p^{-1}$$

so the maps

$$h \longmapsto \delta^{h(p-1)+r}\ , \quad 0 \leqslant r < p-1$$

each continue to p-adic power series $\delta_i^r \exp(t \log \delta^{p-1})$ converging for t in $\underset{\sim}{C}_p$, the completion of an algebraic closure of $\underset{\sim}{Q}_p$, with $\mathrm{ord}_p\ t > -1 + 1/(p-1)$. To avoid irritating exponents I write

$$|t|_p = p^{-\mathrm{ord}_p t}\ .$$

I will refer to the cited series $d(t(p-1)+r)$ as sensible p-adifications of the exponential polynomial d .

We p-adify so as to be able to use the following result : Let $g(t) = \sum x_h t^h$ be a p-adic power series converging for t with $\mathrm{ord}_p\ t > -s + 1/(p-1)$, some $s \geqslant 0$. To account for the convergence we must have

$$\liminf h^{-1} \mathrm{ord}_p\ x_h \geqslant s - 1/(p-1)\ .$$

Now denote by Δ the operator defined by $\Delta f(t) = f(t+1) - f(t)$. Then for $k = 0\ ,\ 1\ ,\ 2\ ,\ \dots\ ,$

$$\mathrm{ord}_p\ \Delta^k g(t) = \mathrm{ord}_p \sum_{h\geqslant 0} x_h\ \Delta^k\ t^h \geqslant \min_{h\geqslant 0} \mathrm{ord}_p\ x_h + \mathrm{ord}_o\ \Delta^k\ t^h\ .$$

But $\Delta^k t^h$ is a polynomial in t of degree $h - k$ and with integer coefficients each divisible by $k!$. Hence if ℓ is an integer then $\Delta^k\ t^h\,|_{t=\ell}$ vanishes for $h < k$ and is always divisible by $k!$. Thus

$$\operatorname{ord}_p \Delta^k g(t) \,|_{t=\ell} \geqslant \min_{h\geqslant k} \operatorname{ord}_p x_h + \operatorname{ord}_p k!$$

which is to say that

$$\liminf k^{-1} \operatorname{ord}_p \Delta^k g(t) \,|_{t=\ell} \geqslant s \ .$$

3. Proof of the Hadamard quotient theorem : old ideas.

We now proceed to a proof of theorem A in apparently special circumstances. Thus, we suppose that $b_h \neq 0$, $h \geqslant 0$. Next, we suppose that the quotient sequence (a_h) , where $a_h b_h = c_h$, $h \geqslant 0$ is a sequence of elements of an algebraic number field $\underset{\sim}{K}$ of degree d over $\underset{\sim}{Q}$ and that the sequence has finite size at most ρ . We denote by n the order of the exponential polynomial b .

In the immediate sequel, p denotes one of finitely many rational primes greater than n with respect to which we may sensibly p-adify both b and c . We consider a typical quotient

$$a(t(p-1)+r) = c(t(p-1)+r)/b(t(p-1)+r) \ , \quad 0 \leqslant r < p-1$$

of p-adic exponential polynomials.

It is known [10] that each $b(t(p-1)+r)$ has at most n zeros in the disc $\{t : \operatorname{ord}_p t > -1 + n/(p-1)\}$. We recall that these zeros lie on the so-called critical circles on which at least two terms of the power series $b(t(p-1)+r)$ share minimal p-adic order ; these critical terms cannot be of degree greater than n . Since $b(t(p-1)+r)$ has coefficients in $\underset{\sim}{Q}_p$ it follows that any of its zeros t_0 outside the unit disc must satisfy $\operatorname{ord}_p t_0 \leqslant -1/n$. Hence for each p and r , $0 \leqslant r < p-1$, there is a polynomial $f_{p,r}$ in $\underset{\sim}{Z}_p[t]$ of degree at most n so that the power series

$$f_{p,r}(t(p-1)+r)\, a(t(p-1)+r)$$

converges for t with $\operatorname{ord}_p t > -1/n$. I should remark that much sharper facts hold : but we only need $f_{p,r}$ in $\underset{\sim}{Z}_p[t]$ and convergence beyond the unit disc to an extent independent of p .

