

SAGBI BASES FOR RINGS OF INVARIANT LAURENT POLYNOMIALS

ALEXANDER DUNCAN[†] AND ZINOVY REICHSTEIN^{††}

ABSTRACT. Let k be a field, $L_n = k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be the Laurent polynomial ring in n variables and G be a group of k -algebra automorphisms of L_n . We give a necessary and sufficient condition for the ring of invariants L_n^G to have a SAGBI basis. We show that if this condition is satisfied then L_n^G has a SAGBI basis relative to any choice of coordinates in L_n and any term order.

1. INTRODUCTION

Let k be a base field and $P_n = k[x_1, \dots, x_n]$ be the polynomial algebra in n variables. Recall that the *initial exponent* $\mathbf{in}(f)$ of $f \in P_n \setminus \{0\}$ is defined as the lexicographically largest $(a_1, \dots, a_n) \in \mathbb{N}^n$ such that $x_1^{a_1} \dots x_n^{a_n}$ occurs in f with a non-zero coefficient. If R is a k -subalgebra of P_n then we define the semigroup of initial exponents of R as

$$(1) \quad \mathbf{In}(R) = \{\mathbf{in}(f) : 0 \neq f \in R\}.$$

A SAGBI basis for R is a finite collection of non-zero elements $p_1, \dots, p_m \in R$ such that $\mathbf{in}(p_1), \dots, \mathbf{in}(p_m)$ generate $\mathbf{In}(R)$ as an additive semigroup. If p_1, \dots, p_m form a SAGBI basis for R , then these elements generate R as a k -algebra. Moreover, an explicit representation of an element $f \in R$ as a polynomial in p_1, \dots, p_m , can be found quickly and efficiently by using the *subduction algorithm* as follows. Choose a product $p_1^{a_1} \dots p_m^{a_m}$, where each $a_i \in \mathbb{N}$ and $\mathbf{in}(f) = a_1 \mathbf{in}(p_1) + \dots + a_m \mathbf{in}(p_m)$. By selecting $\lambda \in k$ so as to cancel the leading term of f , we can ensure that $\mathbf{in}(f - \lambda p_1^{a_1} \dots p_m^{a_m})$ is strictly lexicographically smaller than $\mathbf{in}(f)$. We will write $\mathbf{in}(f) \succ \mathbf{in}(f_1)$, where $f_1 = f - \lambda p_1^{a_1} \dots p_m^{a_m}$. If $f_1 \neq 0$, we can repeat this process on f_1 to get f_2 and so on. As a result we obtain a sequence $f = f_0, f_1, f_2, \dots$, such that

$$(2) \quad \mathbf{in}(f_0) \succ \mathbf{in}(f_1) \succ \mathbf{in}(f_2) \succ \dots$$

1991 *Mathematics Subject Classification.* 13A50, 13P99.

Key words and phrases. SAGBI basis, subduction algorithm, Göbel's conjecture, group action, algebra of invariants, reflection group, abelian semigroup.

[†] A. Duncan is partially supported by an NSERC Canada Graduate Scholarship.

^{††} Z. Reichstein is partially supported by NSERC Discovery and Accelerator Supplement grants.

Any lexicographically decreasing sequence in \mathbb{N}^n has to terminate. Hence, $f_i = 0$ for some $i \in \mathbb{N}$. In other words, the algorithm will terminate after i steps and will yield a desired expression for f as a polynomial in p_1, \dots, p_m .

The reader will undoubtedly notice a strong resemblance between a SAGBI basis for a subalgebra of P_n and a Gröbner basis for an ideal of P_n . In fact, the word ‘‘SAGBI’’, introduced by Robbiano and Sweedler in [7], is an acronym for ‘‘Subalgebra Analog to Gröbner Basis for Ideals’’. Note however, that unlike Gröbner bases, SAGBI bases do not always exist. The question of finding necessary and sufficient conditions for a subalgebra $R \subset P_n$ to have a SAGBI basis is an important open problem; see, e.g., [8].

One reason this problem is so difficult is that the answer depends on the choice of the generators x_1, \dots, x_n for P_n , which is not intrinsic to the embedding $R \hookrightarrow P_n$. In other words, suppose $g: P_n \rightarrow P_n$ is a k -algebra automorphism and $y_i = g(x_i)$ for $i = 1, \dots, n$. We will refer to y_1, \dots, y_n as another choice of *coordinates* in P_n . Writing a non-zero element $f \in P_n$ as a polynomial in y_1, \dots, y_n , we obtain a new initial exponent $\mathbf{in}_y(f)$ and a new semigroup of initial exponents $\text{In}_y(R) = \{\mathbf{in}_y(f) \mid 0 \neq f \in R\}$. In this situation it may happen that $\text{In}(R)$ is a finitely generated semigroup and $\text{In}_y(R)$ is not; see, e.g., [4]. Equivalently, $g^{-1}(R)$ may have a SAGBI basis (relative to x_1, \dots, x_n), even if R does not.

