SAGBI bases in rings of multiplicative invariants

Autor(en): **Reichstein, Zinovy**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **78 (2003)**

PDF erstellt am: **27.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-58753

Comment. Math. Helv. 78 (2003) 185–202
0010-2571/03/010185-18

Commentarii Mathematici Helvetici

SAGBI bases in rings of multiplicative invariants

Zinovy Reichstein

Abstract. Let k be a field and G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$. We show that the ring of multiplicative invariants $k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]^G$ has a finite SAGBI basis if and only if G is generated by reflections.

Mathematics Subject Classification (2000). 13A50, 20C10, 13P99, 52B20, 52B55.

Keywords. SAGBI basis, term order, initial term, subduction algorithm, Gröbner basis, multiplicative groups action, algebra of invariants, integral representation, reflection group, permutation group, convex cone, polyhedral cone, finitely generated semigroup.

1. Introduction

Let $k[x] = k[x_1, \dots, x_n]$ be the polynomial ring in n variables over a field k and let $\mathbb{N}$ denotes the set of non-negative integers. If $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{N}^n$, we shall write $x^{\mathbf{a}}$ in place of $x_1^{a_1} \dots x_n^{a_n}$. We begin by recalling the following:

Definition 1.1. A term order in $k[x]$ is a total order $\succ$ on $\mathbb{N}^n$ such that
(i) $\mathbf{a} \succ (0, \dots, 0)$ for every nonzero $\mathbf{a} \in \mathbb{N}^n$, and
(ii) $\succ$ is compatible with addition, i.e., if $\mathbf{a} \succ \mathbf{b}$ then $\mathbf{a} + \mathbf{c} \succ \mathbf{b} + \mathbf{c}$ for any $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$. (Equivalently, if $\mathbf{a} \succ \mathbf{b}$ and and $\mathbf{c} \succeq \mathbf{d}$ then $\mathbf{a} + \mathbf{c} \succ \mathbf{b} + \mathbf{d}$.)

A prototypical example is the usual lexicographic order on $\mathbb{N}^n$; other examples can be found in, e.g, [3, Section 1.2] and [16, p. 4]. Given a non-zero element $f = \sum c_{\mathbf{a}} x^{\mathbf{a}} \in k[x]$, we define the initial exponent $\mathbf{in}(f)$ of f to be the largest exponent $\mathbf{a}$ (with respect to $\succ$) such that $c_{\mathbf{a}} \neq 0$. If R is a subring of $k[x]$ then we define

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

It is easy to see that $\mathrm{In}(R)$ is a subsemigroup of $\mathbb{N}^n$. If $\{\mathbf{in}(f_\lambda) \,|\, \lambda \in \Lambda\}$ is a generating set for this semigroup, where each $f_\lambda \in R$, then $R = k[f_\lambda \,|\, \lambda \in \Lambda]$. In fact, a simple algorithm, due to Kapur–Madlener [10] and Robbiano–Sweedler [14],

Supported in part by an NSERC research grant.

expresses a given nonzero element $\alpha \in R$ as a polynomial in f_λ as follows. Write $\mathbf{in}(\alpha) = d_1\mathbf{in}(f_{\lambda_1}) + \cdots + d_r\mathbf{in}(f_{\lambda_r})$ for some $d_1, \dots, d_r \in \mathbb{N}$. Dividing the leading coefficient of α by the leading coefficient of $f_{\lambda_1}^{d_1} \dots f_{\lambda_r}^{d_r}$, we obtain a $c \in k$ such that the leading term of α is the same as the leading term of $cf_{\lambda_1}^{d_1} \dots f_{\lambda_r}^{d_r}$. Set $\alpha_1 = \alpha - cf_{\lambda_1}^{d_1} \dots f_{\lambda_r}^{d_r}$. If $\alpha_1 = 0$ then we are done; otherwise we replace α by α_1 and proceed inductively. Since α_1 has a smaller leading exponent than α, and $\mathbb{N}^n$ is well ordered with respect to $\succ$ (see [3, Corollary 2.4.6]), this process will terminate, resulting in an expression for α as a polynomial in f_λ. We shall refer to this procedure as the *subduction algorithm*.

The subduction algorithm is analogous to expressing an element of an ideal of $k[x]$ in terms of a Gröbner basis; for this reason a generating set for the semigroup $\mathrm{In}(R)$ is called a SAGBI basis of R, where SAGBI stands for "Subalgebra Analog to Gröbner Bases for Ideals". (The terms "SAGBI basis" and "subduction algorithm" were introduced by Robbiano and Sweedler in [14].) The analogy with Gröbner bases is not perfect though because not every subring $R \subset k[x]$ has a finite SAGBI basis; see e.g., [14, 1.20 or 4.11], or [16, pp. 99–100]. It is an important open problem to determine which subrings R of $k[x]$ have a finite SAGBI basis; see [16, p. 100].

We will now consider a parallel situation, where R is a subring of the ring $k[x^{\pm 1}] = k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ of Laurent polynomials in n variables over k. Our first task is to define a term order in $k[x^{\pm 1}]$.

Definition 1.2. By a term order in $k[x^{\pm 1}]$ we shall mean a total order $\succ$ on $\mathbb{Z}^n$ compatible with addition. That is, if $\mathbf{a} \succ \mathbf{b}$ then $\mathbf{a}+\mathbf{c} \succ \mathbf{b}+\mathbf{c}$ for any $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{Z}^n$.

Our requirements on $\succ$ are considerably weaker here than in Definition 1.1. In fact, conditions (i) and (ii) of Definition 1.1 cannot both hold in an ordered group; thus we have little choice but to drop (i).

Given a term order in $k[x^{\pm 1}]$, we can define the initial exponent $\mathbf{in}(f)$ for every nonzero $f \in R$ and the semigroup of initial exponents $\mathrm{In}(R)$ in the same way as before; cf. (1). We shall say that $\{f_\lambda \mid \lambda \in \Lambda\} \subset R$ is a SAGBI basis of R if

(a) $\mathbf{in}(f_\lambda)$ generate $\mathrm{In}(R)$ as a semigroup, as λ ranges over Λ, and

(b) the subduction algorithm described above terminates for every $\alpha \in R$.

Note that the steps in the subduction algorithm are not always uniquely determined. Each step involves writing an element of $\mathrm{In}(R)$ as a nonnegative integral linear combination of $\mathbf{in}(f_\lambda)$, and there may be more than one way to do this. Condition (b) requires that the algorithm should terminate no matter what choices are made.

The question we would like to address is:

Question 1.3. Which subrings R of the Laurent polynomial ring $k[x^{\pm 1}]$ have a finite SAGBI basis?

At first glance, this is a rather odd question to ask. First of all, we have to

decide whether or not $\mathrm{In}(R)$ is finitely generated, and as we pointed out above, this is an open problem even in the special case where R is contained in the polynomial ring $k[x]$. Secondly, a priori the existence of a finite SAGBI basis depends on the term order $\succ$. Thirdly, for the purpose of performing computations, we would like the answer to be positive. On the other hand, since $\mathbb{Z}^n$ is not well ordered with respect to $\succ$, there is no reason to expect the subduction algorithm to terminate. Thus even in those cases where we can establish that $\mathrm{In}(R)$ is finitely generated, the answer appears likely to be negative.

The purpose of this paper is to show that, notwithstanding these considerations, Question 1.3 can be completely answered in the case where R is the invariant ring for a multiplicative group action and that for many rings of this type, the answer is, indeed, positive, without any assumptions on the base field k or on the term order $\succ$.

Before stating our main results, we need to introduce some terminology. Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Recall that the natural (multiplicative) action of G on $k[x^{\pm 1}] = k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ is defined by linearly extending the formula $g(x^{\mathbf{a}}) = x^{g(\mathbf{a})}$ to all of $k[x^{\pm 1}]$; here, as usual, $x^{\mathbf{a}} = x_1^{a_1} \ldots x_n^{a_n}$ is a Laurent monomial. Recall also that $g \in \mathrm{GL}_n(\mathbb{R})$ is called a *reflection* if $g^2 = id$, and the eigenvalues of g are -1 (with multiplicity 1) and 1 (with multiplicity $n-1$). We shall say that $G \subset \mathrm{GL}_n(\mathbb{R})$ is a *reflection group* if G is generated by reflections.

