

UNIQUENESS OF CERTAIN BINOMIAL FACTORIZATIONS IN GROUP ALGEBRAS

CHRISTOPHER J. HILLAR

ABSTRACT. Motivated by the study of cyclic resultants, we consider the problem of determining when two binomial factorizations of the form

$$a \prod_{i=1}^m (g_i - h_i), \quad a \in \mathbb{Z}, g_i, h_i \in G$$

are equal in a group algebra $\mathbb{Z}G$. A sufficient condition is given for a group to admit uniqueness of factorization up to natural equivalences. Applied to the Abelian case, this condition is found to recover the known result. As another application, we prove a uniqueness of factorization when the underlying group is $GL_n(\mathbb{C})$.

1. INTRODUCTION

Let G be a group and let $\mathbb{Z}G$ be the group algebra over \mathbb{Z} . We explore the question of when two binomial factorizations in $\mathbb{Z}G$ are equal. We begin by introducing some useful terminology. In the following definition, we view \mathbb{R} as a group under addition.

Definition 1.1. Let G be group and let $S \subset G$. The set S is called *nonderogatory* if for each finitely generated subgroup H containing a subset $\{g_1, \dots, g_n\} \subset S$, there is a group homomorphism $\phi : H \rightarrow \mathbb{R}$ such that $\phi(g_i) \neq 0$ for all i .

Obviously, not every set of group elements has this property – for instance, if any of the elements of S have torsion. Less trivial examples can be found by taking triples $g, h, ghg^{-1}h^{-1}$ of torsion-free elements in a group G . A large class nonderogatory subsets can be obtained from the following.

Proposition 1.2. *The torsion-free elements of an Abelian group are nonderogatory.*

Proof. This follows directly from [5, Lemma 2.7]. □

For a noncommutative example, consider $G = GL_n(\mathbb{C})$. There is a natural homomorphism $\phi : G \rightarrow \mathbb{R}$ given by

$$(1.1) \quad \phi(A) = \log |\det(A)|.$$

We then have the following

Proposition 1.3. *The set of elements of $GL_n(\mathbb{C})$ with determinants outside the unit circle (in the complex plane) is nonderogatory.*

Proof. Follows immediately from (1.1) and the definition. □

1991 *Mathematics Subject Classification.* Primary ; Secondary.

Key words and phrases. group algebras, binomial factorizations, cyclic resultants.

Recall that two elements $x, y \in G$ are called *conjugate* (denoted $x \sim y$) if there exists $z \in G$ such that $x = zyz^{-1}$. The following definition explains what we shall mean by unique factorization of binomials.

Definition 1.4. A subset S of a group G has the *unique binomial factorization* property if the existence of a factorization

$$a \prod_{i=1}^m (g_i - h_i) = b \prod_{i=1}^n (u_i - v_i), \quad a, b \in \mathbb{Z}, \quad g_i^{-1}h_i, u_i^{-1}v_i \in S$$

in $\mathbb{Z}G$ implies that $a, b = \pm 1$, $m = n$, and that up to permutation, for each i , there are elements $c_i \in G$ such that $(g_i - h_i) \sim \pm c_i(u_i - v_i)$.

Example 1.5. To illustrate the need for conjugation in the definition, consider the equation

$$(u - v)(w - x)(y - z) = (uwy - vwy)(1 - y^{-1}w^{-1}xy)(1 - y^{-1}z),$$

which holds in any group algebra. One can then check that

$$\begin{aligned} (u - v) &= wy \cdot (y^{-1}w^{-1})(uwy - vwy)y^{-1}w^{-1} \\ (w - x) &= y \cdot y^{-1}wy(1 - y^{-1}w^{-1}xy)y^{-1} \\ (y - z) &= y(1 - y^{-1}z). \quad \square \end{aligned}$$

Our main theorem gives a sufficient condition for unique factorizations of binomials in a group algebra.

Theorem 1.6. *Nonderogatory subsets of a group G have the unique binomial factorization property.*

The following unique factorization results are direct consequences of Theorem 1.6.

Corollary 1.7. *The torsion-free elements of an Abelian group have the unique binomial factorization property.*

Proof. Follows from Theorem 1.6 and Proposition 1.2. □

Corollary 1.8. *The set of elements of $GL_n(\mathbb{C})$ with determinants outside the unit circle (in the complex plane) have the unique factorization property.*

Proof. Follows from Theorem 1.6 and Proposition 1.3. □

We should remark that there are obstructions to unique factorization that make necessary some kind of supplemental hypothesis. For example, when $G = \mathbb{Z}/2\mathbb{Z}$, we have $\mathbb{Z}G \cong \mathbb{Z}[s]/\langle s^2 - 1 \rangle$, and it is easily verified that

$$(1 - s)(1 - s) = 2(1 - s).$$

One might also wonder what happens when the binomials are not of the form $g - h$. The following example exhibits some of the difficulty in formulating a general statement.

