PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 125, Number 5, May 1997, Pages 1293–1298
S 0002-9939(97)03919-1

FACTORISATION IN THE RING OF EXPONENTIAL POLYNOMIALS

G. R. EVEREST AND A. J. VAN DER POORTEN

(Communicated by William W. Adams)

ABSTRACT. We study factorisation in the ring of exponential polynomials and provide a proof of Ritt's factorisation theorem in modern notation and so generalised as to deal with polynomial coefficients as well as with several variables. We do this in the more general context of a group ring of a divisible torsion-free ordered abelian group over a unique factorisation domain.

We study factorisation in the group ring of a divisible torsion-free ordered abelian group over a unique factorisation domain. A natural instance of such a ring is the ring of exponential polynomials. Thus, in particular we give an account of Ritt's factorisation theorem for exponential polynomials. Ritt's paper [6] deals just with exponential polynomials with constant coefficients and his proof relies on some incongenial normalisations, which we show to be unnecessary. Hence our argument generalises more readily; in particular we remark that our proof applies to exponential polynomials in several variables. Even the case of polynomial coefficients does not seem to appear in the literature, other than for an allusion by Shields [10] to an unpublished manuscript of W. D. Bouwsma. The factorisation theorem for exponential polynomials is not just of intrinsic interest. It plays a critical role in the analysis of recurrence sequences that are divisibility sequences detailed in [1].

1. Exponential polynomials and group rings

Let $\mathbb{K}$ be a field of characteristic zero and let $\mathcal{W}$ be a finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$. Denote by $\mathbb{K}_z\{\mathcal{W}\}$ the ring of all exponential polynomials with coefficients polynomials in $\mathbb{K}[z]$ and frequencies in $\mathcal{W}$; that is, the set of all functions f of the shape

$$f(z) = \sum_{i=1}^{m} F_i(z) \exp(\phi_i z)$$

Received by the editors September 17, 1994 and, in revised form, November 15, 1995.
1991 *Mathematics Subject Classification.* Primary 11B37, 20K20.
Key words and phrases. Exponential polynomial, group ring, factorization.
Work supported in part by grants from the SERC and the Australian Research Council, by a research agreement with Digital Equipment Corporation, and by the hospitality of Macquarie University to the first of us.

where the coefficients $F_i(z)$ belong to $\mathbb{K}[z]$ and the *frequencies* ϕ_i are distinct elements of $\mathcal{W}$. We study factorisation in $\mathbb{K}_z\{\mathcal{W}\}$, noting that the units of the ring are all one term exponential polynomials $F\exp(\phi z)$, with F a nonzero constant.

Set

$$\mathcal{W}_{\mathbb{Q}} = \mathcal{W} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}^s .$$

It is easy to see that any basis $w_1, \ldots, w_s$ of $\mathcal{W}$ induces a corresponding lexicographic ordering on $\mathcal{W}_{\mathbb{Q}}$. Explicitly, if

$$w = a_1 w_1 + \cdots + a_s w_s \text{ and } w' = a'_1 w_1 + \cdots + a'_s w_s, \text{ with the } a_i, a'_i \text{ in } \mathbb{Q}$$

define

$$w > w' \iff \text{ there is an index } k \text{ such that}$$
$$a_1 = a'_1, \ldots\ldots, a_{k-1} = a'_{k-1} \text{ but } a_k > a'_k .$$

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

The ring of exponential polynomials is a special case of the following construction. Let U denote an arbitrary UFD and let G denote a divisible torsion-free abelian ordered group. Write $R = UG$ for the group ring of all finite expressions

$$a = \sum A_i \alpha_i \qquad A_i \in U,\ \alpha_i \in G,$$

where we understand that almost all the A_i vanish, so the sums are finite. This set carries linear addition, with multiplication inherited from U, from the group operation on G, and the distributive law. We refer to an element α_i which appears in a, so with $A_i \neq 0$, as a *frequency* of a. Now we let $\mathcal{W}$ denote a finitely generated $\mathbb{Z}$-module of frequencies, with $\mathcal{W}_{\mathbb{Q}}$ carrying the same meaning as above. In like manner, choosing a basis for $\mathcal{W}_{\mathbb{Q}}$ allows the ordering of G to be extended to a lexicographic ordering of $\mathcal{W}_{\mathbb{Q}}$. Denote the $\mathbb{Z}$-module $\langle \alpha_1, \ldots, \alpha_m \rangle$ generated by the frequencies of a by $\mathcal{A}$. We begin by writing G as an additive group.