Theorem 1.4. *Let $R = k[x^{\pm 1}]^G$ be the ring of multiplicative invariants for a finite subgroup G of $\mathrm{GL}_n(\mathbb{Z})$. Then the semigroup $\mathrm{In}(R)$ is finitely generated if and only if G is a reflection group.*

To place Theorem 1.4 in the context of invariant theory, consider the *linear* action a finite subgroup H of $\mathrm{GL}_n(k)$ on the polynomial ring $k[x] = k[x_1, \ldots, x_n]$, where k is a field whose characteristic is prime to $|H|$. Recall that a nontrivial element g of $\mathrm{GL}_n(k)$ is called a pseudo-reflection if g has finite order and 1 is an eigenvalue of g of multiplicity $n-1$. (Note that for $k \subset \mathbb{R}$ the notions of reflection and pseudo-reflection coincide.) The celebrated theorem of Chevalley, Shephard and Todd asserts that H is generated by pseudo-reflections if and only if the ring of invariants $k[x]^H$ is itself a polynomial ring; cf. e.g., [1, V.5] or [15, 2.4] . A variant of this result in the multiplicative context is due to Farkas, who showed that the multiplicative invariant ring $k[x^{\pm 1}]^G$ for a finite subgroup $G \subset \mathrm{GL}_n(\mathbb{Z})$ is a generalized polynomial ring (i.e., has the form $k[u_1^{\pm 1}, \ldots, u_m^{\pm 1}, w_1, \ldots, w_l]$, where $u_1, \ldots, u_m, w_1, \ldots, w_l$ are independent variables) if and only if G is generated by reflections and the G-lattice $\mathbb{Z}^n/(\mathbb{Z}^n)^G$ is a weight lattice in a suitable sense; see [5] and [6]. (Farkas assumed $k = \mathbb{C}$.) Theorem 1.4 may be viewed as an alternative and perhaps complementary, analogue of the Chevalley–Shephard–Todd theorem in the multiplicative setting. (Farkas' results have been recently refined and extended by Lorenz [12], [13], who showed, in particular, that if $G \subset \mathrm{GL}_n(\mathbb{Z})$ is a reflection subgroup then $k[x^{\pm 1}]^G$ is a semigroup algebra; see [13, Theorem 2.4].)

Our second main result is the following:

Theorem 1.5. *Let G be a finite reflection subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Then the invariant ring $R = k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]^G$ has a finite SAGBI basis.*

Moreover, we will show that if $(\mathbb{Z}^n)^G = (0)$ then $R = k[x^{\pm 1}]^G$ has a canonical "minimal" SAGBI basis, independent of the term order $\succ$; see Remark 7.1.

Of course, if G is not generated by reflections then, by Theorem 1.4 the invariant ring $k[x^{\pm 1}]^G$ cannot have a finite SAGBI basis. Thus Theorems 1.4 and 1.5 can be combined to give a complete answer to Question 1.3 in the case where R is a ring of multiplicative invariants:

Theorem 1.6. *Let $R = k[x^{\pm 1}]^G$ be the ring of invariants for the multiplicative action of a finite group $G \subset \mathrm{GL}_n(\mathbb{Z})$. Then the following are equivalent:*

(a) $\mathrm{In}(R)$ *is finitely generated as a semigroup,*

(b) R *has a finite SAGBI basis, and*

(c) G *is a reflection group.*

We remark that the properties of having a finitely generated semigroup of leading exponents or a finite SAGBI basis are not intrinsic to $R = k[x^{\pm 1}]^G$; they depend on the embedding of R in $k[x^{\pm 1}]$. On the other hand, Theorems 1.4-1.6 require no assumptions on the term order $\succ$ or the base field k. In fact, k can even be replaced by a rather general ring; see Remark 7.2.

Our proofs of Theorems 1.4 and 1.5 (presented, respectively, in Sections 3-4 and 5) are quite elementary; they rely only on a few simple properties of polyhedral cones and reflection groups in $\mathbb{R}^n$. Our background references for these subjects are, respectively, Ewald [4, Part 1] and Bourbaki [1, Chapter V]; some preliminary definitions and results can also be found in Section 2.

To state our last main result, consider the natural (permutation) action of a finite group $H \subset \mathrm{S}_n$ on the polynomial ring $k[x] = k[x_1, \dots, x_n]$. Göbel [7, 5.6] showed that the invariant ring $R = k[x]^H$ has a finite SAGBI basis, with respect to the usual *lexicographic term order* in $k[x]$, if and only if $H = \mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_r}$ for some partition $n_1 + \cdots + n_r = n$. Göbel further conjectured [8, p. 65] that the same should be true for an arbitrary term order in the sense of Definition 1.1 and proved this conjecture in the case where $H = \mathrm{A}_n$ is the alternating group [9]. In Section 6 we will prove Göbel's conjecture, as an application of our Theorem 1.4:

Theorem 1.7. *Let $\succ$ be a term order in $k[x] = k[x_1, \dots, x_n]$ and let $H \subset \mathrm{S}_n$ be a permutation group. Then the ring of invariants $k[x_1, \dots, x_n]^G$ has a finite SAGBI basis with respect to $\succ$ if and only if $H = \mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_r}$ for some partition $n_1 + \cdots + n_r = n$.*

Independent proofs of Theorem 1.7 were recently obtained by Kuroda [11] and Thiéry–Thomassé [17].

2. Preliminaries

2.1. Polyhedral cones

We define the *positive span* $\mathrm{Pos}(X)$ of a subset X of $\mathbb{R}^n$ to be the set of points of the form $r_1\mathbf{v_1}+\cdots+r_m\mathbf{v_m}$, where m ranges over the positive integers, $\mathbf{v_1},\ldots,\mathbf{v_m}$ range over X and $r_1,\ldots,r_m$ range over the non-negative reals.

If $X=\{\mathbf{v_1},\ldots,\mathbf{v_n}\}$ is a finite subset of $\mathbb{R}^n$ (respectively, $\mathbb{Z}^n$), then $\mathrm{Pos}(X)$ is called a *polyhedral cone* (respectively an *integral polyhedral cone*). We shall write $\mathrm{Pos}(\mathbf{v_1},\ldots,\mathbf{v_n})$ in place of $\mathrm{Pos}(\{\mathbf{v_1},\ldots,\mathbf{v_n}\})$.

Lemma 2.1. (a) *$C\subset\mathbb{R}^n$ is a polyhedral cone (respectively an integral polyhedral cone) if and only if there exist finitely many linear forms (respectively, linear forms with integer coefficients) $l_1,\ldots,l_m$ on $\mathbb{R}^n$ such that*

$$C=\{\mathbf{v}\in\mathbb{R}^n\,|\,l_1(\mathbf{v})\geq 0,\ldots,l_m(\mathbf{v})\geq 0\}\,.$$

(b) *A polyhedral cone is closed in $\mathbb{R}^n$.*

Proof. (a) is proved in [4, Theorem V.2.10]. (b) is an immediate consequence of (a). □

Lemma 2.2. *Let $C=\mathrm{Pos}(\mathbf{v_1},\ldots,\mathbf{v_m})$ be an integral polyhedral cone for some $\mathbf{v_i}=(x_{i1},\ldots,x_{in})\in\mathbb{Z}^n$. Denote the (positive) least common multiple of the non-zero minors of the $m\times n$-matrix (x_{ij}) by δ. Then for any lattice point $\mathbf{w}\in C\cap\mathbb{Z}^n$ there exist nonnegative integers $n_1,\ldots,n_r$ such that $\delta\mathbf{w}=n_1\mathbf{v_1}+\cdots+n_m\mathbf{v_m}$.*

Proof. By Carathéodory's theorem (see, e.g., [4, Theorem I.2.3(b)]), we can write $\mathbf{w}$ as a positive linear combination of a linearly independent subset of $\{\mathbf{v_1},\ldots,\mathbf{v_m}\}$. Thus we may assume without loss of generality that $\mathbf{v_1},\ldots,\mathbf{v_m}$ are linearly independent and $\mathbf{w}=r_1\mathbf{v_1}+\cdots+r_m\mathbf{v_m}$, where $r_1,\ldots,r_m>0$. Now Cramer's rule tells us that $|\det(M)|(r_1,\ldots,r_m)\in\mathbb{Z}^m$ for some nonsingular $m\times m$-submatrix M of (x_{ij}). Moreover, since $r_1,\ldots,r_m>0$ we have

$$|\det(M)|(r_1,\ldots,r_m)\in\mathbb{N}^m\,.$$

Consequently, $\delta(r_1,\ldots,r_m)\in\mathbb{N}^m$, as claimed. □

2.2. Saturated semigroups

We shall call a subsemigroup S of $\mathbb{Z}^n$ *saturated* if $n\mathbf{a}\in S$ implies $\mathbf{a}\in S$ for any $\mathbf{a}\in S$ and any integer $n\geq 1$.

