BULL. AUSTRAL. MATH. SOC.
VOL. 36 (1987) 311-329

11B37

REMARKS ON GENERALISED POWER SUMS

ROBERT S. RUMELY AND A.J. VAN DER POORTEN

We give a description of factorisation in the ring of generalised power sums (the sequence of Taylor coefficients of rational functions regular at infinity) with a view to giving detailed bounds on the order of generalised power sum factors and roots of such sums.

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

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

with *roots* α_i, $1 \le i \le m$, distinct nonzero 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*

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

Received 3 November 1986. The first author was supported in part by a Sloan Foundation Fellowship and by N.S.F. grant 8201792. An earlier draft of this note was written whilst the second author was visiting the Institute for Advanced Study, Princeton, N.J. This work was supported in part by A.R.G.S. grants B7915731 and B8215893.

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

Set

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

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

$$a_{h+n} = s_1 a_{h+n-1} + \ldots + s_h a_h, \quad h = 0,1,2,\ldots$$

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

$$(E-\alpha)A(h)\alpha^h = (\Delta A(h))\alpha^{h+1}, \quad h = 0,1,2,\ldots$$

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 *recurrence sequences*. It follows that there is a polynomial $r(X)$, of degree less than n, so that the power series

$$\sum_{h=0}^{\infty} a_h X^h = r(x)/s(x)$$

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

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

$$r(x)/s(x) = \sum_{i=j}^{m} \sum_{j=1}^{n(i)} r_{ij}(1-\alpha_i X)^{-j}$$

$$= \sum_{h=0}^{\infty} \left(\sum_{i=1}^{m} \sum_{j=1}^{n(i)} r_{ij} \begin{pmatrix} h+j-1 \\ j-1 \end{pmatrix} \alpha_i^h \right) X^h$$

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

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

Accordingly, results on generalised power sums are equivalent to corresponding results for Taylor expansions of rational functions. For example: the trivial observation that a product of generalised power sums is again a generalised power sum becomes the more interesting: the *Hadamard product*

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

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

Our remarks below concern factorisation in the ring of generalised power sums, thus Hadamard factorisation of rational functions. Our observations are closely related to those of Bézivin [1], who provides a useful unique factorisation result.

1. The ring of generalised power sums

Let F be a field, and W a finitely generated subgroup of $F^{\times}$. Denote by $F_h(W)$ the ring of all generalised power sums with coefficients in F and roots in W ; that is, the set of all functions f of the form

$$f : \mathbb{Z} \to F : f(h) = \sum_{i=1}^{m} F_i(h)\phi_i^h$$

where the coefficients $F_i(h)$ belong to $F[h]$, and the roots ϕ_i to W .

Since confluent Vandermonde determinants are nonsingular the roots and coefficients of such a function are determined by its values: thus two elements of $F_h(W)$ are the same if and only if they are formally identical. We describe the structure of the ring $F_h(W)$. By the fundamental theorem of finitely generated abelian groups

$$W \simeq \mathbb{Z}/d \times \mathbb{Z}^s \quad \text{for some } d \text{ and } n .$$

Let $\zeta = \zeta_d$ and $\omega_1, \omega_2, \ldots, \omega_s$ be generators for its torsion and free parts respectively. By our discussion above,

$$F_h(W) = F[h, \zeta^h, \omega_1^h, \omega_1^{-h}, \ldots, \omega_s^h, \omega_s^{-h}]$$

is isomorphic to the ring

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

$$F[h,Z,W_1,W_1^{-1},\ldots,W_s,W_s^{-1}]$$

where $h,W_1,\ldots,W_s$ are algebraically independent elements over F (in more naive terms, independent variables), and Z is a generator for a cyclic group of order d .

First consider the subring

$$F[Z] \simeq F[X]/(X^d-1)$$

Since we are assuming that $\mathcal{W} \subset F^\times$, it follows that $\zeta_d \in F$ so $X^d - 1$ is a product of linear polynomials of the shape $X - \zeta_d^j$ for various integers j . If char$(F) = 0$, then each factor appears with multiplicity 1. So by the Chinese Remainder Theorem

$$F[X]/(X^d-1) \simeq \bigoplus_{1\le j\le d} F[X]/(X-\zeta_d^j)$$

$$\simeq \bigoplus_{1\le j\le d} F$$

is a direct sum of d copies of F : this is of course nothing more than discrete Fourier analysis, and in the context of our generalised power sums above, corresponds to the restriction to various arithmetic progressions $h \equiv j \bmod d$. Then

$$F_h(\mathcal{W}) \simeq \bigoplus_{1\le j\le d} F[h,W_1,W_1^{-1},\ldots,W_s,W_s^{-1}]$$

with the isomorphism corresponding to restriction to arithmetic progressions $h \equiv j \bmod d$, with h replaced by dh , and W_i corresponding to ω_i^{dh} .