Lemma 1. *Suppose b, c are elements of R and $a = bc$. Let $\mathcal{B}$ denote the $\mathbb{Z}$-module generated by the frequencies of b, and $\mathcal{C}$ that generated by the frequencies of c. Then*

$$\mathcal{C} \subseteq \langle \mathcal{A}, \mathcal{B} \rangle .$$

Proof. Fix a lexicographic ordering on $\langle \mathcal{B}, \mathcal{C} \rangle_{\mathbb{Q}}$, and let β be the maximal frequency of b. Suppose that $\mathcal{C}$ is not contained in $\langle \mathcal{A}, \mathcal{B} \rangle$ and let γ be the maximal frequency of c not in $\langle \mathcal{A}, \mathcal{B} \rangle$.

If there are no other frequencies β' of b, γ' of c so that $\beta' + \gamma' = \beta + \gamma$ then $\beta + \gamma$ must be a frequency of a so evidently $\gamma \in \langle \mathcal{A}, \mathcal{B} \rangle$. In the contrary case, since $\beta > \beta'$ but $\beta' + \gamma' = \beta + \gamma$, it must be that $\gamma' > \gamma$. So $\gamma' \in \langle \mathcal{A}, \mathcal{B} \rangle$. Therefore $\gamma = -\beta + \beta' + \gamma'$ is in $\langle \mathcal{A}, \mathcal{B} \rangle$ as well. □

Lemma 2 (Ritt [6]). *In fact, if $a = bc$ then, up to a normalisation, each of $\mathcal{B}$ and $\mathcal{C}$ is a $\mathbb{Z}$-module in $\mathcal{A}_{\mathbb{Q}}$. More precisely: If $a = bc$, there is an element $f = \phi$ of G and thus of R so that, setting $b' = bf$, $c' = f^{-1}c$, the $\mathbb{Z}$-modules $\mathcal{B}'$ and $\mathcal{C}'$ generated respectively by the frequencies of b' and of c' are $\mathbb{Z}$-modules in $\mathcal{A}_{\mathbb{Q}}$.*

Proof. Choose a linear map $\langle \mathcal{B}, \mathcal{C} \rangle_{\mathbb{Q}} \to \langle \mathcal{B}, \mathcal{C} \rangle_{\mathbb{Q}} / A_{\mathbb{Q}} : \delta \mapsto \overline{\delta}$ and select a lexicographic ordering on $\langle \mathcal{B}, \mathcal{C} \rangle_{\mathbb{Q}}$ dominated by such an ordering on $\langle \mathcal{B}, \mathcal{C} \rangle_{\mathbb{Q}} / A_{\mathbb{Q}}$. Denote by β and γ the maximal frequency of b, respectively c, with respect to this ordering. Then, necessarily, $\beta + \gamma$ is in $\mathcal{A}$ and since, similarly, the sum $\beta' + \gamma'$ of the minimal

frequencies of b and c belongs to $\mathcal{A}$, we have $(\beta+\gamma)-(\beta'+\gamma')$ in $\mathcal{A}$. This is to say:

$$(\overline{\beta}+\overline{\gamma})-(\overline{\beta'}+\overline{\gamma'})=\overline{0}\,.$$

But both $\overline{\beta}-\overline{\beta'}\geq\overline{0}$ and $\overline{\gamma}-\overline{\gamma'}\geq\overline{0}$. Hence

$$\overline{\beta}-\overline{\beta'}=\overline{\gamma}-\overline{\gamma'}=\overline{0}\,.$$

Thus every frequency of b differs by β', and every frequency of c differs by γ', from an element of $\mathcal{A}_{\mathbb{Q}}$, which entails the allegation of the Lemma. □