Lemma 2.3. *Let S be a saturated subsemigroup of $\mathbb{Z}^n$. Then $S=\mathrm{Pos}(S)\cap\mathbb{Z}^n$.*

Proof. Clearly $S \subset \mathrm{Pos}(S) \cap \mathbb{Z}^n$. To prove the opposite inclusion, note that by Lemma 2.2, for every $\mathbf{w} \in \mathrm{Pos}(S) \cap \mathbb{Z}^n$ there exists a positive integer δ such that $\delta\mathbf{w} \in S$. Since S is saturated, $\mathbf{w} \in S$, as claimed. □

Proposition 2.4. *Let S be a saturated subsemigroup of $\mathbb{Z}^n$. Then the following are equivalent:*

(a) *S is finitely generated (as a semigroup),*

(b) *$\mathrm{Pos}(S)$ is an integral polyhedral cone.*

Proof. (a) $\Longrightarrow$ (b): If S is generated by $\mathbf{x_1}, \dots, \mathbf{x_m}$ then clearly

$$\mathrm{Pos}(S) = \mathrm{Pos}(\mathbf{x_1}, \dots, \mathbf{x_m})$$

is an integral polyhedral cone.

(b) $\Longrightarrow$ (a): By Lemma 2.3, $S = \mathrm{Pos}(S) \cap \mathbb{Z}^n$. The desired result now follows from Gordan's Lemma [4, V.3.4] which says that $\mathrm{Pos}(S) \cap \mathbb{Z}^n$ is finitely generated. □

2.3. The sets $A^{\succ}$ and $X^{\succ}$

Definition 2.5. Given a finite subgroup G of $\mathrm{GL}_n(\mathbb{Z})$, we define

$$A^{\succ}(G) = \{\mathbf{a} \in \mathbb{Z}^n \mid \mathbf{a} \succeq g(\mathbf{a}) \text{ for any } g \in G\}$$

and

$$X^{\succ}(G) = \mathrm{Pos}(A^{\succ}(G))\,.$$

If the reference to G is clear from the context, we shall write $A^{\succ}$ and $X^{\succ}$ in place of $A^{\succ}(G)$ and $X^{\succ}(G)$ respectively.

Lemma 2.6. *Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$ and let $R = k[x^{\pm 1}]^G$. Then*

(a) *$\mathrm{In}(R) = A^{\succ}(G)$.*

(b) *$\mathrm{In}(R)$ is a saturated subsemigroup of $\mathbb{Z}^n$.*

(c) *$\mathrm{In}(R)$ is a finitely generated semigroup if and only if $X^{\succ}(G)$ is an integral polyhedral cone.*

Proof. (a) Suppose $\mathbf{a} \in \mathrm{In}(R)$, i.e., $\mathbf{a} = \mathbf{in}(f)$ for some $f \in R$. Then $x^{\mathbf{a}}$ enters into $f \in R$ with a non-zero coefficient, and hence, so does $x^{g(\mathbf{a})}$ for every $g \in G$. Since $x^{\mathbf{a}}$ is the initial term of f, $\mathbf{a} \succeq g(\mathbf{a})$ for any $g \in G$. Hence, $\mathbf{a} \in A^{\succ}(G)$.

Conversely, suppose $\mathbf{a} \in A^{\succ}(G)$. Then $f = \sum x^{g(\mathbf{a})}$ is a non-zero element of R and $\mathbf{a} = \mathbf{in}(f) \in \mathrm{In}(R)$.

(b) follows from (a), since $A^{\succ}(G)$ is clearly a saturated subsemigroup of $\mathbb{Z}^n$; cf. Definition 2.5.

(c) is immediate from (b) and Proposition 2.4. □

We remark that Lemma 2.6(b) fails if we consider a linear (rather than a multiplicative) action of a finite group G, either on the polynomial ring $k[x]$ or on the Laurent polynomial ring $k[x^{\pm 1}]$. For example, suppose $n = 1$, and $G = \{1, \tau\} \simeq \mathbb{Z}/2\mathbb{Z}$ acts by $\tau(x_1) = -x_1$. Then neither $\mathrm{In}(k[x]^G) = 2\mathbb{N}$ nor $\mathrm{In}(k[x^{\pm 1}]^G) = 2\mathbb{Z}$ is a saturated subsemigroup of $\mathbb{Z}$.

2.4. Fundamental sets

Definition 2.7. Suppose a group G is acting on a set E. We shall call $F \subset E$ a *fundamental set* for this action if each G-orbit in F intersects E in exactly one point. Equivalently, F is a fundamental set for the G-action on E if the following conditions are satisfied.

(i) $\cup_{g \in G} g(F) = E$ and

(ii) If $g(a) \in F$ for some $a \in F$ and $g \in G$, then $g(a) = a$.

Note the we are not assuming anything about the topology of F (or E); for this reason we are prefer the term "fundamental set" to the more commonly used "fundaments region" or "fundamental domain".

Lemma 2.8. *Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$.*

(a) *$A^{\succ}$ is a fundamental set for the G-action on $\mathbb{Z}^n$.*

(b) *If $X^{\succ}$ is an integral polyhedral cone then $X^{\succ}$ is a fundamental set for the G-action on $\mathbb{R}^n$.*

Proof. (a) Immediate from the definition of $A^{\succ}$, since every G-orbit in $\mathbb{Z}^n$ has a unique maximal element with respect to $\succ$.

(b) To prove (i), set $V = \cup_{g \in G} g(X^{\succ})$. Then V contains $\cup_{g \in G} g(A^{\succ})$, which is equal to $\mathbb{Z}^n$ by part (a). Since V is a positive cone, i.e., $rV = V$ for every real number $r > 0$, V contains $\mathbb{Q}^n$. Since V is closed in $\mathbb{R}^n$ (cf. Lemma 2.1(b)), this implies $V = \mathbb{R}^n$, as claimed.

To prove (ii), suppose $g(\mathbf{v}) \in X^{\succ}$ for some $\mathbf{v} \in X^{\succ}$; in other words, $\mathbf{v} \in X^{\succ} \cap g^{-1}(X)$. We want to show $g(\mathbf{v}) = \mathbf{v}$. By Lemma 2.1(a), $X^{\succ} \cap g^{-1}(X^{\succ})$ is an integral polyhedral cone, i.e., $X^{\succ} \cap g^{-1}(X^{\succ}) = \mathrm{Pos}(\mathbf{v_1}, \ldots, \mathbf{v_m})$ for some $\mathbf{v_1}, \ldots, \mathbf{v_m} \in \mathbb{Z}^n$. Thus it is enough to show that $\mathbf{v_1}, \ldots, \mathbf{v_m}$ are fixed by g. In other words, we may assume without loss of generality that $\mathbf{v} = \mathbf{v_i}$ for some $i = 1, \ldots, m$. But then $\mathbf{v} \in X^{\succ} \cap \mathbb{Z}^n = A^{\succ}$ (cf. Lemma 2.3), and the desired identity, $g(\mathbf{v}) = \mathbf{v}$, follows from part (a). □

Corollary 2.9. *$A^{\succ}$ (and thus $X^{\succ}$) cannot be covered by a finite union of hyperplanes in $\mathbb{R}^n$.*

Proof. Assume the contrary: $A^{\succ} \subset H_1 \cup \cdots \cup H_r$, where each H_i is a hyperplane.

By Lemma 2.8(a), $\mathbb{Z}^n = \cup_{g\in G} g(A^{\succ})$. Thus $\mathbb{Z}^n$ is covered by the (finitely many) hyperplanes $g(H_i)$, where $g \in G$ and $1 \le i \le r$, a contradiction. □

3. Proof of Theorem 1.4: the "if" direction

In view of Lemma 2.6(c), it suffices to prove the following:

Proposition 3.1. *Suppose G is a finite reflection subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Then $X^{\succ}$ is an integral polyhedral cone.*

Proof. We will denote the reflections in G by $s_1, \dots, s_m \in G$. Let $\mathbf{e_i}$ be an eigenvector of s_i associated to the eigenvalue -1. Since $s_i \in \mathrm{GL}_n(\mathbb{Z})$, we can choose $\mathbf{e_i} \in \mathbb{Z}^n$; moreover, after possibly replacing $\mathbf{e_i}$ by $-\mathbf{e_i}$, we may assume $\mathbf{e_i} \succeq (0, \dots, 0)$. Define linear forms $l_1, \dots, l_m \colon \mathbb{R}^n \longrightarrow \mathbb{R}$ by $l_i(\mathbf{v}) = <\mathbf{v}, \mathbf{e_i}>$, where

$$<\mathbf{x}, \mathbf{y}> = \sum_{g\in G} g(\mathbf{x}) \cdot g(\mathbf{y}) \,. \tag{2}$$

is a G-invariant positive-definite bilinear form on $\mathbb{R}^n$. (Here $\mathbf{x} \cdot \mathbf{y}$ is the standard inner product on $\mathbb{R}^n$.) Note that s_i is an orthogonal (with respect to $<\cdot, \cdot>$) reflection in the hyperplane $H_i = \{\mathbf{v} \in \mathbb{R}^n \,|\, l_i = 0\}$ and that the linear forms l_i have integer coefficients.