Example 1.9. Let $G = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ so that $\mathbb{Z}G \cong \mathbb{Z}[s, t, t^{-1}]/\langle s^2 - 1 \rangle$. Then,

$$(1 - t^4) = (1 - t^2)(1 + t^2) = (1 - st^2)(1 + st^2)$$

are three different binomial factorizations of the same element. □

The problem of binomial factorization arises in a natural way from the study of cyclic resultants [4, 5, 6]. We briefly sketch the connection. Given a polynomial $f(x) = c \prod_{i=1}^d (x - \lambda_i) \in \mathbb{C}[x]$, the m -th *cyclic resultant* of f is

$$(1.2) \quad r_m(f) = \text{Res}(f, x^m - 1) = c^m \prod_{i=1}^d (\lambda_i^m - 1).$$

Sequences of the form r_m arise as the cardinalities of sets of periodic points for toral endomorphisms. Let A be a d -by- d integer matrix and let $X = \mathbb{T}^d = \mathbb{R}^d / \mathbb{Z}^d$ denote the d -dimensional additive torus. Then, the matrix A acts on X by multiplication mod 1; that is, it defines a map $T : X \rightarrow X$ given by

$$T(\mathbf{x}) = A\mathbf{x} \pmod{\mathbb{Z}^d}.$$

Let $\text{Per}_m(T) = \{\mathbf{x} \in \mathbb{T}^d : T^m(\mathbf{x}) = \mathbf{x}\}$ be the set of points fixed under the map T^m . Under the ergodicity condition that no eigenvalue of A is a root of unity, it follows (see [3]) that $|r_m(f)| = |\text{Per}_m(T)|$, in which f is the characteristic polynomial of A .

Let S denote the ring of sequences over \mathbb{C} under pointwise sum and product, and let $e(\mu)$ denote the exponential sequence $e(\mu)_n = \mu^n$. With this identification, the infinite number of expressions (1.2) can be represented succinctly by

$$e(c) \prod_{i=1}^d (e(\lambda_i) - 1) \in S.$$

When $G = \mathbb{C}^*$, the map $e : \mathbb{Z}G \rightarrow S$ sending $\mu \mapsto e(\mu)$ is an embedding of \mathbb{Z} -algebras [6]. It follows that determining when two polynomials produce equal sequences of cyclic resultants can be reduced to solving a problem in binomial factorization.

Extending earlier work [4], this approach was used in [5] to prove the following characterization theorem describing when two polynomials give rise to equal sets of cyclic resultants.

Theorem 1.10. *Let f and g be polynomials in $\mathbb{C}[x]$. Then, f and g generate the same sequence of nonzero cyclic resultants if and only if there exist $u, v \in \mathbb{C}[x]$ with $\deg(u)$ even, $u(0) \neq 0$, and nonnegative integers $l_1 \equiv l_2 \pmod{2}$ such that*

$$\begin{aligned} f(x) &= x^{l_1} v(x) u(x^{-1}) x^{\deg(u)} \\ g(x) &= x^{l_2} v(x) u(x). \end{aligned}$$

Example 1.11. One can check that the polynomials

$$\begin{aligned} f(x) &= x^3 - 10x^2 + 31x - 30 \\ g(x) &= 15x^5 - 38x^4 + 17x^3 - 2x^2 \end{aligned}$$

both generate the same cyclic resultants. This follows from the factorizations

$$\begin{aligned} f(x) &= (x - 2)(15x^2 - 8x + 1) \\ g(x) &= x^2(x - 2)(x^2 - 8x + 15). \quad \square \end{aligned}$$

The outline of this article is as follows. In Section 2, we describe some reductions for our problem and develop a few elementary tools from the theory of group algebras. In Section 3, we carry out the proof of Theorem 1.6. Finally, to close this introduction, we offer the following open problem.

Conjecture 1.12. *The torsion-free elements of any group have the unique binomial factorization property.*

2. GROUP ALGEBRA TOOLS

We begin with an elementary lemma concerning nonderogatory sets. It basically says that these objects are closed under taking a conjugate closure.

Lemma 2.1. *Let S be a nonderogatory set for a group G and let $T \subset G$. Then,*

$$\{tst^{-1} : t \in T, s \in S\}$$

is a nonderogatory subset of G .

Proof. Let S be as in the lemma and let $t_i \in T, s_i \in S$ for $i = 1, \dots, n$. For a finitely generated subgroup H that contains $\{t_1 s_1 t_1^{-1}, \dots, t_n s_n t_n^{-1}\}$, we must exhibit a homomorphism $\phi : H \rightarrow \mathbb{R}$ with $\phi(t_i s_i t_i^{-1}) \neq 0$ for all i . Let $\tilde{H} = \langle h, s_i, t_i : h \in H, i = 1, \dots, n \rangle$. Since S is nonderogatory, there is a homomorphism $\psi : \tilde{H} \rightarrow \mathbb{R}$ with $\psi(s_i) \neq 0$ for all i . Clearly, $H \subseteq \tilde{H}$, and since $\psi(t_i s_i t_i^{-1}) = \psi(s_i)$, it follows that ψ restricted to H satisfies our requirements. This completes the proof. \square

Next, we make a reduction to binomials of a special form.