Now the ring $F[h,W_1,W_1^{-1},\ldots,W_s,W_s^{-1}]$ is the localisation of the polynomial ring $F[h,W_1,\ldots,W_s]$ with respect to the multiplicative set generated by $W_1,\ldots,W_s$. Since a polynomial ring over a field is a unique factorisation domain, and any localisation of a UFD is again a UFD, it follows that $F[h,W_1,W_1^{-1},\ldots,W_s,W_s^{-1}]$ is a UFD. Its irreducible

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

elements are all associate to irreducible polynomials in $F[h,W_1,\dots,W_s]$ and every such irreducible polynomial except the units $W_1,\dots,W_s$ gives an irreducible element of $F[h,W_1,W_1^{-1},\dots,W_s,W_s^{-1}]$.

The group $\mathbb{W}$ also carries orderings which will be useful below. Set

$$\overline{\mathbb{W}} = \mathbb{W}/\text{torsion} \simeq \mathbb{Z}^s$$

and put

$$\overline{\mathbb{W}}_{\mathbb{Q}} = \overline{\mathbb{W}} \otimes {}_{\mathbb{Z}}\mathbb{Q} \simeq \mathbb{Q}^s$$

For any $w \in \mathbb{W}$, let $\overline{w}$ denote its image in $\overline{\mathbb{W}}$, and regard it as an element of $\overline{\mathbb{W}}_{\mathbb{Q}}$.

Given a basis of $v_1,\dots,v_s$ of $\overline{\mathbb{W}}_{\mathbb{Q}}$, we obtain a corresponding lexicographic ordering of $\overline{\mathbb{W}}_{\mathbb{Q}}$. Explicitly, if

$$u=a_1u_1 +\dots+ a_su_s,\ u'=a_1'u_1 +\dots+ a_s'u_s \quad \text{with the} \quad a_i,a_i' \in \mathbb{Q}$$

define

$$u>u' \Leftrightarrow \text{there is an index } k \text{ such that}$$

$$a_1 = a_1',\dots,a_{k-1} = a_{k-1}', \quad \text{but} \quad a_k > a_k'$$

The lexicographic ordering respects addition: if $v \geq v'$, $w \geq w'$ then $v + w \geq v' + w'$, with equality if and only if $v = v'$, $w = w'$.

Further, we note that for w, $w' \in \mathbb{W}$, we have $\overline{w} = \overline{w}'$ if and only if w and w' differ by a root of unity.

If V is a subgroup of $\mathbb{W}$, all of the above of course applies to the ring $F_h(V)$. In particular, if V is free then $F_h(V)$ is a UFD.

We will now apply these remarks to the study of the factorisation of generalised power sums.

2. Factors of generalised power sums

Let

$$a(h) = \Sigma A_i(h)\alpha_i^h \ , \ b(h) = \Sigma B_j(h)\beta_j^h \ , \ c(h) = \Sigma C_k(h)\gamma_k^h$$

be elements of $F_h(\mathcal{W})$. In practice, we may as well assume that $\mathcal{W}$ is generated by the α_i, β_j and γ_k . Let $\mathcal{A}$ be the subgroup of $\mathcal{W}$ generated by the α_i, $\mathcal{B}$ the subgroup generated by the β_j , and $\mathcal{C}$ the subgroup generated by the γ_k .

It will frequently be useful to be able to speak as if one or more of the groups $\mathcal{W}$, $\mathcal{A}$, $\mathcal{B}$ or $\mathcal{C}$ is free; this can always be achieved by passing to subsequences $h \equiv r \bmod d$. However, if it is appropriate to regard only $a(h)$, or $a(h)$ and $b(h)$ as known and $\mathcal{A}$, or $\langle\mathcal{A},\mathcal{B}\rangle$ is the subgroup generated by the roots in question, it has torsion $\mathbb{Z}/d'$ for some d' dividing d , and it suffices to pass to subsequences mod d' . In any case, the effect is the collapsing together of terms with roots differing just by d-th (respectively d'-th) roots of unity; for example one obtains d generalised power sums

$$\begin{aligned} a_{r,d}(h) &= \sum_{i,j} A_{i,j}(r+hd)\zeta_d^{j(r+hd)}\alpha_i^{r+hd} \\ &= \sum_i \left(\sum_j A_{i,j}(r+hd)\zeta_d^{jr}\alpha_i^r\right)(\alpha_i^d)^h \end{aligned}$$

