A factorization theorem for exponential polynomials

P. D'Aquino and G. Terzo
Seconda Università degli Studi di Napoli

GOAL: We give a factorization theorem for the ring of exponential polynomials in many variables over an algebraically closed field of characteristic 0 with an exponentiation.

1 E-rings

Definition 1. *An exponential ring, or E-ring, is a pair (R, E) with R a ring (commutative with 1) and*

$$E : (R, +) \to (\mathcal{U}(R), \cdot)$$

a map of the additive group of R into the multiplicative group of units of R, satisfying

1. *$E(x + y) = E(x) \cdot E(y)$ for all $x, y \in R$*
2. *$E(0) = 1$.*

Example

1. $(\mathbb{R}, a^x)$, with $a > 0$, and $(\mathbb{C}, e^x)$.
2. (R, E) where R is any ring and $E(x) = 1$ for all $x \in R$.
3. $(S[t], E)$, where S is an E-field of characteristic 0 and $S[t]$ is the ring of formal power series in t over S. Let $f \in S[t]$, where $f = r + f_1$, and $r \in S$,
$$E(f) = E(r) \cdot \sum_{n=0}^{\infty} (f_1)^n / n!$$
4. $K[X]^E$ ring of exponential polynomials over (K, E), an E-ring.

(K, E) is an E-field if K is a field.

2 E-polynomial ring

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{x} = x_1, \ldots, x_n$ is an E-ring constructed as follows by recursion.

- $(R_k, +, \cdot)_{k \geq -1}$ are rings;
- $(B_k, +)_{k \geq 0}$ are torsion free abelian groups, and for the algebraically closed fields, are also divisible groups;
- $(E_k)_{k \geq -1}$ are partial E-morphisms.

Step 0: Let $R_{-1} = K$; $R_0 = (K[\overline{x}], +, \cdot)$; $B_0 =< \overline{x} >$, the ideal generated by $\overline{x}$.
So $R_0 = R_{-1} \oplus B_0$;
$E_{-1} : R_{-1} \longrightarrow R_0$, is the composition of the initial E-morphism over K with the immersion of K into $K[\overline{x}]$.

Inductive step: Suppose $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that:

$$R_k = R_{k-1} \oplus B_k,$$

$$E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot)$$

$\mathcal{U}(R_k) =$ invertible elements of R_k. Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

be an isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (group ring construction).}$$

- R_k is a subring of R_{k+1}
- 1. B_{k+1} is the R_k-submodule of R_{k+1} freely generated by t^b where $b \in B_k$,
  2. $R_{k+1} = R_k \oplus B_{k+1}$ as additive groups
- $R_{k+1} = R_{k-1}[t^{B_k \oplus B_{k-1}}] = R_{k-2}[t^{B_k \oplus B_{k-1} \oplus B_{k-2}}] = \ldots\ldots = K[\overline{x}][t^{B_k \oplus \ldots \oplus B_0}]$
- $E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot)$ defined as follows $E_k(x) = E_{k-1}(r) \cdot t^b$

Get a chain of partial E-rings (domain of $E_{k+1} = R_k$)

$$R_0 \subset R_1 \subset R_2 \cdots \subset R_k \subset \cdots$$

The ring of exponential polynomials is

$$K[\overline{x}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{x}][t^{B_0 \oplus \ldots \oplus B_k \oplus \cdots}] = U[G]$$

group ring where

- $U = K[\overline{x}]$ a UFD
- $G = t^{B_0 \oplus \ldots \oplus B_n \oplus \cdots}$ a divisible torsion free abelian group (G is orderable and a $\mathbb{Q}$-vector space)

Exponentiation on $K[\overline{x}]^E$ is defined as follows

$$E(f) = E_k(f), \text{ if } f \in R_k \text{ and } k \in \mathbb{N}.$$

Proposition 1. *If K is an exponential field of characteristic 0 then the E-polynomial ring $K[\overline{x}]^E$ is an integral domain whose units are of the form $E(\alpha)$, where $\alpha \in K[\overline{x}]^E$.*

Definition 2. *An exponential polynomial $f \in K[\overline{x}]^E$ is irreducible if there are no non-units g and h with $f = gh$.*

3 Associate polynomial

To any exponential polynomial we will associate a classical polynomial.