Lemma 2.2. *Nonderogatory subsets of a group G have the unique binomial factorization property if and only if for all nonderogatory subsets S , the existence of a factorization*

$$af \prod_{i=1}^m (1 - h_i) = bw \prod_{i=1}^n (1 - v_i), \quad a, b \in \mathbb{Z}, h_i, v_i \in S$$

in $\mathbb{Z}G$ implies that $a, b = \pm 1$, $m = n$, and that up to permutation, for each i , we have $h_i \sim v_i$ or $h_i \sim v_i^{-1}$.

Proof. For the only-if direction, suppose we have a factorization as in the lemma. Then, by definition, up to a permutation, for each i , there is an element $c_i \in G$ such that $(1 - h_i) \sim \pm c_i(1 - v_i)$. If $(1 - h_i) = gc_i(1 - v_i)g^{-1}$ for some $g \in G$, then it follows easily that $c_i = 1$ and $h_i = gv_i g^{-1}$. Similarly, when $(1 - h_i) \sim -c_i(1 - v_i)$, we have $h_i \sim v_i^{-1}$.

For the converse, suppose that S is nonderogatory and that we have a factorization

$$a \prod_{i=1}^m (g_i - h_i) = b \prod_{i=1}^n (u_i - v_i), \quad a, b \in \mathbb{Z}, g_i^{-1} h_i, u_i^{-1} v_i \in S.$$

Let $f_i = g_i g_{i+1} \cdots g_m$ and similarly let $w_i = u_i u_{i+1} \cdots u_n$ (additionally, for convenience, we put $f_{m+1} = w_{m+1} = 1$). Also, set $\tilde{h}_i = f_{i+1}^{-1} g_i^{-1} h_i f_{i+1}$ and $\tilde{v}_i = w_{i+1}^{-1} u_i^{-1} v_i w_{i+1}$. Then, it is straightforward to verify that

$$af_1 \prod_{i=1}^m (1 - \tilde{h}_i) = bw_1 \prod_{i=1}^n (1 - \tilde{v}_i).$$

By assumption and Lemma 2.1, this implies that $a, b = \pm 1$, $m = n$, and that up to permutation, for each i , we have $\tilde{h}_i \sim \tilde{v}_i$ or $\tilde{h}_i \sim \tilde{v}_i^{-1}$. In the first case (the other

one is similar), let $k \in G$ be such that $\tilde{h}_i = k\tilde{v}_i k^{-1}$. One now computes,

$$\begin{aligned} (g_i - h_i) &= g_i f_{i+1} (1 - \tilde{h}_i) f_{i+1}^{-1} \\ &= g_i f_{i+1} k (1 - \tilde{v}_i) k^{-1} f_{i+1}^{-1} \\ &= g_i f_{i+1} k w_{i+1}^{-1} u_i^{-1} (u_i - v_i) w_{i+1} k^{-1} f_{i+1}^{-1} \\ &= f_{i+1} k w_{i+1}^{-1} (w_{i+1} k^{-1} f_{i+1}^{-1} g_i f_{i+1} k w_{i+1}^{-1} u_i^{-1}) (u_i - v_i) w_{i+1} k^{-1} f_{i+1}^{-1}, \end{aligned}$$

which is of the desired form. This completes the proof. \square

After many more lemmas, we can prove Theorem 1.6.

Proof of Theorem 1.6. \square

REFERENCES

- [1] J.J. Duistermaat and V. Guillemin, *The spectrum of positive elliptic operators and periodic bicharacteristics*, Inv. Math. 25 (1975) 39-79.
- [2] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics **203**, Springer-Verlag, New York, 1995.
- [3] G. Everest and T. Ward. *Heights of Polynomials and Entropy in Algebraic Dynamics*. Springer-Verlag London Ltd., London, 1999.
- [4] D. Fried, *Cyclic resultants of reciprocal polynomials*, in *Holomorphic Dynamics (Mexico 1986)*, Lecture Notes in Math. 1345, Springer Verlag, 1988, 124-128.
- [5] C. Hillar, *Cyclic resultants*, J. Symb. Comp., to appear.
- [6] C. Hillar and L. Levine, *Polynomial Recurrences and Cyclic Resultants*, submitted.
- [7] A. Iantchenko, J. Sjöstrand, and M. Zworski, *Birkhoff normal forms in semi-classical inverse problems*, Math. Res. Lett. 9 (2002), 337-362.
- [8] E. Miller and B. Sturmfels, *Combinatorial Commutative Algebra*, Springer, 2004.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CA 94720.
E-mail address: `chillar@math.berkeley.edu`