We note that for each root α_i , there is some $r \bmod d$ for which the coefficient of the corresponding root α_i^d is nonzero. This is plain, because $a(h)$ can be recovered from its restrictions $a_{r,d}(h)$:

$$a(h) = d^{-1}\sum_{r,j=1}^{d} a_{r,d}((h-r)/d)\zeta_d^{j(h-r)}$$

PROPOSITION 1. *Suppose* $a(h) = b(h)c(h)$. *Then* $\mathcal{C} \subset \langle\mathcal{A},\mathcal{B}\rangle$.

Proof. First suppose that $\mathcal{B}$ is free, and, fixing a lexicographic ordering on $\overline{\mathcal{W}}_{\mathbb{Q}}$, let β be the unique root of $b(h)$ so that $\overline{\beta}$ is maximal. Suppose that C is not contained in $\langle A,B\rangle$, and let γ be a root of $c(h)$ for which $\gamma \notin \langle A,B\rangle$ and so that $\overline{\gamma}$ is maximal subject to this condition.

There are two possibilities:

(a) There are no other roots β' of $b(h)$, γ' of $c(h)$ so that $\beta\gamma = \beta'\gamma'$. In this case $\beta\gamma$ must appear as a root in $a(h)$, which shows that $\gamma \in \langle A,B\rangle$.

(b) There do exist such roots β', γ'. Since $\overline{\beta}>\overline{\beta}'$ but $\overline{\beta}+\overline{\gamma}=\overline{\beta}'+\overline{\gamma}'$, it must be that $\overline{\gamma}'>\overline{\gamma}$. But this means that $\gamma' \in \langle A,B\rangle$. Hence $\gamma=\beta^{-1}\beta'\gamma' \in \langle A,B\rangle$ as well.

This concludes the proof in this case.

In the general case, suppose the group of roots of unity in B has order D. By passing to subsequences mod D, which has the effect of replacing the group B by the group of D-th powers B^D, we can conclude that C^D is contained in $\langle A^D,B^D\rangle$. But this means that each element $\gamma \in C$ satisfies

$$\gamma^D = \alpha^D\beta^D$$

for some $\alpha \in A$, $\beta \in B$. Thus $\gamma = \zeta_D^j\alpha\beta$ for some D-th root of unity ζ_D. But since the D-th roots of unity are in B we again have $C \subset \langle A,B\rangle$. □

Recall that the order of a generalised power sum is just the order of the recurrence relation satisfied by its values, or is, equivalently, the order of the difference operator which annihilates the sequence of its values.

PROPOSITION 2. *Suppose* W *is fixed, and* $a(h) \in F_h(W)$. *Suppose also that* $a(h)$ *does not indentically vanish on any arithmetic progression. Then there is a finite upper bound on the order of any divisor of* $a(h)$ *belonging to* $F_h(W)$.

The proof will show that the bound is stable under specialisation preserving the rank of W and the property that $a(h)$ does not vanish on arithmetic progressions mod d . (See Section 5 as well.)

Proof. Let $a(h) = b(h)c(h)$ with $b(h), c(h) \in F_h(W)$. Suppose first that W is free. Then by our discussion above

$$F_h(W) \approx F[h, W_1, W_1^{-1}, \ldots, W_s, W_s^{-1}]$$

and we will identify $a(h)$, $b(h)$ and $c(h)$ with elements of this latter ring. By multiplying $a(h)$ by an appropriate element of W (a monomial in the W_j), we can suppose that $a(h)$ belongs to the polynomial ring $F[h, W_1, \ldots, W_s]$ and is not divisible by any of the W_j . By Gauss' Lemma, each of $b(h)$ and $c(h)$ is associate to a polynomial divisor of $a(h)$ in $F[h, W_1, \ldots, W_s]$. Note that the operation of obtaining an associate corresponds to multiplying a generalised power sum by nonzero constants and monomials in the ω_j^h , which does not change its order. By our hypothesis, $a(h)$ is not the zero polynomial. Let N_0 be its degree in h , and N_j its degree in W_j , for $j=1,2,\ldots,s$. These numbers are obvious bounds on the degrees of the corresponding variables in the divisor $b(h)$. Thus the order of $b(h)$ can be no greater than

