RESEARCH

Open Access

Factorizations for difference operators

Jeffrey Bergen[1], Mark Giesbrecht[2], Pappur N Shivakumar[3] and Yang Zhang[3*]

*Correspondence:
zhang39@cc.umanitoba.ca
[3]Department of Mathematics,
University of Manitoba, Winnipeg,
MB, Canada
Full list of author information is
available at the end of the article

Abstract

We consider the factorization problems of difference operators in $\mathbb{C}[x;\sigma]$ for an automorphism σ of finite order. We study the factorization of regular polynomials in $\mathbb{R}[x]$ in the ring of such difference operators and obtain an analogue of the fundamental theorem of algebra for skew polynomial ring $K[x;\sigma]$ over field K.

Keywords: difference operators; factorizations

1 Introduction

Let R be a ring, σ an endomorphism of R, and δ a left σ-derivation of R. That is, δ is an additive mapping from R to R and for any $a, b \in$ R,

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b.$$

The skew polynomial ring $R[x;\sigma,\delta]$ is the set of all polynomials

$$a_0 + a_1 x + \cdots + a_n x^n,$$

where $a_0, \ldots, a_n \in$ R, addition is defined as usual, and multiplication is defined by

$$xa = \sigma(a)x + \delta(a) \quad \text{for all } a \in \text{R}.$$

Linear differential operators ($\sigma = \mathrm{id}_R$, the identity map on R) and linear difference operators ($\delta = 0$, the identically zero function) are special cases of above skew polynomials, which have been studied via algebraic methods since [1]. The study of skew polynomials is now an active and important area in algebra with many applications in other areas such as solving differential/difference equations, engineering, coding theory, *etc.* More recent results and survey can be found in [2–10]. Factorization of skew polynomials is also a recent active area in computer algebra (see, for example, [11–14]). Algorithms for characterization of linear difference and differential equations are of great interest.

One of the great strengths of skew polynomials is their analogy with regular commutative polynomials. A natural question thus arises: Is there an analogue of the fundamental theorem of algebra for skew polynomials? We provide a positive answer for difference operators with finite-order automorphisms over an algebraically closed field.

Throughout this paper, we assume that $R[x;\sigma]$ *is a skew polynomial ring with automorphism* σ *as defined above.*

Springer

2 Some basic results

It is clear that the polynomials $x^2 - 1$ and $x^2 + 1$ in $\mathbb{R}[x]$ factor uniquely into monic, linear polynomials in $\mathbb{C}[x]$. However, the situation is quite different when we look at $\mathbb{R}[x]$ as a subring of the skew polynomial ring $\mathbb{C}[x; \sigma]$. Observe that if $t \in \mathbb{C}$ such that $|t| = 1$, and $\sigma(t)$ is the complex conjugate of t, then

$$x^2 - 1 = \big(x + \sigma(t)\big)(x - t)$$

in $\mathbb{C}[x; \sigma]$. Thus $x^2 - 1$ can be factored in an infinite number of ways in $\mathbb{C}[x; \sigma]$. On the other hand, $x^2 + 1$ remains irreducible in $\mathbb{C}[x; \sigma]$. In this paper we contrast how polynomials factor in skew polynomial rings with how they factor in ordinary polynomial rings.

We next introduce the terminology used throughout the remainder of this paper. We let K denote a field and σ an automorphism of K. Define $K^\sigma = \{a \in K \mid \sigma(a) = a\}$ and, when we examine the special case where $\sigma^2 = 1$, an important subset of K^σ is the set of norms defined by $N(K, \sigma) = \{t\sigma(t) \mid t \in K\}$. When dealing with the field $\mathbb{C}$, unless stated otherwise, we always assume that σ represents complex conjugation.