The dependence on the choice of coordinates is lessened (but not entirely eliminated) if we replace the polynomial ring $P_n = k[x_1, \dots, x_n]$ by the ring $L_n = k[x_1, \dots, x_n]$ of Laurent polynomials, for the simple reason that the automorphism group $\text{Aut}(L_n)$ is much ‘‘smaller’’ and better understood than $\text{Aut}(P_n)$. Let R is a k -subalgebra of L_n . The initial exponent $\mathbf{in}(f)$ is now an element of \mathbb{Z}^n , and $\text{In}(R)$ is a subsemigroup of \mathbb{Z}^n . The subduction algorithm is defined in the same way as before. The only difference is that the lexicographically decreasing sequence (2) in \mathbb{Z}^n is no longer guaranteed to terminate. For this reason the definition of a SAGBI basis is modified in this setting, to require the termination of the subduction algorithm; cf. [6]. That is, $p_1, \dots, p_m \in R \setminus \{0\}$ are said to form a SAGBI basis for a k -subalgebra $R \subset L_n$, if $\mathbf{in}(p_1), \dots, \mathbf{in}(p_m)$ generate $\text{In}(R)$ and the subduction algorithm terminates for all $f \in R$ regardless of the particular choice of product $p_1^{a_1} \dots p_m^{a_m}$ used at each step.

Before proceeding to state our main result, we briefly recall that $\text{Aut}(L_n)$ is the semidirect product $\mathbb{G}_m^n \rtimes \text{GL}_n(\mathbb{Z})$. Here we identify an element $(t_1, \dots, t_n) \in \mathbb{G}_m^n$ with the *scaling* automorphism of L_n , taking each x_i to $t_i x_i$, and an element $g \in \text{GL}_n(\mathbb{Z})$ with the *multiplicative* automorphism taking each $x^{\mathbf{a}} = x_1^{a_1} \dots x_n^{a_n}$ to $x^{g(\mathbf{a})}$. We will denote by π the natural projection

$$(3) \quad \pi: \text{Aut}(L_n) \rightarrow \text{GL}_n(\mathbb{Z}).$$

To define π explicitly, note that every $g \in \text{Aut}(L_n)$ preserves the set of invertible elements of L_n , which are of the form $\lambda x^{\mathbf{a}}$ for some $\lambda \in k^*$ and $\mathbf{a} \in \mathbb{Z}^n$. In particular, $g(x_i) = \lambda_i x_1^{a_{i1}} \dots x_n^{a_{in}}$ for some $\lambda_i \in k^*$ and $a_{ij} \in \mathbb{Z}$.

For such $g \in \text{Aut}(L_n)$,

$$(4) \quad \pi(g) = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ \dots & & & \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{pmatrix}.$$

Our main result can now be stated as follows.

Theorem 1.1. *Let k be a field, $L_n = k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be the Laurent polynomial ring in n variables and G be a finite subgroup of $\text{Aut}(L_n)$.*

- (1) $\text{In}(L_n^G)$ is finitely generated,
- (2) L_n^G has a finite SAGBI basis,
- (3) $\pi(G)$ is generated by reflections.

Theorem 1.1 is a generalization of [6, Theorem 1.6], where G is assumed to act on L_n multiplicatively, i.e., $G \subset \text{GL}_n(\mathbb{Z})$. Further results for multiplicative actions can be found in [9]. A novel feature of Theorem 1.1 is that condition (3) is independent of the choice of coordinates in L_n . Indeed, as we mentioned above, a different choice of coordinates in L_n corresponds to replacing L_n^G by $g(L_n^G)$ for some $g \in \text{Aut}(L_n)$ or equivalently, to replacing G by the conjugate subgroup $G' = gGg^{-1}$ in $\text{Aut}(L_n)$. Clearly, $\pi(G')$ is generated by reflections if and only if $\pi(G)$ is generated by reflections.

We also note that our proof of Theorem 1.1 below shows that Theorem 1.1 remains valid if the initial exponent $\mathbf{in}(f)$ are defined relative to any term order in L_n , not necessarily the lexicographic order. Recall that a term order in L_n is a linear order on \mathbb{Z}^n , compatible with the group structure; cf. [6, Definition 1.2]. In view of these remarks, Theorem 1.1 can be restated as follows.

Theorem 1.2. *Let G be a finite subgroup of $\text{Aut}(L_n)$.*

- (a) *If $\pi(G)$ is generated by reflections then L_n^G has a SAGBI basis relative to any choice of coordinates and term order in L_n .*
- (b) *If $\pi(G)$ is not generated by reflections then $\text{In}(L_n^G)$ is not finitely generated (and, in particular, L_n^G does not have a SAGBI basis) for any choice of coordinates and term order in L_n . \square*

The rest of this paper is structured as follows. Sections 4 and 5 will be devoted to the proof of Theorem 1.1. The main new phenomenon we encounter, compared to the proof of [6, Theorem 1.6], is that the semigroup $\text{In}(L_n^G)$ is no longer saturated in \mathbb{Z}^n . In order to deal with the resulting complications, we prove the Sandwich Lemma 3.1 in Section 3. In Section 6 we use a similar argument (also based on the Sandwich Lemma) to prove a generalized form of Göbel's conjecture. (For background material and references on Göbel's original conjecture, see the first paragraph of Section 6.) In the last section we work out an explicit example.