Let $C = \{\mathbf{v} \in \mathbb{R}^n \,|\, l_i(\mathbf{v}) \ge 0 \text{ for } i = 1, \dots, m\}$. By Lemma 2.1(a), C is an integral polyhedral cone. Our goal is to prove that $X^{\succ} = C$.

First we will show that $X^{\succ} \subset C$. Recall that $X^{\succ}$ is defined as $\mathrm{Pos}(A^{\succ})$; thus it is enough to show that $A^{\succ} \subset C$. Assume the contrary: there exists a $\mathbf{v} \in A^{\succ}$ such that $\mathbf{v} \notin C$, i.e., $l_i(\mathbf{v}) < 0$ for some $i = 1, \dots, m$. Then by our choice of $\mathbf{e_i}$

$$s_i(\mathbf{v}) = \mathbf{v} - 2\frac{l_i(\mathbf{v})}{<\mathbf{v}, \mathbf{v}>}\mathbf{e_i} \succ \mathbf{v} \,,$$

contradicting $\mathbf{v} \in A^{\succ}$. This proves that $X^{\succ} \subset C$.

To prove the opposite inclusion, recall that by Corollary 2.9 $X^{\succ}$ is not contained in a finite union of hyperplanes. Since $X^{\succ} \subset C$, neither is C. Thus

$$C_0 = \{\mathbf{v} \in \mathbb{R}^n \,|\, l_i(\mathbf{v}) > 0 \text{ for } i = 1, \dots, m\}$$

is non-empty and is a chamber for the collection of hyperplanes $H_1, \dots, H_m$; cf. [1, V.3.1]. Consequently, $C = \overline{C_0}$ (see [1, V.1.3, formula (6)]) and $C \subset \mathbb{R}^n$ is a fundamental set for the G-action on $\mathbb{R}^n$ (see [1, V.3.3, Theorem 2]).

We are now ready to show that $C \subset X^{\succ}$. Suppose $C = \mathrm{Pos}(\mathbf{v_1}, \dots, \mathbf{v_t})$ for some $\mathbf{v_1}, \dots, \mathbf{v_t} \in \mathbb{Z}^n$. Then it is enough to show that each $\mathbf{v_i}$ lies in $A^{\succ}$. Set $\mathbf{v} = \mathbf{v_i}$ and choose a $g \in G$ such that $g(\mathbf{v}) \in A^{\succ}$; cf. Lemma 2.8(a). Since $A^{\succ} \subset X^{\succ} \subset C$, both $\mathbf{v}$ and $g(\mathbf{v})$ lie in C. Since C is a fundamental set for the G-action on $\mathbb{R}^n$, this implies $\mathbf{v} = g(\mathbf{v})$. In particular, $\mathbf{v} \in A^{\succ}$, as claimed. This completes the proof of Proposition 3.1. □

4. Proof of Theorem 1.4: the "only if" direction

Assume that $\mathrm{In}(k[x^{\pm 1}]^G)$ is a finitely generated semigroup for some $G \subset \mathrm{GL}_n(\mathbb{Z})$. We want to show that G is generated by reflections. By Lemma 2.6(c), $X^{\succ}$ is an integral polyhedral cone. Thus in order to complete the proof of Theorem 1.4 it suffices to establish the following:

Proposition 4.1. *Suppose X is a fundamental set for the natural action of a finite subgroup $G \subset \mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$. If X is a polyhedral cone then G is generated by reflections.*

For the purpose of proving Theorem 1.4, we only need a special case of Proposition 4.1, where $G \subset \mathrm{GL}_n(\mathbb{Z})$ and $X = X^{\succ}(G)$ is an *integral* polyhedral cone. Note however, that if $G \subset \mathrm{GL}_n(\mathbb{Z})$ and $X(G)$ is a polyhedral cone then Propositions 3.1 and 4.1 imply that $X(G)$ is automatically integral.

The rest of this section will be devoted to proving Proposition 4.1. Let $< \cdot, \cdot >$ be the G-invariant positive-definite bilinear from on $\mathbb{R}^n$ given by (2).

Since X is a fundamental set for the G-action on $\mathbb{R}^n$, X is not contained in a hyperplane; thus $\dim(X) = n$. Let $h_1, \ldots, h_m$ be the (closed) facets (i.e., $(n-1)$-dimensional faces) of X, $H_i = \mathrm{Span}_{\mathbb{R}}(h_i)$ be the hyperplane in $\mathbb{R}^n$ containing h_i, and s_i be the orthogonal (with respect to $< \cdot, \cdot >$) reflection in H_i.

Lemma 4.2. (a) *The boundary of X is contained in $Y = \cup_{g(X) \neq X} g(X)$.*

(b) *$s_i \in G$ for any $i = 1, \ldots, m$.*

Proof. (a) Assume the contrary: a boundary point $\mathbf{v}$ of X does not lie in Y. Since Y is a closed subset of $\mathbb{R}^n$ (cf. Lemma 2.1(b)), $B \cap Y = \emptyset$ for some open ball B centered at $\mathbf{v}$. Since $\mathbf{v}$ is a boundary point of X (cf. Lemma 2.1(b)), there exists a $\mathbf{w} \in B - X$. Thus $\mathbf{w} \notin Y \cup X$. On the other hand, since X is a fundamental set for the G-action on $\mathbb{R}^n$, we know that $Y \cup X = \mathbb{R}^n$, a contradiction.

(b) Suppose $\mathbf{v}$ lies in a facet h_i of X. By part (a), $g^{-1}(\mathbf{v}) \in X$, for some $1 \neq g \in G$. Since X is a fundamental set for G, this is only possible if $g^{-1}(\mathbf{v}) = \mathbf{v}$. In other words, every facet h_i lies in the union of the linear spaces L_g, where

$$L_g = (\mathbb{R}^n)^g = \{\mathbf{x} \in \mathbb{R}^n \mid g(\mathbf{x}) = \mathbf{x}\} \tag{3}$$

and g ranges over those $g \in G$ for which $g(X) \neq X$. But then each supporting hyperplane H_i also lies in $\cup_{g \in G} L_g$. Since H_i cannot be covered by a finite number of proper linear subspaces, we conclude that $H_i \subset L_{g_i}$ for some $1 \neq g_i \in G$. Since $\dim(H_i) = n - 1$ and $\dim(L_{g_i}) \leq n - 1$, this is only possible if $H_i = L_{g_i}$. Since g_i preserves $< \cdot, \cdot >$ and fixes each point of H_i, we conclude that g_i is the orthogonal reflection in H_i, i.e., $g_i = s_i$. Thus $s_i \in G$, as claimed. □

We are now ready to complete the proof of Proposition 4.1. Let G_0 be the subgroup of G generated by $s_1, \ldots, s_m$, and let F be the collection of hyperplanes

of the form $g_0(H_i)$, where $g_0 \in G_0$ and $i = 1, \dots, m$. Note that F is a G_0-invariant collection of hyperplanes in $\mathbb{R}^n$ and that G_0 contains the orthogonal reflection $g_0 s_i g_0^{-1}$ in the hyperplane $g_0(H_i)$.

Since X is a fundamental set for the G-action on $\mathbb{R}^n$, it cannot be covered by finitely many hyperplanes. Thus we can choose a point $\mathbf{v}$ in X such that $g(\mathbf{v}) \neq \mathbf{v}$ for any $1 \neq g \in G$. In particular $\mathbf{v} \notin H$ for any hyperplane $H \in F$; otherwise $s(\mathbf{v}) = \mathbf{v}$, where $s \in G_0 \subset G$ is the orthogonal reflection in H. Now let C be the (unique) chamber, relative to the collection of hyperplanes F, such that $\mathbf{v} \in C$. Since $H_1, \dots, H_m \in F$, we have $C \subset X$. Moreover, since X is closed in $\mathbb{R}^n$ (cf. Lemma 2.1(b)), $\overline{C} \subset X$. By [1, Lemma V.3.1.1], $\overline{C}$ is a fundamental set for the action of G_0 on $\mathbb{R}^n$. In particular, every point in $\mathbb{R}^n$ can be written in the form $g_0(\mathbf{c})$ for some $\mathbf{c} \in \overline{C}$ and $g_0 \in G_0$.