For the following remarks it becomes convenient to write G multiplicatively. Let $\{x_1,\ldots,x_g\}$ denote a basis for $\mathcal{A}_{\mathbb{Q}}$, so selected, for convenience, that each frequency α_i of a is a $\mathbb{Z}$-linear combination of the x_j. Then each α_i becomes a monomial

$$\alpha_i=x_1^{\mu_{i1}}\cdots x_g^{\mu_{ig}}$$

in the variables $x:=(x_1,\ldots,x_g)$ and with the exponents μ_{ij} in $\mathbb{Z}$. After multiplication by an appropriate such monomial, which just corresponds to multiplication by a unit in R, we lose no generality in supposing that the exponents all are non-negative integers. Thus the element $a\in R$ becomes a polynomial

$$a(x)=\sum A_i x^{\mu_i}$$

in the g variables $x=(x_1,\ldots,x_g)$, and with coefficients in U. By Lemma 2, every factorisation of a corresponds to some factorisation of the polynomial $a(x)$ into polynomials in fractional powers of the x_i. Thus, to understand factorisation in the ring $R=UG$, it is appropriate to digress to mention factorisation in fractional powers in rings of polynomials.

2. Factorisation of polynomials in fractional powers

If fractional powers are permitted, a binomial $x-A$ defined over an algebraically closed field has almost arbitrary 'factorisations', because $x^{1/k}-\sqrt[k]{A}$ is a 'factor' for every positive integer k. Plainly, therefore, any general discussion of factorisation in fractional powers must avoid such polynomials. Fortunately, the following is true, and is proved in [5].

Proposition. *Let $P(x,y)$ be an irreducible polynomial of bi-degree d_x, d_y defined over an algebraically closed field $\mathbb{K}$ of characteristic zero. Suppose $P(x,y)$ has at least three terms. Then $P(x,y)$ has at most $d_x d_y$ factors over $\mathbb{K}$ in fractional powers of x and y.*

This yields a quantitative version of a result dating at least back to Ritt [6] and Gourin [2]; for details see Schinzel [9].

The upshot is that given an arbitrary polynomial $a(x_1,\ldots,x_g)$ over a unique factorisation domain U we should first factorise it as a product of irreducible polynomials. Next we remove, for separate consideration, those factors that are just a product of a monomial and of a polynomial in some monomial m in the variables. In that case, the irreducible factor is effectively just a polynomial in the one variable m; we will refer to it in that way. Here we use the term *monomial* in $x_1,\ldots,x_g$ for a rational function $x_1^{a_1}\cdots x_n^{a_n}$ with integral, but not necessarily nonnegative, exponents.

The separated factors are effectively just polynomials in a single variable; were we working over an algebraically closed domain, they would be precisely the irreducible

factors with just two terms. In practice, they are products of such binomials over an extension ring of the base ring U. The Proposition now shows, for details see [5], that the remaining irreducible factors each yield just finitely many irreducible polynomial factors in fractional powers of $x_1, \ldots, x_g$.

3. Factorisation in the ring $R = UG$ — in particular in the ring of exponential polynomials

We are now in a position to state a factorisation theorem for the ring $R = UG$. Indeed, our remarks above at §1 show that factorisation in that ring corresponds to factorisation in an appropriate ring of polynomials over U in fractional powers of their variables. And our remarks above at §2 show that an irreducible polynomial is a product of monomials, of polynomials in some monomial, and of polynomials which have a finite factorisation into irreducibles even when fractional powers are permitted. Seeing that monomials correspond to units in the ring R, it remains only to deal with polynomials in a monomial. We note again that over an algebraically closed field such polynomials factorise into binomials.

In the spirit of Ritt [6], we refer to a two term element of R as a *simple* element. After normalising by appropriate elements of U and of G, such simple elements are of the shape $C\gamma - C'$, with C and C' having no prime factor in common. A product of normalised simple elements, each with the same frequency γ, corresponds to just a polynomial in γ. On organising the simple factors appropriately, one sees that the simple factors yield a finite product

$$\prod P_i(\gamma_i)$$

of polynomials P_i with frequencies γ_i not rational multiples one of the other. That we must deal separately with simple factors is illustrated amply by the example $\gamma - 1$, which has $\frac{1}{k}\gamma - 1$ as a factor for each $k = 1, 2, 3, \ldots$.

For the rest we notice that elements of U already factorise in a way that is unique up to order and associates.

Our arguments and definitions now readily yield:

Theorem 1. *An element of $R = UG$ factors, uniquely up to units and associates, as a finite product of irreducibles of U, a finite product of polynomials $P_i(\phi_i)$ with the frequencies ϕ_i not rational multiples one of the other, and a finite product of elements of R, each irreducible in R.*

Specifically, taking $U = \mathbb{K}[z]$, we obtain the following factorisation theorem for the ring of exponential polynomials.