$$N = (N_0 + 1)(N_1 + 1) \ldots (N_s + 1) .$$

In the general case let d be the number of roots of unity in W , Then by passing to subsequences $h \equiv r \bmod d$, we can arrange that

$$a(r + hd) = b(r + hd)c(r + hd)$$

is a factorisation taking place in $F_h(W^d)$, with W^d free. Then for each r we obtain a bound $N^{(r)}$ for the order of

$$b_{r,d}(h) = b(r + hd) .$$

But on recalling the formula whereby we may recover $b(h)$ from the $b_{r,d}(h)$ it follows that the order of $b(h)$ is certainly no greater than

$$d(N^{(1)} + N^{(2)} + \ldots + N^{(d)}) \qquad \square$$

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

We can summarise the content of these propositions in the following informal manner: *Suppose it is alleged that* $b(h)$ *might divide* $a(h)$ *in the ring of generalised power sums. Then there is an a priori bound on the order of the cofactor* $c(h)$. For by Proposition 1 we can take for W the group $\langle A, B\rangle$, and by Proposition 2, the order of $c(h)$ is then bounded.

3. Roots of generalised power sums

The following proposition yields a similar allegation concerning the order of a putative k-th root of a generalised power sum.

PROPOSITION 3. *Suppose* $a(h) = \{b(h)\}^k$ *for some generalised power sum* $b(h)$ *and some positive integer* k. *Let* $A^{1/k}$ *be the group consisting of all possible* k-*th roots of elements of* A. *Denote by* L *the field obtained by adjoining to* F *all the* k-*th roots of the coefficients and the roots of* $a(h)$. *Then there exists a generalised power sum* $\hat{b}(h)$ *belonging to* $L_h(A^{1/k})$, *such that*

$$a(h) = \{\hat{b}(h)\}^k .$$

(Note that there is no loss of generality in assuming from the outset that $L = F$*).*

The proof will show that the bound is stable under specialisation preserving the rank of W and the property that $a(h)$ does not vanish on arithmetic progressions mod d.

Proof. Let $W = B$ be the group generated by the roots of $b(h)$; obviously A is a subgroup of W.

First suppose that A is free. Fix a lexicographic ordering of $\overline{W}_{\mathbb{Q}}$, and let α be the root of $a(h)$ such that $\overline{\alpha}$ is largest under this ordering. Let d be the number of roots of unity in W. We claim that the roots β of $b(h)$ for which $\overline{\beta}$ is largest all are of the shape $\zeta_d^j\alpha^{1/k}$ for some d-th root of unity. Let β be a root for which $\overline{\beta}$ is maximal. Then there is an arithmetic progression $h=r+ld$ for

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

which β^d occurs as a root of

$$b_{r,d}(l) = b(r + ld) .$$

The roots of $b_{r,d}(l)$ belong to W^d, which is free. Hence β^d is the unique maximal root, and it follows that $(\beta^d)^k = \alpha^d$, since $(\beta^d)^k$ is the unique maximal product of any k roots of $b_{r,d}(l)$. This shows that $\beta = \zeta_d^j \alpha^{1/k}$, (after possibly replacing d by kd and enlarging W).

Let $A(h)$ be the coefficient of α^h in $a(h)$ and denote by $B_j(h)$ the coefficient of $(\zeta_d^j \alpha^{1/k})^h$ in $b(h)$. The only terms of $b(h)$ which can possibly contribute to $A(h)$ are the terms $b_j(h)(\zeta_d^j \alpha^{1/k})^h$, $j=0,1,\ldots,d-1$. Hence, having fixed a k-th root $\alpha^{1/k}$ of α once and for all, we have

$$\left[\sum_{j=1}^{d} B_j(h)(\zeta_d^j \alpha^{1/k})^h\right]^k = A(h)\alpha^h ,$$

or

$$\left[\sum_{j=1}^{d} B_j(h)\zeta_d^{jh}\right]^k = A(h)$$

Restricting to a subsequence $h=r+ld$ as before, it follows that, for each r

$$\left[\sum_{j=1}^{d} B_j(r + ld)\zeta_d^{jr}\right]^k = A(r + ld)$$

But it is well-known, [4], that this implies the same equation viewed as an identity in polynomials in l. Thus we can see that $A(r+ld)$ is the k-th power of a polynomial in l, whence $A(h)$ is the k-th power of a polynomial in h. We will wet

$$A(h) = \{P(h)\}^k$$

Comparing equations, we see that for each r there is a k-th root of unity $\zeta_k(r)$ such that for all integers l,

$$\sum_{j=1}^{d} B_j(r + ld)\zeta_d^{jr} = \zeta_k(r)P(r + ld) .$$

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

Hence substituting $l = (h-r)/d$ as we may, and solving inversely, we obtain

$$B_j(h) = \{d^{-1} \sum_{r=1}^{d} \zeta_k(r)\zeta_d^{-jr}\} P(h) = c_j P(h)$$

for an appropriate constant c_j .

