SOME FACTS THAT SHOULD BE BETTER KNOWN, ESPECIALLY ABOUT RATIONAL FUNCTIONS

dedicated to the memory of Kurt Mahler

A. J. van der Poorten*
School of Mathematics, Physics, Computing and Electronics
Macquarie University
NSW 2109
Australia

ABSTRACT. Recurrence sequences, the sequences satisfying linear homogeneous recurrence relations with constant coefficients, are popular amongst professionals and amateurs alike. Yet it is peculiarly difficult to find congenial summaries of well known basic facts, whilst recent deep results remain hidden in the technical literature. The present note seeks to remedy that situation. Of course, it emphasises those aspects of special interest to the author and to maintain the class of this article it views recurrence sequences in their manifestation as the sequence of Taylor coefficients of a rational function.

The following remarks include those I made in a talk at the Study Institute. But much of what I write is influenced by informal conversations at the meeting and by my being reminded, all too frequently, that the well known is often not generally known, let alone known well.

1. Algebraic and 'Possibly Rational' Power Series

1.1 Let $\sum a_h X^h$ be a formal power series over a field $\mathbf{F} = \mathrm{Q}(a_0, a_1, a_2 \ldots)$ of characteristic zero representing a function algebraic over the field of rational functions $\mathbf{F}(X)$. Fairly little is known about the sequence (a_h) of Taylor coefficients of such algebraic power series but the following is plain (*cf* Mahler [39], 45–46): The field $\mathbf{F}$ is finitely generated over the field of rationals Q and indeed, the a_h all belong to a subring R of $\mathbf{F}$ finitely generated (of finite type) over Z. This says, exactly: There is a finite number, say t, of algebraically independent transcendentals $x = (x_1, \ldots, x_t)$ and a y algebraic over $\mathrm{Q}(x)$ so that $\mathbf{F} = \mathrm{Q}(x)[y]$. Further, for $j = 1, 2, \ldots, g$, say, there are polynomials $U_j \in \mathrm{Z}[y; x]$ and $V_j \in \mathrm{Z}[x]$ so that R is the ring $\mathrm{Z}[U_1(y; x)/V_1(x), \ldots, U_g(y; x)/V_g(x)]$. In the case $t = 0$ we have $\mathbf{F} = \mathbf{K}$, an algebraic number field, and R a subring (usually referred to as a ring of S-integers) in that field.

1.2 Of course if $\sum a_h X^h$ represents a rational function, then *a fortiori* the sequence (a_h) of its Taylor coefficients has the above properties. The conditions just stated are those minimally necessary in order that $\sum a_h X^h$ might possibly be rational. In the sequel we

* Work partially supported by the Australian Research Council.

mention various theorems and conjectures concerning circumstances in which possibly rational series are indeed rational. An additional observation may be useful: As is evident in the number field case, the condition on the ring R, namely that it be of finite type, is such that we may describe it as a ring of (generalised) integers of $\mathbf{F}$. With that in mind, below we speak of having an 'integrality condition' on the coefficients a_h when the series $\sum a_h X^h$ is possibly rational. This terminology also emphasises that the notion 'possibly rational' is an arithmetic condition (from which we will draw analytic consequences). Moreover it is congenial, and loses rather little generality (see our remarks on "heights", at 4.1 below), to think of the a_h as actual rational integers. We may speak that way, whilst always intending the generality detailed above.

1.3 Though a digression, it would be wrong not to mention further properties possessed by the sequence (a_h) of Taylor coefficients of an algebraic function: We have Eisenstein's theorem which, in the number field case, asserts that there is a rational integer d, say, so that the sequence $(d^h a_h)$ is a sequence of algebraic integers. In general, we have a monomial $V(x)$ in the $V_j(x)$ so that the sequence $(V^h a_h)$ is a sequence of elements of $\mathbf{Z}[y;x]$. Note that this is stronger than the notion "possibly rational" stated above because that notion says only that there is a sequence of integers (n_h) so that the $V^{n_h} a_h$ belong to $\mathbf{Z}[y;x]$.

1.4 Finally, there is the following less well known fact: I suppose, for convenience, that the a_h belong to $\mathbf{Q}$. By Eisenstein's theorem we may reduce modulo p^s for all but finitely many rational primes p and for all positive integers s. Denote the reduction mod p^s of $\sum a_h X^h$ by $\sum \overline{a}_h X^h$. Then, if $\sum a_h X^h$ is algebraic, each map $h \mapsto \overline{a}_h$ is given by a finite p-automaton. The survey [34] explains these matters in detail. If $\sum a_h X^h$ is rational then the maps $h \mapsto \overline{a}_h$ are periodic.

2. Introductory Generalities

2.1 A *generalised power sum* $a(h)\,,\ h = 0, 1, 2, \ldots\ldots$ is an expression of the shape

$$a(h) = \sum_{i=1}^{m} A_i(h)\alpha_i^h\ ,\ h = 0, 1, 2, \ldots\ldots \tag{2.1.1}$$

with *roots* $\alpha_i\,, 1 \le i \le m\,$, distinct non-zero quantities, and *coefficients* $A_i(h)$ polynomials respectively of degree $n(i) - 1\,$, for positive integers $n(i)\,,\ 1 \le i \le m$. The generalised power sum $a(h)$ is said to have *order*

$$n = \sum_{i=1}^{m} n(i)\,.$$

Set

$$s(X) = \prod_{i=1}^{m}(1 - \alpha_i X)^{n(i)} = 1 - s_1 X - \cdots - s_n X^n\,. \tag{2.1.2}$$

Then the sequence (a_h) with $a_h = a(h)$, $h = 0, 1, 2, \ldots\ldots$ satisfies the linear homogeneous recurrence relation

$$a_{h+n} = s_1 a_{h+n-1} + \cdots + s_n a_h\,,\ h = 0, 1, 2, \ldots\,. \tag{2.1.3}$$

2.2 To see this let $E : f(h) \mapsto f(h+1)$ be the shift operator and $\Delta = E - 1$ the difference operator. Then

$$(E - \alpha)A(h)\alpha^h = (\Delta A(h))\alpha^{h+1}$$

and since $\Delta A(h)$ has lower degree than does A, by linearity and induction it is plain that

$$\prod_{i=1}^{m}(E - \alpha_i)^{n(i)}$$

annihilates the sequence (a_h) as asserted. Thus generalised power sums are interesting in that they coincide with the sequences satisfying the recurrence relations (2.1.3). It follows that there is a polynomial $r(x)$, of degree less than n, so that the power series

$$\sum_{h=0}^{\infty} a_h X^h = \frac{r(X)}{s(X)} \tag{2.2.1}$$

is a rational function; to see this multiply by $s(X)$ and note the recurrence relation.

2.3 Conversely given a rational function as above, with $\deg r < \deg s$, a partial fraction expansion yields

$$\frac{r(X)}{s(X)} = \sum_{i=1}^{m}\sum_{j=1}^{n(i)} \frac{r_{ij}}{(1 - \alpha_i X)^j} = \sum_{h=0}^{\infty}\left(\sum_{i=1}^{m}\sum_{j=1}^{n(i)} r_{ij}\binom{h+j-1}{j-1}\alpha_i^h\right)X^h$$

and the coefficients of X^h, $h = 0, 1, 2, \ldots\ldots$ are indeed the values of a generalised power sum as described.

2.4 Accordingly, results on generalised power sums are equivalent to corresponding results for the Taylor coefficients of rational functions. For example, the trivial observation that the product of generalised power sums is again a generalised power sum becomes the more interesting: the Hadamard product (the "students' product")

$$\sum_{h=0}^{\infty} a_h b_h X^h$$

of rational functions $\sum a_h X^h$, $\sum b_h X^h$ is again rational.

2.5 In the argot used within the subcult of those fascinated with such matters, a sequence (a_h) satisfying a relation (2.1.3) is often called a *recurrence sequence* of *order* n; the polynomial $X^n s(X^{-1})$ reciprocal to the polynomial (2.1.2) is called the *characteristic* or *companion polynomial* of the recurrence sequence. Our "roots" α_i are the distinct zeros

of the companion polynomial. The archetypal example of a recurrence sequence is of course the celebrated Fibonacci sequence (f_h) defined by

$$f_{h+2} = f_{h+1} + f_h\,,\ h = 0, 1, 2, \ldots \text{ with } f_0 = 0\,, f_1 = 1\ ;$$

and generated by

$$\frac{X}{1 - X - X^2} = \sum_{h=0}^{\infty} f_h X^h\,.$$

2.6 The expression (2.1.1) for the $a_h = a(h)$ as a generalised power sum provides a well known formula for the terms of the recurrence sequence. Slightly less well known is the formula obtained from directly expanding (2.2.1). In terms of the given *initial values* $a_0, a_1, \ldots, a_{n-1}$ of (a_h) one has

$$r(X) = \sum_{j=0}^{n-1} \left(a_j - \sum_{i=1}^{j} s_i a_{j-i} \right) X^j\,,$$

and

$$s(X)^{-1} = \sum_{h=0}^{\infty} \sum_{j_1 + 2j_2 \cdots + nj_n = h} \frac{(j_1 + j_2 \cdots + j_n)!}{j_1! \ldots j_n!} s_1^{j_1} \cdots s_n^{j_n} X^h\,.$$

For the Fibonacci numbers this yields (with the usual conventions for interpreting the combinatorial symbol)

$$f_{h+1} = \sum_j \binom{h-j}{j}\,.$$

3. Exponential Polynomials

3.1 The Complex Case

3.1.1 It is plain that the generalised power sum is the restriction to the nonnegative integers of an *exponential polynomial*

$$a(z) = \sum_{i=1}^{m} A_i(z) e^{z \log \alpha_i}\ , z \in \mathbf{C}\,.$$

Note, however, that, because we are free to choose the branches of the $\log \alpha_i$ the continuation is not well defined.

3.2 The Ring of Exponential Polynomials

3.2.1 The ring of exponential polynomials has a unique factorisation theorem, essentially due to Ritt [51]. The units of the ring are of course the exponential polynomials $Ae^{\omega z}$, with constants $A \neq 0$. Irritatingly, the exponential polynomials of the shape $1 - Ae^{\theta z}$ have factors $1 - A^{1/n}e^{\theta z/n}$ for all positive integers n. Plainly we have to treat these exponential polynomials separately, and we do that by referring to them as *simple* exponential polynomials. We note that a product of simple exponential polynomials with the same *frequency* θ yields a polynomial over the base field in the single variable $e^{\theta z}$.

3.2.2 Finally, there are honest-to-goodness *irreducible* exponential polynomials. However, in the light of the presence of simple exponential polynomials, the existence of irreducibles is not at all obvious. One argues as follows: Suppose that the free Z-module generated by the frequencies $\omega_1, \ldots, \omega_m$ of the given exponential polynomial has a Z-basis $\tau_1, \ldots, \tau_t$. Setting $x_i = e^{\tau_i z}$, and multiplying by an appropriate unit if necessary, displays the given exponential polynomial as a polynomial in z and the x_i. Factorisations of the given exponential polynomial correspond to factorisations of that polynomial in polynomials in the variables z and fractional powers of the x_i. Monomial (one term) factors correspond to units or to powers of z; binomial (two term) factors with coefficients independent of z correspond to associates of simple exponential polynomials; the remaining irreducible factors are polynomials in z and either binomial expressions in z and the x_i, or polynomials with at least three terms. For these last polynomials Ritt [51] shows that there is a finite (this is the point of difficulty) factorisation in fractional powers of the x_i. The matter of factorisation of polynomials in fractional powers is detailed by Schinzel [62], see pages 101–113; the present argument is discussed in [26].

3.2.3 The upshot is that, up to units of the ring, an exponential polynomial has a unique factorisation as a product of a polynomial in z, a finite number of polynomials each in a single variable $e^{\theta_j z}$, with the respective frequencies θ_j linearly independent over $\mathbf{Q}$, and a finite number of irreducible exponential polynomials.

3.2.4 The factorisation theories for exponential polynomials and for generalised power sums are rather different (see [8] and [60]). A principal reason is that the Z-module generated by the frequencies $\omega_1, \ldots, \omega_m$ of an exponential polynomial corresponding to the given generalised power sum is no longer free since we must identify frequencies mod $2\pi i$; note also the example at 3.4 below.

