Algebraic Construction of Quasi-split Algebraic Tori

Armin Jamshidpey *[1], Nicole Lemire†[2], and Éric Schost ‡[1]

[1]David Cheriton School of Computer Science, University of Waterloo, Waterloo, Canada

[2]Department of Mathematics, University of Western Ontario, London, Canada

June 7, 2019

Abstract

The main purpose of this work is to give a constructive proof for a particular case of the no-name lemma. Let G be a finite group, K a field that is equipped with a faithful G-action, and L a sign permutation G-lattice (see below for the definition). Then G acts naturally on the group algebra $K[L]$ of L over K, and hence also on the quotient field $K(L) = Q(K[L])$. A well-known variant of the no-name lemma asserts that the invariant sub- field $K(L)^G$ is a purely transcendental extension of K^G. In other words, there exist $y_1, \ldots, y_n$ which are algebraically independent over K^G such that $K(L)^G \cong K^G(y_1, \ldots, y_n)$. In this article, we give an explicit construction of suitable elements $y_1, \ldots, y_n$.

Keywords: Algebraic tori, Lattices, Multiplicative invariants, No-name lemma.
2010 Mathematics Classification Subject: Primary 14Q99, Secondary 13A50, 68W30.

1 Introduction

An algebraic F-torus T is an algebraic group defined over a field F which *splits* over an algebraic closure $\bar{F}$ of F, that is, which is isomorphic to a torus (a finite product of copies of the multiplicative group $\mathbb{G}_m$) over $\bar{F}$. In general, $\bar{F}$ is not the smallest field over which T splits: it is known that an algebraic F-torus T splits over a finite Galois extension of F. There is a unique minimal such extension, say K; if $G = \mathrm{Gal}(K/F)$, then G is called the splitting group of T. For more details, see [16, p. 27].

*Corresponding author. Email address: armin.jamshidpey@uwaterloo.ca.
†nlemire@uwo.ca
‡eschost@uwaterloo.ca

For a finite group G, a G-lattice is a free $\mathbb{Z}$-module of finite rank, $L \cong \mathbb{Z}^n$, together with a group homomorphism $G \to \mathrm{Aut}(L) \cong \mathrm{GL}(n, Z)$. Given a module basis of L, any group homomorphism $G \longrightarrow \mathrm{GL}(n, \mathbb{Z})$, with $n = \mathrm{rank}(L)$, gives such an action. If K is a field, the group algebra $K[L]$ of L over K is isomorphic to the K-algebra of Laurent polynomials $K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$, for some indeterminates $x_1, \dots, x_n$. If K is equipped with a faithful action of G (that is, a G-field), we can extend the action of G on lattice L to an action on $K[L]$; the ring $K[L]^G$ of *multiplicative invariants* consists of those elements in $K[L]$ invariant under the action of G. The fraction field $K(L)$ of $K[L]$ is isomorphic to $K(x_1, \dots, x_n)$, and the subfield of invariants under the action of G is written $K(L)^G$.

It is known that there is a duality between the category of algebraic tori with splitting group G and G-lattices. For a given algebraic torus T with splitting group G, its character module $\mathrm{Hom}(T, \mathbb{G}_m)$ is a G-lattice. Conversely, if L is a G-lattice, with $G = \mathrm{Gal}(K/F)$ for some finite Galois extension K/F, then $T = \mathrm{Spec}(K[L]^G)$ is an algebraic F-torus with splitting group G, coordinate ring $K[L]^G$ and function field $K(L)^G$.

A G-lattice L is called *permutation* (resp. *sign permutation*) if it has a $\mathbb{Z}$-basis which is permuted (resp. up to sign changes) by G. In particular, an algebraic torus whose corresponding G-lattice is a permutation lattice is called a *quasi-split torus*. Quasi-split algebraic tori are characterized as being representable as a direct product of groups of the form $R_{E/F}(\mathbb{G}_m)$, where $R_{E/F}$ is the Weil restriction with respect to a finite separable field extension E/F. Note that $R_{E/F}(\mathbb{G}_m)$ is a F-group scheme with F-points $E^\times$ and character lattice $\mathbb{Z}[G/H]$, where K/F is a Galois closure of E/F, $G = \mathrm{Gal}(K/F)$ and H is the subgroup of G which fixes the subfield E. The Weil restriction here is not necessarily with respect to a finite Galois extension K/F as this would only produce character lattices which are direct sums of the group ring.

A specific case of the no-name lemma asserts that if L is a permutation G-lattice and K is a faithful G-field, then $K(L)^G$ is rational over K^G [11, Chapter 9.4]; in particular, with $G = \mathrm{Gal}(K/F)$, $K(L)^G$ is F-rational. The term "no-name lemma" was first used by Dolgachev in [3], expressing the fact that many researchers discovered the result independently. It is actually more general than the version stated here; see [3, p. 6], [1, Section 3.2], [10, Proposition 1.3], [4, Remark 2.4], [5, Proposition 1.1] and [11, Proposition 9.5.1]. In this paper, we give a constructive proof of the particular case described above (and of a slight generalization thereof, using signed permutation matrices), by exhibiting a basis for such a field of invariants. In concrete terms, we start from a subgroup of $\mathrm{GL}(n, \mathbb{Z})$ and describe the field of functions of an associated torus. We note that our proofs follow a strategy offered by the known proof of [10, Proposition 1.4] and [11, Proposition 9.5.1].