But the function $r \to \zeta_k(r)$ is periodic with period d . Hence there is a generalised power sum $f(h)$ of the form

$$\sum_{j=1}^{d} F_j(\zeta_d^j)^h = f(h) \ , \ F_j \in \mathbb{Q}[\zeta_d, \zeta_k]$$

such that $f(h)=\zeta_k(h)^{-1}$ for all integers h . We set

$$\hat{b}(h) = f(h)b(h) \ .$$

By our construction, for each r mod d , the coefficient of $(\alpha^{1/k})^{ld}$ in $\hat{b}(r+ld)$ is

$$P(r + ld)(\alpha^{1/k})^r$$

But the collection of leading terms of $\hat{b}(h)$, with respect to our lexicographic ordering, can also be written as

$$\sum_{j=0}^{d-1} Q_j(h)(\zeta_d^j\alpha^{1/k})^h \ ,$$

for certain polynomials $Q_j(h)$. Substituting $h=r+ld$, and comparing the two expressions, we see that one solution, and hence the unique solution, for the $Q_j(h)$ is given by

$$Q_o(h) = P(h) \ ; \ Q_j(h) = 0 \ , \ j = 1,2,\ldots,d - 1 \ .$$

Thus under the lexicographic ordering, $\hat{b}(h)$ has a unique maximal root, namely $\alpha^{1/k}$.

We will now see that all the roots of $\hat{b}(h)$ belong to the group $\langle\alpha^{1/k}, A\rangle$.

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

For brevity set $\beta = \alpha^{1/k}$. Suppose our assertion to be false, and let γ be a root of $\hat{b}(h)$ not in $\langle\beta,A\rangle$ for which $\overline{\gamma}$ is maximal. Consider the product $\beta^{k-1}\gamma$. If there is no other products of roots $\gamma_1\gamma_2\cdots\gamma_k$ of $\hat{b}(h)$ equal to $\beta^{k-1}\gamma$, then necessarily $\beta^{k-1}\gamma$ appears as a root of $a(h)$, and so $\gamma \in \langle\beta,A\rangle$. On the other hand, if there is such a product, then in $\overline{\mathcal{W}}_{\mathbb{Q}}$ we have a sum of $\overline{\gamma}$ and $k-1$ copies of $\overline{\beta}$ equalling the sum of the k $\overline{\gamma}_j$'s :

$$\overline{\beta} + \overline{\beta} + \ldots + \overline{\beta} + \overline{\gamma} = \overline{\gamma}_1 + \overline{\gamma}_2 + \ldots + \overline{\gamma}_k \ .$$

Recalling that $\overline{\beta}$ is maximal we see that, because addition in $\overline{\mathcal{W}}_{\mathbb{Q}}$ respects the lexicographic ordering, this equation entails that $\overline{\gamma}_j \geq \overline{\gamma}$ for all j . In fact, even equality, say for $j=k$, implies $\overline{\beta}=\overline{\gamma}_1=\ldots=\overline{\gamma}_{k-1}$. But β is the unique root of $\hat{b}(h)$ of maximal size; hence $\beta=\gamma_1=\ldots=\gamma_{k-1}$ and so $\gamma=\gamma_k$, in contradiction to our having a new set of roots with product β^{k-1} . Hence we must have $\overline{\gamma}_j > \overline{\gamma}$ for all j . But then, by our definition of γ , we must have $\gamma_j \in \langle\beta,A\rangle$ for all j , and it follows that $\gamma=\beta^{-(k-1)}\Pi\gamma_j$ is in $\langle\beta,A\rangle$ after all. This verifies our allegation. We note that of course, $\langle\beta,A\rangle \subset A^{1/k}$.