Let $f \in K[\overline{x}]^E$, $f \in R_k$ for some $k \in \mathbb{N}$, then

$$f = \sum_{h=1}^{N} a_h t^{\alpha_h},$$

where $a_h \in K[\overline{x}]$ and $\alpha_h \in B_0 \oplus \ldots \oplus B_{k-1}$.

Definition 3. *The support of f is the $\mathbb{Q}$-vector space generated by $\alpha_1, \ldots, \alpha_N$, and is denoted by $supp(f)$.*

• Let $\{\nu_1, \ldots, \nu_p\}$ be a $\mathbb{Q}$-base for $supp(f)$. Then

$$\alpha_i = \sum_{j=1}^{p} r_{ij}\nu_j$$

for all $i = 1, \ldots, N$, and $r_{i,j} \in \mathbb{Q}$.

• Wlog we can assume $r_{ij} \in \mathbb{Z}$. Moreover, we can assume all r_{ij}'s positive integers since we can multiply f by an invertible element, i.e. a purely exponential term. Then f is a polynomial in $t^{\nu_1}, \ldots, t^{\nu_p}$, with coefficients in a UFD, $U = K[\overline{x}]$. Let

$$y_1 = t^{\nu_1}, \ldots, y_p = t^{\nu_p}.$$

If we substitute each α_i by its expression in terms of the bases $\nu_1, \ldots, \nu_p$ we transform f into a classical polynomial in the variables $y_1, \ldots, y_p$

$$f \in K[\overline{x}]^E \rightsquigarrow Q(y_1, \ldots, y_p) \in U[y_1, \ldots, y_p]$$

where $U = K[\overline{x}]$. We will refer to $Q(y_1, \ldots, y_p)$ as the **associate polynomial of** f.

Definition 4. *An exponential polynomial f is simple if* $\dim(supp(f)) = 1$.

In what follows a monomial in $y_1, \ldots, y_p$ is a term $y_1^{m_1} \cdot \ldots \cdot y_p^{m_p}$ with $m_i \in \mathbb{Z}$.

Definition 5. *A classical polynomial $Q(y_1, \ldots, y_p)$ is essentially 1-variable if there are monomials τ_1, τ_2 in $y_1, \ldots, y_p$ such that $Q(y_1, \ldots, y_p) = \tau_1 P(\tau_2)$, where P is a polynomial in just one variable.*

Example:

The polynomial

$$Q(x, y) = x^2y(3x^3y^9 - 2x^2y^6 + 1) = \tau_1 P(\tau_2),$$

where $\tau_1 = x^2y$, $\tau_2 = xy^3$ and $P(z) = 3z^3 - 2z^2 + 1$, is an essentially 1-variable.

Remarks:

1. The correspondence between f and Q holds modulo a monomial in $y_1, \ldots, y_p$ which corresponds to an invertible element of $K[\overline{x}]^E$;

2. f is a simple polynomial iff Q is essentially 1-variable polynomial.

Let $Q(y_1, \ldots, y_p) \in K[y_1, \ldots, y_p]$ be an irreducible polynomial over a UFD U. It can happen that for some $\mu_1, \ldots, \mu_p \in \mathbb{N}_+$, $Q(y_1^{\mu_1}, \ldots, y_p^{\mu_p})$ becomes reducible. For example,

$$Q(x, y) = x - y \text{ is irreducible, but } Q(x^3, y^6) = (x - y^2)(x^2 + xy^2 + y^4).$$

Definition 6. *A polynomial $Q(y_1, \ldots, y_p)$ is power irreducible over U if for each $\mu_1, \ldots, \mu_p \in \mathbb{N}_+$, $Q(y_1^{\mu_1}, \ldots, y_p^{\mu_p})$ is irreducible.*