We claim that $G = G_0$. Indeed, suppose $g \in G$. Write $g(\mathbf{v})$ as $g_0(\mathbf{c})$ for some $\mathbf{c} \in \overline{C}$. Since X is a fundamental set for the action of G on $\mathbb{R}^n$ and both $\mathbf{v}$ and $\mathbf{c} = g_0^{-1} g(\mathbf{v})$ lie in X, we conclude that $\mathbf{v} = \mathbf{c}$, or equivalently $g_0^{-1} g \in \mathrm{Stab}_G(\mathbf{v})$. But $\mathrm{Stab}_G(\mathbf{v}) = \{1\}$ by our choice of $\mathbf{v}$. Thus $g = g_0 \in G_0$. This shows that $G = G_0$, i.e., G is generated by reflections. □

5. Proof of Theorem 1.5

We now return to the situation of Section 3; we begin by recalling the notations introduced there. Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Denote the reflections contained in G by $s_1, \dots, s_m$; we shall assume that these elements generate G. For each $i = 1, \dots, m$ choose an eigenvector $\mathbf{e_i} \in \mathbb{Z}^n$ of s_i associated to eigenvalue -1. After possibly replacing $\mathbf{e_i}$ by $-\mathbf{e_i}$, we may assume $\mathbf{e_i} \succ (0, \dots, 0)$ for every i. We fix a G-invariant positive-definite bilinear form $< \cdot, \cdot >$ defined over $\mathbb{Z}$; cf. (2). For $i = 1, \dots, m$, set $l_i(\mathbf{v}) = <\mathbf{v}, \mathbf{e_i}>$ and $H_i = \{\mathbf{v} \in \mathbb{R}^n \,|\, l_i(\mathbf{v}) = 0\}$; note that each l_i is a linear form on $\mathbb{R}^n$ with integer coefficients. In Section 3 we showed that

$$C_0 = \{\mathbf{v} \in \mathbb{R}^n \,|\, l_i(\mathbf{v}) > 0 \text{ for } i = 1, \dots, m\}$$

is a chamber for the collection of hyperplanes $H_1, \dots, H_m$ and

$$X^{\succ} = \overline{C_0} = \{\mathbf{v} \in \mathbb{R}^n \,|\, l_i(\mathbf{v}) \geq 0 \text{ for } i = 1, \dots, m\}. \tag{4}$$

After possibly renumbering the reflections $s_1, \dots, s_m$, we may assume that the hyperplanes $H_1, \dots, H_t$ are the walls of C_0 for some $t \leq m$. That is,

$$X^{\succ} = \{\mathbf{v} \in \mathbb{R}^n \,|\, l_i(\mathbf{v}) \geq 0 \text{ for } i = 1, \dots, t\}. \tag{5}$$

Lemma 5.1. $<\mathbf{e_i}, \mathbf{e_j}> \leq 0$ *for any distinct* $i, j = 1, \dots, t$.

Proof. Since $A^{\succ}$ is not contained in a finite union of hyperplanes (see Corollary 2.9), there exists a point $\mathbf{v} \in A^{\succ} \cap C_0$. Now by the definition of $A^{\succ}$,

$$\mathbf{n_i} = s_i(\mathbf{v}) - \mathbf{v} = -2\frac{l_i(\mathbf{v})}{<\mathbf{v}, \mathbf{v}>}\mathbf{e_i}$$

is an inward normal vector to H_i. Note that $l_i(\mathbf{v}) > 0$, because $\mathbf{v}$ lies in C_0. Thus $\mathbf{n_i}$ is a negative multiple of $\mathbf{e_i}$ for every $i = 1, \ldots, t$. The lemma now follows from by [1, Proposition V.3.4.3(iii)], which says that $<\mathbf{n_i}, \mathbf{n_j}> \leq 0$. □

Lemma 5.2. *Suppose* $\mathbf{v} \in \mathbb{Z}^n$. *Then the following are equivalent:*

(a) $g(\mathbf{v}) = \mathbf{v}$ *for every* $g \in G$,
(b) *both* $\mathbf{v}$ *and* $-\mathbf{v}$ *lie in* $A^{\succ}$,
(c) *both* $\mathbf{v}$ *and* $-\mathbf{v}$ *lie in* $X^{\succ}$,
(d) $l_i(\mathbf{v}) = 0$ *for every* $i = 1, \ldots, m$,
(e) $l_i(\mathbf{v}) = 0$ *for every* $i = 1, \ldots, t$.

Proof. (a) ⇔ (b): By Definition 2.5, $\mathbf{v} \in A^{\succ}$ iff $\mathbf{v} \succeq g(\mathbf{v})$ for every $g \in G$. Thus $-\mathbf{v} \in A^{\succ}$ iff $\mathbf{v} \preceq g(\mathbf{v})$ for every $g \in G$, and $\mathbf{v}, -\mathbf{v}$ both lie in $A^{\succ}$ iff $\mathbf{v} = g(\mathbf{v})$ for every $g \in G$, i.e., $\mathbf{v} \in (\mathbb{Z}^n)^G$.

(b) ⇔ (c) follows from the fact that $A^{\succ} = X^{\succ} \cap \mathbb{Z}^n$; cf. Lemma 2.3.

(c) ⇔ (d) follows from (4).

(c) ⇔ (e) follows from (5). □

Lemma 5.3. (a) $(\mathbb{R}^n)^G = \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \ldots, \mathbf{e_m})^{\perp} = \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \ldots, \mathbf{e_t})^{\perp}$, *where* $W^{\perp}$ *denotes the orthogonal complement of a subspace* W *in* $\mathbb{R}^n$.

(b) $(\mathbb{Z}^n)^G = (0)$ *if and only if* $\mathbf{e_1}, \ldots, \mathbf{e_t}$ *span* $\mathbb{R}^n$.

Proof. (a) is an immediate consequence of Lemma 5.2. (b) Follows from (a) and the fact that the vector space $(\mathbb{R}^n)^G$ is defined over $\mathbb{Q}$. □

Remark 5.4. In the language of [4], Lemma 5.3(b) can be restated as follows: $(\mathbb{Z}^n)^G = (0)$ if and only if $X^{\succ}$ has an apex at (0); cf. [4, Lemma V.2.2(c)].

Proposition 5.5. $A^{\succ} \cap \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \ldots, \mathbf{e_t})$ *is well ordered with respect to* $\succ$.

Proof. (a) Assume the contrary: there exists an infinite strictly decreasing sequence

$$\mathbf{a_1} \succ \mathbf{a_2} \succ \mathbf{a_3} \succ \ldots \tag{6}$$

in $A^{\succ} \cap \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \ldots, \mathbf{e_t})$. Note that $l_1(\mathbf{a_i})$ is a non-negative integer for every $i \geq 1$. Thus we can choose $i_1 \geq 1$ so that $l_1(\mathbf{a_{i_1}}) \leq l_1(\mathbf{a_i})$ for every $i \geq 1$. Now choose i_2 so that $l_1(\mathbf{a_{i_2}}) \leq l_1(\mathbf{a_j})$ for all $j \geq i_1 + 1$, i_3 so that $l_1(\mathbf{a_{i_2}}) \leq l_1(\mathbf{a_h})$ for all $h \geq i_2 + 1$, etc. Thus after replacing the sequence (6) by a subsequence we may assume that $l_1(\mathbf{a_1}) \leq l_1(\mathbf{a_2}) \leq \ldots$. Proceeding inductively (with l_1 replaced by l_2, then l_3, etc.), we conclude that, after replacing (6) by a subsequence, we may assume $l_j(\mathbf{a_{i+1}}) \geq l_j(\mathbf{a_i})$ for every $j = 1, \ldots, t$ and every $i \geq 1$.