We now show that the coefficients of $\hat{b}(h)$ belong to the field L described in the Theorem. As usual, it suffices to give the proof assuming that A is free. Write

$$\hat{b}(h) = \sum_{i=1}^{m} \sum_{j=0}^{n(i)-1} \hat{b}_{ij} h^j \gamma_i^h$$

where the $\hat{b}_{ij}$ are constants. Mapping each monomial $h^j\gamma_i^h$ to the ordered pair (j,γ_i) in $\mathbb{N} \times \overline{\mathcal{W}}_{\mathbb{Q}}$, and giving the latter its natural lexicographic ordering, we obtain an ordering on the monomials in $\hat{b}(h)$. Let I and J be such that $h^J\gamma_I^h$ is maximal amongst all terms appearing in $\hat{b}(h)$. Clearly then, $h^{kJ}\gamma_I^{kh}$ is the unique maximal term in $a(h)$,

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

and its coefficient is $\hat{b}_{IJ}^{k}$. Thus $\hat{b}_{IJ}$ belongs to L . Now suggest that not all the coefficients $\hat{b}_{ij}$ belong to L ; and choose i and j so that $h^j\gamma_i^h$ is maximal for those terms. Arguing as in the proof above that the roots of $\hat{b}(h)$ belong to $A^{1/k}$, it follows that the coefficient of

$$(h^J\gamma_I)^{k-1}(h^j\gamma_i^h)$$

in $a(h)$ has the form

$$k\,\hat{b}_{IJ}^{k-1}\,\hat{b}_{ij} + \text{terms belonging to } L ,$$

implying that $\hat{b}_{ij}$ belongs to L as well, in contradiction to our claim. This completes this part of our argument.

We have proved all the above on the assumption that A is free. If this is not the case and D is the number of roots of unity in A , then by passing to subsequences mod D , and assembling the results as above, we obtain the general result:

$$\hat{b}(h) = \sum_{r,j=1}^{D} D^{-1}\,\hat{b}_{r,D}((h-r)/D)\zeta_D^{J(h-r)} .$$

Here the roots of each $\hat{b}_{r,D}$ belong to $(A^D)^{1/k}$, and so the roots of $\hat{b}$ belong to $A^{1/k}$, as alleged; similarly, of course, since the coefficients of each $\hat{b}_{r,D}$ belong to L so do the coefficients of $\hat{b}$. □

Combining Propositions 3 and 2, we obtain the assertion that *if the generalised power sum $a(h)$ has a k-th root in the ring of generalised power sums, then it has such a k-th root of order bounded in terms of $a(h)$ alone.*

4. Factorisation Theorems

For completeness, we should mention results of Ritt [5] and of Bezivin [1]. We do so without proof. The following proposition is in effect dealt with *en passant* above (compare Ritt's proof with that of

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

our Proposition 1 above); by $A^{1/\infty}$ we denote the group of all possible roots of elements of A .

PROPOSITION 4. *As before,* $a(h) \in F_h(A)$. *Suppose also that* $a(h)$ *does not identically vanish on any arithmetic progression. Then every factor of* $a(h)$ *in the ring of generalised power sums is the associate of an element with roots in* $A^{1/\infty}$. □

Ritt deals with exponential polynomials; expressions

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

defined over $\mathbb{C}$. Our generalised power sums are restrictions of these functions to $z=0,1,2,\ldots$. As remarked earlier, a given generalised power sum $a(h)$ may be viewed as an element of a polynomial ring $F[h,W_1,W_1^{-1},\ldots,W_s,W_s^{-1}]$ with variables W_i arising from roots of $a(h)$, namely those corresponding to the generators of a subgroup of $A^{1/\infty}$. Not dissimilarly, Ritt notes that an exponential polynomial may be viewed as a polynomial in several variables. He calls an exponential polynomial corresponding to a polynomial in a single variable a *simple* exponential polynomial. The example $\exp(z\omega)-A$, and its factors $\exp(z\omega/k)-A^{1/k}$, for all positive integers k , shows that such exponential polynomials, other than for polynomials proper (those just in z), are arbitrarily factorisable in the ring of exponential polynomials.