For $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x; \sigma]$ and $t \in K$, the (standard) evaluation of $f(x)$ at $x = t$ is defined as $f(t) = a_n t^n + \cdots + a_1 t + a_0$. When we study polynomials over fields, one of the first facts we prove is that linear factors correspond to roots. Note that this is not the case in skew polynomial rings: if σ denotes complex conjugation, then

$$f(x) = x^2 - 1 = (x - i)(x - i)$$

in $\mathbb{C}[x; \sigma]$, yet $f(i) \neq 0$. To better understand the role of linear factors in skew polynomial rings, we define σ-*evaluation* as follows.

Definition 2.1 Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in K[x; \sigma]$ and $t \in K$. Then we define the σ-*evaluation* $f(t; \sigma) \in K$ as $f(t; \sigma) = a_n(t\sigma(t) \cdots \sigma^{n-1}(t)) + a_{n-1}(t\sigma(t) \cdots \sigma^{n-2}(t)) + \cdots + a_2(t\sigma(t)) + a_1 t + a_0$. If $f(t; \sigma) = 0$, we say that t is a σ-*root* of $f(x)$.

Observe that if $\sigma = \mathrm{id}_R$, and $K[x; \sigma] = K[x]$ is an ordinary polynomial ring, then a σ-root is the same as an ordinary root. Lemma 2.2 and Theorem 2.3 show us that the role of σ-roots in the skew polynomial case generalizes the role of roots in the ordinary case.

Lemma 2.2 ([15]) *If* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x; \sigma]$ *and* $t \in K$, *then there exists a unique* $q(x) \in K[x; \sigma]$ *such that*

$$f(x) = q(x)(x - t) + f(t; \sigma).$$

When $f(x) = q(x)(x - t)$, instead of simply saying that $x - t$ is a factor of $f(x)$, we may sometimes use the more precise terminology that $x - t$ is a (right) factor of $f(x)$. We can now see the relationship between (right) factors and σ-roots.

Theorem 2.3 *Suppose* $f(x) \in K[x; \sigma]$. *Then* $x - t$ *is a right factor of* $f(x)$ *if and only if* t *is a* σ-*root of* $f(x)$.

Proof Using Lemma 2.2, there exists a unique $q(x) \in K[x; \sigma]$ such that $f(x) = q(x)(x - t) + f(t; \sigma)$. Therefore, if t is a σ-root of $f(x)$, then $f(t; \sigma) = 0$, and we can see that $x - t$ is certainly

a (right) factor of $f(x)$. Conversely, if $x - t$ is a (right) factor of $f(x)$, then $f(x) = h(x)(x - t)$ for some $h(x) \in K[x; \sigma]$. But then, by Lemma 2.2, the quotient $h(x)$ and remainder (0) are unique, so $f(t; \sigma) = 0$. □

For ordinary polynomials of degree 2, being reducible is equivalent to having a root. In our situation, we now show that it is equivalent to having a σ-root.

Corollary 2.4 *Suppose $f(x) \in K[x; \sigma]$ has degree 2; then $f(x)$ is reducible in $K[x; \sigma]$ if and only if $f(x)$ has a σ-root in K.*

Proof One direction follows immediately from Theorem 2.3, for if $f(x)$ has a σ-root in K, then it has a right factor of degree one in $K[x; \sigma]$ and is therefore reducible. In the other direction, if $f(x)$ is reducible and has degree 2, then it is easy to see that it must have a monic, linear right factor. Theorem 2.3 now asserts that $f(x)$ has a σ-root in K. □

One of the examples that motivated this paper was the fact that $x^2 + 1$ remains irreducible in $\mathbb{C}[x; \sigma]$. Thus the situation of quadratic polynomials where $\sigma^2 = 1$ is of particular interest. We can now determine precisely that irreducible quadratics in $K^\sigma[x]$ remain irreducible in $K[x; \sigma]$.