Definition 7. *A polynomial $Q(y_1, \ldots, y_p)$ is primary in y_i if the g.c.d. of the exponents of y_i in all terms of Q is 1.*

Definition 8. *A polynomial $Q(y_1, \ldots, y_p)$ is primary if it is primary in each variable.*

Example:

- $Q(x, y) = 3x^2y - 5y^3 + x^3$ is primary in both x and y.
- $R(x, y) = 3x^2y - 5y^3 + x^4$ is not primary in x since $R(x, y) = P(x^2, y)$, where $P(x, y) = 3xy - 5y^3 + x^2$

Remark:

If $Q(y_1, \ldots, y_p)$ is a non primary polynomial then there exists a unique p-upla $t_1, \ldots, t_p$ of positive integers such that

$$Q(y_1, \ldots, y_p) = P(y_1^{t_1}, \ldots, y_p^{t_p})$$

where $P(y_1, \ldots, y_p)$ is primary.

4 Factorization Theorem

Known results:

- Ritt in [8] was the first to consider a factorization theory for exponential polynomials of the following form

$$f(z) = a_1 e^{\alpha_1 z} + \ldots + a_n e^{\alpha_n z},$$

  where $a_i, \alpha_i \in \mathbb{C}$.

- Gourin and Macoll in [6], [7] gave refinements of Ritt's factorization theorem for exponential polynomials of the form

$$f(z) = p_1(z) e^{\alpha_1 z} + \ldots + p_n(z) e^{\alpha_n z},$$

  where α_i are complex numbers and $p_i(z) \in \mathbb{C}[z]$.

- Only in the mid '90s van der Poorten and Everest obtained a factorization theorem in a more general context for exponential polynomials of the second form over an algebraically closed field of characteristic 0 with exponentiation.

We generalize the results obtained in [8], [3], [4] to any exponential polynomial with coefficients in an algebraically closed field K of characteristic 0 with exponentiation.

Major issues for exponential polynomial:

If fractional powers are permitted:

1. A binomial as $y - 1$ defined over an algebraically closed field K may have infinitely many factors. Indeed, $y^{\frac{1}{k}} - \epsilon$, where ϵ is a kth root of unity, is a factor for any positive integer k.

2. The polynomial $(x - y)$ becomes reducible

$$(x - y) = (x^{\frac{1}{3}} - y^{\frac{1}{3}})(x^{\frac{2}{3}} + x^{\frac{1}{3}} y^{\frac{1}{3}} + y^{\frac{2}{3}}).$$

There is a correspondence between a factorization of f and a factorization of Q in fractional powers of the variables.

($\Rightarrow$) It follows from:

Lemma 1. *Let $f(\overline{x}) \in K[\overline{x}]^E$ and suppose that $f(\overline{x}) = g(\overline{x}) \cdot h(\overline{x})$, where $g(\overline{x}), h(\overline{x}) \in K[\overline{x}]^E$. Then $supp(g), supp(h)$ are contained in $supp(f)$.*

For the proof we use the construction of the E-polynomial ring and the fact that G is an ordered group.

Corollary 1. *Suppose f factorizes as $f = gh$. Let Q, P and R be the associate polynomials of f, g and h, respectively. There is a monomial τ such that $Q = P'R'$ where $P' = P\tau$, $R' = \tau^{-1}R$.*

($\Leftarrow$) It follows from:

Theorem 1. *Let $Q(y_1, \ldots, y_p)$ be a (primary) irreducible polynomial over U, a unique factorization domain containing all roots of unity. Assume also that Q is not essentially a 1-variable polynomial. Then $Q(y_1, \ldots, y_p)$ has a factorization into primary irreducible polynomials in the ring generated over U by all fractional powers of $y_1, \ldots, y_p$, and the number of these irreducible factors is finite.*

Proof: First of all notice that any factorization of $Q^{(t)} = Q(y_1^{t_1}, \ldots, y_p^{t_p})$ for $t_1, \ldots, t_p \in \mathbb{N}$ gives a factorization in fractional powers of the variables of $Q(y_1, \ldots, y_p)$. Hence we will study the factorizations of $Q(y_1^{t_1}, \ldots, y_p^{t_p})$.