Now denote by F_p a polynomial in $\underset{\sim}{Z}_p[t]$ divisible in that ring by each of the $f_{p,r}$. Then for each r , $0 \leqslant r < p-1$, we have

$$\liminf k^{-1} \operatorname{ord}_p \Delta^k F_p(t(p-1)+r)\, a(t(p-1)+r) \,|_{t=0} \geqslant 1/n + 1/(p-1) \ .$$

Consider the $(h+1) \times (h+1)$ determinant

$$K_h = |F_p(i+j)\, a(i+j)|_{0\leqslant i,j\leqslant h} \ ,$$

noting that simple row and column manipulation yields

$$K_h = \left| \Delta^k F_p(t(p-1)+r)\ a(t(p-1)+r)\Big|_{t=0} \right|_{0\leqslant i,j\leqslant h,\, i+j=k(p-1)+r} .$$

It is not difficult to deduce that as $h \longrightarrow \infty$

$$\liminf h^{-2} \operatorname{ord}_p K_h \geqslant (1/n + 1/(p-1))/(p-1) .$$

So we see that for h sufficiently large :

$$h^{-2} \operatorname{ord}_p K_h > 1/n(p-1) .$$

Now if we were lucky enough to have each F_p with rational integer coefficients then the remarks above would readily lead to a proof of theorem A. For we would lose no generality in supposing F_p independent of p, we would have archimedean information

$$\limsup h^{-2} \log \sigma_h K \leqslant d \log \rho$$

on the one hand, whilst on the other hand we could combine the pieces of p-adic data. Provided only that

$$\sum \frac{\log p}{p-1} > nd \log \rho$$

we would have $K_h = 0$ for all sufficiently large h, whence $\sum F(h)\, a_h X^h$ would have been proved rational. But then a result of POLYA-CANTOR [2] yields the rationality of $\sum a_h X^h$.

Unfortunately it would beg the question to suppose that F_p belongs to $\mathbb{Z}[t]$.

Nevertheless, as we see below, we can arrange a sufficiently good approximation to this state of affairs.

4. Proof of the Hadamard quotient theorem : new ideas.

To obtain the result that for h sufficiently large, say $h \geqslant H_0$, we have

$$\operatorname{ord}_p K_h(F_p\ a) > \frac{h^2}{n(p-1)} ,$$

we use only that

$$\operatorname{ord}_p \Delta^k F_p(t(p-1)+r)\ a(t(p-1)+r)\ \Big|_{t=0} \geqslant k\left(\frac{1}{n} + \frac{1}{p-1}\right)/(p-1)$$

with $k(p-1)+r \leqslant 2h$. Thus if we were to truncate the coefficients of the F_p modulo

$$M(p\ ;\ H) = p^{2H((1/n)+(1/(p-1)))^2} ,$$

we would retain the inequalities above for $H_0 \leqslant h \leqslant H$ but with the F_p now elements of $\mathbb{Z}[X]$ with coefficients not exceeding $M(p\ ;\ H)$. By the Chinese remainder theorem, we may construct a polynomial f in $\mathbb{Z}[X]$ with coefficients not exceeding

$$M := M(H) = \prod_{p \in P} M(p\ ;\ H)$$

so that f plays the role of f_p each $p \in P$, P being the set of primes with which we are dealing. The degree of f is at most

$$\max_{p \in P} n(p-1)$$

indeed we can avoid the some what clumsy and naïve notion of truncation by describing f as being so constructed as to satisfy

$$\|f - F_p\|_p \leqslant M(p\ ,\ H)^{-1}\ , \quad p \in P$$

here $\|\ \|_p$ is the maximum of the valuations of the coefficients and for the existence of f we appeal to the approximation theorem rather than the equivalent Chinese remainder theorem.