Corollary 2.5 *Let $f(x) = x^2 + ax + b \in K^\sigma[x]$ and suppose $\sigma^2 = 1$. Then $f(x)$ is reducible in $K[x; \sigma]$ if and only if either* (i) *$f(x)$ is reducible in $K^\sigma[x]$, or* (ii) *$a = 0$ and $-b \in N(K, \sigma)$.*

Proof If $f(x)$ is reducible in $K^\sigma[x]$, then it is certainly reducible in $K[x; \sigma]$. Furthermore, if $a = 0$ and $-b \in N(K, \sigma)$, then $-b = t\sigma(t)$ for some $t \in K$ and

$$f(x) = x^2 - (-b) = x^2 - \big(t\sigma(t)\big) = \big(x + \sigma(t)\big)(x - t).$$

This proves one half of the result.

To see the converse, Corollary 2.4 tells us that if $f(x)$ is reducible in $K[x; \sigma]$, then it has a σ-root $t \in K$. If t is a σ-root, then it satisfies the equation

$$t\sigma(t) + at + b = 0.$$

Since $\sigma^2 = 1$, we know that $t\sigma(t) \in K^\sigma$. However, $b \in K^\sigma$, therefore it follows that $at \in K^\sigma$. If $a \neq 0$, then the fact that $a \in K^\sigma$ implies that $t \in K^\sigma$. Since t is an ordinary root of $f(x)$ in K^σ, we see that $f(x)$ is reducible in $K^\sigma[x]$. On the other hand, suppose $a = 0$. Our equation above now tells us that $-b = t\sigma \in N(K, \sigma)$, thereby concluding the proof. □

The next corollary completely describes the situation for the examples $x^2 - 1, x^2 + 1 \in \mathbb{R}[x] \subseteq \mathbb{C}[x; \sigma]$ that were mentioned at the start of this paper.

Corollary 2.6 *Let $f(x) = x^2 + ax + b \in \mathbb{R}[x]$.*
  (i) *$f(x)$ is reducible in $\mathbb{C}[x; \sigma]$ if and only if $f(x)$ is reducible in $\mathbb{R}[x]$.*
  (ii) *If $f(x)$ is reducible, then the factorization of $f(x)$ in $\mathbb{C}[x; \sigma]$ into monic, linear factors is unique when $a \neq 0$, whereas $f(x)$ factors an infinite number of ways into monic, linear factors when $a = 0$.*

Proof In light of Corollary 2.5, in order to prove part (i), it suffices to show that if $a = 0$ and $-b \in N(\mathbb{C}, \sigma)$, then $f(x)$ is reducible in $\mathbb{R}[x]$. However, in this situation, $N(\mathbb{C}, \sigma)$ is equal to the set of positive real numbers. Therefore, if $-b \in N(\mathbb{C}, \sigma)$, then $-b = c^2$ for some $c \in \mathbb{R}$. Thus

$$f(x) = x^2 - (-b) = (x + c)(x - c),$$

as required.

For the proof of part (ii), let $\operatorname{cis}(\theta) = \cos\theta + i\sin\theta$ for every $\theta \in \mathbb{R}$. Then, when we are in the case where $a = 0$, we can rewrite the equation above as

$$f(x) = x^2 - (-b) = (x + c)(x - c) = \big(x + c\big(\operatorname{cis}(-\theta)\big)\big)\big(x - c\big(\operatorname{cis}(\theta)\big)\big).$$

By letting θ range between 0 and 2π, we can see that $f(x)$ does factor an infinite number of ways in $\mathbb{C}[x; \sigma]$.

Finally, suppose $a \neq 0$; the argument in the proof of Corollary 2.5 indicates that any factorization of $f(x)$ actually takes place in $\mathbb{R}[x]$. Since there is only one way to factor $f(x)$ in $\mathbb{R}[x]$, it follows that the factorization of $f(x)$ in $\mathbb{C}[x; \sigma]$ is also unique. □

When we look back at Corollaries 2.5 and 2.6, it becomes natural to look for an example where reducibility in $\mathsf{K}[x; \sigma]$ is not equivalent to reducibility in $\mathsf{K}^\sigma[x]$.