3.3 Zeros of Complex Exponential Polynomials

3.3.1 Given an exponential polynomial

$$a(z) = \sum_{i=1}^{m} A_i(z)e^{\omega_i z},$$

denote by $\mathcal{C}_a$ the convex hull of the set $\{\overline{\omega}_1, \ldots, \overline{\omega}_m\}$ determined by the complex conjugates of the frequencies of $a(z)$. Then all but finitely many of the zeros of $a(z)$ lie in half-strips in

the directions of the exterior normals to $\mathcal{C}_a$ — other than for a slight (logarithmic) curving caused by the polynomial coefficients of $a(z)$. More quantitatively, suppose that an edge of the polygon $\mathcal{C}_a$ has length l. Then the number of zeros of $a(z)$ in a portion of those half-strips orthogonal to that edge and of length R is, as $R \to \infty$,

$$\frac{lR}{2\pi} + \mathrm{O}(1)\,.$$

To see this is easy. Suppose that $\overline{\omega}_j$ and $\overline{\omega}_k$ are adjacent vertices of $\mathcal{C}_a$ (or, if $\mathcal{C}_a$ degenerates to a single segment, are its endpoints). Then our claim is obvious for the two-term exponential polynomial $A_j(z)e^{\omega_j z} + A_k(z)e^{\omega_k z}$, and holds for $a(z)$ because its remaining terms are dominated by the given terms in the half-strips described. For a little more detail, and references, see [69]; also [70].

If Γ denotes the perimeter of $\mathcal{C}_a$ and γ is the number of its vertices, then in any disc of radius R, an exponential polynomial $a(z)$ of order n has at most

$$\frac{\Gamma R}{2\pi} + \frac{1}{2}\gamma(n-1)$$

zeros (see Voorhoeve [78], [77]).

3.3.2 *Ritt's quotient theorem* [53]. *If every zero of an exponential polynomial $b(z)$ is a zero of an exponential polynomial $c(z)$, then there is an exponential polynomial $a(z)$, and a polynomial $f(z)$ which divides each coefficient of $b(z)$ in the ring of polynomials, so that*

$$a(z)b(z) = f(z)c(z)\,.$$

If $b(z)$ has just one term there is nothing to prove to speak of, so we suppose that b has infinitely many zeros. If so, to each side of the polygon $\mathcal{C}_b$ there corresponds a parallel side of $\mathcal{C}_c$ of length at least as great. By an evident analogue of the Euclidean algorithm we may find exponential polynomials a and r so that for some polynomial f we have

$$f(z)c(z) = a(z)b(z) + r(z)\,,$$

and an edge of $\mathcal{C}_r$ is strictly shorter than the corresponding edge of $\mathcal{C}_b$. Counting zeros, the remarks of 3.3.1 entail that $r(z)$ vanishes identically.

The weaker hypothesis, that $c(z)/b(z)$ has fewer poles than one should expect, already yields the conclusion of the theorem (*cf* [64]). The example $(e^z - 1)/z$ reminds one that the polynomial $f(z)$ really is needed.

3.3.3 Given Ritt's quotient theorem, it is not unreasonable to suppose that *if two exponential polynomials have infinitely many zeros in common then (all but finitely many of) those zeros are accounted for by the exponential polynomials having a common exponential polynomial factor*. This peculiarly intractable conjecture of H. S. Shapiro [63] happens to have been seminal in sparking my interest in the matters surveyed in this paper (*cf* [48]).

By the factorisation results mentioned above, it suffices to consider just simple and irreducible exponential polynomials, and at 3.6 below we see that one can deal with the

zeros supplied by simple factors. Only the results of Diab ([24], [25]), who copes with the case of exponential polynomials corresponding to polynomials in just two variables (in the sense described at 3.2.2), seem to advance beyond this point.

3.3.4 Given the factorisation theory of 3.2, on the one hand we have the Ritt gcd of two exponential polynomials, which is the product of their common factors in the ring of exponential polynomials. On the other hand, there is an analytic gcd, which we can construct as follows (see, for example, [68], Ch.8): Consider the common zeros $z_1, z_2, \ldots\ldots$ of the given exponential polynomials. The exponent of convergence ρ of these numbers is at most that of the zeros of an exponential polynomial; thus $\rho \leq 1$. By the Weierstraß product theorem, the canonical product $h(z)$, say, of the common zeros is analytic and, by Borel's theorem, its order is ρ. By the Hadamard factorisation theorem, $h(z)$ is uniquely determined up to normalisation by a unit; that is, by a factor of the shape $Ae^{\omega z}$. Shapiro's conjecture is equivalent to the allegation that, up to units, and a possible polynomial factor, *the Hadamard* gcd *of two exponential polynomials coincides with their Ritt* gcd. It is equivalent to ask whether the Hadamard gcd of two exponential polynomials has order 0 or 1, and whether it is indeed an exponential polynomial.

3.4 Hadamard Inversion

3.4.1 We shall determine those rational functions whch are Hadamard invertible. Plainly, the rational function $(1-X)^{-1}$ is the unit for Hadamard multiplication; we note that the Hadamard inverse (the word should probably be "reciprocal") of a rational power series $\sum a_h X^h$ cannot possibly be rational unless the collection of all prime divisors of the a_h is finite.

Above we saw that if an exponential polynomial has at least two terms ($m \geq 2$), then it has infinitely many zeros in $\mathbf{C}$. It follows that, unless, essentially, $m = 1$ and the coefficient is a non-zero constant, a generalised power sum cannot have a generalised power sum reciprocal. The matter of "essentially" is not really delicate. In the final analysis (a classical result of Pólya [44]), the only Hadamard invertible rational functions, vanishing at ∞, are of the shape

$$\sum_{j=0}^{k-1} \frac{B_j \beta_j^j X^j}{(1-\beta_j^k X^k)} \ ,$$

corresponding to the generalised power sums

$$b(h) = B_j \beta_j^h \text{ according as } h \equiv j \bmod k \ .$$

3.4.2 Thus a rational function is Hadamard invertible only if its Taylor coefficients are composed from just finitely many primes. Indeed, the necessity of that condition is obvious as explained in our introductory remarks on the notion "possibly rational". It is somewhat less obvious that the condition is also sufficient, but this is entailed by the fact that if a generalised power sum is properly (in a nondegenerate way) of order at least 2 then the set of those primes dividing at least one of its terms is infinite. Thus the Hadamard inverse of a rational function is rational if and only if it is possibly rational. There are proofs of various levels of sophistication for this fact, ranging from the original observation of Pólya

through (for these see below) the Hadamard Quotient Theorem to the implications of the inequalities of Schmidt–Schlickewei for sums of generalised units.

3.4.3 The example also illustrates one of the subtle difficulties in moving between exponential polynomials and generalised power sums. If ζ denotes a primitive k-th root of unity then the generalised power sum of the example is

$$b(h) = k^{-1} \sum_{j=0}^{k-1} B_j \beta_j^h \left(\sum_{i=0}^{k-1} \zeta^{i(h-j)} \right) .$$

Its analytic continuations as exponential polynomials should be of order k^2. Yet it is more natural to view b as continued by k exponential polynomials each of order 1. (In the p-adic case we are forced to a number of continuations in much this way; thus it is certainly not unreasonable to view a generalised power sum as continued by more than one exponential polynomial).

3.5 The p-Adic Case

3.5.1 There are infinitely many primes (indeed, a set of positive density) so that a given generalised power sum can be suitably embedded in the field of p-adic rationals $\mathbf{Q}_p$ and analytically continued to exponential polynomials on $\mathbf{C}_p$, the algebraic closure of the completion of $\mathbf{Q}_p$. Cassels [19] provides an elegant description. There are two steps in the embedding process, the first of which will provide a useful notion of *specialisation* of a generalised power sum.

3.5.2 Recall, as in the introduction, that each element ϕ of the field $\mathbf{F} = \mathbf{Q}(x)[y]$, containing the terms

$$a(h) = \sum_{i=1}^{m} A_i(h) \alpha_i^h \ , \ h = 0, 1, 2, \ldots \ldots$$

of the generalised power sum a, has a representation

$$\phi = U_\phi(y; x)/V_\phi(x) ,$$

with $U_\phi \in \mathbf{Z}[y; x]$ and $V_\phi \in \mathbf{Z}[x]$ say relatively prime to the set of coefficients of U_ϕ and with its set of coefficients relatively prime over $\mathbf{Z}$. We may then refer to $V_\phi \in \mathbf{Z}[x]$ as *the* denominator of ϕ. Denote the defining polynomial of y over $\mathbf{Z}[x]$ by $F[x](Y)$, and suppose that it is of degree r.

3.5.3 Cassels' idea is to introduce a finite set Γ of elements of $\mathbf{F}$ with the property that whenever $\gamma \in \Gamma$ and $\gamma \neq 0$ then also $\gamma^{-1} \in \Gamma$. It will be convenient to require that Γ contains the discriminant and leading and trailing coefficients of $F[x](Y)$. Set

$$V_\Gamma(x) = \prod_{\gamma \in \Gamma} V_\gamma(x) .$$

It is easy to see, by induction on t, that there are infinitely many t-tuples of rational integers $c = (c_1, \ldots, c_t)$ so that $V_\Gamma(c) \neq 0$. Whenever $V_\Gamma(c) \neq 0$, we refer to a map $x \mapsto c$, together

with an induced map $y = y(x) \mapsto y(c)$ with $y(c)$ some zero of $F[c](Y)$, as a Γ-specialisation of $\mathbf{F}$. (This is an abuse of language; we specialise only the elements of a subring containing $\mathbf{Q}[x, \gamma : \gamma \in \Gamma]$.)

I allege that (unless $\gamma = 0$) if $\gamma = \gamma(y(x); x) \in \Gamma$, its Γ-specialisation $\gamma(y(c); c)$ is a nonzero element of an algebraic number field $\mathbf{K} = \mathbf{Q}(c)[y(c)]$ of degree at most r over $\mathbf{Q}$. We need only check that the specialisation of γ is indeed nonzero. For that it suffices to note that the element γ^{-1} belongs to Γ and thus also has an image under the specialisation.

3.5.4 We say more about specialisation below. For the present, we turn to the second step in the *p-adification* process.

We note that, having selected a Γ-specialisation $x \mapsto c$, there are infinitely many rational primes p so that both $V_\Gamma(c) \not\equiv 0 \bmod p$ and the reduction of the irreducible factor of the polynomial $F[c](Y)$ with $y(c)$ a zero, viewed as a polynomial over $\mathbf{F}_p$, has a linear factor $Y - \overline{y(c)}$. The first condition excludes just finitely many primes and the second condition is satisfied by all those primes p with a prime ideal factor of degree 1 in the number field $\mathbf{K} = \mathbf{Q}(c)[y(c)]$. By the Tchebotarev density theorem we are left with a set of *admissible* primes of positive density in the set of all primes.

3.5.5 Subject to $\xi_i \equiv c_i \bmod p \ , i = 1, \dots, t$ we now select t algebraically independent elements $\xi = (\xi_1, \dots, \xi_t)$ of $\mathbf{Q}_p$, as we may since $\mathbf{Q}_p$ has uncountable transcendence degree over $\mathbf{Q}$. Then, by Hensel's lemma, there is an element η of $\mathbf{Q}_p$ with $\eta \equiv \overline{y(c)} \bmod p$ and $F[\xi](\eta) = 0$ in $\mathbf{Q}_p$. By the remarks above, the map $(y; x) \mapsto (\eta; \xi)$ yields an embedding of $\mathbf{F}$ into $\mathbf{Q}_p$ under which nonzero elements of Γ become units in $\mathbf{Q}_p$. We have such an embedding for each p admissible with respect to the selected Γ-specialisation and the given polynomial F.

3.5.6 Given a generalised power sum

$$a(h) = \sum_{i=1}^{m} A_i(h)\alpha_i^h \ , \ h = 0, 1, 2, \dots \dots$$

we insist that, at the least, Γ contains the roots α_i. Then there are admissible p for which we obtain an embedding of the generalised power sum into $\mathbf{Q}_p$ so that the α_i become units in $\mathbf{Q}_p$. (It is convenient, and does no harm, not to change notation to indicate that elements once in $\mathbf{F}$ are now in $\mathbf{Q}_p$).