2. NOTATIONAL CONVENTIONS

The following symbols are used throughout this paper.

\mathbb{N}	the set of non-negative integers
Σ_n	the symmetric group on n letters
k	base field
$P_n = k[x_1, \dots, x_n]$	polynomial ring in n variables
$L_n = k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$	Laurent polynomial ring in n variables
π	projection $\text{Aut}(L_n) \rightarrow \text{GL}_n(Z)$; see (3) and (4)
G	finite subgroup of $\text{Aut}(L_n)$
\overline{G}	$= \pi(G)$
\succ	term order in L_n or P_n
in	the initial exponent relative to \succ
In	the semigroup of initial exponents relative to \succ

We will write bold letters \mathbf{a} , \mathbf{b} , etc., for elements of \mathbb{R}^n . If $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$, we will abbreviate $x_1^{a_1} \dots x_n^{a_n}$ as $x^{\mathbf{a}}$.

All semigroups in this paper will be contained in \mathbb{Z}^n and in particular, will be abelian. We will use the words “semigroup” and “monoid” interchangeably; that is, all semigroups will be assumed to have an identity element. In particular, by the “semigroup generated by a set $S \subset \mathbb{Z}^n$ ” we will mean

$$\{a_1 s_1 + \dots + a_r s_r \mid r, a_1, \dots, a_r \in \mathbb{N} \text{ and } s_1, \dots, s_r \in S\}.$$

With the exception of Theorem 1.2 above, the term order \succ will remain in the background; our arguments will work for any term order. The reader will lose little by assuming that \succ is the lexicographic order from now on.

3. THE SANDWICH LEMMA

The purpose of this section is to prove the following theorem, which will play a key role in the sequel.

Lemma 3.1 (Sandwich Lemma). *Suppose A and B are subsemigroups of \mathbb{Z}^n such that $mA \subset B \subset A$ for some integer $m \geq 1$. Then A is finitely generated if and only if B is finitely generated.*

Our proof will rely on the following classical result, which may be viewed as a variant of the Hilbert Basis Theorem; see [2, Lemma A] or [1, Section 2.4].

Lemma 3.2 (Dickson’s Lemma). *Suppose $A \subset \mathbb{N}^n$ has the property that $\mathbf{a} \in A$ and any $\mathbf{n} \in \mathbb{N}^n$ we have $\mathbf{a} + \mathbf{n} \in A$. Then there exists a finite set $S \subset \mathbb{N}^n$ such that $A = \{\mathbf{s} + \mathbf{n} \mid \mathbf{s} \in S, \mathbf{n} \in \mathbb{N}^n\}$. \square*

Proof of the Sandwich Lemma. Since $mA \simeq A$ and $mB \subset mA \subset B$, it suffices to only prove one direction. We will thus assume that A is finitely generated and aim to prove that then B is finitely generated as well.

In fact, we may assume without loss of generality that $A = \mathbb{N}^n$. Indeed, since A is finitely generated there is a surjective semigroup homomorphism

$\phi : \mathbb{N}^n \rightarrow A$ for some $n \geq 1$. Then $A' = \mathbb{N}^n$ and $B' = \phi^{-1}(B)$ satisfy $mA' \subset B' \subset A'$. If we know that the theorem holds for A' and B' then B' is finitely generated and hence, so is $B = \phi(B')$.

From now on we will assume that $A = \mathbb{N}^n$. Set

$$R := \{(r_1, \dots, r_n) \in \mathbb{N}^n \mid 0 \leq r_i < m\}.$$

Then every element \mathbb{N}^n can be written as $m\mathbf{q} + \mathbf{r}$ for some $\mathbf{q} \in \mathbb{N}^n$ and $\mathbf{r} \in R$. Given $\mathbf{r} \in R$, set

$$Q_{\mathbf{r}} := \{\mathbf{q} \in \mathbb{N}^n \mid m\mathbf{q} + \mathbf{r} \in B\}.$$

(Our notation is meant to be suggestive: we think of elements of R as “remainders” and elements of $Q_{\mathbf{r}}$ as “quotients”.) Since we are assuming that $m\mathbb{N}^n \subset B$, each $Q_{\mathbf{r}}$ satisfies the requirements of Lemma 3.2. Thus for every $\mathbf{r} \in R$ there is a finite set $F_{\mathbf{r}} \subset \mathbb{N}^n$ such that

$$Q_{\mathbf{r}} = \{\mathbf{s} + \mathbf{n} \mid \mathbf{s} \in F_{\mathbf{r}}, \mathbf{n} \in \mathbb{N}^n\}.$$

We claim that

$$\left(\bigcup_{\mathbf{r} \in R} \bigcup_{\mathbf{s} \in F_{\mathbf{r}}} m\mathbf{s} + \mathbf{r}\right) \cup \{m\mathbf{e}_i \mid i = 1, \dots, n\}$$

is a (finite) set of generators for B . Here

$$\mathbf{e}_1 = (1, 0, \dots, 0), \dots, \mathbf{e}_n = (0, \dots, 0, 1);$$

note that $m\mathbf{e}_i \in m\mathbb{N}^n \subset B$.