Example 2.7 Let $\mathsf{K} = \mathbb{Q}(i)$ and once again let σ denote complex conjugation. In this case, $x^2 - 2$ and $x^2 - 5$ are irreducible in $\mathsf{K}^\sigma[x] = \mathbb{Q}[x]$. However, since $2, 5 \in N(\mathbb{Q}, \sigma)$, these polynomials become reducible in $\mathbb{Q}(i)[x; \sigma]$ as we have

$$x^2 - 2 = \big(x + (1 - i)\big)\big(x - (1 + i)\big) \quad \text{and} \quad x^2 - 5 = \big(x + (2 - i)\big)\big(x - (2 + i)\big).$$

On the other hand, since $-2, 3 \notin N(\mathbb{Q}(i), \sigma)$, the polynomials $x^2 + 2$ and $x^2 - 3$ are irreducible in $\mathbb{Q}[x]$ and remain irreducible in $\mathbb{Q}(i)[x; \sigma]$.

3 Main theorems

In order to complete our description of the factoring of polynomials in $\mathbb{C}[x; \sigma]$, we first need to prove a result that holds in any algebraically closed field.

Theorem 3.1 *Let* K *be an algebraically closed field and let* σ *be an automorphism of* K *of order* n. *Then every non-constant reducible skew polynomial in* $\mathsf{K}[x; \sigma]$ *can be written as a product of irreducible skew polynomials of degree less than or equal to* n.

Proof Since σ has order n, K has dimension n over the subfield K^σ. It is well known that the centre of $\mathsf{K}[x; \sigma]$ is the polynomial ring $\mathsf{K}^\sigma[x^n]$. Now suppose that $f(x)$ is a non-constant element of $\mathsf{K}[x; \sigma]$. Since $\mathsf{K}[x; \sigma]$ is a finite module over the Noetherian ring $\mathsf{K}^\sigma[x^n]$, $\mathsf{K}[x; \sigma]$ contains no infinite direct sums of $\mathsf{K}^\sigma[x^n]$-submodules. As a result, the sum

$$f(x)\mathsf{K}^\sigma\big[x^n\big] + f(x)^2 \mathsf{K}^\sigma\big[x^n\big] + f(x)^3 \mathsf{K}^\sigma\big[x^n\big] + \cdots$$

cannot be direct. Therefore, there exist $a_1(x), \ldots, a_m(x) \in \mathsf{K}^\sigma[x^n]$, with at least two nonzero $a_i(x)$, such that

$$f(x)a_1(x) + f(x)^2 a_2(x) + \cdots + f(x)^m a_m(x) = 0.$$

By cancelling any common factors of $f(x)$ on the left, we obtain

$$a_j(x) + f(x)a_{j+1}(x) + \cdots + f(x)^{m-j}a_m(x) = 0.$$

Observe that $a_j(x)$ is a nonzero element of $\mathsf{K}^\sigma[x^n] \cap f(x)\mathsf{K}[x;\sigma]$. Therefore, there exists $g(x) \in \mathsf{K}[x;\sigma]$ such that $f(x)g(x)$ is a nonzero element of $\mathsf{K}^\sigma[x^n]$.

Since K is algebraically closed and n-dimensional over K^σ, non-constant polynomials in $\mathsf{K}^\sigma[y]$ can all be factored into a product of polynomials of degree at most n. If we let $y = x^n$, then

$$f(x)g(x) \in \mathsf{K}^\sigma\left[x^n\right] = \mathsf{K}^\sigma[y].$$

Therefore, there exist non-constant $h_1(y), \ldots, h_m(y) \in \mathsf{K}^\sigma[y]$, all of degree at most n, such that

$$f(x)g(x) = h_1(y) \cdots h_m(y).$$

For each i, the polynomial $h_i(y) = h_i(x^n) \in \mathsf{K}^\sigma[x]$ can also be factored in $\mathsf{K}^\sigma[x]$ as a product of non-constant polynomials of degree at most n. As a result, we have actually factored $f(x)g(x)$ in $\mathsf{K}[x,\sigma]$ as a product of polynomials of degree at most n.