Thus for each i we have $\alpha_i^{p-1} \equiv 1 \bmod p$, whence the p-adic logarithms

$$\log_p \alpha_i^{p-1} = \log_p \left(1 - (1 - \alpha_i^{p-1})\right)$$

are defined, and satisfy $\operatorname{ord}_p (\log_p \alpha_i^{p-1}) \geq 1$. Finally, we recall that the p-adic exponential $\exp_p t$ converges for $t \in \mathbf{C}_p$ with $\operatorname{ord}_p t > 1/(p-1)$. Since p is fixed in the course of any paragraph, below we omit the subscripts p.

With all this, we obtain p-adic analytic functions

$$a_{p,r}(t) = \sum_{i=1}^{m} A_i(r + (p-1)t)\alpha_i^r \exp\left(t \log \alpha_i^{p-1}\right) \ , \ r = 0, 1, \dots, p-2 \ ,$$

converging for $t \in \mathbf{C}_p$ with $\operatorname{ord} t > -1 + 1/(p-1)$ and continuing (or, as the French* say, "prolonging") the given generalised power sum in the sense that $a_{p,r}(h) = a(r + (p-1)h)$ for $0 \leq r < p-1$ and $h = 0, 1, 2, \ldots\ldots$

3.5.7 A p-adic exponential polynomial has just finitely many zeros in its domain of definition. Provided that $p > n \geq 3$, an exponential polynomial of order n defined over $\mathbf{Q}_p$ has at most $(n-2)p$ zeros in $\mathbf{C}_p$. What we currently know of these matters is detailed in [46].

3.6 The Lech-Mahler Theorem

3.6.1 The following result is quite delightful: *If a rational function $\sum a_h X^h$ has infinitely many zero Taylor coefficients, then the set $\{k : a_k = 0\}$ is the union of finitely many complete arithmetic progressions $\{hd + r \geq 0 : h \in \mathbf{Z}\}$ together with at most finitely many isolated points.*
Indeed, if a generalised power sum $a(h)$, $h = 0, 1, \ldots$ has infinitely many zeros then for each admissible prime p (in the sense of 3.5.6) there is a nonempty set $\mathcal{R}$ of integers r, with $0 \leq r < p-1$, so that the p-adic analytic functions $a_{p,r}(t)$ have infinitely many zeros on the compact set $\mathbf{Z}_p$. Thus these $a_{p,r}(t)$ vanish identically, verifying that $a(h) = 0$ for all h of the shape $r + (p-1)j$, with $j \in \mathbf{Z}$.

We see that if $a(z)$ is an exponential polynomial continuing the given generalised power sum to $\mathbf{C}$ then every zero of the exponential polynomials $\sin \frac{\pi}{p-1}(z-r)$ with $r \in \mathcal{R}$ is a zero of $a(z)$. By Ritt's quotient theorem it follows that these functions are factors of $a(z)$ in the ring of exponential polynomials, and account for all but finitely many of the integer zeros of $a(z)$. We can thus report, in congenial terminology, that an exponential polynomial has infinitely many integer zeros if and only if it is sinful.

3.6.2 If two exponential polynomials have common zeros of the shape $\vartheta + h\theta$, for infinitely many $h \in \mathbf{Z}$, then, after translation and rescaling, one has two exponential polynomials that are jointly sinful, and that sinfulness accounts for all but finitely many of those common zeros. Thus, in Shapiro's Conjecture at 3.3.3, one can deal with common zeros supplied by simple factors.

3.6.3 Sinfulness entails that the generalised power sum has distinct pairs of roots so that α_i/α_j is a nontrivial root of unity. In yet more judgmental language, a generalised power sum, or the corresponding recurrence sequence, is said to be *degenerate* if it has such pairs of roots. For different reasons, a generalised power sum is also judged degenerate if any of its roots is a root of unity. The definition implies that a nondegenerate generalised power sum has at most finitely many zeros; indeed that it takes any given value at most finitely many times.

3.6.4 The theorem cited comprises results of Skolem [66], Mahler [37], Lech [33] and Mahler [38], with the argument of Cassels bypassing the increasing technical complication in this chain of successive generalisations. Actually, [38] inadvertently and, so to speak, independently duplicates the result of Lech; as is admitted in the 'Addendum'. Privately, Mahler spoke with feeling about his embarrassment at realising he had refereed Lech's paper and had then forgotten it.

---

* This remark is a blow for bilingualism.

4. Auxiliary Facts

4.1 Heights

4.1.1 It used to be not at all obvious how one should measure the size of an algebraic number α. The old-fashioned way was to take its defining polynomial $P_\alpha \in \mathbf{Z}[X]$,

$$P_\alpha(X) = p_0 X^r + p_1 X^{r-1} + \cdots + p_r\,,$$

irreducible with relatively prime coefficients and $P_\alpha(\alpha) = 0$; then α was said to have height $\max|p_i|$. One also used, the typiste's nightmare, 'house': $\overline{|\alpha|} = \max_\sigma\{|\sigma\alpha|\}$, with the max taken over the conjugates $\sigma\alpha$ of α; a 'denominator' d so that $d\alpha$ is an algebraic integer; and, of course, the degree r of α.

4.1.2 Given an algebraic number field $\mathbf{K}$, we define the absolute logarithmic height $\mathrm{h}(\alpha)$ of $\alpha \in \mathbf{K}$ as follows : Appropriately normalise the absolute values $|\ \ |_v$ of $\mathbf{K}$ so that, for $\beta \neq 0$ one has the product formula

$$\sum_v \log|\beta|_v = 0\,.$$

My personal, somewhat eccentric, choice is to think of the sum over the v as being with repetition according to multiplicity (the local degrees $n_v = [\mathbf{K}_v : \mathbf{Q}_v]$); then, for example, for all infinite places v and natural numbers n one may take $|n|_v = n$, which feels comfortable. However, it is probably more sensible to correctly take powers to normalise the absolute values and to let the sum be what it seems to be.

Having defined $\log^+(\ \ ) = \max\{0, \log(\ \ )\}$, we set

$$\mathrm{h}(\alpha) = ([\mathbf{K} : \mathbf{Q}])^{-1} \sum_v \log^+|\alpha|_v\,.$$

If one prefers an honest height, rather than its logarithm, as I do†, set $\mathrm{H}(\alpha) = \exp \mathrm{h}(\alpha)$. Then, for a rational number a/b expressed in lowest terms, one has $\mathrm{H}(a/b) = \max\{|a|, |b|\}$, just as with the old-fashioned height. Note that $\mathrm{H}(\alpha) = 1$ if and only if $\alpha = 0$ or α is a root of unity. The normalisation by $[\mathbf{K} : \mathbf{Q}]$ is important so that the height of α is not affected by our replacing $\mathbf{K}$ by some extension field.

4.1.3 As it happens, the absolute height just defined appears — without the normalisation and in heavy disguise, in work of Mahler (see [39], pp 5–10), where it is used to compute inequalities for the old-fashioned height. The Mahler measure $\mathrm{M}(P)$ of a polynomial P is

$$\mathrm{M}(P) = \exp\left(\int_0^1 \log|P(e^{2\pi i t})|dt\right)\,,$$

† Whilst presenting a seminar in Paris in 1987 I got involved in a slanging match* with Serge Lang on whether I should follow Bombieri or French practice in this matter; the capitalisation is the compromise reached.

* Actually, just an exchange in which firm opinions were stated; but the combination of "slanging" and S. Lang is irresistible.

and, in effect by Jensen's theorem, one has, taking $P = P_\alpha$ as in 4.1.1 above, that

$$\mathrm{M}(P_\alpha) = |p_0| \prod_\sigma \max\{1, |\sigma\alpha|\}\,,$$

so $\mathrm{M}(P_\alpha) = (\mathrm{H}(\alpha))^r$. It helps to notice that, in the definition of $\mathrm{h}(\alpha)$, the sum over the nonarchimedean values provides the contribution made to the height by the denominator of α.

4.1.4 By proper use of the absolute height, one can deal with algebraic numbers in almost the same comfort as one deals with rational integers. For example, consider the well known fundamental lemma of transcendence theory:

$$\text{If } n \in \mathbf{Z} \text{ and } |n| < 1 \text{ then } n = 0\,.$$

One obtains its generalisation to arbitrary places of a number field $\mathbf{K}$, as follows: Start with the product formula and observe that for any subset T of the places v of $\mathbf{K}$, either $\alpha = 0$ or

$$\sum_v \log|\alpha|_v = 0 \text{ implies}$$
$$\sum_{v\in T} \log|\alpha|_v = -\sum_{v\notin T} \log|\alpha|_v \geq -\sum_{v\notin T} \log^+|\alpha|_v \geq -\sum_v \log^+|\alpha|_v = -[\mathbf{K}:\mathbf{Q}]\mathrm{h}(\alpha)\,.$$

This is Liouville's theorem in mild disguise, and generalised. Indeed, if β, with $|\beta| \leq 1$, is of degree r over $\mathbf{Q}$ and p/q is a rational in lowest terms approximating β, consider $\alpha = \beta - p/q$. With q large enough one has $\mathrm{h}(\alpha) \simeq \log q$ and the inequality above yields

$$\log|\alpha| = \log|\beta - p/q| \;\&\; -r\log q\,.$$

4.1.5 The (projective) height $\mathrm{H}(\beta)$ of an $(m+1)$-tuple $\beta = (\beta_0, \ldots, \beta_m)$ of elements of $\mathbf{K}$ is given by $\log \mathrm{H}(\beta) = ([\mathbf{K}:\mathbf{Q}])^{-1} \sum_v \max_{1\leq i\leq m} \log|\beta_i|_v$. One uses the same notation in mentioning the height of a point $\beta = (\beta_0 : \beta_1 : \cdots : \beta_m)$ in the projective space $P^m(\mathbf{K})$.

4.1.6 Following Bombieri [14], we define the height $\mathrm{H}(a)$ of a sequence (a_h) of elements a_h of a number field $\mathbf{K}$ by

$$\log \mathrm{H}(a) = ([\mathbf{K}:\mathbf{Q}])^{-1} \limsup_{h\to\infty} h^{-1} \sum_v \max_{0\leq i\leq h} \log|a_i|_v\,,$$

with the sum and normalisations as at 4.1.2 . The definition implies that the height of a sequence is invariant under multiplication by a nonzero element of $\mathbf{K}$; by the product formula, the sequences (a_h) and (ca_h) have the same height. Our purpose is to attach a height to the sequence of coefficients of a power series $\sum a_h X^h \in \mathbf{K}[[X]]$ and this is achieved, felicitously, by the given definition. Plainly, the invariance under multiplication by nonzero algebraic constants is desirable. Moreover, the nonarchimedean values progressively pick up the lowest common multiple of the denominators of $a_0, \ldots, a_h$, so that the height is

a suitable arithmetic measure of the growth of the sequence. The geometric progression $(1, \alpha, \alpha^2, \ldots\ldots)$ has height $\mathrm{H}(\alpha)$; the harmonic sequence $(1, 1/2, 1/3, \ldots\ldots)$ has height e.

4.1.7 There are circumstances in which one can refine the notion "possibly rational" introduced at 1.2 (the following being a weaker condition): If a series $\sum a_h X^h$ is defined over a number field and has finite height $\mathrm{H}(a) = A < \infty$, one says that it represents a G-function (in the sense of [14]). We will have circumstances in which a series being a G-function suffices for it to be 'possibly rational' (because the additional requirements are entailed by the context). Notice that, if the a_h are in $\mathbf{Q}$, we are stating a blatantly necessary condition for rationality of the series.

4.2 Specialisation and Lifting

4.2.1 Recall the introductory remarks at 1.1 since we assume that notation. En route to the p-adification process explained at 3.5 we saw that there are infinitely many embeddings of rings R of finite type (for example, those rings containing the terms of given generalised power sums) into algebraic number fields of bounded degree. This is an important observation because our methods for discovering the rationality of series apply, in the first instance, only to those series with Taylor coefficients in a number field. Our approach therefore is to specialise the data (in the manner sketched at 3.5.3) into a number field. One then shows that the specialisations of the series under investigation represent rational functions. Finally, one argues that this conclusion may be lifted, back up to the original data.

4.2.2 To achieve this program it is important to be able to guarantee that the specialisations are 'non-destructive': they must not introduce degeneracy or vanishing. But that is done by placing the data in the set Γ controlling the specialisations. For, as observed at 3.5.3, nonzero elements of Γ specialise to nonzero elements.