To prove the claim, recall that every $\mathbf{b} \in B$ can be written as $\mathbf{b} = m\mathbf{q} + \mathbf{r}$ for some $\mathbf{r} \in R$ and some $\mathbf{q} \in Q_{\mathbf{r}}$. Writing \mathbf{q} as $\mathbf{s} + \mathbf{n}$ for some $\mathbf{s} \in F_{\mathbf{r}}$ and some $\mathbf{n} \in \mathbb{N}^n$, we see that $\mathbf{b} = (m\mathbf{s} + \mathbf{r}) + m\mathbf{n}$. Since $m\mathbf{n}$ is an \mathbb{N} -linear combination of $m\mathbf{e}_1, \dots, m\mathbf{e}_n$, the claim follows. \square

4. FINITE GENERATION OF THE SEMIGROUP OF INITIAL EXPONENTS

In this section we will prove that conditions (1) and (3) of Theorem 1.1 are equivalent.

Let $\overline{G} = \pi(G) \subset \text{GL}_n(\mathbb{Z})$. For $\mathbf{a} \in \mathbb{Z}^n$ let $S_{\mathbf{a}}$ be the subgroup of G given by $S_{\mathbf{a}} = \pi^{-1}(\text{Stab}_{\overline{G}}(\mathbf{a}))$. In other words, for every $s \in S_{\mathbf{a}}$ there exists a non-zero scalar $\eta_{\mathbf{a}}(s) \in k$ such that $s \cdot x^{\mathbf{a}} = \eta_{\mathbf{a}}(s)x^{\mathbf{a}}$. It is easy to see that $\eta_{\mathbf{a}}$ is, in fact, a multiplicative character $S_{\mathbf{a}} \rightarrow k^*$.

For a given set D of distinct representatives for the left cosets of $S_{\mathbf{a}}$, we define

$$\Omega_D(\mathbf{a}) := \sum_{d \in D} d(x^{\mathbf{a}}).$$

Recall that the support $\text{supp}(f) \subset \mathbb{Z}^n$ of $f \in L_n$ is defined as the set of exponents \mathbf{a} such that $x^{\mathbf{a}}$ occurs in f with a non-zero coefficient. For $S \subset L_n$ we define $\text{Supp}(S)$ to be the union of $\text{supp}(f)$, as f ranges over S .

Lemma 4.1. *For any $\mathbf{a} \in \mathbb{Z}^n$ the following are equivalent:*

- (a) $\mathbf{a} \in \text{Supp}(L_n^G)$,

- (b) $\eta_{\mathbf{a}}$ is the trivial character of $S_{\mathbf{a}}$,
- (c) $\Omega_D(\mathbf{a})$ is independent of the choice of D ,
- (d) $\Omega_D(\mathbf{a}) \in L_n^G$ for any D ,
- (e) $\Omega_D(\mathbf{a}) \in L_n^G$ for some D .

If the equivalent conditions of Lemma 4.1 hold then, in view of (c) we will write $\Omega(\mathbf{a})$ in place of $\Omega_D(\mathbf{a})$.

Proof. (a) \Rightarrow (b): If $s \cdot x^{\mathbf{a}} \neq x^{\mathbf{a}}$ for some $s \in S_{\mathbf{a}}$ then no $f \in L_n$ containing \mathbf{a} in its support can be invariant under the action of s .

(b) \Rightarrow (c): Suppose $s \cdot x^{\mathbf{a}} = x^{\mathbf{a}}$ for any $s \in S_{\mathbf{a}}$. Then replacing $d \in D$ by another representative $d' = ds$ in the same left coset of $S_{\mathbf{a}}$, does not change $d(\mathbf{a})$.

(c) \Rightarrow (d): Let $h \in G$. It is easy to see that if d_1, \dots, d_r are representatives of distinct left cosets of $S_{\mathbf{a}}$ in G then so are hd_1, \dots, hd_r . Hence, $h(\Omega_D(\mathbf{a})) = \Omega_D(\mathbf{a})$.

(d) \Rightarrow (e): Obvious.

(e) \Rightarrow (a): If $\Omega_D(\mathbf{a}) \in L_n^G$ then clearly $\mathbf{a} \in \text{Supp}(\Omega_D(\mathbf{a})) \subset \text{Supp}(L_n^G)$. \square

If H is a subgroup of $\text{GL}_n(\mathbb{Z})$ then, following [6, Definition 2.5], we set

$$A(H)^{\succ} := \{\mathbf{a} \in \mathbb{Z}^n \mid h(\mathbf{a}) \succeq \mathbf{a} \quad \forall h \in H\}.$$

It is easy to see that $A(H)^{\succ} = \text{In}(L_n^H)$; see [6, Lemma 2.6].