But the polynomial f may be replaced by any multiple $F = f_0\ f$, where f_0 is some nonzero element of $\mathbb{Z}[X]$. To see this we need only notice that each F_p may replaced by a multiple $f_0\ F_p$ since, in the first instance each F_p was described as divisible by a given polynomial. Then we have F such that

$$\|F - f_0\ F_p\|_p \leqslant M(p\ ,\ H)^{-1}\ ,$$

we shall choose f_0 to have degree $N = c_1\ H^{1/2}\ (\log H)^{-1/2}$. Here and in the immediate sequel $c_0\ , c_1\ , \dots$ denote positive constants and H is supposed large relative to the parameters n and $p \in P$. Modulo M there are some M^N possibilities for f_0 and, using foresight, we wish $F = f_0\ f$ to have coefficients no larger in alsolute value than $M^{c_0/N}$, modulo M of course. In applying the box principle, we see that if each "pigeonhole" contains polynomials F with coefficients difering modulo M by no more than $M^{c_0/N}$ then with c_0 appropriately large (but not depending on H) there are fewer than M^N pigeonholes required ([1]). Hence our construction succeeds and we have

$$\operatorname{ord}_p K_h(Fa) > h^2/n(p-1) \quad H_0 \leqslant h \leqslant H\ , \quad p \in P$$

with F of degree $cH^{1/2}\ (\log H)^{-1/2}$ and with coefficients not exceeding $M^{c_0/N}$ in absolute value. A priori H_0 needs only be large enough to validate the p-adic inequalities. Since we may choose H as large as we wish it certainly suffices to set $H_0 = H^{1/2} \log H$.

([1]) Because the coefficients of the polynomial multipliers are congruent modulo $M(p\ ,\ H)$ to $f_0\ F_p$, therefore

$$(*) \quad \operatorname{ord}_p \Delta^k F(.\ (p-1)+1)\ a(.\ (p-1)+1) \geqslant k\left(\frac{1}{n} + \frac{1}{p-1}\right)\frac{1}{p-1} > \frac{k}{n(p-1)}$$

with $k(p-1)+1 \leqslant 2H$ (and k large enough) and then

$$\operatorname{ord}_p K_h(Fa) > \frac{k^2}{n(p-1)} \quad \text{for} \quad H_0 < h < H$$

It now follows that for $H_0 \leq h \leq H$ we have the upper bound

$$\log \sigma_h(K(Fa)) < h^2 \, d \log \rho + d \, c_2 \, h \, H^{1/2} (\log H)^{1/2} .$$

Given the p-adic inequalities and our remarks in section 1 we see that $K_h(Fa) = 0$ for $H^{1/2} \log H \leq h \leq H$ if

$$\sum_{p \in P} \frac{\log p}{n(p-1)} > d \log \rho + d \, c_2 \, h^{-1} H^{1/2} (\log H)^{1/2} .$$

Plainly, if H is large enough then the second term on the right is arbitrarily small. On the other hand, as remarked in section 2, the sum

$$\sum_{p \in P} \frac{\log p}{n(p-1)}$$

may be chosen arbitrarily large whence indeed we obtain $K_h(Fa) = 0$ for $H^{1/2} \log H \leq h \leq H$.

But this implies that there is a recurrence sequence (d_h) of order at most $H^{1/2} \log H$ so that

$$d_h = F(h) \, a_h = F(h) \, c_h / b_h \quad \text{for} \quad H^{1/2} \log H \leq h \leq H .$$

But then the recurrence sequence $(b_h \, d_h - F(h) \, c_h)$ vanishes over a range considerably larger than is its order. Hence the recurrence vanishes identically and we have, for all $h \geq 0$,

$$b_h \, d_h = F(h) \, c_h .$$

It follows that the polynomial F divides the exponential polynomial bd in the ring of exponential polynomials. But by the Polya-Cantor lemma [3] we may suppose b contains no polynomial factor. For such a factor must also divide c and we may suppose therefore that this common factor of c and b has already been removed. It follows then that F must divide d in the ring of exponential polynomials whence indeed, by [3] once again, we see that (a_h) is a recurrence sequence, exactly as we wished so show.