Moreover, one can avoid introducing multiplicative relations. This is not obvious but can be seen as follows: Suppose that $g_1, \ldots, g_s$ are multiplicatively independent elements of the domain R. Given H sufficiently large relative to the data, consider the specialisations of R induced by $x \mapsto c = (c_1, \ldots, c_t)$, with each rational integer c_i satisfying $|c_i| < H$. Select an admissible such specialisation (there are $\mathrm{O}(H^t)$ such) and denote the image of g_j by $\overline{g}_j$; the $\overline{g}_j$ will be elements of some number field $\mathbf{K}$ of degree r over $\mathbf{Q}$. We have $\mathrm{h}(\overline{g}_j) \ll \log H$, with the implied constant depending only on the data and not on the selected specialisation. By a result of Loxton and van der Poorten [36], if the $\overline{g}_j$ are multiplicatively dependent then there is, already, a multiplicative relation

$$\overline{g}_1^{a_1} \cdots \overline{g}_s^{a_s} = 1\,,$$

in integers a_j, not all zero, with the $|a_j| \ll (\log H)^{s-1}$. Accordingly, we augment Γ with the elements

$$g_1^{b_1} \cdots g_s^{b_s} - 1 \text{ for all integer vectors } b \text{ with } |b_j| \ll (\log H)^{s-1}\,.$$

This prevents the g_j from specialising to multiplicatively dependent elements under any Γ-specialisation induced by $x \mapsto c$ with each c_i satisfying $|c_i| < H$. With Γ augmented, only $\ll H^{t-1}(\log H)^{s^2-1}$ of the original $\mathrm{O}(H^t)$ specialisations induced by $x \mapsto c$ fail to yield

an admissible specialisation; if H is large enough (relative to the data) this leaves plenty to spare.

4.2.3 The idea of specialising in this context already appears in work of Cantor [15], [16]. I should have known the argument given at 4.2.2, since it relies on a result in which I had involvement, but it had to be shown to me, blow-by-blow, by David Masser† (*cf* [40]).

4.3 Additive Relations in Fields

4.3.1 The following inequality is a consequence of the p-adic analogue of the Thue-Siegel-Roth-Schmidt theorem:
Let $\mathbf{K}$ *be a number field and* T *a finite subset of its values; denote by* S *a finite set of primes of* Q *including those lying below the nonarchimedean values of* T*. Write* $\mathcal{N}$ *for the norm from* $\mathbf{K}$ *to* Q*. Then, for every* $\epsilon > 0$*, the inequality*

$$\prod_{v\in T} |z_1 + \cdots + z_m|_v > \left(\prod_{p\in S\cup\{\infty\}} \prod_{i=1}^{m} |\mathcal{N} z_i|_p \right)^{-1} \left(\prod_{v\in T} \max_{1\le i\le n} |z_i|_v \right) (\mathrm{H}(z))^{-\epsilon}$$

holds for all but at most finitely many m*-tuples* $z = (z_1, \ldots, z_m)$ *in* $\mathbf{K}^m$ *for which*
(i) *no proper or improper subsum of* $z_1 + \cdots + z_m$ *vanishes; and*
(ii) z *is such that* $(\mathcal{N}z_1, \ldots, \mathcal{N}z_m)$ *is an* m*-tuple of* S*-integers.*

4.3.2 After discussion with Hans Peter Schlickewei at an Oberwolfach meeting (he is responsible for the above-mentioned p-adic analogue of the Thue-Siegel-Roth-Schmidt theorem), I had noticed a weaker version of this result and had reported it at Budapest in 1981. After my lecture, Birch promptly told me that the inequality has more profound implications than just for recurrence sequences (see below at 4.3.3). Subsequently Schlickewei and I prepared a manuscript [47]; because of my clumsiness it has not as yet been published. Meanwhile, quite independently, Evertse [27] proved the stronger inequality and put the matter in the public domain.

4.3.3 Early in 1982, Vojta‡ (see [76]) surprised me by writing that Birch had told him that I had proved that an equation

$$x_1 + \cdots + x_n = 1$$

has only finitely many nontrivially distinct solutions $x_1, \ldots, x_n$ belonging to a finitely generated subgroup of $\mathbf{F}^\times$, with $\mathbf{F}$ a field of characteristic zero. I then began to understand what Birch had said to me in Budapest. Indeed, the bounds at 4.3.1 prevent excessive vanishing. If $z_1 + \cdots + z_m = 0$ then, at all places v, we have $|z_1 + \cdots + z_{m-1}|_v = |z_m|_v$. Once we suitably identify 'equivalent' solutions it is easy to see that the inequality at 4.3.1 entails there are only finitely many 'inequivalent' solutions. Moreover, when one turns from inequalities to equations, specialisation and lifting arguments apply. Thus the inequality at 4.3.1 implies information on the number of 'essentially distinct' solutions of linear relations

† IAS Princeton, January 1986

‡ Paul Vojta, correspondence c.January, 1982

in elements of finitely generated subgroups of arbitrary fields of characteristic zero. The specialisation and lifting arguments are easy when applied to generalised power sums, but in the general case they require as much as is mentioned at 4.2.2.

4.3.4 There is, by now, an extensive literature dealing with applications of the present results. The book by Shorey and Tijdeman [65] provides a useful introduction. A suitable point to access yet more recent material is the survey [28].

4.4 A Criterion for Rationality

4.4.1 We know that $\sum a_h X^h$ represents a rational function vanishing at ∞ if and only if, for some n, there is a recurrence relation $a_{h+n} = s_1 a_{h+n-1} + \cdots + s_n a_h$ for all $h = 0, 1, \ldots$. Thus, necessarily, the Kronecker-Hankel determinants

$$K_N(a) = \begin{vmatrix} a_0 & a_1 & \cdots & a_N \\ a_1 & a_2 & \cdots & a_{N+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_N & a_{N+1} & \cdots & a_{2N} \end{vmatrix}$$

vanish for $N = n, n+1, \ldots$. This condition is also sufficient. Indeed, suppose $K_{n-1}(a) \neq 0$ but $K_n(a) = 0$. Then, we may set $b_h = a_{h+n} - s_1 a_{h+n-1} - \cdots - s_n a_h$, with certain constants $s_1, \ldots, s_n$, and we have $b_h = 0$ for $h = 0, 1, \ldots, n$. But

$$K_{n+1}(a) = \begin{vmatrix} a_0 & a_1 & \cdots & a_{n-1} & 0 & 0 \\ a_1 & a_2 & \cdots & a_n & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{n-1} & a_n & \cdots & a_{2n-2} & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & b_{n+1} \\ 0 & 0 & \cdots & 0 & b_{n+1} & b_{n+2} \end{vmatrix} = -b_{n+1}^2 K_{n-1}(a)\,.$$

Thus $K_{n+1}(a) = 0$ implies $b_{n+1} = 0$, and, by induction, $K_N(a) = 0$ for $N = n, n+1, \ldots$ entails $b_h = 0$ for $h = 0, 1, \ldots$.

4.4.2 Suppose (as at 4.1.6) that (a_h) is a sequence of elements of a number field $\mathbf{K}$ and has height $\mathrm{H}(a) = A < \infty$. It is convenient to define the height $\mathrm{H}(K(a))$ of the sequence of Kronecker-Hankel determinants by

$$\log \mathrm{H}(K(a)) = ([\mathbf{K} : \mathbf{Q}])^{-1} \limsup_{h \to \infty} h^{-2} \sum_v \max_{0 \leq N \leq h} \log |K_N(a)|_v\,;$$

note that this is not the same definition of height of a sequence as at 4.1.6, where we divide just by h^{-1}. Then, but (*cf* [32]) this is not as obvious as may seem at first, $\mathrm{H}(K(a)) = \mathrm{H}(a) = A$.

4.4.3 Let Δ be the forward difference operator introduced at 2.2 and, here, acting on the subscript of a. Manipulation of rows and columns in the Kronecker-Hankel determinant shows that

$$K_N(a) = \left|\Delta^{i+j} a_0\right|_{0 \leq i,j \leq N}\,.$$

4.4.4 Let $x(t) = \sum x_h t^h$ be a power series with coefficients in $\mathbf{C}_p$ and converging on the disc $\{t \in \mathbf{C}_p : \operatorname{ord} t > -c + 1/(p-1)\}$, some $c > 1/(p-1)$. Then $\limsup_{h\to\infty} h^{-1}\operatorname{ord} x_h = c - 1/(p-1)$. One has

$$\frac{\Delta^k x(0)}{k!} = \sum_{h=k}^{\infty} x_h S(h,k)\,,$$

where the integers $S(h,k)$ are the Stirling numbers of the second kind. It follows, recalling $\operatorname{ord} k! = (k - \sigma(k))/(p-1)$, where $\sigma(k)$ is the sum of the p-adic digits of k, that

$$\limsup_{k\to\infty} k^{-1}\operatorname{ord}\Delta^k x(0) \le \lim_{k\to\infty} k^{-1}\operatorname{ord} k! + \limsup_{h\to\infty} h^{-1}\operatorname{ord} x_h = c\,.$$

On the other hand,

$$x_h = \sum_{k=h}^{\infty} \frac{\Delta^k x(0)}{k!} s(h,k)\,,$$

where the integers $s(h,k)$ are the Stirling numbers of the first kind. This yields

$$c = \lim_{k\to\infty} k^{-1}\operatorname{ord} k! + \limsup_{h\to\infty} h^{-1}\operatorname{ord} x_h \le \limsup_{k\to\infty} k^{-1}\operatorname{ord}\Delta^k x(0)\,;$$

and we have proved

$$\limsup_{k\to\infty} k^{-1}\operatorname{ord}\Delta^k x(0) = c\,.$$

4.4.5 At 3.5.6 we saw that recurrence sequences yield maps $h \mapsto a(r + (p-1)h)$ that can be analytically continued to maps on the disc $\{t \in \mathbf{C}_p : \operatorname{ord} t > -1 + 1/(p-1)\}$. This is the context in which the following criterion turns out to be useful:
Let (a_h) be a sequence of elements of a number field $\mathbf{K}$ with finite height $\mathrm{H}(a) = A$. Suppose there is a set $\mathcal{P}$ of rational primes p for which the $p-1$ maps, with $0 \le r < p-1$,

$$h \mapsto a_{r+(p-1)h}$$

may be analytically continued to maps on the disc $\{t \in \mathbf{C}_p : \operatorname{ord} t > -1 + 1/(p-1)\}$. If

$$\prod_{p\in\mathcal{P}} p^{1/(p-1)} > A^{[\mathbf{K}:\mathbf{Q}]}$$

then $\sum a_h X^h$ is a rational function.

4.4.6 If Δ_{p-1} is the difference operator $\Delta_{p-1} : f(h) \mapsto f(h+p-1) - f(h)$, then a generalisation of the remark at 4.4.3 yields

$$K_N(a) = \left|\Delta_{p-1}^{\lfloor i/(p-1)\rfloor + \lfloor j/(p-1)\rfloor} a_{r+s}\right|_{\substack{r\equiv i, s\equiv j \pmod{p-1} \\ 0\le r,s<p-1}}$$

By applying 4.4.4 we can now verify that the data of the criterion implies: for $p \in \mathcal{P}$,

$$\liminf_{N\to\infty} N^{-2}\operatorname{ord}_p K_N(a) \ge \frac{1}{p-1}\,.$$

Let T be the set of all places above the primes $p \in \mathcal{P}$. Then, on applying Liouville's theorem (4.1.4) we have, for all sufficiently large N, either $K_N(a) = 0$ or

$$-N^{-2} \sum_{v \in T} \log |K_N(a)|_v \, . \sum_{p \in \mathcal{P}} \frac{1}{p-1} \log p < [\mathbf{K} : \mathbf{Q}] N^{-2} \log \mathrm{H}(K_N(a)) \, . \log A \, .$$

But this is just a restatement (recall 4.4.1) of the criterion.

4.4.7 Even if all rationality proofs rely on proving the vanishing of the $K_N(a)$, the form of the criteria may well disguise that fact. The discussion at chapitre 5 of [1] is instructive; see also Chapter 5 of [30].