Claim. There are only finitely many sets of positive integers

$$t_{11}, \ldots, t_{1p}; t_{21}, \ldots, t_{2p}; \ldots\ldots; t_{n1}, \ldots, t_{np}$$

such that $Q(y_1^{t_{i1}}, \ldots, y_p^{t_{ip}})$, for $i = 1, \ldots, n$ are reducible.

Step 1. For $i = 1, \ldots, p$ let ϵ_i be a primitive t_ith root of unity. The transformations

$$\tau_{\epsilon_i} : y_i \mapsto \epsilon_i^k y_i$$

for $0 \leq k < t_i$ leave $Q(y_1^{t_1}, \ldots, y_p^{t_p})$ unchanged.

The next lemma shows that from one irreducible factor of $Q(y_1^{t_1}, \ldots, y_p^{t_p})$ all the others can be obtained via the group G of transformations generated by τ_{ϵ_i}.

Lemma 2. *Let $Q(y_1, \ldots, y_p)$ be irreducible over U and suppose that for some positive integers $t_1, \ldots, t_p$, $Q^{(t)} = Q(y_1^{t_1}, \ldots, y_p^{t_p})$ is reducible, and $Q_1, \ldots, Q_s$ are the irreducible factors. Any fixed factor Q_i is transformed in all the other factors Q_j's by the above transformations.*

Corollary 2. *1. Each Q_i in the identity $Q^{(t)} = Q_1 \ldots Q_s$ contains all the variables.*

2. If Q_i is primary then all Q_j's are primary.

3. If Q_i is a polynomial in more than two terms then all Q_j's are polynomials in more than two terms.

Step 2. If the irreducible factor Q_1 of $Q^{(t)}$ is primary then Q_1 also consists of more than two terms.

Step 3. If an irreducible factor Q_1 of $Q^{(t)} = Q(y_1^{t_1}, \ldots, y_p^{t_p})$ is primary then each t_j satisfies the relation $t_j \leq M^2$, where $M = max(d_{y_1}, \ldots, d_{y_p})$.

Factorization Theorem for exponential polynomials: *An element $f \neq 0$ of $K[\overline{x}]^E$, where K is an algebraically closed field of characteristic 0, factors uniquely up to units and associates, as a finite product of irreducibles of $K[\overline{x}]$, a finite product of irreducible of $K[\overline{x}]^E$ whose support is of dimension bigger than* 1*, and a finite product of elements g_j of $K[\overline{x}]^E$, where $supp(g_{j_1}) \neq supp(g_{j_2})$, for $j_1 \neq j_2$ and whose supports are of dimension* 1*.*

(EXISTENCE) Let $f(\overline{x}) \in K[\overline{x}]^E$, and $Q(y_1, \ldots, y_p)$ the associate polynomial. Consider a factorization of the associate polynomial

$$Q = Q_1 \cdot \ldots \cdot Q_r \cdot P_1 \cdot \ldots \cdot P_s.$$

1. Q_i are essentially 1-variable polynomials;

2. P_j are not essentially 1-variable irreducible polynomials.

1. The Q_i's correspond to the simple factors of f, and we will multiply those which have the same support in order to have all the factors of f of dimension 1 of different support.
2. Each P_j contributes only for a finite number of irreducible factors in fractional powers of y_h. If $P_j(y_1, \ldots, y_p) = V(y_1^{n_1}, \ldots, y_p^{n_p})$, for some $n_1, \ldots, n_p \in \mathbb{N}$ and $V(y_1, \ldots, y_p)$ primary then necessarily, $V(y_1, \ldots, y_p)$ is also irreducible otherwise $P_j(y_1, \ldots, y_p)$ would be reducible. From substitution of y_i by $t^{n_i \nu_i}$ we get a factor of f.

Let $r_1, \ldots, r_p$ be positive integers such that

$$V(y_1^{r_1}, \ldots, y_p^{r_p}) = V_1 \cdot \ldots \cdot V_q$$

where V_j are primary and irreducible, and q is the maximum number of irreducible primary factors (by Theorem 1 such q exists). By replacing each y_h by $t^{n_i \nu_i / r_i}$ in V_k get the irreducible factors of length > 2 of the exponential polynomial f.