5. Comments.

In attempting to fill the gags and repair the errors that riddled my earlier alleged proofs of theorem A I came to the eventual view that the methods I was trying to use could not possibly prove the Polya-Cantor lemma. Accordingly, I asked myself how I could use that result en route to a proof of theorem A. At this point I had the idea of appropriately truncating elements of $\underset{\sim}{Z}_p$ so as to abtain polynomials with integer coefficients. Eventually it became obvious that I had only uncovered the details of the proof sketched by POURCHET [8].

I want to acknowledge the patience and care of those particularly J.-P. BEZIVIN

and Philippe ROBBA, who prevented me from perpetuating the errors to which I allude above.

It is quite plain that the ideas in section 4 coincide with those intended in [8]. One sees this most clearly by noting that the somewhat eccentric detail given in the otherwise wellknown propositions of [8] is exactly the kind of detail I use above. For example, one does need an estimate on the order of the exponential polynomial $Fc - bd$ in order to then be able to conclude that it vanishes identically. POURCHET, as I do, glides over the fact that strictly speaking one needs a factorisation theory in the ring of exponential polynomials in order to deduce that F divides d ; if required this theory is provided by RITT [9]. See also remarks in my survey with TIJDEMAN [12]. It seems that my choice of a very large degree for F saves me from requiring some of the detail considered relevant in [8].

6. Further details of the proof of theorem A.

We have assumed that the sequence (a_h) has finite size. In fact, suppose that initially we sensibly specialised the exponential polynomials c and b. Then by the hypothesis of theorem A the a_h are S-integers of the algebraic number field $\underset{\sim}{K}$. Hence

$$d \log \sigma_h a = \sum_\nu \max_{0\leqslant k\leqslant h} (\log |c_k|_\nu - \log |b_k|_\nu)$$

$$\leqslant d \log \sigma_h c + \sum_{\nu\in S} \max_{0\leqslant k\leqslant h} |\log |b_k|_\nu| ,$$

and the latter sum is bounded by $d|S| \log \sigma_h b$ where $|S|$ is the number of valuations in S . Thus because $|S|$ is finite it follows that every sensible specialisation of the sequence (a_h) has finite size.

We can only have proved that every sensible specialisation of $\sum a_h X^h$ is a rational function. Suppose that, in fact, a is an exponential polynomial. Thus we have $c(h) = a(h)\, b(h)$ in the ring of generalised power sums. Then after multiplying by some appropriate $\gamma^h = \alpha^h \beta^h$ we can suppose the characteristic roots of each of the sums to have so normalised as to validate the following result of RITT [9] : there is a positive integer u so that each β_i^u is a monomial

$$\gamma_1^{u(1i)}, \ldots, \gamma_m^{u(mi)}$$

in the roots γ_j of c , with the u_{ji} integers satisfying $0 \leqslant u_{ji} \leqslant u$. The same holds for the roots α_i of the divisor a .

Since b is given we are given u and thus we have an a priori bound on the number of roots of the putative divisor a ; it is then easy to obtain such a bound M , say, on the order of a . Thus $\sum a_h X^h$ is rational if, and only if, its Kronecker determinants $K_h a$ vanish for $h \geqslant M$. But we may control our specialisation so that a specialisation of K_M vanishes if, and only if, $K_M = 0$.

Thus if every sensible specialisation of $\sum a_h X^h$ is rational then indeed the original Hadamard quotient is rational.

It remains to deal with the possibility that some b_h vanish by the theorem of LECH-MAHLER, for references see [6], the set of h for which $b_h = 0$ consists of finitely many isolated points and finitely many complete arithmetic progressions $(hd + r)$ some $d > 0$ and certain r, $0 \leqslant r < d$. If must needs be replace (b_h) by the sequences (b_{hd+r}) disregarding those that vanish identically. Change notation so that each surviving sequence is called (b_h). Now $b_h = 0$ for at most finitely many h so after a translation we lose no generality in supposing $b_h \neq 0$ for $h \geqslant 0$. Eventually any missing a_h are given by evaluating the discovered exponential polynomial $a(h)$ at h in $\underset{\sim}{Z}$. As for the missing arithmetic progressions, those a_{hd+r} may be selected arbitrarily provided only that each $\sum a_{hd+r} X^h$ be rational, $0 \leqslant r < d$.