5. Recurrence Sequences

5.1 Growth

5.1.1 Recall the inequality at 4.3.1, take $z_i = A_i(h)\alpha^h$ and S a finite set of rational primes lying below the place v and the primes arising in the factorisations of the α_i. This provides an immediate application to generalised power sums: *For every $\epsilon > 0$, the inequality*

$$|A_1(h)\alpha_1^h + \cdots + A_m(h)\alpha_m^h|_v > \left(\prod_{p \in S \cup \{\infty\}} \prod_{i=1}^{m} |\mathcal{N} A_i(h)|_p \right)^{-1} \left(\max_{1 \le i \le m} |A_i(h)\alpha_i^h|_v \right) e^{-\frac{1}{2}\epsilon h}$$
$$> e^{-\epsilon h} \max_{1 \le i \le m} |\alpha_i|_v^h$$

holds for all but at most finitely many h for which no proper or improper subsum of $A_1(h)\alpha_1^h + \cdots + A_m(h)\alpha_m^h$ vanishes.
We have used the fact that the roots α_i are given; this enables us to select a finite set S with

$$\prod_{p \in S \cup \{\infty\}} \prod_{i=1}^{m} |\mathcal{N}\alpha_i^h|_p = 1 \, ;$$

the contribution of the coefficients $A_i(h)$ disappears into the ϵ.

Thus a nondegenerate generalised power sum defined over a number field grows, in every valuation, pretty well as one would expect it to; that is, according to its maximal term. This is no great surprise. It is a fairly elementary matter to see (even over an arbitrary field of characteristic zero) that a nondegenerate generalised power sum has expected growth for all but a very thin set of h (*cf* [35]). The depth of the present inequality lies in its exclusion of all but small h.

5.1.2 Suppose that, given v, the roots α_i of the generalised power sum are ordered so that we have

$$|\alpha_1|_v \ge \cdots \ge |\alpha_k|_v > |\alpha_{k+1}|_v \ge \cdots \ge |\alpha_m|_v \, .$$

If $k = 1$ we have the *unique dominant root* case and the inequalities are not very surprising. When $k = 2$, techniques based upon Baker's method in diophantine approximation may be applied; the results are stronger; and are effective. Shorey and Tijdeman [65] provide a full description. The general case over number fields was inaccessible until the inequalities reported above became available.

5.1.3 There are only finitely many places v at which one does not have $|\alpha_i|_v = 1$ for $i = 1, \dots, m$. It follows that most primes divide the terms of a nondegenerate recurrence sequence arbitrarily rarely (relative to h) and that, if $m \geq 2$, the totality of the terms is divisible by infinitely many primes (as mentioned at 3.4.2). Indeed, Evertse [27], Theorem 3, shows *inter alia* that (the norm of) the greatest prime divisor of the term a_h of a nondegenerate recurrence sequence defined over a number field, and with at least two distinct roots, goes to ∞ with h.

5.1.4 Bézivin [9] studies the procedure for determining, just given the recurrence relation — and not, generally speaking, the initial values, whether a prime divides terms of an integer recurrence sequence. In [10] he applies methods of classical analytic number theory to estimate the greatest prime factor of the terms of a restricted class of recurrence sequences.

5.2 Total Multiplicity

5.2.1 By the results on additive relations in fields (as at 4.3.3) the equation

$$a_h = A_1(h)\alpha_1^h + \cdots + A_m(h)\alpha_m^h = 0$$

has infinitely many solutions h only if this yields just finitely many projectively distinct solutions in the α_i^h, or if proper subsums vanish. But, because vanishing subsums yield linear relations of the same shape, our remark applies also to them. Presuming no vanishing proper subsum, distinct h yield projectively equivalent solutions only if we have degeneracy as described at 3.6.3. Thus, the present arguments provide a new proof for the Lech-Mahler theorem.

5.2.2 Suppose that two nondegenerate recurrence sequences (a_h) and (b_h) have infinite intersection. Then we have infinitely many pairs (h, l) yielding solutions to a relation

$$A_1(h)\alpha_1^h + \cdots + A_m(h)\alpha_m^h - B_1(l)\beta_1^l - \cdots - B_{m'}(l)\beta_{m'}^l = 0\,.$$

Nondegeneracy of the given sequences entails we have $m = m'$ and that, for all but finitely many of the solutions (h, l), we have (after reindexing the β_i if necessary) $A_i(h)\alpha_i^h = B_i(l)\beta_i^l$ for $i = 1, \dots, m$. However, if

$$A(h)\alpha^h = B(l)\beta^l$$

has infinitely many solutions $(h, l) \in \mathbf{Z}^2$, say with $h \leq l$, then there are integers $d > 0$ and r so that $\alpha^d = \beta$ and $A(r + hd)\alpha^r = B(h)$ for all $h \in \mathbf{Z}$. Thus nondegenerate recurrence sequences have infinite intersection if and only if one is a subrecurrence of the other.

The requirement that the given recurrence sequences be nondegenerate is not as severe a restriction as may seem. Indeed, a degenerate recurrence sequence is just a a number of nondegenerate recurrence sequences interweaved (as at 3.4.1); possibly with each having a

polynomial term. If β is not a root of unity and $A(h) = B(l)\beta^l$ has infinitely many solutions $(h, l) \in \mathbf{Z}^2$ then, for practical purposes, β is a rational integer and $A(h)$ is of the shape Ah^k, some $k \geq 1$. Detailing the precise result in the general case is a little distasteful; it is "merely an exercise in degeneracy"†. However, it does yield an extraordinary generalisation of the Lech-Mahler theorem when we view that result as dealing with the intersection of recurrence sequences and the trivial recurrence sequence $(0, 0, \ldots\ldots)$.

5.2.3 In particular, a nondegenerate recurrence sequence intersects with itself (up to finitely many indices) only trivially. Hence, a nondegenerate recurrence sequence (a_h) has *finite total multiplicity*: there are only finitely many pairs (h, l), with $h \neq l$, so that $a_h = a_l$.

With some extra work (see [28], Theorem 9) one can show that the more general equations $c_{h,l}a_h = a_l$, with the $c_{h,l}$ merely restricted to a ring R finitely generated over $\mathbf{Z}$, have just finitely many solutions (h, l) with $h \neq l$.

5.2.4 Moreover, we have dealt with the following: "Take the terms a_h of a nondegenerate recurrence sequence and throw them into a (very large) sack. Now shake the sack to thoroughly mix its contents. Sequentially select an infinite set of elements $\{b_0, b_1, \ldots\ldots\}$ from the sack. Suppose it happens to happen, rather improbably, that the sequence (b_h) is again a recurrence sequence!" Then there is an integer $d > 0$ and and a nonempty set $\mathcal{R}$ of integers r, with $0 \leq r < d$, so that for all h we have $b_h = a_{r_h+hd}$ with $r_h \in \mathcal{R}$ and with the sequence (r_h) a periodic sequence.

5.2.5 *A Confession.* It was this question that moved me to concoct utterly fallacious proofs (please, do not look at [29] and [73]) of its answer and other celebrated conjectures of the subject. En route, I needed a growth estimate for recurrence sequences and stumbled upon the much deeper results mentioned at 4.3 and applied above. For [29] there is a corrigendum [71] of sorts (some claims are still too sloppy), but [73] defies repair since some of its 'results' cannot be true. The criterion at 4.4.5 is a sanitised version of the viciously false allegation at [73], 1284–85. Those claims which I have managed to retrieve, necessarily by different arguments from those originally suggested, are mentioned below at **6**.

5.3 Multiplicity

5.3.1 Whether a given recurrence sequence (a_h) of order n is degenerate or not is a decidable question ([4]; *cf* [54]).

5.3.2 If it is nondegenerate then (as we saw at 3.6 or 5.2) its *c-multiplicity*, the cardinality of the set $\{h : a_h = c\}$, is finite. Beukers [5] has shown that with just five exceptions (up to normalisation) a nondegenerate binary recurrence sequence of rational integers has $\pm c$-multiplicity at most 3. The exceptions are:

$a_{h+2} = a_{h+1} - 2a_h$	and	$a_0 = a_1 = 1$	with $a_0 = a_1 = 1$, $a_2 = a_4 = a_{12} = -1$;
$a_{h+2} = a_{h+1} - 2a_h$	and	$a_0 = 1$, $a_1 = -1$	with $a_0 = 1$, $a_1 = a_3 = a_{11} = -1$;
$a_{h+2} = 3a_{h+1} - 4a_h$	and	$a_0 = a_1 = 1$	with $a_0 = a_1 = 1$, $a_2 = a_6 = -1$;
$a_{h+2} = 2a_{h+1} - 3a_h$	and	$a_0 = a_1 = 1$	with $a_0 = a_1 = a_5 = 1$, $a_2 = -1$;
$a_{h+2} = a_{h+1} + a_h$	and	$a_0 = 1$, $a_1 = -1$	with $a_0 = 1$, $a_1 = a_3 = a_4 = -1$.

† I quote a colleague whom I refrain from naming.

In response to Ward's conjecture to the effect that the 0-multiplicity of certain classes of nondegenerate ternary integer recurrence sequences is at most 5, Kubota [31] shows that the multiplicity of a binary integer recurrence sequence does not exceed 4. The (essentially) unique extreme example arises by setting $b_{h+1} = (-1)^h a_h$ in the first exception above. Then $b_{h+2} = -b_{h+1} - 2b_h$ and $b_0 = 0,\ b_1 = 1$ yields $b_2 = b_3 = b_5 = b_{13} = -1$.

5.3.3 Loxton and van der Poorten [35] have suggested that, given n, there is a uniform bound for the multiplicity of nondegenerate recurrence sequences of order n, regardless of the field of definition. There is no serious evidence, one way or the other, but the matter seems inaccessible, except for $n = 2$ which has been settled favourably (5.3.5). However, one must suppose that the field of definition has characteristic zero; both Lech [33] and Mahler [38] emphasise that matters of degeneracy and multiplicity are not as clearly linked in positive characteristic as in characteristic zero. Lech [33] quotes an example equivalent to (a_h), with $a_h = (X+Y)^h - X^h - Y^h$, which satisfies the recurrence relation

$$a_{h+3} = (2X+2Y)a_{h+2} - (X^2+3XY+Y^2)a_{h+1} + (X^2Y+XY^2)a_h\,.$$

In characteristic $p > 0$ the a_h vanish if and only if h is a power of p.

5.3.4 Even the matter of the 0-multiplicity of ternary recurrences of rational integers (which is equivalent to the question of the multiplicity of binary recurrences over certain Galois extensions of small degree) is very difficult. Actually, it has long been believed that the unique extreme case† is

$$a_{h+3} = 2a_{h+2} - 4a_{h+1} + 4a_h\,,\quad a_0 = a_1 = 0\,,\ a_2 = 1\,;$$

it has just six zeros, namely $a_0 = a_1 = a_4 = a_6 = a_{13} = a_{52} = 0$. This example was noticed by Berstel (*cf* [41]), allegedy by 'randomly' testing recurrence relations. Kubota ([31], III) claims to be able to show the bound six, but this has not been substantiated. Beukers [6] proves that the 0-multiplicity of a ternary recurrence of rational numbers does not exceed seven and remarks on the "enormous amount of computation that will be involved" to obtain the bound six. In addition to the example cited he mentions:

$$\begin{aligned} &a_{h+3} = a_{h+2} - a_h \quad \text{and}\ \ a_0 = 0\,,\ a_1 = 1\,,\ a_2 = 0 \quad \text{with}\ \ a_0 = a_2 = a_3 = a_7 = a_{16} = 0\,;\\ &a_{h+3} = 2a_{h+2} - 4a_h \ \ \text{and}\ \ a_0 = 0\,,\ a_1 = 1\,,\ a_2 = 0 \quad \text{with}\ \ a_0 = a_2 = a_3 = a_8 = a_{24} = 0\,. \end{aligned}$$

The diophantine inequalities of Beukers and Tijdeman [7] underlie this study. The discussion [67] provides instructive reading.

5.3.5 Beukers and Tijdeman [7] show *inter alia* that a nondegegenerate binary recurrence sequence of multiplicity four or more is a recurrence sequence of algebraic numbers. Applying deep techniques from the theory of diophantine approximation, they provide an absolute bound, of sorts, in the algebraic case.