Corollary 4.2. $\text{In}(L_n^G) = A(\overline{G})^{\succ} \cap \{\mathbf{a} \in \mathbb{Z}^n \mid \eta_{\mathbf{a}} = 1\}$.

Proof. The inclusion $\text{In}(L_n^G) \subset A(\overline{G})^{\succ}$ is clear from the definition. On the other hand, by Lemma 4.1

$$\text{In}(L_n^G) \subset \text{Supp}(L_n^G) \subset \{\mathbf{a} \in \mathbb{Z}^n \mid \eta_{\mathbf{a}} = 1\}.$$

This shows that $\text{In}(L_n^G) \subset A(\overline{G})^{\succ} \cap \{\mathbf{a} \in \mathbb{Z}^n \mid \eta_{\mathbf{a}} = 1\}$.

To prove the opposite inclusion, note that by Lemma 4.1 if $\eta_{\mathbf{a}} = 1$ then $\Omega(\mathbf{a}) \in L_n^G$. If moreover $\mathbf{a} \in A(\overline{G})^{\succ}$, then $\mathbf{a} = \mathbf{in}(\Omega(\mathbf{a})) \in \text{In}(L_n^G)$. \square

We are now ready to show that conditions (1) and (3) of Theorem 1.1 are equivalent. Let $\mathbf{a} \in \mathbb{Z}^n$. Clearly $S_{r\mathbf{a}} = S_{\mathbf{a}}$ and $\eta_{r\mathbf{a}} = \eta_{\mathbf{a}}^r$ for any non-zero integer r . This implies that $\eta_{r\mathbf{a}} = 1$ for any r divisible by the order of $S_{\mathbf{a}}$. Taking $r = |\overline{G}|$ we see that $\eta_{r\mathbf{a}} = 1$ for every $\mathbf{a} \in \mathbb{Z}^n$. Thus by Corollary 4.2, $|G| \cdot A(\overline{G})^{\succ} \subset \text{In}(L_n^G) \subset A(\overline{G})^{\succ}$. Equivalently,

$$|G| \cdot \text{In}(L_n^{\overline{G}}) \subset \text{In}(L_n^G) \subset \text{In}(L_n^{\overline{G}}).$$

By [6, Theorem 1.6], $\text{In}(L_n^{\overline{G}})$ is finitely generated if and only if \overline{G} is generated by reflections. Lemma 3.1 now tells us that the same is true of $\text{In}(L_n^G)$. In other words, conditions (1) and (3) of Theorem 1.1 are equivalent.

5. TERMINATION OF THE SUBDUCTION ALGORITHM

In this section we will finish the proof of Theorem 1.1. We have shown that conditions (1) and (3) are equivalent. Moreover, by definition (2) \Rightarrow (1). Thus it remains to show that (3) \Rightarrow (2). This implication is a consequence of the following proposition.

Proposition 5.1. *Let G be a finite subgroup of $\text{Aut}(L_n)$. Assume that $\pi(G) \subset \text{GL}_n(\mathbb{Z})$ is generated by reflections. If $\mathbf{a}_1, \dots, \mathbf{a}_m$ generate the semi-group $\text{In}(L_n^G)$ then $p_1 = \Omega(\mathbf{a}_1), \dots, p_m = \Omega(\mathbf{a}_m)$ form a SAGBI basis in L_n^G .*

The proof of this proposition is essentially the same as the proof of [6, Proposition 5.8]; for the sake of completeness we outline the argument below.

Proof. Suppose we apply the subduction algorithm to express $f \in L_n^G$ as a polynomial in p_1, \dots, p_m . The algorithm produces a sequence of elements $f_0 = f, f_1, f_2, \dots$ with initial terms

$$(5) \quad \mathbf{in}(f_0) \succ \mathbf{in}(f_1) \succ \mathbf{in}(f_2) \succ \dots$$

We need to show that this sequence will terminate, regardless of the choice of f or the choices we made in carrying out the subduction algorithm. We will argue by contradiction: assume that the above sequence does not terminate for some $f \in L_n^G$.

Let us embed $G \subset \text{GL}_n(\mathbb{Z})$ into $\text{GL}_n(\mathbb{R})$ in the natural way, lifting the G -action from \mathbb{Z}^n to \mathbb{R}^n . An easy exercise in linear algebra shows that \mathbb{R}^n is the direct sum of two G -invariant subspaces,

$$(\mathbb{R}^n)^G = \{\mathbf{v} \in \mathbb{R}^n \mid g(\mathbf{v}) = \mathbf{v} \quad \forall g \in G\}$$

and

$$(\mathbb{R}^n)_0 = \{\mathbf{v} \in \mathbb{R}^n \mid \sum_{g \in G} g(\mathbf{v}) = \mathbf{0}\}$$

and that $(\mathbb{R}^n)_0$ is the orthogonal complement of $(\mathbb{R}^n)^G$ relative to any G -invariant scalar product on \mathbb{R}^n . We also have G -invariant linear maps $\pi_1: \mathbb{R}^n \rightarrow (\mathbb{R}^n)^G$ and $\pi_2: \mathbb{R}^n \rightarrow (\mathbb{R}^n)_0$ given by

$$\pi_1(\mathbf{v}) = \sum_{g \in G} g(\mathbf{v}) \quad \text{and} \quad \pi_2(\mathbf{v}) = |G|\mathbf{v} - \pi_1(\mathbf{v}),$$

which are simply the orthogonal projections of $|G|\mathbf{v}$ onto $(\mathbb{R}^n)^G$ and $(\mathbb{R}^n)_0$ respectively. Note that both π_1 and π_2 are defined over the integers (i.e., carry \mathbb{Z}^n into itself); this is the reason we did not divide by $|G|$ in the formulas.