Definition 1. *Let G be a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$. The G-lattice L_G corresponding to G is the rank n lattice $\mathbb{Z}^n = \{[a_1, \dots, a_n]^T : a_i \in \mathbb{Z}\}$ on which G acts naturally by left-multiplication. Note that $\mathbb{Z}^n$ has a standard basis $\{\boldsymbol{e}_i : i = 1, \dots, n\}$, where $\boldsymbol{e}_i$ is the column vector $[\delta_{i,j}, i = 1, \dots, n]^T$.*

Suppose further that we are given an isomorphism $\iota : G \to \mathrm{Gal}(K/F)$, for some finite Galois extension K/F (in what follows, we simply say that K/F has Galois group G). Then, through the identification $K[x_1^{\pm 1},\dots,x_n^{\pm 1}] \simeq K[L_G]$, $K[x_1^{\pm 1},\dots,x_n^{\pm 1}]$ is equipped with the G-action defined as follows:

- for g in G and α in K, we write $g(\alpha) = (\iota(g))(\alpha)$ (so G acts as the Galois group on K);
- for g in G and $j = 1,\dots,n$, $g(x_i) = \prod_{j=1}^n x_j^{g_{j,i}}$, where $g_{j,i}$ is the (j,i)th -entry of g (so that we also have $g(\boldsymbol{e}_i) = \sum_{j=1}^n g_{j,i}\boldsymbol{e}_j$).

If we let T_G be the algebraic torus corresponding to L_G, then T_G is an algebraic F-torus which splits over K, with character lattice L_G and function field $K(x_1,\dots,x_n)^G$.

Conjugate subgroups of $\mathrm{GL}(n,\mathbb{Z})$ correspond to isomorphic lattices, and isomorphic algebraic tori; in particular, for G a finite subgroup of $\mathrm{GL}(n,\mathbb{Z})$, L_G is a (signed) permutation lattice if and only if G is conjugate to a group of (signed) permutation matrices. Computationally, we do not have an efficient algorithm at hand to decide whether a given lattice is (signed) permutation. Hence, in our main results, we will assume that G is a subgroup of the group $\mathbb{S}_n$ of permutation matrices of size n, or more generally of the group $\mathbb{S}_n^{\pm 1}$ of signed permutation matrices of size n. In such a case, for i in $\{1,\dots,n\}$ and g in G, $g(\boldsymbol{e}_i) = \pm\boldsymbol{e}_j$ for some index j in $\{1,\dots,n\}$ (all signs being $+1$ if G is a subgroup of $\mathbb{S}_n$), and the action of $g \in G$ on x_i is given by

$$g(x_i) = \begin{cases} x_j & \text{if } g(\boldsymbol{e}_i) = \boldsymbol{e}_j \\ x_j^{-1} & \text{if } g(\boldsymbol{e}_i) = -\boldsymbol{e}_j. \end{cases}$$

For such groups G, the F-rationality of the torus T_G means that for $K(x_1,\dots,x_n)$, endowed with the G-action we just described, there exist algebraically independent $y_1,\dots,y_n$ in $K(x_1,\dots,x_n)$ such that $K(x_1,\dots,x_n)^G = F(y_1,\dots,y_n)$. However, the proofs of the no-name lemma we are aware of are nonconstructive. The goal of this paper is to exhibit such an algebraically independent set $\{y_i : i = 1,\dots,n\}$; we state two such results. Note that the first result is a special case of the general version of the no-name lemma. In particular, this can be applied to get an explicit transcendence basis of the function field of a quasi-split algebraic torus T_G, provided G is given as a group of permutation matrices.

In both our theorems, we rely on the notion of a *normal element* of a finite Galois extension K/F with Galois group G; we recall that $\alpha \in K$ is normal if α and all its Galois conjugates form an F-basis of K. Any finite Galois extension admits a normal element [9, Theorem 6.13.1]; there exist algorithms to construct one, in characteristic zero [6] or in positive characteristic [15, 12].

Theorem 2. *Let G be a subgroup of $\mathbb{S}_n$, let K/F be a finite Galois extension with Galois group G, and let $\alpha \in K$ be a normal element for K/F. Then $K(x_1,\dots,x_n)^G = F(y_1,\dots,y_n)$, with*

$$y_i = \sum_{g\in G} g(\alpha x_i), \quad i = 1,\dots,n.$$

Our second statement is similar, but deals with the more general case of signed permutations (if the group G below happens to be a subgroup of $\mathbb{S}_n$, the construction is not the same as in the previous theorem).