5.3.6 If an exponential polynomial $a(z) = \sum_{i=1}^{m} A_i(z) e^{z \log \alpha_i}$ of order n has real frequencies $\log \alpha_i$ then it has at most $n-1$ real zeros. This is just problem 75 of [45], Part V, Chap.1

† It is great fun allowing a spreadsheet to display such examples.

and is a simple application of Rolle's theorem. It follows immediately that a nonconstant recurrence sequence with real nonnegative roots and of order n has 0-multiplicity at most $n-1$ and multiplicity at most n. For recurrence sequences with real roots one observes that if there are as many as $2n-1$ zeros then at least n have the same parity, and, without loss of generality, that parity may be taken to be even. That yields a recurrence sequence with nonnegative real roots and with 0-multiplicity at least n. Aside from trivially degenerate cases, it follows that a recurrence sequence with real roots and of order n has 0-multiplicity at most $2n-2$.

5.3.7 A recent paper of Deshommes [23] approaches the matter of the 0-multiplicity of ternary integer recurrence sequences from a new direction; or rather, by classical methods — the spirit of her detailed and delicate investigation is that of §75 of the bible of cubic matters [22]. Together with the relatively straightforward parts of Beuker's manuscript [6] her results and arguments should help to confirm the belief that the 0-multiplicity of a nondegenerate ternary integer recurrence sequence is at most six and that cases with as many as four zeros are already exceptional.

5.3.8 These questions of fine multiplicity of recurrence sequences are very beautiful and deserve further study.

6. Discovering Rational Functions

6.1 Polynomials

6.1.1 The following theorem of Davenport, Lewis and Schinzel [21] influences my remarks and speculations: *Let $f(X,Y)$ be a polynomial with integer coefficients. Suppose that every arithmetic progression contains some integer x so that the equation $f(x,Y)=0$ has an integral solution y. Then there exists a polynomial $g(X)$ with rational coefficients so that $f(X,g(X))=0$ identically.* Notice, in explanation of the title of this Chapter, that one 'discovers' the polynomial g.

6.1.2 The condition "every arithmetic progression contains some integer $x\ldots$" is, of course, the same as "every arithmetic progression contains infinitely many integers $x\ldots$". In our contexts, that will always be tantamount to "$\ldots$every nonegative integer $x\ldots$". The reason is as at 3.6.1 in the proof of the Lech-Mahler theorem.

6.1.3 In the spirit of the results and conjectures mentioned below, I feel compelled to suggest that a natural generalisation of the theorem will read: "Let $f(X,Y)$ be a polynomial over a field $\mathbf{F}$ of characteristic zero and suppose that every arithmetic progression contains some integer x for which the equation $f(x,Y)=0$ has a solution y in a given ring R finitely generated over $\mathbf{Z}$. Then there exists a polynomial $g(X)$ so that $f(X,g(X))=0$ identically."

6.1.4 I mention these matters because much of the content of the results, conjectures and speculations which follow is a matter of replacing "polynomial" by "exponential polynomial" in the data of the remarks above.

6.1.5 Actually, for polynomials a great deal more is known. I quote (in small part) from [20]: Siegel's theorem (together with specialisation arguments) yields a theoretically complete answer as to whether the diophantine equation $f(X,Y) = 0$, with $f(X,Y) \in \mathbf{F}[X,Y]$ has infinitely many solutions $(X,Y) \in R^2$; here R is, as above, finitely generated over $\mathbf{Z}$ — so we are speaking of (generalised) integer solutions. There are infinitely many solutions if and only if there is a rational parametric solution of a special form. More loosely (thus yet more in my words): there are infinitely many solutions if and only if it is obvious on grounds of shape and structure (in retrospect, at any rate) that there are infinitely many solutions.

6.1.6 The theorem at 6.1.1 has generalisations. For example, Ribenboim [50] considers polynomials in several variables over arbitrary fields.

6.1.7 It is not clear to me whether the analogy between polynomials and exponential polynomials is proper or is only accidental. Certainly, the arguments are rather different. A polynomial (in a single variable) has just finitely many zeros. One uses that to simplify the situation to one involving just linear polynomials; at which point the claims become evident. The argument for exponential polynomials is necessarily quite different.

6.2 The Pólya-Cantor Lemma

6.2.1 *Let $\sum a_h X^h$ be a power series with coefficients belonging to a finitely generated ring R and let by f be a polynomial. If $\sum f(h)a_h X^h$ is a rational function then so is $\sum a_h X^h$.* Note that the enunciation commences with: "If $\sum a_h X^h$ is possibly rational…".

6.2.2 To see the claim it suffices by induction on the degree of f (and given our remarks at 4.2 on specialisation) to deal with $f(h) = h - \theta$, with θ algebraic. One selects appropriate rational primes p admissible as at 3.5.5 and prime to θ. Then there are integers k so that $k - \theta \equiv 0 \mod p$ and that of course entails $k + hp \equiv \theta \mod p$ for all $h \in \mathbf{Z}$. We obtain

$$(k + hp - \theta)a_h = \sum_{i=1}^{m} B_i(k + hp)\alpha_i^{k+hp} \equiv \sum_{i=1}^{m} B_i(\theta)\alpha_i^{k+h} \mod p\,.$$

Assuming, as we may, that the difference product of the α_i is not $0 \mod p$ it follows that

$$B_i(\theta) \equiv 0 \mod p\ .$$

We have this for each i and infinitely many p. Thus $B_i(h) = (h - \theta)A_i(h)$ for polynomials $A_i(h)$ and so $a_h = \sum_{i=1}^{m} A_i(h)\alpha_i^h$, verifying the lemma.

6.2.3 The general result is due to David Cantor [16]; the original notion is that of Pólya [44]. We have: if the derivative of a possibly rational power series (as at 1.2) is rational then the given possibly rational series is in fact rational. Thus, rather remarkably, if $\sum a_h X^h$ is possibly rational, a seemingly weak arithmetic condition on the sequence of Taylor coefficients (a_h), then the rationality of the series $\sum h a_h X^h$ entails that all its poles have multiplicity greater than one.

6.2.4 Bézivin [11] points out that if D denotes the differential operator d/dX then the Pólya-Cantor lemma asserts that: Suppose that the power series $y(X)$ is possibly rational. If f is a polynomial over the ground field $\mathbf{F}$ and L is any differential operator of the shape $L = f(XD)$ then the rationality of Ly entails the rationality of y.

6.3 The Hadamard Quotient Theorem

6.3.1 *Let* $\mathbf{F}$ *be a field of characteristic zero and* (a'_h) *a sequence of elements of a subring* R *of* $\mathbf{F}$ *which is finitely generated over* $\mathbf{Z}$. *Let* $\sum b_h X^h$ *and* $\sum c_h X^h$ *be formal series over* $\mathbf{F}$ *representing rational functions. Denote by* J *the set of integers* $h \geq 0$ *such that* $b_h \neq 0$. *Suppose that* $a'_h = c_h/b_h$ *for all* $h \in J$. *Then there is a sequence* (a_h) *with* $a_h = a'_h$ *for* $h \in J$, *such that the series* $\sum a_h X^h$ *represents a rational function.*

6.3.2 This is a far-reaching generalisation of the result of Pólya-Cantor. It asserts that if the Hadamard quotient of two rational functions is possibly rational then it is indeed rational. Pisot's conjecture to this effect, in the special case that the quotient has Taylor coefficients in $\mathbf{Z}$, is cited by Benzaghou [3], Appendice. The steps of my proof are detailed in [75] and the lecture notes of Rumely [57] provide a full account, almost from first principles. There are descriptions of earlier, more clumsy, versions of my proof in [72] and [74]. The proof fills the gaps in the claims made by Pourchet [49].

6.3.3 We note that the Hadamard Quotient Theorem asserts: If exponential polynomials $c(z)$ and $b(z)$ have the property that the quotients $c(h)/b(h)$ of their values at the nonnegative integers happen all to belong to a finitely generated ring R, then $b(z)$ divides $c(z)$ in the ring of exponential polynomials. Thus every zero of $b(z)$ in $\mathbf{C}$ is a zero of $c(z)$. The converse sequence of implications is true by Ritt's quotient theorem at 3.3.2 and the remarks opening this paper.

6.3.4 If the dividing recurrence sequence (b_h) has, for some absolute value, a unique dominant root, then the arguments required seem less deep. Cantor [17] gives the general proof in this case. Moreover, he remarks that p-adic considerations imply that the 'integrality' of the sequence of quotients (c_h/b_h) entails the 'integrality' of the sequence (c_{-h}/b_{-h}). Thus a minimal root may count as a dominant root. Nevertheless, if the generalised power sum $b(h)$ has order four or more there are examples for which there is no place at which it has a unique dominant root.

6.3.5 Suppose that the given generalised power sums $b(h) = \sum_{i=1}^{m} B_i(h)\beta_i^h$ and $c(h)$ are defined over a number field $\mathbf{K}$ and that, for some place v of $\mathbf{K}$,

$$|\beta_1|_v > |\beta_2|_v \geq \cdots \geq |\beta_m|_v \,.$$

Set $(B_1(h))^{-1}\,\beta_1^{-h} b(h) = 1 - \overline{b}(h)$ and consider, for each nonnegative integer h,

$$\begin{aligned}(B_1(h))^{N+1}\,\beta_1^h a(h) &= (B_1(h))^N\, c(h)\left(1-\overline{b}(h)\right)^{-1}\\ &= (B_1(h))^N\, c(h)\left(1+\overline{b}(h)+\cdots+\left(\overline{b}(h)\right)^N + r_N(h)\right)\\ &= d_N(h) + \overline{r}_N(h)\,.\end{aligned}$$

Here $d_N(h)$ is a generalised power sum (which has dirty big order depending on N) so there is a difference operator F_N, defined over $\mathbf{K}$, annihilating the sequence $(d_N(h))$. We are left with

$$F_N\left((B_1(h))^{N+1}\,\beta_1^h a(h)\right) = F_N\left(\overline{r}_N(h)\right)\,.$$

The integrality data on the a_h guarantees that the sequence on the left has finite height (and that is the only way that this information is used). Furthermore, once N is fixed that height is some number C, independent of N (since N is gobbled up by h going to ∞). Because $|\beta_i/\beta_1|_v < 1$, for $i = 2, \dots, m$, there is a constant $\delta > 0$ so that the remainder on the right has v-adic value less than $\exp(-\delta N h)$ for large h. Fixing N so that $N\delta > C$, as we were free to have done, we now apply the criterion at 4.1.4 (Liouville's theorem) to deduce that, for all sufficiently large h,

$$F_N\left(\left(B_1(h)\right)^{N+1}\beta_1^h a(h)\right) = 0\,.$$

Hence $\left(B_1(h)\right)^{N+1}\beta_1^h a(h)$ is a generalised power sum and, by the Pólya-Cantor lemma, so is $a(h)$, as we wished to show.

It was after coughing for a while that I felt able to conclude with the remark: This quite straightforward argument is very much simpler than that required in the general case when we do not have the use of a dominating root.

6.4 Hadamard Roots of Rational Functions

6.4.1 The following very natural claim remains a conjecture: *Let f be a polynomial and $\sum f(a'_h)X^h$ a formal power series representing a rational function over a field $\mathbf{F}$ of characteristic zero. If the a'_h all belong to subring $R \subset \mathbf{F}$ of finite type over $\mathbf{Z}$ then there is a sequence (a_h), with $f(a'_h) = f(a_h)$ for all $h = 0, 1, \dots$, so that $\sum a_h X^h$ is a rational function.*

6.4.2 I have heard of special cases of the conjecture being attributed to Pisot and to Schutzenberger but know no references other than a mention by Benzaghou [3], Appendice; he remarks that Pisot proves the case $f(a) = a^k$ when the a'_h are in $\mathbf{Z}$ and the given recurrence sequence (b_h), with $b_h = f(a'_h)$, has a unique maximal root with respect to the usual absolute value and that root has multiplicity one.

6.4.3 Only the case $f(a) = a^k$ seems to appear in the literature. The one real advance comes from a paper of Perelli and Zannier [42]. They remove the condition on the multiplicity of the dominant root in the special case when the roots are positive rational integers. Generalising their idea, Rumely and van der Poorten [61] prove that there is no loss of generality in assuming that all the roots are simple and that the data is given over a number field. Our argument, which is in the spirit of that at 6.3.5, does need a unique dominant root, but just in the weak sense described at 6.3.4. However, the argument required to show that a unique minimal root will do is non-trivial; it invokes the Grünwald-Wang theorem (see [2]; 82–83, 93*ff*). Recently, Everest showed me† that the principal argument should deal with arbitrary polynomials f in the unique maximal and simple root case.