Now consider the element $\mathbf{b} = \mathbf{a_2} - \mathbf{a_1} \prec (0, \ldots, 0)$. Since we are assuming that $\mathbf{a_1}$ and $\mathbf{a_2}$ lie in $\mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \ldots, \mathbf{e_t})$, we can write $\mathbf{b} = r_1\mathbf{e_1} + \cdots + r_t\mathbf{e_t}$, where $r_1, \ldots, r_t$ are rational numbers. Since $l_j(\mathbf{b}) \leq 0$ for every $j = 1, \ldots, t$, and

$<\mathbf{e_i}, \mathbf{e_j}> \leq 0$ whenever $i \neq j$, [1, Lemma V.3.5.6] says that each $r_i \geq 0$, i.e., $r_i = \frac{p_i}{q}$, where $p_1, \dots, p_t, q \in \mathbb{N}$ and $q \neq 0$. Now

$$q\mathbf{b} = p_1\mathbf{e_1} + \dots + p_t\mathbf{e_t}\,.$$

The left hand side $\prec (0, \dots, 0)$, and the right hand side is $\succeq (0, \dots, 0)$ by our choice of the vectors $\mathbf{e_i}$. This contradiction shows that $A^{\succ}$ is well ordered. □

Corollary 5.6. *Suppose $G \subset \mathrm{GL}_n(\mathbb{Z})$ is a finite reflection group and $(\mathbb{Z}^n)^G = (0)$. If the initial exponents of the elements $f_\lambda \in k[x^{\pm 1}]^G$ generate $\mathrm{In}(k[x^{\pm 1}]^G)$ then $\{f_\lambda\}$ is a SAGBI basis of $k[x^{\pm 1}]^G$.*

Proof. By Lemma 5.3(b), $\mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \dots, \mathbf{e_t}) = \mathbb{R}^n$ and by Proposition 5.5

$$A^{\succ} = A^{\succ} \cap \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \dots, \mathbf{e_t})$$

is well ordered. The subduction algorithm will create a strictly decreasing sequence of leading terms in $A^{\succ}$; this sequence has to terminate. Thus the algorithm will terminate as well. □

Note that by Theorem 1.4 there exists a finite collection of elements $f_\lambda \in k[x^{\pm 1}]^G$ such that $\mathbf{in}(f_\lambda)$ generate $\mathrm{In}(k[x^{\pm 1}]^G)$ as a semigroup. Thus in the case where $(\mathbb{Z}^n)^G = (0)$, Theorem 1.5 is an immediate consequence of Corollary 5.6. We now turn to the general case, i.e., to the case where $(\mathbb{Z}^n)^G$ may not be trivial.

Example 5.7. Let $n = 1$ and $G = \{1\}$, so that $k[x^{\pm 1}]^G = k[x^{\pm 1}]$ (here $x = x_1$). Of course, $\mathbb{Z}^G = \mathbb{Z} \neq (0)$. The initial exponents, 1 and -1, of the elements $f_1 = x$ and $f_2 = x^{-1} - x^{-2}$ generate $\mathrm{In}(k[x^{\pm 1}]^G) = \mathbb{Z}$. We also have $k[x^{\pm 1}]^G = k[x^{\pm 1}] = k[f_1, f_2]$. Assume for simplicity that k is a field of characteristic 0.

We will now attempt to apply the subduction algorithm to express $\alpha = x^{-1}$ as a polynomial in f_1 and f_2. The first step yields $\alpha_1 = \alpha - f_2 = x^{-2}$, the second $\alpha_2 = \alpha_1 - f_2^2 = 2x^{-3} - x^{-4}$, etc. If we carry our the subduction algorithm by subtracting off scalar multiple of a power of f_2 at each stage, the "remainder" α_i after i steps will have leading exponent $-i-1$, and the algorithm will not terminate. We conclude that f_1 and f_2 do not form a SAGBI basis of $k[x^{\pm 1}] = k[x^{\pm 1}]^G$. □

Example 5.7 shows that Corollary 5.6 fails if $(\mathbb{Z}^n)^G \neq (0)$. Fortunately, it can be salvaged in this more general situation, if we choose our elements f_λ a little more carefully.

Recall that $X^{\succ} = \mathrm{Pos}(A^{\succ})$ is an integral polyhedral cone. Write $X^{\succ} = \mathrm{Pos}(\mathbf{v_1}, \dots, \mathbf{v_r})$, where $\mathbf{v_1}, \dots, \mathbf{v_r} \in X^{\succ} \cap \mathbb{Z}^n = A^{\succ}$, and let

$$f_i = \sum_{g \in G} x^{g(\mathbf{v_i})}\,.$$

The following Proposition completes the proof of Theorem 1.5.

Proposition 5.8. *$f_1, \dots, f_r$ form a SAGBI basis of $k[x^{\pm 1}]^G$.*

Proof. By our construction the initial forms $\mathbf{in}(f_1), \dots, \mathbf{in}(f_r)$ generate $A^{\succ} = \mathrm{In}(k[x^{\pm 1}]^G)$ as a semigroup. To show that they form a SAGBI basis, suppose we apply the subduction algorithm to express a given element $\alpha \in k[x^{\pm 1}]^G$ in terms of $f_1, \dots, f_r$. This algorithm will produce a sequence of elements $\alpha_0 = \alpha, \alpha_1, \alpha_2, \alpha_3 \dots$ with leading terms

$$\mathbf{in}(\alpha_0) \succ \mathbf{in}(\alpha_1) \succ \mathbf{in}(\alpha_2) \succ \dots . \tag{7}$$

Our goal is to show that this sequence will terminate. The idea of the proof is to consider the orthogonal decomposition $\mathbf{in}(\alpha_i) = \mathbf{b_i} + \mathbf{z_i}$, where $\mathbf{b_i} \in (\mathbb{R}^n)^G$ and $\mathbf{z_i} \in \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \dots, \mathbf{e_t})$; cf. Lemma 5.3(a). We would then like to show that the sequence $\{\mathbf{z_i}\}$ terminates because of Proposition 5.5 and the sequence $\{\mathbf{b_i}\}$ terminates because it can only assume finitely many values. Since we are working over $\mathbb{Z}$, rather than $\mathbb{R}$, this needs to be done with some care (in particular, the $\mathbf{b_i} \in (\mathbb{R}^n)^G$ and $\mathbf{z_i} \in \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \dots, \mathbf{e_t})$ defined below are the orthogonal components of $|G|\,\mathbf{in}(\alpha_i)$, rather than $\mathbf{in}(\alpha_i)$), but this is the idea behind the argument to follow.

Assume, to the contrary, that the sequence (7) of initial terms does not terminate. Let $p\colon \mathbb{R}^n \longrightarrow (\mathbb{R}^n)^G$ be given by

$$p(\mathbf{v}) = \sum_{g \in G} g(\mathbf{v})\,.$$

We claim that for every monomial $x^{\mathbf{v}}$ that appears in α there exists a monomial $x^{\mathbf{w}}$ that appears in α_1, such that $p(\mathbf{v}) = p(\mathbf{w})$. Indeed, suppose $\alpha_1 = \alpha - c f_1^{d_1} \dots f_r^{d_r}$, where $0 \neq c \in k$, $d_1, \dots, d_r \in \mathbb{N}$, and

$$d_1\mathbf{v_1} + \dots + d_r\mathbf{v_r} = \mathbf{in}(\alpha)\,.$$

Every monomial that occurs in α_1 either (i) occurs in α or (ii) occurs in $f_1^{d_1} \dots f_r^{d_r}$ (or both). In case (i) the claim is trivial: we can take $\mathbf{w} = \mathbf{v}$. In case (ii), $\mathbf{v}$ has the form

$$\mathbf{v} = d_1 g_1(\mathbf{v_1}) + \dots + d_r g_r(\mathbf{v_r})$$

for some $g_1, \dots, g_r \in G$. Thus

$$p(\mathbf{v}) = d_1 p(\mathbf{v_1}) + \dots + d_r p(\mathbf{v_r}) = p(d_1\mathbf{v_1} + \dots + d_r\mathbf{v_r}) = p(\mathbf{in}(\alpha))\,,$$

so that in case (ii), we can take $\mathbf{w} = \mathbf{in}(\alpha)$. This proves the claim.

Let $E = \{p(\mathbf{v})\}$, where $x^{\mathbf{v}}$ ranges over the monomials of α and let $\mathbf{b_i} = p(\mathbf{in}(\alpha_i))$. Applying the claim inductively, we see that $\mathbf{b_i} \in E$ for every $i \geq 1$. Since E is a finite set, there is an infinite subsequence $\mathbf{w_1} \succ \mathbf{w_2} \succ \dots$ of the sequence of initial terms (7) such that $p(\mathbf{w_1}) = p(\mathbf{w_2}) = \dots$, say, $p(\mathbf{w_i}) = \mathbf{b}$ for every $i \geq 1$.