PROPOSITION 5 (Ritt). *Up to associates and the order of the factors, an exponential polynomial is uniquely factorisable as the product of simple exponential polynomials, each corresponding to a polynomial in a different variable, and of finitely many exponential polynomials irreducible in the ring of exponential polynomials.* □

A quite intricate argument is required to yield the existence of irreducible exponential polynomials and the finiteness of the factorisation. Because of the presence of infinitely many roots of unity in $\mathbb{C}$ and the consequential opportunity to restrict potential irreducibles to arithmetic progressions and then decompose them further, it is no straightforward

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

matter to translate Proposition 5 to a corresponding statement for generalised power sums. However, Bézivin, in effect by restricting his discussion to a ring $F_h(F^\times)$ of generalised power sums, with F finitely generated over $\mathbb{Q}$ as in our discussion, provides a unique factorisation result for generalised power sums not identically zero on an arithmetic progression. His factorisation theorem *inter alia* yields a useful result (equivalent to Proposition 3 of [*6*]) which the present authors prove by somewhat different p-adic methods in [*6*].

5. Specialisation

In the present section we develop tools sufficient to show that the bounds on the order of a quotient, respectively k-th root generalised power sum found in Propositions 2 and 3 remain stable under specialisations preserving the rank of $\mathcal{W}$ (and preserving the fact that $a(h)$ does not vanish identically on progressions mod d).

Denote by $\underline{x}=(x_1,x_2,\ldots,x_t)$ a transcendence basis for the field F over $\mathbb{Q}$. Then $F=\mathbb{Q}(\underline{x})[y]$ with y algebraic over $\mathbb{Q}(\underline{x})$, say with defining polynomial

$$H(Y;\underline{x}) = H_0(\underline{x})Y^d + H_1(\underline{x})Y^{d-1} + \ldots + H_d(\underline{x}) ,$$

where the $H_i(\underline{x})$ are elements of $\mathbb{Z}[\underline{x}]$. Each element ϕ in F has a representation

$$\phi = U_\phi(y;\underline{x})/V_\phi(\underline{x})$$

as a quotient of polynomials $U_\phi(y;\underline{x})$, $V_\phi(\underline{x})$ respectively in $\mathbb{Z}[y;x]$, $\mathbb{Z}[\underline{x}]$; we may suppose that the polynomials $U_\phi(y;\underline{x})$, $V_\phi(\underline{x})$ are relatively prime in $\mathbb{Z}[y;\underline{x}]$ in which case we may refer to $V_\phi(\underline{x})$ as the denominator of ϕ .

In the sequel Γ denotes a finite set of elements of F with the property that whenever γ is in Γ and $\gamma\neq 0$ then also γ^{-1} , is in Γ .

Given generalised power sums

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

$$a(h) = \Sigma A_i(h)\alpha_i^h \ , \ b(h) = \Sigma B_j(h)\beta_j^h$$

defined over F , we suppose that Γ contains, as always, the coefficients and discrimant of $H(y;\underline{x})$, as well as the roots α_i, β_j and the coefficients of the $A_i(h)$ and the $B_j(h)$ from these power sums. Next set

$$V_\Gamma(\underline{x}) = \Pi_{\gamma\varepsilon\Gamma} V_\gamma(\underline{x}) \ ,$$

and suppose that the total degree of V_Γ does not exceed Δ .

Let $\underline{c} = (c_1, c_2, \ldots c_t)$ be any t-tuple of rational integers so that

$$V_\Gamma(\underline{c}) \neq 0 \ .$$

It is easy to see, by induction on t , that there are infinitely many such t-tuples; indeed, were we to restrict $\underline{c}$ so that each of its entries satisfied $|c_i| < H$, we would have $<<H^t$ t-tuples of integers of which only $<<\Delta H^{t-1}$ would be excluded. Here, and below, the symbol $<<$ implies a dependence on unspecified constants independent of H (and in the present instance of Δ) and not relevant to the conclusions drawn. We will use this remark in applying a helpful observation of Masser [3], and of Schlickeweli, below.

The set Γ generates a subdomain R of F , and the map induced by

$$\underline{x} = (x_1, x_2, \ldots, x_t) \mapsto \underline{c} = (c_1, c_2, \ldots c_t)$$

maps the domain R into an algebraic number field K of degree at most d over $\mathbb{Q}$; in particular y is mapped to a zero $y(\underline{c})$ of the polynomial $H(Y;\underline{c})$. We refer to the induced map together with a specified choice of zero $y(\underline{c})$ of $H(Y;\underline{c})$ as a Γ-specialisation of F .

To see the claim implied above, note that for each ρ in R its denominator $V_\rho(\underline{x})$ divides some positive power of $V_\Gamma(\underline{x})$. Hence $V_\rho(\underline{c}) \neq 0$ and the image of ρ is defined by the specialisation. *A fortiori* each element γ of Γ has a defined image, and since also γ^{-1}

is in Γ (whenever $\gamma \neq 0$) it too has a well-defined image. Thus a Γ-specialisation has the property of mapping non-zero elements of Γ to non-zero elements of K .