Arguing as in the proof of [6, Proposition 5.8], we see that the sequence

$$\pi_1(\mathbf{in}(f_0)), \pi_1(\mathbf{in}(f_1)), \pi_1(\mathbf{in}(f_2)), \dots$$

assumes only finitely many values. Thus, we can choose an infinite subsequence $\mathbf{w}_1 \succ \mathbf{w}_2 \succ \mathbf{w}_3 \succ \dots$ of the sequence (5) such that $\pi_1(\mathbf{w}_i) = \mathbf{c}$ is the

same for every $i \geq 1$. The argument in the proof of [6, Proposition 5.8] then shows that

$$\pi_2(\mathbf{w}_1) \succ \pi_2(\mathbf{w}_2) \succ \dots$$

is an infinite strictly decreasing sequence in $A^\succ(\overline{G}) \cap (\mathbb{R}^n)_0$. On the other hand, by [6, Lemma 5.3(a) and Proposition 5.5] this sequence has to terminate. This contradiction shows that the sequence (5) always terminates. This completes the proof of Proposition 5.1 and thus of Theorem 1.1. \square

6. THE GENERALIZED GÖBEL'S CONJECTURE

We now return to the setting we introduced at the beginning of Section 1, where we asked which k -subalgebras R of the polynomial algebra $P_n = k[x_1, \dots, x_n]$ have a SAGBI basis. Suppose $G \subset \Sigma_n$ acts on P_n by permuting the variables. Here, Σ_n denotes the permutation group on n letters. Göbel [3, p. 65] conjectured that $R = P_n^G$ has a SAGBI basis if and only if G is conjugate to $\Sigma_{n_1} \times \dots \times \Sigma_{n_k}$ for some partition (n_1, \dots, n_r) of n . This conjecture was proved independently by Kuroda [5], Thiéry–Thomassé [10] and the second author [6].

Now, in the spirit of Theorem 1.1, we replace Σ_n with $N = \mathbb{G}_m^n \rtimes \Sigma_n$, where Σ_n acts on \mathbb{G}_m^n by permuting the factors. Note that N is naturally embedded into the group $\text{Aut}(L_n) = \mathbb{G}_m^n \rtimes \text{GL}_n(\mathbb{Z})$. Moreover, every element of $N \subset \text{Aut}(L_n)$ preserves the polynomial ring P_n and restricts to an automorphism of P_n . That is, \mathbb{G}_m^n acts by rescaling and Σ_n by permuting the variables x_1, \dots, x_n . We will denote the natural projection $N \rightarrow N/(\mathbb{G}_m^n) = \Sigma_n$ by π , as before.

Theorem 6.1 (Generalized Göbel's conjecture). *Suppose G is a finite subgroup of $\mathbb{G}_m^n \rtimes \Sigma_n$, acting naturally on $P_n = k[x_1, \dots, x_n]$. Then P_n^G has a finite SAGBI basis if and only if $\pi(G) \simeq \Sigma_{n_1} \times \dots \times \Sigma_{n_k}$ for some partition (n_1, \dots, n_r) of n .*

Proof. Recall from the introduction that we only need to show that $\text{In}(P_n^G)$ is finitely generated; termination of the subduction algorithm is automatic in P_n .

We will use the notations of Section 4, except that we always take \mathbf{a} in \mathbb{N}^n , rather than in all of \mathbb{Z}^n . In particular, we will denote $\pi(G)$ by \overline{G} and view it as a subgroup of Σ_n . Note that if $\eta_{\mathbf{a}} = 1$ for some $\mathbf{a} \in \mathbb{N}^n$ then, by definition, $\Omega(\mathbf{a}) \in P_n$. Arguing exactly as in Section 4 we show that

$$\text{In}(P_n^G) = A(\overline{G})^\succ \cap \{\mathbf{a} \in \mathbb{N}^n \mid \eta_{\mathbf{a}} = 1\}$$

and thus

$$|G| \cdot (A(\overline{G})^\succ \cap \mathbb{N}^n) \subset \text{In}(P_n^G) \subset A(\overline{G})^\succ \cap \mathbb{N}^n.$$

We know that $\text{In}(P_n^G) = A(\overline{G})^\succ \cap \mathbb{N}^n$ is a finitely generated semigroup if and only if $\overline{G} \simeq \Sigma_{n_1} \times \dots \times \Sigma_{n_k}$ for some partition (n_1, \dots, n_r) of n (this is Göbel's original conjecture). The desired conclusion now follows from the Sandwich Lemma 3.1. \square