Theorem 3. *Let G be a subgroup of $\mathbb{S}_n^{\pm 1}$, let K/F be a finite Galois extension with Galois group G, and let $\alpha \in K$ be a normal element for K/F. Then $K(x_1, \ldots, x_n)^G = F(y_1, \ldots, y_n)$, with*

$$y_i = \sum_{g \in G} g\left(\frac{\alpha}{1 + x_i}\right), \quad i = 1, \ldots, n.$$

There are many algorithms for finding the invariant rings for polynomial invariants [14, 2]. For multiplicative invariants, the algorithmic landscape is not developed to the same extent. In [13] the author introduced an algorithm to compute a generating set for the ring of multiplicative invariants, when the acting group is a subgroup of a reflection group. A more general algorithm for computing the ring of multiplicative invariants is given by Kemper in [8]. It is worth mentioning that although both above algorithms may be applied to our problem, they will not necessarily produce a transcendence basis of the invariant field.

Acknowledgements. A large part of this work was done while the first author was a PhD student at the University of Western Ontario. The second and third authors are supported by an NSERC Discovery Grant. We thank Gregor Kemper and Lex Renner for their feedback on an earlier version of this work.

2 Proofs and examples

In what follows, we use the following notation: we still write $\mathbb{S}_n$, resp. $\mathbb{S}_n^{\pm 1}$, for the groups of permutation, resp. signed permutation matrices of size n. Note that $\mathbb{D}_n$, the group of diagonal matrices in $\mathrm{GL}_n(\mathbb{Z})$ (diagonal matrices with entries in $\{\pm 1\}$) is a normal subgroup of $\mathbb{S}_n^{\pm 1}$ such that $\mathbb{S}_n^{\pm 1} = \mathbb{D}_n \rtimes \mathbb{S}_n$ is a semidirect product. We let $\mathfrak{S}_n$ be the symmetric group of size n. Since $\mathbb{S}_n$ is naturally isomorphic to $\mathfrak{S}_n$, we see that there is a natural group homomorphism $\rho : \mathbb{S}_n^{\pm 1} \to \mathfrak{S}_n$ obtained by mapping a signed permutation matrix to the permutation ρ_g such that $\rho_g(i) = j$, where j is the index of the unique non-zero entry in the ith column of g. Note that the kernel of the group homomorphism is $\mathbb{D}_n$. Hence, in terms of the action defined in the previous section, for g in $\mathbb{S}_n^{\pm 1}$ and for all i, j in $\{1, \ldots, n\}$, we have $g(x_i) = x_{\rho_g(i)}^{\pm 1}$. For a subgroup G of $S_n^{\pm 1}$ and i, j as above, we also denote by $G_{i,j}^{\pm}$ the set of all g in G such that $g(x_i) = x_j^{\pm 1}$, that is, $\rho_g(i) = j$.

We start with a lemma that generalizes known facts about Moore matrices over finite fields (see Example 5 below). Let G be a subgroup of $\mathbb{S}_n^{\pm 1}$ and let K/F be a finite Galois extension with Galois group isomorphic to G, as in the previous section. Through this isomorphism, G acts on (column) vectors entrywise: for $g \in G$ and a column vector in K^m, written as $C = [\mu_1 \;\; \mu_2 \;\; \cdots \;\; \mu_m]^T$, we define $g(C) = [g(\mu_1) \;\; g(\mu_2) \;\; \cdots \;\; g(\mu_m)]^T$.

Let then M be in $M_{n,n}(K)$. For such a matrix, and for $i = 1, \ldots, n$, its ith column is written $M_i = [\mu_{1,i} \;\; \mu_{2,i} \;\; \cdots \;\; \mu_{n,j}]^T$. We say that G *permutes the columns of M up to sign* if for g in G and i in $\{1, \ldots, n\}$, we have $g(M_i) = \pm M_{\rho_g(i)}$.

Lemma 4. *Let K/F be a finite Galois extension with Galois group G. Let M be in $M_{n,n}(K)$ and assume that G permutes the columns of M up to sign. Assume also that the entries of the first column of M are F-linearly independent. Then M is invertible.*

Proof. Assume by contradiction that there is a non-zero vector in the left nullspace of M; take $\boldsymbol{x} \in K^n$ to be a vector with the minimum number of non-zero entries among the non-zero left nullspace elements (that is, such that $\boldsymbol{x}^T M = 0$). Let $k \in \{1, \ldots, n\}$ be such that $x_k \neq 0$ and let $\boldsymbol{y} = \frac{1}{x_k}\boldsymbol{x} \in K^n$, so that $y_k = 1$, and $\boldsymbol{y}$ is still in the left nullspace of M.

For i in $\{1, \ldots, n\}$, we have the equality $\boldsymbol{y}^T M_i = 0$, where M_i is the ith column of M. For g in G, we deduce $g(\boldsymbol{y}^T M_i) = g(\boldsymbol{y})^T g(M_i) = \pm g(\boldsymbol{y})^T M_{\rho_g(i)} = 0$. Since this is true for all i, we obtain that $g(\boldsymbol{y})$ is in the left nullspace of M as well. This further implies that $\boldsymbol{y}' = g(\boldsymbol{y}) - \boldsymbol{y}$ is in the left nullspace of M. However, since $y_k = 1$, $g(y_k) = 1$, so that $y'_k = 0$. By construction of $\boldsymbol{x}$, this implies that $\boldsymbol{y}' = 0$, so that $g(\boldsymbol{y}) = \boldsymbol{y}$.