7. Some remarks on theorem B.

The alleged result asserts that given exponential polynomials b, c and a sequence (a'_h) so that the a'_h might possibly be the values of an exponential polynomial a' evaluated at h, then there is indeed an exponential polynomial a so that identically $b \circ a = c$. Given this viewpoint it seems reasonable to make simple transformations and translations in order to be able to study p-adic exponential polynomials b and c, thus a sensible p-adification, in the expectation of being able to demonstrate that the p-adic power series $a = b^{-1} \circ c$ converge beyond the unit disc. When b is given as a nondegenerate exponential polynomial growth considerations [14] imply that a is piecewise linear. In effect, the only other case is b a polynomial.

Though theorem B is known in some special cases, my earlier attempts to provide a detailed proof led me into sinful error. Accordingly, I mention the result here only because it was the belief that I could deal with it that led me to believe that I could handle theorem A. The reader may properly heat theorem B as a conjecture. I claim only that I kind of think that I sort of know how to perhaps attack the question with possible success ; I could easily be wrong.

REFERENCES

[1] BOMBIERI (E.). - On G-functions, Recent progress in analytic number theory, Edited by H. Halberstam and C. Hooley. Vol. 2, n° 24, p. 1-67. - London, New York, Toronto [etc.], Academic Press, 1981.

[2] CANTOR (D. G.). - On arithmetic properties of the Taylor series of rational functions, Canadian J. of Math., t. 21, 1969, p. 378-382.

[3] CANTOR (D. G.). - On arithmetic properties of the Taylor series of rational functions, II, Pacific J. of Math., t. 41, 1972, p. 329-334.

[4] CASSELS (J. W. S.). - An embedding theorem for fields, Bull. Austral. math. Soc., t. 14, 1976, p. 193-198 ; Addendum : ibid t. 14, 1976, p. 479-480.

[5] GOLDSTEIN (L. J.). - Analytic number theory. - Englewood Cliffs, Prentice Hall, 1971.

[6] LOXTON (J. H.) and VAN DER POORTEN (A. J.). - On the growth of recurrence sequences, Proc. Cambridge phil. Soc., t. 81, 1977, p. 369-376.

[7] PARENT (D. P.). - Exercices de théorie des nombres. - Paris, Gauthier-Villars, 1978 (Collection μ_B).

[8] POURCHET (Y.). - Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles, C. R. Acad. Sc. Paris, t. 288, 1979, série A, p. 1055-1057.

[9] RITT (J. F.). - A factorisation theory for functions $\sum_{i=1}^{n} a_i\, e^{\alpha_i X}$, Trans. Amer. math. Soc., t. 29, 1927, p. 584-596.

[10] ROBBA (Philippe). - Nombre de zéros des fonctions exponentielles - Polynômes, d'après A. J. Van Der Poorten, Groupe d'étude d'Analyse ultramétrique, 4e année, 1976/77, n° 9, 3 p.

[11] SALEM (R.). - Algebraic numbers and Fourier analysis. - Boston (D. C.) Heath and company, 1963 (Heath mathematical Monographs).

[12] VAN DER POORTEN (A. J.) and TIJDEMAN (R.). - On common zeros of exponential polynomials, Enseignement mathématiques, Genève, t. 21, 1975, p. 57-67.

[13] VAN DER POORTEN (A. J.). - Some topics of recurrent interest, Colloquium in number theory [Budapest, 1981], Macquarie University Mathematical Report 81-0037 (à paraître dans les Colloquia mathematica Societatis Janos Bolyai).

[14] VAN DER POORTEN (A. J.) and SCHLICKEWEI (H. P.). - The growth conditions for recurrence sequences (à paraître).