(UNIQUENESS) It is enough to prove that if $g(\overline{x})$ divides $h(\overline{x}) \cdot l(\overline{x})$ in $K[\overline{x}]^E$ and $g(\overline{x})$ has no factor in common with $h(\overline{x})$ then $g(\overline{x})$ divides $l(\overline{x})$. Suppose

$$g(\overline{x}) \cdot s(\overline{x}) = h(\overline{x}) \cdot l(\overline{x}) \tag{1}$$

for some $s(\overline{x}) \in K[\overline{x}]^E$, and $(g(\overline{x}), h(\overline{x})) = 1$.

Let $G(\overline{y}), H(\overline{y}), L(\overline{y}), S(\overline{y})$ be the associate polynomials to $g(\overline{x}), h(\overline{x}), l(\overline{x}), s(\overline{x})$, respectively. Clearly, $(G(\overline{y}), H(\overline{y})) = 1$, since any non trivial common factor of $G(\overline{y})$ and $H(\overline{y})$ would give a non trivial common factor of $g(\overline{x})$ and $h(\overline{x})$.

Equation (1) implies the following relation over a unique factorization domain

$$G(\overline{y}) \cdot S(\overline{y}) = H(\overline{y}) \cdot L(\overline{y}). \tag{2}$$

Since G has no common factors with H then G divides L. This imples that the exponential polynomial g divides l. So the uniqueness of the factorization of f follows.

Consequences in exponential algebra:

- If f in $K[\overline{x}]^E$ is irreducible and with support of dimension more than 1 then f is prime. For, if f divides gh then by the factorization theorem f must occur in the factorization of one of g or h.

- The factorization theorem has been used in order to characterize those exponential polynomials over exponential fields introduced by Zilber in [9] which have no solutions in the field. This implies Picard's Little theorem for exponential polynomials over a Zilber field (see [1]).

- The factorization of exponential polynomials of the form

  $$f(z) = a_1 e^{\alpha_1 z} + \ldots + a_n e^{\alpha_n z},$$

  where $a_i, \alpha_i \in \mathbb{C}$, has been used by van der Poorten and Tijdeman (see [5]) in the analysis of recurrence sequences in connection with Shapiro's Conjecture.

References

[1] P. D'Aquino, A. Macintyre and G. Terzo: *Schanuel Nullstellensatz for Zilber fields*, Fundamenta Mathematicae 207, (2010), 123-143.

[2] A. Macintyre: *Exponential Algebra*, in Logic and Algebra. Proceedings of the international conference dedicated to the memory of Roberto Magari, (A. Ursini et al. eds), Lecture Notes in Pure Applied Mathematics 180, (1991), 191-210.

[3] A. J. van der Poorten: *Factorisation in fractional powers*, Acta Arithmetica 70, (3), (1995), 287-293.

[4] A. J. van der Poorten and G. R. Everest: *Factorisation in the ring of exponential polynomials*, Proceedings of the American Mathematical Society, 125, (5), (1997), 1293-1298.

[5] A.J. van der Poorten and R. Tijdeman: *On common zeros of exponential polynomials* L'Enseign. Math. Série , 21 (1975) pp. 5767.

[6] E. Gourin: *On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves*, Transactions of the American Mathematical Society 32, (1930), 485-501.

[7] L. A. MacColl: *A factorization theory for polynomials in x and in functions $e^{\alpha x}$*, Bulletin American Mathematical Society, (41), (1935), 104-109.

[8] J.F. Ritt: *A factorization theorem of functions $\sum_{i=1}^{n} a_i e^{\alpha_i z}$*, Transactions of American Mathematical Society 29, (1927), 584-596.

[9] B. Zilber: *Pseudo-exponentiation on algebraically closed fields of characteristic zero*, Annals of Pure and Applied Logic, 132, (1), (2004), 67-95.