Since this is true for all g, we deduce that $\boldsymbol{y}$ is in F^n. Then, the relation $\boldsymbol{y}^T M_1 = 0$ implies that $\boldsymbol{y} = 0$, a contradiction. □

Remark. *The hypotheses in the above lemma imply that the induced unsigned action of the group G on the columns of M is a transitive action. Let $H = \mathrm{Stab}_G(M_1)$. Then $h \in H$ fixes M_1 and so $M_1 \in (K^H)^n$. But then the n entries of M_1 are contained in K^H and are also F-linearly independent. The size of an F-linearly independent set in K^H can be at most $[K^H : F]$. Then $n \leq [K^H : F] = [K^H : K^G] = [G : H] \leq n$ implies that $[G : H] = n$. But then the orbit of M_1 under the action of G has size $[G : H] = [G : \mathrm{Stab}_G(M_1)] = n$.*

Example 5. *Let $F = \mathbb{F}_q$, for some prime power q, and let $K = \mathbb{F}_{q^n}$. The Galois group of K/F is cyclic of size n, generated by the Frobenius map $x \mapsto x^q$. Let then $(\alpha_1, \ldots, \alpha_n)$ be in K, and consider the* Moore matrix *$M = [m_{i,j}]_{1 \leq i,j \leq n}$, with $m_{i,j} = \alpha_i^{q^{j-1}}$. The Frobenius map permutes the columns of M, and we recover the fact that if $(\alpha_1, \ldots, \alpha_n)$ are F-linearly independent, M is invertible [7, Corollary 1.3.4].*

We can now prove our first result.

Proof of Theorem 2. We first prove the result under the additional assumption that G acts transitively on L_G. The elements $(y_1, \ldots, y_n)$, with $y_i = \sum_{g \in G} g(\alpha x_i)$ as defined in the theorem, are invariant under the action of G. We will show below that $K(x_1, \ldots, x_n) = K(y_1, \ldots, y_n)$; this will prove that $K(x_1, \ldots, x_n)^G = F(y_1, \ldots, y_n)$, since $K(x_1, \ldots, x_n) = K(y_1, \ldots, y_n)$ implies that $K(y_1, \ldots, y_n)^G = K^G(y_1, \ldots, y_n) = F(y_1, \ldots, y_n)$.

For i, j in $\{1, \ldots, n\}$, let $G_{i,j} = \{g \in G : g(x_i) = x_j\}$, so that we can rewrite y_i as

$$y_i = \sum_{j=1}^{n} \sum_{g \in G_{i,j}} g(\alpha) x_j, \quad i = 1, \ldots, n.$$

Note that $G_{i,i} = \mathrm{Stab}_G(x_i)$ and so is a subgroup of G. Since the action of G on L_G is transitive, $G_{i,j}$ is non-empty for every $1 \leq i, j \leq n$. Take such indices i, j, and fix some $g_{i,j}$ in $G_{i,j}$. If $g \in G_{i,j}$, then $g_{i,j}^{-1} g(x_i) = x_i$ shows that g is in $g_{i,j} G_{i,i}$. Since we also have $g_{i,j} G_{i,i} \subseteq G_{i,j}$, we see that $G_{i,j} = g_{i,j} G_{i,i}$.

We now show that the matrix M with ith row the coordinate vector of y_i with respect to the K-basis $\{x_1, \ldots x_n\}$ is invertible. The matrix M has entries $m_{i,j} = \sum_{g \in G_{i,j}} g(\alpha)$, $i, j = 1, \ldots, n$. We will apply Lemma 4 to show that M is invertible, which is sufficient to prove the theorem.

We check the hypothesis of the lemma. First, let $\rho : G \to \mathfrak{S}_n$, $\rho(g) = \rho_g$ be the group homomorphism that corresponds to the action of G on $(x_1, \ldots, x_n)$, so that $\rho_g(i) = j$ if and only if $g(x_i) = x_j$ for all $1 \leq i, j \leq n$. We will show that the columns of M are permuted by the action of G. Let thus h be in G. Note that for g in $G_{i,j}$, hg is in $G_{i,\rho_h(j)}$. Then since $G_{i,j} = g_{i,j} G_{i,i}$ is a left coset of $G_{i,i}$ where $g_{i,j}$ is an arbitrary element of $G_{i,j}$, we see that $hG_{i,j} = hg_{i,j} G_{i,i} = G_{i,\rho_h(j)}$ since $hg_{ij} \in G_{i,\rho_h(j)}$. We then get

$$h(m_{i,j}) = \sum_{g \in G_{i,j}} hg(\alpha) = \sum_{\sigma \in G_{i,\rho_h(j)}} \sigma(\alpha) = m_{i,\rho_h}(j).$$

This shows that $h(M_j) = M_{\rho_h(j)}$ for all $j = 1, \ldots, n$, so that G permutes the columns of M.