By Theorem 1 of Chapter II in [1], the degrees of factors of $f(x)g(x)$ are at most n.

Thus $f(x)$ has been factored in $\mathsf{K}[x;\sigma]$ as a product of polynomials of degree at most n.

□

Using Theorem 3.1 and Corollary 2.4, we now have the following.

Corollary 3.2 *Every non-constant polynomial in $\mathbb{C}[x;\sigma]$ is a product of linear and irreducible polynomials. Furthermore, the quadratic $f(x) = x^2 + a_1x + a_0$ is irreducible in $\mathbb{C}[x;\sigma]$ if and only if there does not exist some $t \in \mathbb{C}$ such that $t\sigma(t) + a_1t + a_0 = 0$.*

Proof Theorem 3.1 asserts that every non-constant polynomial in $\mathbb{C}[x;\sigma]$ is a product of linear and irreducible polynomials. In addition, Corollary 2.4 tells us that $f(x) = x^2 + a_1x + a_0$ is irreducible in $\mathbb{C}[x;\sigma]$ if and only if $f(x)$ does not have a σ-root in $\mathbb{C}$. However, when we look at the definition of σ-roots in the quadratic case, it is clear that $f(x)$ does not have a σ-root if and only if there does not exist $t \in \mathbb{C}$ such that $t\sigma(t) + a_1t + a_0 = 0$. □

Author details
[1]Department of Mathematical Sciences, DePaul University, Chicago, IL 60614, USA. [2]David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada. [3]Department of Mathematics, University of Manitoba, Winnipeg, MB, Canada.

References

1. Ore, O: Theory of non-commutative polynomials. Ann. Math. **34**(22), 480-508 (1933)
2. Bergen, J: Derivation algebras of rings related to Heisenberg algebras. J. Algebra Appl. **3**(2), 181-191 (2004)
3. Bergen, J, Grzeszczuk, P: Jacobson radicals of ring extensions. J. Pure Appl. Algebra **216**(12), 2601-2607 (2012)
4. Bergen, J, Grzeszczuk, P: Skew power series rings of derivation type. J. Algebra Appl. **10**(6), 1383-1399 (2011)
5. Cohn, PM: Free Rings and Their Relations. Academic Press, San Diego (1985)
6. Cohn, PM: Skew Fields. Cambridge University Press, Cambridge (1995)
7. Jacobson, N: Finite Dimensional Division Algebras over Fields. Springer, Berlin (2010)
8. McConnell, JC, Robson, JC: Noncommutative Noetherian Rings. Graduate Studies in Mathematics, vol. 30. Am. Math. Soc., Providence (2001)
9. Shivakumar, PN, Zhang, Y: On series solution of $y'' + \phi(x)y = 0$ and applications. Adv. Differ. Equ. **2013**, 47 (2013)
10. Shivakumar, PN, Wu, Y, Zhang, Y: Shape of Dum, a constructive approach. WSEAS Trans. Math. **10**(1), 22-31 (2011)
11. Churchill, R, Zhang, Y: Irreducibility criteria for skew polynomials. J. Algebra **322**(11), 3797-3822 (2009)
12. Eberly, W, Giesbrecht, M: Efficient decomposition of separable algebras. J. Symb. Comput. **37**, 35-81 (2004)
13. von zur Gathen, J, Gerhard, J: Modern Computer Algebra, 3rd edn. Cambridge University Press, Cambridge (2013)
14. Giesbrecht, M, Zhang, Y: Factoring and decomposing Ore polynomials over $F_q(t)$. In: Proceedings of the ACM 28th International Symposium on Symbolic and Algebraic Computation (ISSAC '03), pp. 127-134. ACM, New York (2003)
15. Lam, TY, Leroy, A: Vandermonde and Wronskian matrices over division rings. J. Algebra **119**(2), 308-336 (1988)