We claim that this is impossible. Consider the sequence $\mathbf{z_i} = |G|\,\mathbf{w_i} - \mathbf{b}$ for $i \geq 1$. Then

(i) $\mathbf{z_1} \succ \mathbf{z_2} \succ \mathbf{z_3} \succ \dots$,

(ii) $\mathbf{z_i} \in A^{\succ}$ for each $i \geq 1$, and

(iii) $\mathbf{z_i} \in \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \dots, \mathbf{e_t})$ for each $i \geq 1$.

(i) is obvious because $\mathbf{w_i}$ form a strictly decreasing sequence. To prove (ii), note that $\mathbf{w_i} \in A^{\succ}$, i.e., $\mathbf{w_i} \succeq g(\mathbf{w_i})$ for any $g \in G$. Multiplying both sides by the positive integer $|G|$ and subtracting $\mathbf{b} = g(\mathbf{b})$, we obtain $\mathbf{z_i} \succeq g(\mathbf{z_i})$, as desired. To prove (iii), we only need to show that $\mathbf{z_i}$ is orthogonal to every $\mathbf{c} \in (\mathbb{R}^n)^G$; cf. Lemma 5.3(a). Indeed,

$$<\mathbf{z_i}, \mathbf{c}> = |G| <\mathbf{w_i}, \mathbf{c}> - <p(\mathbf{w_i}), \mathbf{c}> = |G| <\mathbf{w_i}, \mathbf{c}> - \sum_{g \in G} <g(\mathbf{w_i}), g(\mathbf{c})> = 0\,.$$

This proves (iii).

Thus $\{\mathbf{z_i}\}$ is a strictly decreasing sequence in $A^{\succ} \cap \mathrm{Span}_{\mathbb{R}}(\mathbf{e_1}, \dots, \mathbf{e_t})$, contradicting Proposition 5.5. This shows that the subduction algorithm will terminate, i.e., $f_1, \dots, f_r$ form a SAGBI basis of $k[x^{\pm 1}]^{\succ}$, as claimed. □

6. Proof of Theorem 1.7

In this section we will deduce Göbel's conjecture (Theorem 1.7) from Theorem 1.4.

Elements of H may be viewed as $n \times n$-permutation matrices; this gives a natural inclusion $H \subset \mathrm{GL}_n(\mathbb{Z})$. However, since we are interested in *polynomial* invariants of H, we will apply Theorem 1.4 not to H itself but to the larger group $G = <H, D> \subset \mathrm{GL}_n(\mathbb{Z})$, where D is the subgroup of diagonal matrices in $\mathrm{GL}_n(\mathbb{Z})$. (In other words, $D = \{\mathrm{diag}(\epsilon_1, \dots, \epsilon_n)\}$, where each $\epsilon_i = \pm 1$.) It is easy to see that $G \simeq D \rtimes H$ is a finite group.

The idea of the proof is to relate $\mathrm{In}(k[x]^H)$ to $\mathrm{In}(k[x^{\pm 1}]^G)$, where $k[x^{\pm 1}] = k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ is the Laurent polynomial ring. To define $\mathrm{In}(k[x^{\pm 1}]^G)$, we need to extend our term order $\succ$ from $k[x]$ to $k[x^{\pm 1}]$. There is a unique such extension (which, by abuse of notation, we shall continue to denote by $\succ$): for any $\mathbf{a}$ and $\mathbf{b} \in \mathbb{Z}^n$ we define

$$\mathbf{a} \succ \mathbf{b} \text{ iff } \mathbf{a} + m(1, \dots, 1) \succ \mathbf{b} + m(1, \dots, 1) \text{ for some } m \gg 0. \tag{8}$$

One easily checks that this definition is independent of the choice of m, as long as $\mathbf{a} + m(1, \dots, 1)$ and $\mathbf{b} + m(1, \dots, 1) \in \mathbb{N}^n$, and that the resulting order is a term order in $k[x^{\pm 1}]$ in the sense of Definition 1.2. Moreover, relative to this term order, $\mathrm{In}(k[x]^H) = \mathrm{In}(k[x^{\pm 1}]^G)$; indeed, both are equal to

$$\{\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n \mid a_1, \dots, a_n \geq 0 \text{ and } h(\mathbf{a}) \succeq \mathbf{a} \text{ for every } h \in H\}.$$

Theorem 1.4 now tells us that $\mathrm{In}(k[x]^H) = \mathrm{In}(k[x^{\pm 1}]^G)$ has a finite SAGBI basis if and only if G is a reflection group. Theorem 1.7 is thus a consequence of the following group-theoretic lemma.

Lemma 6.1. *Let $H \subset \mathrm{S}_n$ and $G = D \rtimes H \subset \mathrm{GL}_n(\mathbb{Z})$ be as above. Then the following conditions are equivalent:*

(a) *G is a reflection group,*
(b) *H is generated by transpositions,*
(c) *$H = \mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_r}$ for some partition $n_1 + \cdots + n_r = n$.*

The equivalence (b) $\Longleftrightarrow$ (c) is a simple exercise in finite group theory; we leave it to the reader.

(b) $\Longrightarrow$ (a): D is clearly generated by reflections. Since a transposition in H (viewed as an element of $\mathrm{GL}_n(\mathbb{Z})$) is a reflection, (b) says that H is also generated by reflections. Hence, so is $G = <D, H>$.

Our proof of the implication (a) $\Longrightarrow$ (b) relies on the following claim: Write $g = dh$, where $d \in D$ and $h \in H$. If g is a reflection then $h = id$ or h is a transposition. Indeed, since $G = D \rtimes H$, $id = g^2 = (dhdh^{-1})h^2$ implies (i) $h^2 = id$, i.e., h is a product of, say, r disjoint transpositions, and (ii) $dhdh^{-1} = id$, i.e., d and h commute. It is now easy to see that the only eigenvalues of g are -1 and 1, and that -1 occurs with multiplicity $\geq r$. If g is a reflection, this implies $r \leq 1$, i.e., $h = id$ or h is a transposition. This proves the claim.

Now suppose G is generated by reflections $g_1 = d_1h_1, \ldots, g_m = d_mh_m$, where each $d_i \in D$ and each $h_i \in H$. Then $H = G/D$ is generated by $h_1, \ldots, h_m$. The claim tells us that each $h_i = id$ or a transposition. Thus H is generated by transpositions. This completes the proof of Lemma 6.1 and thus of Theorem 1.7.

7. Final remarks

Remark 7.1. Suppose $G \subset \mathrm{GL}_n(\mathbb{Z})$ is a finite reflection group and $(\mathbb{Z}^n)^G = (0)$. Then there is a canonical choice of a SAGBI basis $\{f_1, \ldots, f_r\}$ in $R = k[x^{\pm 1}]^G$ independent of the term order $\succ$.

Indeed, in this case the integral polyhedral cone $X^{\succ}$ has an apex at 0 (cf. Remark 5.4); thus by [4, Lemma V.3.5], $\mathrm{In}(R) = A^{\succ} = X^{\succ} \cap \mathbb{Z}^n$ has a unique minimal system of (semigroup) generators $\mathbf{v_1}, \ldots, \mathbf{v_r}$. Now define

$$f_i = \sum_{g \in G} x^{g(\mathbf{v_i})} ;$$

for $i = 1, \ldots, r$. These elements form a SAGBI basis by Corollary 5.6 (or alternatively, by Proposition 5.8). To see that this SAGBI basis is independent of the term order, let $\succ'$ be another term order in $k[x^{\pm 1}]$, $\mathbf{v_1}', \ldots, \mathbf{v_r}'$ be a minimal set of generators for $A^{\succ'} = X^{\succ'} \cap \mathbb{Z}^n$ and

$$f_i' = \sum_{g \in G} x^{g(\mathbf{v_i'})} .$$

If $s_1, \ldots, s_m$ are the reflections in G, set $H_i = (\mathbb{R}^n)^{s_i}$, as before. Since $X^{\succ}$ and $X^{\succ'}$ are both chambers for the G-invariant collection of hyperplanes $H_1, \ldots, H_m$, there exists a $g_0 \in G$ such that $X^{\succ'} = g_0(X^{\succ})$; see [1, Lemma V.3.1.2]. Then $g_0(\mathbf{v_1}), \ldots, g_0(\mathbf{v_r})$ is another minimal system of generators of $A^{\succ'}$; thus, up to

renumbering, $\mathbf{v_i}' = g_0(\mathbf{v_i})$ for $i = 1, \dots, r$. Consequently, $f_i = f_i'$ for every $i = 1, \dots, r$, as claimed.