Finally, the first column M_1 has entries $\sum_{g \in G_{i,1}} g(\alpha)$, $i = 1, \ldots, n$. Since α is a normal element of the Galois extension K/F with Galois group G, the set $\{g(\alpha) : g \in G\}$ is F-linearly independent. Since $G = \sqcup_{i=1}^n G_{i,1}$ is a disjoint union, and all $G_{i,1}$ are non-empty, the set

$$\left\{ \sum_{g \in G_{i,1}} g(\alpha),\ i = 1, \ldots, n \right\}$$

is F-linearly independent as well. So Lemma 4 applies, and we conclude that M is invertible, as claimed.

We can now give the proof of our claim in the general case. Let $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ be the standard basis of L_G, and let $\{\boldsymbol{e}_{j_k} \mid k = 1, \ldots, r\}$ and correspondingly $\{x_{j_k} \mid k = 1, \ldots, r\}$ be a complete set of G-orbit representatives among the basis vectors, and the indeterminates $x_1, \ldots, x_n$ respectively. Then $L_k = \oplus_{\boldsymbol{e}_i \in G\boldsymbol{e}_{j_k}} \mathbb{Z}\boldsymbol{e}_i$ is a transitive permutation G-lattice for each $k = 1, \ldots, r$, and $K(L_k) = K(x_i \mid x_i \in Gx_{j_k})$.

The lattice $L_G = \oplus_{k=1}^r L_k$ is a direct sum of transitive permutation G-lattices, so that $K(x_1, \ldots, x_n)$ is the compositum of the fields $K(L_k)$, $k = 1, \ldots, r$. Thus, using the result established in the transitive case, we obtain $K(x_1, \ldots, x_n)^G = F(y_i \mid x_i \in Gx_{j_k}, k = 1, \ldots, r)$, where for all k and for $x_i \in Gx_{j_k}$, we have $y_i = \sum_{g \in G} g(\alpha x_i)$. $\square$

Example 6. *Let K be the splitting field of $x^4 - 2$ over $F = \mathbb{Q}$. Then* $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$, *$K = \mathbb{Q}(\theta, i)$, with $\theta = \sqrt[4]{2}$, and $\{1, \theta, \theta^2, \theta^3, i, i\theta, i\theta^2, i\theta^3\}$, is a $\mathbb{Q}$-basis for K. Let $n = 4$, let $G \leq \mathrm{GL}(4, \mathbb{Z})$ be generated by*

$$r = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \textit{and} \quad s = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

and let $(x_1, \dots, x_4)$ *be new indeterminates, on which* G *acts as in Definition 1; this action is transitive. One can verify that* G *is isomorphic to* $\mathrm{Gal}(K/\mathbb{Q})$*; through this isomorphism, the action of* r *and* s *on the generators of* K *is given by*

$$\begin{array}{ll} r(i) = i & r(\theta) = i\theta \\ s(i) = -i & s(\theta) = \theta. \end{array}$$

Now, define

$$\alpha = 1 + \theta + \theta^2 + \theta^3 + i + i\theta + i\theta^2 + i\theta^3 = (\sum_{i=0}^{3} \theta^i)(1 + i);$$

this is a normal element in $K/\mathbb{Q}$*. Note that* $G_{1,1} = \mathrm{Stab}_G(x_1) = \langle s \rangle$*. Since* $r^i(x_1) = x_{i+1}, i = 0, 1, 2, 3,$ *we see that* $G_{i,i} = \mathrm{Stab}_G(x_i) = r^i \mathrm{Stab}_G(x_1) r^{-i}$ *and so* $G_{1,1} = G_{3,3} = \langle s \rangle$ *and* $G_{2,2} = G_{4,4} = \langle r^2 s \rangle$*. Also note that* $r^{j-i} \in G_{i,j}$*, where we may consider all exponents of* r *modulo 4. This shows that the elements* $(y_1, \dots, y_4)$ *of Theorem 2, expressed on the basis* $(x_1, \dots, x_4)$*, are given by the coordinate matrix*

$$M = \begin{bmatrix} (1+s)(\alpha) & r(1+s)(\alpha) & r^2(1+s)(\alpha) & r^3(1+s)(\alpha) \\ r^3(1+r^2s)(\alpha) & (1+r^2s)(\alpha) & r(1+r^2s)(\alpha) & r^2(1+r^2s)(\alpha) \\ r^2(1+s)(\alpha) & r^3(1+s)(\alpha) & (1+s)(\alpha) & r(1+s)(\alpha) \\ r(1+r^2s)(\alpha) & r^2(1+r^2s)(\alpha) & r^3(1+r^2s)(\alpha) & (1+r^2s)(\alpha) \end{bmatrix}.$$