We now give a sketch of the proof [3] that:

PROPOSITION 6. *There are* Γ-*specialisations* f *so that if* $g_1, g_2, \ldots g_m$ *are multiplicatively independent elements of the domain* R, *then their specialisations* $f(g_1), f(g_2), \ldots, f(g_m)$ *are multiplicatively independent elements of a number field.*

Proof. Given H sufficiently large (relative to the data), we will find such a specialisation induced by $\underline{x} \rightarrow \underline{c}$ with each rational integer c_i; satisfying $|c_i| < H$. Consider a specialisation f induced by such a $\underline{c}$. The logarithm of the absolute value of the height of the $f(g_k)$ is $<<$ Log$H$ (with the implied constant depending only on the data and not on the specialisation) . By a result of Loxton and van der Poorten [2], whenever the $f(g_k)$ *are* multiplicatively dependent then there already is a non-trivial multiplicative relation

$$f(g_1)^{a_1} \ldots f(g_m)^{a_m} = 1 ,$$

in integers a_k , not all zero, with $|a_k| << (\text{Log}H)^{m-1}$. Suppose we were to restrict the admissible specialisations by augmenting Γ by the elements

$$g_1^{a_1} \ldots g_m^{a_m} - 1, \quad \text{with} \quad |a_k| << (\text{Log}H)^{m-1} .$$

and their reciprocals, thus preventing these elements from specialising to zero (for with the g_k multiplicatively independent, these expressions do not already vanish). Then no Γ-specialisation $\underline{x} \mapsto \underline{c}$ with each rational integer c_i satisfying $|c_i| < H$ can cause the given multiplicatively independent elements to specialise to multiplicatively dependent elements. One can verify that the degree Δ of V_Γ. (with Γ augmented as described) satisfies $\Delta << (\text{Log}H)^{m^2-1}$, so, as remarked above,

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

at most $H^{t-1}(\mathrm{Log}H)^{m^2-1}$ elements $\underline{c}$ of the original $\ll H^t$ can fail to yield an acceptable specialisation. But $H^{t-1}(\mathrm{Log}H)^{m^2-1} \ll H^t$ once H is sufficiently large relative to the data, proving the existence of the required specialisations. □

We may apply Proposition 6 to obtain the following corollaries of the remarks following Propositions 2 and 3: *Suppose it is alleged that* $b(h)$ *might divide* $a(h)$ *in the ring of generalised power sums. Then there are infinitely many specialisations of the given generalised power sums for which there is an a priori bound (depending only on the data and not on the specialisation) on the order of the specialised putative cofactor* $c(h)$. Similarly, *if it is alleged that the generalised power sum* $a(h)$ *might have a* k*-th root in the ring of generalised power sums, then there are infinitely many specialisations of the given generalised power sum which, if they have such a* k*-th root, have such a* k*-th root of order bounded in terms of* $a(h)$ *alone.* Such claims do not hold for specialisations not necessarily preserving the multiplicative independence of the generators of the group containing the roots of the given generalised power sums. These remarks enable us to generalise results [6], [7] proved for generalised power sums defined over algebraic number fields to the corresponding results for generalised power sums defined over arbitrary fields of characteristic zero.

References

[1] J.-P. Bézivin, "Factorisation de suites récurrentes linéaires et applications", *Bull. Soc. Math. France* 112 (1984), 365-376.

[2] J.H. Loxton and A.J. van der Poorten, "Miltiplicative dependence in number fields", *Acta Arith.* 42 (1983), 291-302.

[3] D.W. Masser, "Specializations of finitely generated subgroups of abelian varieties", *Trans. Amer. Math. Soc.* (to appear).

[4] G. Pólya and G. Szegö, *Problems and Theorems in Analysis I, II*, (Springer 1976).

[5] 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.

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press

[6] R.S. Rumely and A.J. van der Poorten, "A note on the Hadamard k-th root of a rational function", *J. Austral. Math. Soc.* (to appear).

[7] A.J. van der Poorten, "The Hadamard Quotient Theorem for rational functions", (in preparation).

Department of Mathematics,
The University of Georgia,
Athens,
Georgia 30602
United States of America.

School of Mathematics, Physics,
Computing and Electronics,
Macquarie University,
New South Wales 2113
Australia.

https://doi.org/10.1017/S0004972700026587 Published online by Cambridge University Press