7. AN EXAMPLE

Consider the cyclic subgroup $G = \langle h \rangle$ of $N = \mathbb{G}_m^n \rtimes \Sigma_n \subset \text{Aut}(L_n)$, where

$$h: \begin{aligned} x_1 &\mapsto \lambda_1 x_2 \\ x_2 &\mapsto \lambda_2 x_3 \\ &\dots \\ x_n &\mapsto \lambda_n x_1 \end{aligned}$$

for some $\lambda_1, \dots, \lambda_n \in k$. To ensure that h has finite order, we will assume that the product $\lambda_1 \lambda_2 \cdots \lambda_n$ is a root of unity, say a primitive d th root of unity. We will denote this product by ζ .

Since $\pi(h)$ is the n -cycle $(12 \dots n)$ in Σ_n , Theorem 1.1 tells us that L_n^G has a SAGBI basis if and only if $n = 2$. Similarly, Theorem 6.1 tells us that P_n^G has a SAGBI basis if and only if $n = 2$.

We will now set $n = 2$, and find explicit SAGBI bases for these rings, relative to the lexicographic term order where $x_1 \succ x_2$. To reduce the number of subscripts, we will write x and y instead of x_1 and x_2 , respectively. We begin by computing the groups $S_{\mathbf{a}}$ and the characters $\eta_{\mathbf{a}}: S_{\mathbf{a}} \rightarrow k^*$. If $\mathbf{a} = (s, s)$, for some integer s then $S_{\mathbf{a}}$ is the whole group G . Moreover, $h \cdot x^s y^s = \zeta^s x^s y^s$ so $\eta_{(s,s)}(h) = \zeta^s$. The character $\eta_{(s,s)}$ is trivial if and only if s is divisible by d .

Now let $\mathbf{a} = (s, t)$, where $s > t$. Here $S_{\mathbf{a}}$ is the subgroup $\langle h^2 \rangle$ of G of index 2. Since $h^2 \cdot x^s y^t = \zeta^{s+t} x^s y^t$, the character $\eta_{\mathbf{a}}: S_{\mathbf{a}} \rightarrow k^*$ is given by $\eta_{(s,t)}(h^2) = \zeta^{s+t}$. This character is trivial if and only if $s + t$ is divisible by d . Using Corollary 4.2, we conclude that

$$\begin{aligned} \text{In}(L_2^G) &= A(\overline{G})^\succ \cap \{\mathbf{a} \in \mathbb{Z}^n \mid \eta_{\mathbf{a}} = 1\} \\ &= \{(s, s) \mid s \in d\mathbb{Z}\} \cup \{(s, t) \mid s > t \text{ and } s + t \in d\mathbb{Z}\} \subset \mathbb{Z}^2. \end{aligned}$$

Similarly,

$$\begin{aligned} \text{In}(P_2^G) &= A(\overline{G})^\succ \cap \{\mathbf{a} \in \mathbb{N}^n \mid \eta_{\mathbf{a}} = 1\} \\ &= \{(s, s) \mid s \in d\mathbb{N}\} \cup \{(s, t) \mid s > t \text{ and } s + t \in d\mathbb{N}\} \subset \mathbb{N}^2. \end{aligned}$$

Lemma 7.1. (a) If $d = 2r + 1$ is odd then the semigroup $\text{In}(L_2^G)$ is generated by

$$\mathbf{a}_1 = (d, d), \mathbf{a}_2 = (-d, -d) \text{ and } \mathbf{a}_3^{odd} = (r + 1, r).$$

Moreover, $\Omega(\mathbf{a}_1) = x^d y^d$, $\Omega(\mathbf{a}_2) = x^{-d} y^{-d}$, and $\Omega(\mathbf{a}_3^{odd}) = x^{r+1} y^r + \zeta^r \lambda_1 x^r y^{r+1}$ form a SAGBI basis of $\text{In}(L_2^G)$.

(b) If $d = 2r$ is even then the semigroup $\text{In}(L_2^G)$ is generated by

$$\mathbf{a}_1 = (d, d), \mathbf{a}_2 = (-d, -d), \mathbf{a}_3^{even} = (r + 1, r - 1) \text{ and } \mathbf{a}_4^{even} = (d + 1, d - 1).$$

Moreover, $\Omega(\mathbf{a}_1) = x^d y^d$, $\Omega(\mathbf{a}_2) = x^{-d} y^{-d}$, $\Omega(\mathbf{a}_3^{even}) = x^{r+1} y^{r-1} - \lambda_1 \lambda_2^{-1} x^{r-1} y^{r+1}$ and $\Omega(\mathbf{a}_4^{even}) = x^{d+1} y^{d-1} + \lambda_1 \lambda_2^{-1} x^{d-1} y^{d+1}$ form a SAGBI basis of $\text{In}(L_2^G)$.