Now since $M_j = r^{j-1} M_1$ *for all* $j = 1, 2, 3, 4$*, it is clear that the action of* r *permutes the columns. In particular,* $rM_j = M_{j+1}$ *(modulo 4). One can check that* $sM_1 = M_1$ *and since* $|Stab_G(M_1)| = 8/4 = 2$*, this shows that* $Stab_G(M_1) = \langle s \rangle$*. Then* $sr^{j-1}M_1 = r^{1-j}sM_1$ *shows that* $sM_j = M_{5-j}, j = 1, \dots, 4$ *so* s *also permutes the columns of* M*.*

Remark. *With the assumptions of the previous theorem, we can actually compute the coordinate ring of the torus; we obtain*

$$K[L_G]^G \cong K[x_1^{\pm 1}, x_2^{\pm 1}, \dots, x_n^{\pm 1}]^G = F[y_1, \dots, y_n]_{x_1 \cdots x_n},$$

for $y_1, \dots, y_n$ *as in the theorem. Indeed, we have* $K[x_1^{\pm 1}, x_2^{\pm 1}, \dots, x_n^{\pm 1}] = K[x_1, \dots, x_n]_{x_1 \cdots x_n}$*. We are interested in* $K[L_G]^G$*, that is,* $\big(K[x_1^{\pm 1}, x_2^{\pm 1}, \dots, x_n^{\pm 1}]\big)^G = \big(K[x_1, \dots, x_n]_{x_1 \cdots x_n}\big)^G$*. The proof of Theorem 2 shows that* $K[x_1, \dots, x_n] = K[y_1, \dots, y_n]$*. On the other hand since* G *permutes the* x_i*'s,* $x_1 \cdots x_n$ *is invariant under the action of* G*, and we can conclude*

$$\big(K[x_1, \dots, x_n]_{x_1 \cdots x_n}\big)^G = \big(K[y_1, \dots, y_n]_{x_1 \cdots x_n}\big)^G = K^G[y_1, \dots, y_n]_{x_1 \cdots x_n} = F[y_1, \dots, y_n]_{x_1 \cdots x_n}.$$

One could further rewrite $x_1 \cdots x_n$ *as a degree* n *homogeneous polynomial in* $y_1, \dots, y_n$ *(but the expression obtained this way is not particularly handy).*

We conclude with the proof of our second main result. The proof follows that of Theorem 2, the only difference being in the description of the coordinate matrix M. As in Theorem 2, we first prove the result under the extra assumption that G acts transitively up to sign on L_G.

Proof of Theorem 3. Assume first that the action of G is transitive (up to sign). For i in $\{1,\dots,n\}$, define $z_i = (1+x_i)^{-1}$. Then, for $g \in G$,

$$g(z_i) = \begin{cases} z_j & \text{if } g(x_i) = x_j \\ 1 - z_j & \text{if } g(x_i) = x_j^{-1}, \end{cases}$$

and $K(x_1,\dots,x_n) = K(z_1,\dots,z_n)$. The elements y_i can be rewritten as $y_i = \sum_{g\in G} g(\alpha z_i)$, for i in $\{1,\dots,n\}$; as before, in order to prove that $K(z_1,\dots,z_n)^G = F(y_1,\dots,y_n)$, it is enough to prove that $K(y_1,\dots,y_n) = K(z_1,\dots,z_n)$. This will be done by writing $(1, y_1,\dots,y_n)$ as K-linear combinations of $(1, z_1,\dots,z_n)$, and proving that the coordinate matrix is invertible.

For i, j in $\{1,\dots,n\}$, let $G^{\pm}_{i,j}$ be defined as in the preamble of this section, that is $G^{\pm}_{i,j} = \{g \in G : g(z_i) = z_j \text{ or } g(z_i) = 1 - z_j\}$. By the transitivity assumption, $G^{\pm}_{i,j}$ is non-empty for every $1 \le i, j \le n$. Let us further define $G^{+}_{i,j} = \{g \in G : g(z_i) = z_j\}$ and $G^{-}_{i,j} = \{g \in G : g(z_i) = 1 - z_j\}$, so that $G_{i,j} = G^{+}_{i,j} \sqcup G^{-}_{i,j}$.

Note that $G^{+}_{i,i} = \mathrm{Stab}_G(z_i)$. Both $G^{\pm}_{i,i}$ and $G^{+}_{i,i}$ are subgroups of G. One can show that the left cosets of $G^{+}_{i,i}$ in G are the non-empty sets in the collection

$$\{G^{+}_{i,j} : 1 \le j \le n\} \cup \{G^{-}_{i,j} : 1 \le j \le n\}$$

By the transitivity assumption, the sets $G^{\pm}_{i,j} \neq \emptyset$ so one can guarantee that either $G^{+}_{i,j} \neq \emptyset$ or $G^{-}_{i,j} \neq \emptyset$ (although both are possible). If $G^{+}_{i,j} \neq \emptyset$, and g^{+}_{ij} is an arbitrary element of $G^{+}_{i,j}$, then $G^{+}_{i,j} = g^{+}_{ij} G^{+}_{i,j}$ and if $G^{-}_{i,j} \neq \emptyset$ and g^{-}_{ij} is an arbitrary element of $G^{-}_{i,j}$, then $G^{-}_{i,j} = g^{-}_{ij} G^{+}_{i,j}$.