Theorem 2. *An exponential polynomial in z factors, uniquely up to units and associates, as a product of a polynomial in z, a finite product of polynomials $P_i(\exp(\phi_i z))$ with the frequencies ϕ_i not rational multiples one of the other, and a finite product of exponential polynomials each irreducible in the ring of exponential polynomials.*

4. Factorisation in RH — exponential polynomials in several variables

It seems reasonable to call a ring with the factorisation properties of UG a *factorisation domain*. Now let R denote a factorisation domain and suppose H is

a divisible torsion-free ordered abelian group. Then it is plain that the theory for RH is identical to that we have described above.

Theorem 3. *Let R denote an arbitrary factorisation domain and let H denote an arbitrary torsion-free divisible ordered group. Then the group ring RH is a factorisation domain.*

Specifically,

Theorem 4. *An exponential polynomial in several variables $z = (z_1, z_2, \dots)$ factors, uniquely up to units and associates, as a product of a polynomial in $z = (z_1, z_2, \dots)$, a finite product of polynomials $P_i(\exp(\sum_j \phi_{ij} z_j))$ with the quantities $\sum_j \phi_{ij} z_j$ not rational multiples one of the other, and a finite product of exponential polynomials each irreducible in the ring of exponential polynomials.*

5. Remarks

We are indebted to an anonymous referee for pointing out that that our original remarks in fact described factorisation in the group ring of a torsion-free ordered abelian group over a UFD. The interesting point is of course the apparent problems raised by the possible divisibility of that group. When the group G has torsion there are new issues; in effect these are touched upon in [8]. Whilst various remarks above are attributed to [6], Ritt does not of course deal with a context as general as ours; and his arguments are rather different. The present notions do not seem to exist in the literature in the context of group rings. Some matters in Karpilovsky [3] relate peripherally, and [7] describes a possibly unexpected context in which our group rings appear. The interesting application of Theorem 2 arises in [1] as follows: the question concerns recurrence sequences (a_h), say defined over $\mathbb{Z}$, with the property that $a_m \mid a_n$ whenever $m \mid n$; the Fibonacci numbers provide the well-known instance. By virtue of the result of [4] one notices that the divisibility condition entails the existence of an exponential polynomial $a(z)$, where $a(h) = a_h$ for integers h, with the property that $a(z) \mid a(dz)$ in the ring of exponential polynomials for any integer $d > 0$. Theorem 2 now confirms that $a(z)$ is essentially just a product of simple exponential polynomials, whence (a_h) is essentially a product of second order recurrence sequences, confirming a longstanding conjecture of Ward.

References

[1] J.–P. Bézivin, A. Pethő and A. J. van der Poorten, *A full characterisation of divisibility sequences*, Amer. J. Math. **112** (1990), 985–1001. MR **91k:**11017

[2] Eli Gourin, *On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves*, Trans. Amer. Math. Soc. **32** (1930), 485–501.

[3] Gregory Karpilovsky, *Unit groups of classical rings*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1988, pp. xiv+370. MR **90e:**20007

[4] A. J. van der Poorten, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sc. Paris (Série 1) **306** (1988), 97–102. MR **89c:**11153

[5] A. J. van der Poorten, *Factorisation in fractional powers*, Acta Arith. **LXX** (1995), 287–293. MR **96c:**12001

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

[7] Joseph Rosenblatt, *Phase retrieval*, Comm. Math. Phys. **95** (1984), 317–343. MR **86k:**82075

[8] Robert S. Rumely and A. J. van der Poorten, *Remarks on generalised power sums*, Bull. Austral. Math. Soc. **36** (1987), 311–329. MR **88j:**11008

[9] Andrzej Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor, 1982. MR **84k:**12010

[10] Alan Shields, *On quotients of exponential polynomials*, Comm. Pure and Appl. Math. **16** (1963), 27–31. MR **26:**6411

School of Mathematics and Physics, University of East Anglia, Norwich NR4 7JT, England

E-mail address: g.everest@uea.ac.uk

Centre for Number Theory Research, Macquarie University, New South Wales 2109, Australia

E-mail address: alf@mpce.mq.edu.au