Proof. In view of Proposition 5.1, we only need to prove that the given set of initial exponents generates $\text{In}(L_2^G)$ in parts (a) and (b). That is, we

want to show that any given $(s, t) \in \text{In}(L_2^G)$ can be expressed as a \mathbb{N} -linear combination of our generators. Choose $k \in \mathbb{Z}$ so that $s + t = kd$.

(a) If $d = 2r + 1$ is odd then

$$(s, t) = ((r + 1)k - s)(d, d) + (s - t)(r + 1, r).$$

(b) Suppose $d = 2r$ is even. We may assume without loss of generality that $s > t$; otherwise $(s, t) = (s, s)$ is a non-negative integer multiple of \mathbf{a}_1 or \mathbf{a}_2 . Since $s + t$ is divisible by d , it is even, and hence, so is $s - t$. Let $m = (s - t)/2$. Now

$$(s, t) = \frac{k - m}{2}(d, d) + m(r + 1, r - 1)$$

if $k - m$ is even, and

$$(s, t) = \frac{k - m - 1}{2}(d, d) + (m - 1)(r + 1, r - 1) + (d + 1, d - 1)$$

if $k - m$ is odd. □

We now turn to the problem of constructing a SAGBI basis for P_2^G .

Lemma 7.2. (a) *The semigroup $\text{In}(P_2^G)$ is generated by*

$$\mathbf{b}_i = (d - i, i) \text{ and } \mathbf{c}_j = (2d - j, j) ,$$

as i ranges from 0 to $\lfloor \frac{d-1}{2} \rfloor$ and j ranges from 1 to d .

(b) *The elements $\Omega(\mathbf{b}_i) = x^{d-i}y^i + \zeta^i \lambda_1^{d-2i} x^i y^{d-i}$ and $\Omega(\mathbf{c}_j) = x^{2d-j}y^j + \zeta^j \lambda_1^{2d-2j} x^j y^{2d-j}$ form a SAGBI basis for $\text{In}(P_n^G)$, as i ranges from 0 to $\lfloor \frac{d-1}{2} \rfloor$ and j ranges from 1 to d .*

Proof. By the definition of a SAGBI basis in a subalgebra of P_n , (b) is an immediate consequence of (a). Thus we only need to show that every $(s, t) \in \text{In}(P_2^G)$ lies in Λ , where Λ is the semigroup generated by all \mathbf{b}_i and \mathbf{c}_j . If $s = t$ this is obvious, since in this case $(s, t) = (s, s)$ is a non-negative integer multiple of $\mathbf{c}_d = (d, d)$. We may thus assume that $s > t$. After subtracting a suitable non-negative integer multiple of \mathbf{c}_d , we may assume that $0 \leq t \leq d - 1$. Moreover, after subtracting a suitable multiple of $\mathbf{b}_0 = (d, 0)$, we may assume that $0 < s - t \leq d$. Thus $s + t = (s - t) + 2t \leq 3d - 2$, i.e., $s + t = d$ or $2d$. In other words, $(s, t) = \mathbf{b}_t$ or \mathbf{c}_t . In particular, $(s, t) \in \Lambda$, as claimed. □

The set of generators given in Lemma 7.2 is not minimal. In fact, if $d = 2r$ is even, we only need $\mathbf{b}_0, \dots, \mathbf{b}_{r-1}, \mathbf{c}_{d-1}$ and \mathbf{c}_d , and if d is odd, only $\mathbf{b}_0, \dots, \mathbf{b}_r$ and \mathbf{c}_d . We leave a proof of these assertions as an exercise for the reader.

REFERENCES

- [1] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. An introduction to computational algebraic geometry and commutative algebra.
- [2] Leonard Eugene Dickson. Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *American Journal of Mathematics*, 35(4):413–422, 1913.
- [3] Manfred Göbel. The optimal lower bound for generators of invariant rings without finite SAGBI bases with respect to any admissible order. *Discrete Math. Theor. Comput. Sci.*, 3(2):65–70 (electronic), 1999.
- [4] Manfred Göbel. Finite SAGBI bases for polynomial invariants of conjugates of alternating groups. *Math. Comp.*, 71(238):761–765 (electronic), 2002.
- [5] Shigeru Kuroda. The infiniteness of the SAGBI bases for certain invariant rings. *Osaka J. Math.*, 39(3):665–680, 2002.
- [6] Zinovy Reichstein. SAGBI bases in rings of multiplicative invariants. *Comment. Math. Helv.*, 78(1):185–202, 2003.
- [7] Lorenzo Robbiano and Moss Sweedler. Subalgebra bases. In *Commutative algebra (Salvador, 1988)*, volume 1430 of *Lecture Notes in Math.*, pages 61–87. Springer, Berlin, 1990.
- [8] Bernd Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.
- [9] Mohammed Tesemma. On multiplicative invariants of finite reflection groups. *Comm. Algebra*, 35(7):2258–2274, 2007.
- [10] N. M. Thiéry and S. Thomassé. Convex cones and SAGBI bases of permutation invariants. In *Invariant theory in all characteristics*, volume 35 of *CRM Proc. Lecture Notes*, pages 259–263. Amer. Math. Soc., Providence, RI, 2004.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2, CANADA