Let M^* be the coordinate matrix of $(1, y_1,\dots,y_n)$ with respect to the K-basis $(1, z_1,\dots,z_n)$; we have to show that $\det(M^*) \neq 0$. By definition, for i in $\{1,\dots,n\}$, we have

$$\begin{aligned} y_i = \sum_{g\in G} g(\alpha z_i) &= \sum_{j=1}^{n} \Big(\sum_{g\in G^{+}_{i,j}} g(\alpha) z_j + \sum_{g\in G^{-}_{i,j}} g(\alpha)(1 - z_j) \Big) \\ &= \sum_{j=1}^{n} \sum_{g\in G^{-}_{i,j}} g(\alpha) + \sum_{j=1}^{n} \Big(\sum_{g\in G^{+}_{i,j}} g(\alpha) - \sum_{g\in G^{-}_{i,j}} g(\alpha) \Big) z_j. \end{aligned}$$

For $i, j \in \{1,\dots,n\}$, define $m_{i,j} = \sum_{g\in G^{+}_{i,j}} g(\alpha) - \sum_{g\in G^{-}_{i,j}} g(\alpha)$ and $c_i = \sum_{j=1}^{n} \sum_{g\in G^{-}_{i,j}} g(\alpha)$. The matrix M^* is then

$$M^* = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ c_1 & m_{1,1} & \cdots & m_{1,n} \\ \vdots & \vdots & & \vdots \\ c_n & m_{n,1} & \cdots & m_{n,n} \end{bmatrix}.$$

Let us write

$$M = \begin{bmatrix} m_{1,1} & \cdots & m_{1,n} \\ \vdots & & \vdots \\ m_{n,1} & \cdots & m_{n,n} \end{bmatrix}.$$

Since $\det(M^*) = \det(M)$, it is enough to show that the determinant of M is non-zero; this will be done using Lemma 4. We now check that the hypotheses of the lemma are satisfied.

As before, let $\rho : G \to \mathfrak{S}_n$, $\rho(g) = \rho_g$ be the group homomorphism that corresponds to the action of G on $\{z_1, \dots, z_n\}$, so that $\rho_g(i) = j$ if and only if g is in $G^{\pm}_{i,j}$. We will show that the columns $M_1, \dots, M_n$ of M are permuted up to sign by the action of G.

Let h be in G and i, j be in $\{1, \dots, n\}$. We can then write

$$h(m_{i,j}) = h\Big(\sum_{g\in G^+_{i,j}} g(\alpha) - \sum_{g\in G^-_{i,j}} g(\alpha)\Big) = \sum_{g\in G^+_{i,j}} hg(\alpha) - \sum_{g\in G^-_{i,j}} hg(\alpha).$$

As in the proof of Theorem 2, we have $hG^{\pm}_{i,j} = G^{\pm}_{i,\rho_h(j)}$, but more precisely, we can write

$$\begin{cases} G^+_{i,\rho_h(j)} & = hG^+_{i,j} \\ G^-_{i,\rho_h(j)} & = hG^-_{i,j} \end{cases} \text{ if } h \in G^+_{j,\rho_h(j)} \quad \text{and} \quad \begin{cases} G^+_{i,\rho_h(j)} & = hG^-_{i,j} \\ G^-_{i,\rho_h(j)} & = hG^+_{i,j} \end{cases} \text{ if } h \in G^-_{j,\rho_h(j)}. \tag{1}$$

In the first case, we deduce

$$m_{i,\rho_h(j)} = \sum_{g\in G^+_{i,\rho_h(j)}} g(\alpha) - \sum_{g\in G^-_{i,\rho_h(j)}} g(\alpha) = \sum_{g\in G^+_{i,j}} hg(\alpha) - \sum_{g\in G^-_{i,j}} hg(\alpha) = h(m_{i,j});$$

in the second case, we get

$$m_{i\rho_h(j)} = \sum_{g\in G^+_{i,\rho_h(j)}} g(\alpha) - \sum_{g\in G^-_{i,\rho_h(j)}} g(\alpha) = \sum_{g\in G^-_{i,j}} hg(\alpha) - \sum_{g\in G^+_{i,j}} hg(\alpha) = -h(m_{i,j}).$$

In other words, $h(M_j) = \pm M_{\rho_h(j)}$, so G permutes the columns of M up to sign. Secondly, the first column M_1 has entries

$$\sum_{g\in G^+_{i,1}} g(\alpha) - \sum_{g\in G^-_{i,1}} g(\alpha), i = 1, \dots, n.$$

Since α is a normal element of the Galois extension K/F with Galois group G, and since $G = \sqcup_{i=1}^n G^{\pm}_{i,j} = \sqcup_{i=1}^n (G^+_{i,1} \sqcup G^-_{i,1})$ is a disjoint union, with all $G^{\pm}_{i,j}$ non-empty (by the transitivity of the action), this set is F-linearly independent.