Remark 7.2. The arguments we used in proving Theorems 1.4 and 1.5 are quite insensitive to the base field k. Informally speaking, the action takes place in the exponents of monomials (both literally and metaphorically), and the coefficients of these monomials play only a minor role in our considerations. In fact,

(a) Theorems 1.4 and 1.7 remain true if the base field k is replaced by a (not necessarily commutative) ring. Our only requirements are that k should be non-trivial (i.e., $k \neq (0)$) and should have no zero divisors (otherwise, $\mathrm{In}(R)$ may not be a semigroup). The proof remains the same, with one exception: if k does not have a unit element, then $f = \sum x^{g(\mathbf{a})}$ in the proof of Lemma 2.6(a) should be redefined as $f = \sum c x^{g(\mathbf{a})}$, where c is a nonzero element of k.

(b) Theorem 1.5, Theorem 1.6 and Proposition 5.8 remain true if k is assumed to be a ring with a unit element 1 and without zero divisors, provided that we modify the definition of the subduction algorithm (as described in the Introduction) as follows: each f_λ is required to be monic i.e., its initial terms should have coefficient 1. (Otherwise we will have trouble defining the subduction algorithm, before we can even ask whether it terminates or not.) Corollary 5.6 remain true, if we impose this additional requirement on $\{f_\lambda\}$. The proofs remain unchanged.

We conclude this paper with the example that originally motivated Theorem 1.4.

Example 7.3. Let $C_2 = \{1, \tau\}$ be a group of order 2. Consider the action of $G_n = \mathrm{S}_n \times C_2$ on

$$L_n = \{\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n \mid a_1 + \dots + a_n = 0\} \simeq \mathbb{Z}^{n-1},$$

where S_n acts by permuting the coordinates and C_2 acts via $\tau(\mathbf{a}) = -\mathbf{a}$. For $n \geq 3$, the resulting integral representation $G \longrightarrow \mathrm{GL}(L_n)$ is easily seen to be faithful; thus we can think of G_n as a finite subgroup of $\mathrm{GL}(L_n) = \mathrm{GL}_{n-1}(\mathbb{Z})$. This representation and the ring of multiplicative invariants $R_n = k[L_n]^{G_n}$ (here $k[L_n] = k[x_1^{\pm 1}, \dots, x_{n-1}^{\pm 1}]$) arise in crystallography; in particular, one would like to know whether or not this ring has a SAGBI basis; cf. [2].

It is easy to see that G_n is generated by reflections if and only if $n \leq 4$. Indeed, the reflections in G_3 are (ij) and $(ij)\tau$, where $1 \leq i < j \leq 3$; these elements clearly generate G_3. The reflections in G_4 are elements of the form (ij) where $1 \leq i < j \leq 4$ and $(ij)(hl)\tau$, where $\{i, j, h, l\} = \{1, 2, 3, 4\}$; these elements generate G_4. For $n \geq 5$ the only reflections in G_n are transpositions in S_n; the subgroup they generate is S_n, not all of G_n. Thus Theorem 1.4 tells us that the semigroup $A^{\succ} = \mathrm{In}(R_n)$ is not finitely generated for any $n \geq 5$. The following direct proof of this fact, in the case where $\succ$ is the restriction of the usual lexicographic order of $\mathbb{Z}^n$ to L_n, was shown to us by J. Friedman:

Denote the j-th component of $\mathbf{a} \in \mathbb{Z}^n$ by $a[j]$, so that $\mathbf{a} = (a[1], \ldots, a[n])$. The semigroup of initial terms $A_n^{\succ} = \mathrm{In}(k[L_n]^{G_n})$ with respect to this order consists of elements $\mathbf{a} \in \mathbb{Z}^n$ satisfying the following conditions:

(i) $\mathbf{a} \in L_n$, i.e., $a[1] + \cdots + a[n] = 0$,

(ii) $a[1] \geq \cdots \geq a[n]$, and

(iii) $(a[1], \ldots, a[n]) \succeq (-a[n], \ldots, -a[1])$

Assume the contrary: there exists a finite set F of generators for $A_n^{\succ}$. Write $F = F_0 \cup F_1 \cup F_2 \cup \ldots$, where F_i consists of those $\mathbf{f} \in F$ with $f[1] + f[n] = i$.

Consider the element $\mathbf{a} = (t^2 + 1, t, t, 0, \ldots, 0, -2t - 1, -t^2)$ of $A^{\succ}$, where $t \geq 2$ is an integer parameter, to be specified later. Write $\mathbf{a} = \mathbf{f_1} + \ldots + \mathbf{f_N}$ as a sum of (not necessarily distinct) elements of F. Since $a[1] + a[n] = 1$, exactly one of the elements $\mathbf{f_i}$ (say, $\mathbf{f_N}$) lies in F_1, and all others lie in F_0. On the other hand, for any $\mathbf{f} \in F_0$, $f[2] + f[n-1] \geq 0$. Thus

$$-t - 1 = a[2] + a[n-1] = (f_1[2] + f_1[n-1]) + \cdots + (f_N[2] + f_N[n-1]) \geq f_N[2] + f_N[n-1] \geq \min_{\mathbf{f} \in F_1} (f[2] + f[n-1]) .$$

The last inequality cannot hold for sufficiently large t, a contradiction. Thus $A^{\succ}$ is not finitely generated for any $n \geq 5$. □

Theorem 1.5 also tells us that $L_n^{G_n}$ has a finite SAGBI basis for $n = 3$ and 4. Explicit SAGBI bases in these cases and some computations with them can be found in [2]. □

Acknowledgments. I would like to thank Joel Friedman for suggesting Proposition 2.4 and contributing the argument of Example 7.3, Martin Lorenz and the referee for bringing the papers [12] and [13] to my attention, and Joe Buhler, Claudio Procesi, Nicolas Thiéri and Rekha Thomas for stimulating discussions.

References

[1] N. Bourbaki, *Groupes et Algébres de Lie*, Hermann, 1968.

[2] J. Buhler and Z. Reichstein, *Symmetric functions and the phase problem in crystallography*, submitted for publication. Preprint available at http://math.ubc.ca/~reichst/pub.html

[3] D. Cox, J. Little, D. O'Shea, *Using algebraic geometry*, Graduate Texts in Mathematics, **185**, Springer-Verlag, New York, 1998.

[4] G. Ewald, *Combinatorial Convexity and Algebraic Geometry*, Springer-Verlag, 1996.

[5] D. R. Farkas, Multiplicative invariants, *LÉnseignement Mathématique* **30** (1984), 141–157.

[6] D. R. Farkas, Reflection groups and multiplicative invariants, *Rocky Mountain J. Math.* **16** no. 2 (1986), 215–222.

[7] M. Göbel, A constructive description of SAGBI bases for polynomial invariants of permutation groups, *J. Symbolic Comput.* **26** (1998), no. 3, 261–272.

[8] M. 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** (1999), no. 2, 65–70 (electronic).

[9] M. Göbel, Rings of polynomial invariants of the alternating group have no finite SAGBI bases with respect to any admissible order, *Inform. Process. Lett.* **74** (2000), no. 1-2, 15–18.

[10] D. Kapur and K. Madlener, A completion procedure for computing a canonical basis for a k-subalgebra, *Computers and mathematics* (Cambridge, MA, 1989), 1–11, Springer, New York, 1989.
[11] S. Kuroda, The infiniteness of the SAGBI bases for certain invariant rings, *Osaka J. Math.* **39** (2002), no. 3, 665–680.
[12] M. Lorenz, Regularity of multiplicative invariants, *Comm. Algebra* **24** (1996), no. 3, 1051–1055.
[13] M. Lorenz, Multiplicative invariants and semigroup algebras, *Algebr. Represent. Theory* **4** (2001), no. 3, 293–304.
[14] L. Robbiano and M. Sweedler, Subalgebra bases, *Commutative algebra* (Salvador, 1988), 61–87, Lecture Notes in Math., 1430 (1990), Springer, Berlin, 1990.
[15] B. Sturmfels, *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, 1993.
[16] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series, vol. 8, Amer. Math. Soc., 1995.
[17] N. M. Thiéry and S. Thomassé, *SAGBI bases of permutation groups and convex cones*, Proceedings of the Workshop on Invariant Theory (Kingston, Ontario, April 2002), to appear.

Z. Reichstein
Department of Mathematics
University of British Columbia
Vancouver, BC V6T 1Z2
Canada
e-mail: reichst@math.ubc.ca

(Received: March 5, 2002)