6.4.4 Noting that the dominant (and simple) root case is, so to speak, generic, the conjecture at 6.4.1 is not too wild a speculation. The conjecture asserts: If an exponential polynomial $b(z)$ has the property that its values b_h at the nonnegative integers are all of the shape

† Joint work, in progress.

$f(a'_h)$, for some polynomial f and so that $\sum a'_h X^h$ is possibly rational (in the sense of 4.1.7; so that it is a G-function), then there is an exponential polynomial $a(z)$ so that $f(a(z)) = b(z)$ identically. This asserts a great deal about the location of the zeros of $b(z)$ in $\mathbf{C}$; for example, if $f(a) = a^k$, then each zero of b has multiplicity divisible by k. The converse is known (though a new proof in modern notation would be a boon). Ritt [52] proves that if F(Y(z)) is a monic polynomial with exponential polynomial coefficients then its meromorphic zeros are exponential polynomials. Thus, taking $F(Y(z)) = Y^k - b(z)$, if each zero of the exponential polynomial $b(z)$ has multiplicity divisible by k, then there is an exponential polynomial $a(z)$ with $(a(z))^k = b(z)$.

6.5 Matters of Capacity

6.5.1 Let L be a linear differential operator with rational function coefficients and let $y(X)$ be a formal power series which is possibly rational. Bézivin and Robba [13] say that L is a "Pólya operator" if the rationality of Ly entails that y is rational. The operators of 6.2.4 are a very special case.

6.5.2 For a prime ideal $\mathfrak{p}$ of $\mathbf{K}$ denote by $\overline{\mathbf{K}}_\mathfrak{p}$ the associated residue field; similarly let $L_\mathfrak{p}$ be the reduction of an operator $L \in \mathbf{K}(X)[D]$, whenever that is defined (as it is for all but a finite number of $\mathfrak{p}$). I quote, without explanation, the main result of [13]:
Let $\mathbf{K}$ be a number field and let $L \in \mathbf{K}(X)[D]$ be a differential operator. Suppose that
(a) *0 is not an irregular singularity of L, and*
(b) *there is an infinite set S of prime ideals of $\mathbf{K}$ with*

$$\sum_{\mathfrak{p}\in S,\, \mathfrak{p}|p} \frac{1}{p} \log p = \infty ,$$

such that for all $\mathfrak{p} \in S$ the reduced equation $L_\mathfrak{p} y = 0$ has no nonzero solution in $\overline{\mathbf{K}}_\mathfrak{p}((X))$. Then L is a Pólya operator.

6.5.3 The following result of Bézivin [12] appears to have a different flavour:
For $i = 1, \ldots, m$ let a_i and b_i be sets of complex numbers with $|a_i| < 1$; denote by g_i the maps $g_i : \mathbf{C} \to \mathbf{C} : z \mapsto a_i z + b_i$. Let $\mathcal{A} \subseteq \mathbf{C}$ be the intersection of all subsets of $\mathbf{C}$ containing the origin and stable under the maps g_i. Finally let $f_0, f_1, \ldots, f_m$ be rational functions. If the formal power series $y(X)$ satisfies the functional equation

$$y(X) = f_0(X) + \sum_{i=1}^{m} f_i(X) y\left(\frac{a_i X}{1 + b_i X}\right) ,$$

and the transfinite diameter $\gamma(\mathcal{A})$ *of the set $\mathcal{A}$ is strictly less than 1, then $y(X)$ is the Taylor series of a rational function.*

6.5.4 The rationality criteria mentioned at 4.4.7 (see [1], chapitre 5) assert, in simplest form:
If $f(z) = \sum_{h=-N}^{\infty} a_h z^{-h}$ is a convergent Laurent series with rational integer coefficients which has a meromorphic continuation to $\mathbf{C}\backslash E$ then $f(z)$ is rational if E has transfinite diameter $\gamma(E) < 1$.

It is peculiarly uninstructive to explain that the transfinite diameter of E is given by

$$\lim_{h\to\infty} \max_{\{z_1,\dots,z_h\}\in E} \Big(\prod_{i\neq j} |z_i - z_j|\Big)^{1/(h^2-h)} .$$

It may be more helpful (*cf* 4.1.3) to claim that it is also given by $e^{-V(E)}$, where

$$V(E) = \inf_{\nu(E)=1} \int\!\!\int_{E\times E} -\log|x-y| d\nu(x) d\nu(y) ,$$

with the inf taken over all probability measures on E.
The vanishing criterion at 4.1.4 together with the discussion at 4.4.1-2 does an equivalent job to the rationality criterion just cited; so one must be a reformulation of the other. I found it instructive to compare the proof given at 6.3.5 with the original proof of Cantor [17]. The two must be the same, but this is not obvious at a glance. Indeed, 6.3.5 is my idiosyncratic reconstruction, from memory, of Cantor's proof. I boggled slightly when I happened to look subsequently at his actual argument, which relies on notions introduced above.

6.5.5 Underlying all this is a grand theory of "capacity on algebraic curves", currently being written by Rumely [59]; see [55], [56] and [58]. Rumely's work extends a theory for the projective line due to David Cantor [18]; the introduction to this last-mentioned paper is especially useful. The work itself generalises an old result of Fekete and Szegő.

6.5.6 We have not as yet succeeded in finding a capacity-theoretic interpretation of the proof of the Hadamard Quotient Theorem. Notwithstanding the generality and sophistication of the results discovering rational functions just mentioned, I have the impression that all rely on the equivalent of unique dominant root situations.

6.6 Finite Data

6.6.1 The preceding sections have dealt with generalised power sums taking values of some given shape for all $h \in \mathbf{N}$; or, equivalently, for an h in every arithmetic progression. It seems safe to speculate that a nondegenerate generalised power sum takes values of given shape only finitely many times, unless it is itself of that shape and takes such values for all h.

6.6.2 Such wild statements should be carefully qualified. For example, if $\alpha_1\alpha_2 = -1$, the Lucas sequence (a_h), with recurrence relation $a_{h+2} = (\alpha_1+\alpha_2)a_{h+1}+a_h$, and initial values $a_0 = 2$, $a_1 = \alpha_1 + \alpha_2$, satisfies $a_{2h} = a_h^2 + 2(-1)^{h+1}$. Thus the nondegenerate recurrence sequence (a_h) has infinitely many values of the shapes $X^2\pm 2$ without, too blatantly, having those shapes. Of course, one might argue that the trouble comes from the degeneracy of the recurrence sequence (a_h^2), but that is not altogether a convincing excuse; a better approach is to beware of simple exponential polynomials.

6.6.3 There are results, though they are restricted to cases in which Baker's method, or considerable ingenuity, or both may be applied. I defer to the book of Shorey and Tijdeman [65] for references and discussion; papers by London and Finkelstein (*aka* Steiner), Nemes and Pethő, Pethő, Shorey, and Shorey and Stewart will be of particular interest.

6.7 An Application: Divisibility Sequences

6.7.1 At the First Conference of the Canadian Number Theory Society, Banff 1988, Pethő put to me that I might have insight into an old problem concerning a class of recurrence sequences with amusing divisibility properties. Indeed, it turned out that we could settle the question forthwith. I confine myself, here, to a brief sketch. A detailed proof, with appropriate history and references, is in preparation [43]. Moreover, in response to my sending a copy of this paper* to Bézivin I received a draft of his independent "Solution d'une conjecture de M. Ward sur les suites récurrentes arithmétiques". I use his remarks to avoid an oversight and a blunder.

6.7.2 Consider the Fibonacci numbers (*cf* 2.5)

h	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...
f_h	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	.....

One notices such phenomena as $13 \mid 377$ and $55 \mid 6765$ — the reason is that, respectively, $7 \mid 14$ and $10 \mid 20$. Indeed, the Fibonacci sequence has the interesting property that $h \mid k$ implies $f_h \mid f_k$.

6.7.3 Let $\sum a_h X^h$ represent a rational function defined over a field $\mathbf{F}$ of characteristic zero and vanishing at ∞. Then the sequence of Taylor coefficients (a_h) is called a *divisibility sequence* (or a *suite récurrente arithmétique*) if the set of quotients $\{a_k/a_h : h \mid k\}$ is a subset of a ring R of finite type over $\mathbf{Z}$. (Should $a_h = a_k = 0$, it is useful to define the quotient to be 0.) In the classical, and simpler, formulation one supposes the a_h to be rational integers and for the quotients to belong to $\mathbf{Z}$. However, the more general setting introduces no new problems. We shall show that (a_h) is a divisibility sequence if and only if the generating rational function is either, trivially, just a geometric series, or (up to multiplication by a non-zero constant and an easily overlooked rational function $(XD)^k(1-X)^{-1}$ with $D = d/dX$) the Hadamard product of rational functions $X/s(X)$ with s a quadratic polynomial with distinct zeros.

6.7.4 Recall the factorisation theory in the ring of exponential polynomials (see 3.2.3) whereby an exponential polynomial in the variable z is a product of irreducible exponential polynomials, simple exponential polynomials and a (readily overlooked) polynomial in z. Let d be a rational integer $d > 1$. If $f(z)$ is an irreducible exponential polynomial then $f(dz)$ is not divisible (by virtue of its irreducibility!) by $f(z)$ in the ring of exponential polynomials; nor can $f(z)$ divide any irreducible exponential polynomial other than its own associates. Simple exponential polynomials factor into exponential polynomials of the shape $\exp(\omega z) - A$. If a product $g(z)$ of such exponential polynomials is to divide $g(dz)$ in the ring of exponential polynomials for all d then necessarily each A is a root of unity. It is easy to blunder here† by claiming that all the As are necessarily 1; the example $(\exp(\omega z) - 1)(\exp(2\omega z) + 1)(\exp(6\omega z) - 1)$ shows that this is not so. Finally, a

* I nearly perpetrated the crass pleonasm of writing "a copy of an earlier version..."

† At Banff I alleged that Andrew Granville had tried to confuse me on this point; but Bézivin's example shows that I was already confused and that Granville was attempting to alleviate my condition.

polynomial factor $p(z)$ divides an exponential polynomial $f(z)$ if and only if all coefficients of f are divisible by $p(z)$ in the ring of polynomials. Thus if $p(z)$ divides $f(dz)$ for all d, then necessarily $p(z)$ is of the shape Bz^k, some nonzero constant B and some nonnegative integer k.

We may conclude that, if an exponential polynomial $a(z)$ divides $a(dz)$ in the ring of exponential polynomials, for all integers $d > 1$, then $a(z)$ divides a finite product

$$z^k \prod (\exp(\omega_i z) - 1) .$$

6.7.5 By the Hadamard Quotient Theorem, if $a_h \,\big|\, a_{dh}$ for all $h = 0, 1, 2, \ldots$ (in the sense that the quotients all belong to a ring R as described), there is a rational function

$$\sum \frac{a_{dh}}{a_h} X^h ,$$

which is to say, a generalised power sum $b(h) = a(dh)/a(h) \quad h = 0, 1, 2, \ldots$. I allege that analytic continuation $\mathbf{N} \hookrightarrow \mathbf{C}$, yields an identity in exponential polynomials $b(z) = a(dz)/a(z)$. This claim caused some muttering at Banff and from the referee; I therefore add an explanation (though I believe it to be gratuitous): Let $\mathcal{A}$ be the subgroup of $\mathbf{F}^\times$ generated by the roots of the generalised power sum a. If thought desirable, one may suppose that $\mathcal{A}$ is free by replacing h by hl (l being the order of the torsion subgroup) weakening the data. Bézivin has reminded me that Proposition 1 of Rumely and van der Poorten [60] states that the given generalised power sum identity entails that the roots of the generalised power sum b belong to the group generated by $\mathcal{A}$ and $\mathcal{A}^d$, that is, to $\mathcal{A}$. Thus, given a minimal generating set for $\mathcal{A}$, a selection of a logarithm of each of the generators effects the claimed continuation.

Hence, if (a_h) is a divisibility sequence then, after multiplying by a congenial unit of the ring of exponential polynomials, we see that there is a recurrence sequence

$$\overline{a}_h = Ah^k \prod_i \left(\frac{\alpha_i^h - \beta_i^h}{\alpha_i - \beta_i} \right) ,$$

and $a(h)$ divides $\overline{a}(h)$ in the ring of generalised power sums.

References

[1] Yvette Amice, *Les nombres p-adiques*, Presses Universitaires de France (1975)

[2] E. Artin and J. Tate, *Class Field Theory*, Harvard University

[3] Benali Benzaghou, 'Algèbres de Hadamard', *Bull. Soc. Math. France* **98** (1970), 209–252

[4] J. Berstel and M. Mignotte, 'Deux propriétés décidables des suites récurrentes linéaires, *Bull. Soc. Math. France* **104** (1976), 175–184

[5] F. Beukers, 'The multiplicity of binary recurrences', *Compositio Math.* **40** (1980), 251–267

[6] F. Beukers, 'The zero-multiplicity of ternary recurrences', manuscript (c.1982)

[7] F. Beukers and R. Tijdeman, 'On the multiplicities of binary complex recurrences', *Compositio Math.* **51** (1984), 193–213

[8] Jean-Paul Bézivin, 'Factorisation de suites récurrentes linéaires et applications', *Bull. Soc. Math. France*, **112** (1984), 365–376

[9] Jean Paul Bézivin, 'Diviseurs premiers de suites récurrentes linéaires, *Europ. J. Combin.* **7** (1986), 199–204

[10] Jean Paul Bézivin, 'Sur les diviseurs premiers des suites récurrentes linéaires, *Ann. Fac. des Sciences de Toulouse* **8** (1986-1987), 61–73

[11] Jean-Paul Bézivin, 'Une propriété arithmétique de certains opérateurs différentiels, *Manuscripta Math.* **61** (1988), 103–129

[12] Jean-Paul Bézivin, 'Solutions rationnelles de certaines équations fonctionnelles', *Aequationes Math.*

[13] J. -P. Bézivin and P. Robba, 'Rational solutions of linear differential equations', *J. Austral. Math. Soc.* **44** (1988)

[14] E. Bombieri, 'On G-functions', in H. Halberstam and C. Hooley, eds., *Recent progress in analytic number theory*, Academic Press (1981), Chapter 24, Vol. 2, 1–67

[15] David G. Cantor, 'On arithmetic properties of coefficients of rational functions', *Pacific J. Math.* **15** (1965), 55–58

[16] David G. Cantor, 'On arithmetic properties of the Taylor series of rational functions', *Canad. J. Math.* **21** (1969), 378–382

[17] David G. Cantor, 'On arithmetic properties of the Taylor series of rational functions II', *Pacific J.Math.* **41** (1972), 329–334

[18] David G. Cantor, 'On an extension of the definition of transfinite diameter and some applications', *J. für Math.* **316** (1980), 160–207

[19] J. W. S. Cassels, 'An embedding theorem for fields', *Bull. Austral. Math. Soc.* **14** (1976) 193–198; Addendum: *ibid* **14** (1976) 479–480

[20] H. Davenport, D. J. Lewis and A. Schinzel, 'Equations of the form $f(x) = g(y)$', *Quart. J. Math.* **12** (1961), 304–312

[21] H. Davenport, D. J. Lewis and A. Schinzel, 'Polynomials of certain special types', *Acta Arith.* **9** (1964), 107–116

[22] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, American Mathematical Society Translations of Mathematical Monographs, vol **10** (1964)

[23] Bernadette Deshommes, 'Sur les zéros des fonctions symétriques complètes (cas cubique)', to appear; see also a report at *Groupe d'étude d'analyse ultramétrique (Amice, Christol, Robba)*, Inst. Henri Poincaré, Paris (1986/87)

[24] Ahmad Diab, 'Sur les zéros communs des polynômes exponentiels', *C. R. Acad. Sc. Paris*, **281** (1975), A757–758

[25] Ahmad Hajj Diab, *Arithmétique des polynômes exponentiels*, Thèse 3^{e} cycle, Université de Bordeaux (1976)

[26] G. R. Everest and A. J. van der Poorten, 'The ring of exponential polynomials', (in preparation)

[27] Jan-Hendrik Evertse, 'On sums of S-units and linear recurrences', *Compositio Math.* **53** (1984), 225–244

[28] J. -H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, 'S-unit equations and their application', Report **W 87-03**, Mathematical Institute, University of Leiden (januari, 1987), to appear in A Baker, ed. *Proceedings of the Durham Symposium on Transcendence Theory* (1986)

[29] J. P. Glass, J. H. Loxton and A. J. van der Poorten, 'Identifying a rational function', *C. R. Math. Rep. Acad. Sci. Canada* **3** (1981), 279–284

[30] Neal Koblitz, *p-Adic numbers, p-adic analysis, and zeta-functions*, Springer GTM **58** (1977)

[31] K. K. Kubota, 'On a conjecture of M. Ward', I: *Acta Arith.* **33** (1977), 11–28; II: *ibid* 29–48; III: *ibid* 99–109

[32] V. Laohakosol, J. H. Loxton and A. J. van der Poorten, 'Integer p-adic functions', *Macquarie Math. Reports*, **87-0008** (June, 1987) = *Coll. Math. Soc. János Bolyai*(Budapest, 1987)

[33] Christer Lech, 'A note on recurring series', *Ark. Mat.* **2** (1953), 417–421

[34] Leonard Lipshitz and Alfred J. van der Poorten, 'Rational functions, diagonals, automata and arithmetic,' in R. A. Mollin, ed. *First Conference of the Canadian Number Theory Association* (Banff, 1988), Walter de Gruyter and Co. (1989)

[35] J. H. Loxton and A. J. van der Poorten, 'On the growth of recurrence sequences', *Math. Proc. Camb. Phil. Soc.* **81** (1977), 369–376

[36] J. H. Loxton and A. J. van der Poorten, 'Multiplicative dependence in number fields', *Acta Arith.* **42** (1983), 291–302

[37] K. Mahler, 'Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen', *Proc. Akad. Wet. Amsterdam* **38** (1935), 51–60

[38] K. Mahler, 'On the Taylor coefficients of rational functions', *Proc. Camb. Phil. Soc.* **52** (1956), 39–48; 'Addendum', *ibid.* **53** (1957), 544

[39] Kurt Mahler, *Lectures on Transcendental Numbers*, Springer Lecture Notes in Mathematics **546** (1976)

[40] D. W. Masser, 'Specializations of finitely generated subgroups of abelian varieties', manuscript (c.1986)

[41] Maurice Mignotte, 'Suites récurrentes linéaires', *Sém. Delange-Pisot-Poitou*, Inst. Henri Poincaré, Paris, 15e année (1973/74), n°G14

[42] A. Perelli and U. Zannier, 'Arithmetic properties of certain recurrence sequences', *J. Austral. Math. Soc. (Ser. A)* **37** (1984), 4–16

[43] Attila Pethő and Alfred J. van der Poorten, 'A full characterisation of divisibility sequences' (tentative title; in preparation*)

[44] G. Pólya, 'Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen', *J. für Math.*, **151** (1920), 1–31

[45] G. Pólya and G. Szegő, *Problems and theorems in analysis*, Springer-Verlag (4th edition; translation 1976)

[46] A. J. van der Poorten and Robert S. Rumely, 'Zeros of p-adic exponential polynomials II', *J. Lond. Math. Soc.* (2) **36** (1987), 1–15

[47] A. J. van der Poorten and H. P. Schlickewei, 'The growth conditions for recurrence sequences', *Macquarie Math. Reports* **82-0041** (August, 1982) Macquarie University, Australia 2109

[48] A. J. van der Poorten and R. Tijdeman, 'On common zeros of exponential polynomials', *L'Ens. Math. II*$^{\rm e}$ *Série*, **21** (1975), 57–67

[49] Yves Pourchet, 'Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles', *C. R. Acad. Sc. Paris* **288** (1979), A1055–1057

[50] P. Ribenboim, 'Polynomials whose values are powers', *J. für Math.* **268/269** (1974), 34–40

[51] J. F. Ritt, 'A factorisation theory for functions $\sum_{i=1}^{n} a_i e^{\alpha_i z}$ ', *Trans. Amer. Math. Soc.*, **29** (1927), 584–596

[52] J. F. Ritt, 'Algebraic combinations of exponentials', *Trans. Amer. Math. Soc.* **31** (1929), 654–679

[53] J. F. Ritt, 'On the zeros of exponential polynomials', *Trans. Amer. Math. Soc.*, **31** (1929), 680–686

[54] Philippe Robba, 'Zéros de suites récurrentes linéaires', *Groupe d'étude d'analyse ultramétrique (Amice, Barsky, Robba)*, Inst. Henri Poincaré, Paris (1977/78) n°13

[55] Robert Rumely, 'Capacity theory on algebraic curves and canonical heights', *Groupe d'étude d'analyse ultramétrique (Amice, Christol, Robba)*, Inst. Henri Poincaré, Paris (1984/85) n°22

[56] Robert Rumely, 'Arithmetic over the ring of all algebraic integers', *J. für Math.* **368** (1986), 127–133

[57] Robert S. Rumely, 'Notes on van der Poorten's proof of the Hadamard Quotient Theorem', *Sém. Théorie des Nombres de Paris* 1986-87, Birkhäuser (1988)

[58] Robert Rumely, 'A Fekete-Szegő theorem with splitting conditions', *J. für Math.*

[59] Robert Rumely, *Capacity Theory on Algebraic Curves*, (in preparation)

[60] Robert S. Rumely and A. J. van der Poorten, 'Remarks on generalised power sums', *Bull. Austral. Math. Soc.* **36** (1987), 311–329

[61] Robert S. Rumely and A. J. van der Poorten, 'A note on the Hadamard kth root of a rational function', *J. Austral. Math. Soc. (Ser. A)* **43** (1987), 314–327

* *Added in proof*: This will become a joint paper with Jean-Paul Bézivin.

[62] Andrzej Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor (1982)

[63] H. S. Shapiro, 'The expansion of mean-periodic functions in series of exponentials', *Comm. Pure and Appl. Math.* , **11** (1958), 1–21

[64] Alan Shields, 'On quotients of exponential polynomials', *Comm. Pure and Appl. Math.*, **16** (1963), 27–31

[65] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press (1986)

[66] T. Skolem, 'Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen', *Comptes rendus du 8e congrès des mathématiciens scandinaves* (Stockholm, 1934), 163–188 (Lund, Hakan Ohlssons Boktryckeri, 1935)

[67] R. Tijdeman, 'Multiplicities of binary recurrences', *Séminaire de théorie des nombres de Bordeaux*, année 1980-1981, exp. n°29

[68] E. C. Titchmarsh, *The theory of functions*, Oxford University Press (1952)

[69] A. J. van der Poorten, 'A note on the zeros of exponential polynomials', *Compositio Math.* **31** (1975) 109–113

[70] A. J. van der Poorten, 'On the number of zeros of functions', *L'Ens. Math. II*$^{\text{e}}$ *Série*, **23** (1977), 19–38

[71] A. J. van der Poorten, 'Identification of rational functions; lost and regained', *C. R. Math. Rep. Acad. Sci. Canada* **4** (1982), 309–314

[72] A. J. van der Poorten, 'Hadamard operations on rational functions', *Groupe d' étude d'analyse ultramétrique (Amice, Christol, Robba)*, Inst. Henri Poincaré, Paris (1982/83) n°4

[73] A. J. van der Poorten, 'Some problems of recurrent interest', *Coll. Math. Soc. János Bolyai*(Budapest, 1981) **34** *Topics in Number Theory* North Holland (1984), 1265–1294

[74] A. J. van der Poorten, 'p–Adic methods in the study of Taylor coefficients of rational functions', (to Kurt Mahler on his 80th birthday), *Bull. Austral. Math. Soc.* **28** (1984), 109–117

[75] Alfred J. van der Poorten, 'Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles', *C. R. Acad. Sc. Paris* **306** Série 1, (1988), 97–102

[76] P. A. Vojta, *Integral points on varities*, PhD Thesis, Harvard University (1983)

[77] Marc Voorhoeve, 'On the oscillation of exponential polynomials', *Math. Z.*, **151** (1976), 277–294

[78] Marc Voorhoeve, *Zeros of exponential polynomials*, PhD Thesis, Leiden (1977)