So Lemma 4 applies, and we conclude that $K(y_1, \dots, y_n) = K(z_1, \dots, z_n)$; this implies that $K(x_1, \dots, x_n)^G = F(y_1, \dots, y_n)$. This finishes the proof in the transitive case; the proof in the general case follows as in Theorem 2. $\square$

Example 7. *Let $K = \mathbb{Q}(\rho)$, where ρ is a primitive 5-th root of unity, so that $K/\mathbb{Q}$ is Galois, with $\mathrm{Gal}(K/\mathbb{Q}) \cong C_4$. Take $n = 3$, assume $G \le \mathrm{GL}(3, \mathbb{Z})$ is generated by*

$$\sigma = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

and let (x_1, x_2, x_3) *be indeterminates over* K*, on which* G *acts as in Definition 1; this action is not transitive. One can also verify that* G *is isomorphic to* $\mathrm{Gal}(K/\mathbb{Q})$*;* $\sigma(\rho) = \rho^2$*. This implies that* $\sigma^k(\rho) = \rho^{2^k}$*,* $k = 0, 1, 2, 3$*. In particular,* $\sigma^3(\rho) = \rho^8 = \rho^3$*.*

We choose ρ *as our normal element of the extension* $K/\mathbb{Q}$*. (A primitive pth root of unity is a normal element for the extension over* $\mathbb{Q}$ *that it generates.)*

In this example, note that $G^+_{1,1} = G^+_{2,2} = \{\mathrm{id}\}$*,* $G^-_{1,1} = G^-2,2 = \{\sigma^2\}$*,* $G^+_{1,2} = G^-_{2,1} = \{\sigma\}$*, and* $G^-_{1,2} = G^+_{2,1} = \{\sigma^3\}$*. Also,* $G^+_{3,3} = \langle\sigma^2\rangle$ *and* $G^-_{3,3} = \sigma G^+_{3,3} = \langle\sigma, \sigma^3\rangle$*.*

With (z_1, z_2, z_3) *and* (y_1, y_2, y_3) *defined as before, the matrix* M^* *giving the coordinates of* $(1, y_1, y_2, y_3)$ *on the basis* $(1, z_1, z_2, z_3)$ *is*

$$M^* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \rho^3 + \rho^4 & \rho - \rho^4 & \rho^2 - \rho^3 & 0 \\ \rho^2 + \rho^4 & \rho^3 - \rho^2 & \rho - \rho^4 & 0 \\ \rho^2 + \rho^3 & 0 & 0 & \rho - \rho^2 - \rho^3 + \rho^4 \end{bmatrix}.$$

Remark that due to the non-transitivity of the action of G*, the bottom-right* 3×3 *submatrix of* M^**, while invertible, does not satisfy the assumptions of Lemma 4 (this matrix is block diagonal, with blocks corresponding to* $K(z_1, z_2)$ *and* $K(z_3)$*, for which the lemma applies).*

References

[1] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group). In *Algebraic groups and homogeneous spaces*, volume 19 of *Tata Inst. Fund. Res. Stud. Math.*, pages 113–186. Tata Inst. Fund. Res., Mumbai, 2007.

[2] Harm Derksen and Gregor Kemper. *Computational invariant theory*, volume 130 of *Encyclopaedia of Mathematical Sciences*. Springer, Heidelberg, enlarged edition, 2015. With two appendices by Vladimir L. Popov, and an addendum by Norbert A'Campo and Popov, Invariant Theory and Algebraic Transformation Groups, VIII.

[3] Igor V. Dolgachev. Rationality of fields of invariants. In *Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985)*, volume 46 of *Proc. Sympos. Pure Math.*, pages 3–16. Amer. Math. Soc., Providence, RI, 1987.

[4] Mátyás Domokos. Covariants and the no-name lemma. *J. Lie Theory*, 18(4):839–849, 2008.

[5] Shizuo Endô and Takehiko Miyata. Invariants of finite abelian groups. *J. Math. Soc. Japan*, 25:7–26, 1973.

[6] Kurt Girstmair. An algorithm for the construction of a normal basis. *J. Number Theory*, 78(1):36–45, 1999.

[7] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996.

[8] Gregor Kemper. Using extended Derksen ideals in computational invariant theory. *J. Symbolic Comput.*, 72:161–181, 2016.

[9] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[10] H. W. Lenstra, Jr. Rational functions invariant under a finite abelian group. *Invent. Math.*, 25:299–325, 1974.

[11] Martin Lorenz. *Multiplicative invariant theory*, volume 135 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2005. Invariant Theory and Algebraic Transformation Groups, VI.

[12] Alain Poli. A deterministic construction for normal bases of abelian extensions. *Comm. Algebra*, 22(12):4751–4757, 1994.

[13] Marc Stetson Renault. *Computing generators for rings of multiplicative invariants*. PhD thesis, Temple University, 2002.

[14] Bernd Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. Springer, second edition, 2008.

[15] Joachim von zur Gathen and Mark Giesbrecht. Constructing normal bases in finite fields. *J. Symbolic Comput.*, 10(6):547–570, 1990.

[16] V. E. Voskresenskiĭ. *Algebraic groups and their birational invariants*, volume 179 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1998. Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ].