NONCOMMUTATIVE RATIONAL FUNCTIONS INVARIANT UNDER THE ACTION OF A FINITE SOLVABLE GROUP

IGOR KLEP[1], JAMES ELDRED PASCOE[2], GREGOR PODLOGAR, AND JURIJ VOLČIČ[3]

Abstract. This paper describes the structure of invariant skew fields for linear actions of finite solvable groups on free skew fields in d generators. These invariant skew fields are always finitely generated, which contrasts with the free algebra case. For abelian groups or solvable groups G with a well-behaved representation theory it is shown that the invariant skew fields are free on $|G|(d-1)+1$ generators. Finally, positivity certificates for invariant rational functions in terms of sums of squares of invariants are presented.

Contents

Date: June 21, 2020.

2010 *Mathematics Subject Classification.* Primary 13J30, 16K40, 20C15; Secondary 20F16, 26C15, 47A63.

Key words and phrases. Noncommutative rational function, invariant field, group representation, positive rational function.

[1]Supported by the Slovenian Research Agency grants J1-8132, N1-0057 and P1-0222. Partially supported by the Marsden Fund Council of the Royal Society of New Zealand.

[2]Partially supported by NSF MSPRF DMS 1606260.

[3]Supported by the NSF grant DMS 1954709.

1. Introduction

Classical invariant theory studies polynomials that are preserved under linear group actions [Kra84, Stu08, DK15]. By the Chevalley–Shepard–Todd theorem [Stu08, Theorem 2.4.1] for a finite group $G \subseteq \mathrm{GL}_n(\mathbb{C})$, the ring of invariants $\mathbb{C}[x_1, \dots, x_n]^G$ is isomorphic to a polynomial ring (in the same number of variables) if and only if G is a complex reflection group. Similarly, one considers the rational invariants $\mathbb{C}(x_1, \dots, x_n)^G$. Noether's problem asks when this invariant field is rational, that is, isomorphic to a field of rational functions. This is a subtle question which heavily depends on the structure of the group; however, in recent years much progress has been made along the lines of [Sal84, CTS07, Pey08, CHKK10, Mor12, CHHK15, JS]. Examples of invariant fields give the simplest negative answers to the Lüroth problem, i.e., examples of unirational varieties which are not rational [AM72, Sal84]. Lüroth's problem has a positive answer in one variable (every field between K and $K(x)$ must be K or purely transcendental over K), and in two variables over $\mathbb{C}$. In complex analysis, these problems pertain to complex automorphisms and holomorphic equivalence of domains, geometry of symmetric domains and realizations of symmetric analytic functions [GR08, Sat14, AY17]. On the practical side, symmetries are regularly applied in control system design to analyze a system by decomposing it into lower-dimensional subsystems [GM85, vdS87, Kwa95].

We study the free noncommutative analogue of the above program over an algebraically closed field $\mathbb{F}$ of characteristic 0. Let $x = (x_1 \dots, x_d)$ be a tuple of noncommuting indeterminates. A **noncommutative polynomial** is a formal linear combination of words in x with coefficients in $\mathbb{F}$. For example,

$$17x_1^4 + 13x_1x_2 - 9x_2x_1 + 39.$$

We denote the free associative algebra of noncommutative polynomials on d generators by $\mathbb{F}\langle x_1, \dots, x_d\rangle$. A **noncommutative rational expression** is a syntactically valid combination of noncommutative polynomials, arithmetic operations $+, \cdot, ^{-1}$, and parentheses, e.g.

$$\left(216x_1^3x_2^4x_1^5 - ((x_1x_2 - x_2x_1)^{-1} + 3)^8\right)^{-1}.$$

These expressions can be naturally evaluated on d-tuples of matrices. An expression is called nondegenerate if it is valid to evaluate it on at least one such tuple of matrices. Two nondegenerate expressions with the same evaluations wherever they are both defined are equivalent. A **noncommutative rational function** is an equivalence class of a nondegenerate rational expression. They form the **free skew field** $\mathbb{F}\langle\!(x_1, \dots, x_d)\!\rangle$, which is the universal skew field of fractions of the free algebra $\mathbb{F}\langle x_1, \dots, x_d\rangle$. We refer the reader to [BGM05, Coh06, HMV06, BR11, KVV12, Vol18] for more on the free skew field.

We analyze the invariants in a free skew field under the action of a finite solvable group. For example, a symmetric noncommutative rational function r in two variables satisfies the equation

$$r(x, y) = r(y, x).$$

Naturally, this corresponds to an action of the symmetric group with two elements, S_2, and we denote the ring of symmetric noncommutative rational functions in two variables by $\mathbb{F}\langle\!\!\langle x,y\rangle\!\!\rangle^{S_2}$. Similarly, $\mathbb{F}\langle x,y\rangle^{S_2}$ is the ring of symmetric noncommutative polynomials. By a theorem of Wolf, see e.g. [Coh06, §6.8], we have

$$\mathbb{F}\langle x,y\rangle^{S_2} \cong \mathbb{F}\langle u_1,u_2,\dots\rangle.$$

In fact, the polynomial invariants $\mathbb{F}\langle x_1,\dots,x_d\rangle^G$ are, except in some trivial cases, always isomorphic to a free algebra in countably infinitely many variables [Coh06, §6.8]. As was observed by Agler and Young [AY14] (see also [CPTD18] and [AMY18]),

$$\mathbb{F}\langle x,y\rangle^{S_2} \subseteq \mathbb{F}\langle\!\!\langle x+y,(x-y)^2,(x-y)(x+y)(x-y)\rangle\!\!\rangle,$$

where $\mathbb{F}\langle\!\!\langle x+y,(x-y)^2,(x-y)(x+y)(x-y)\rangle\!\!\rangle$ denotes the subfield of $\mathbb{F}\langle\!\!\langle x,y\rangle\!\!\rangle$ generated by $x+y$, $(x-y)^2$, and $(x-y)(x+y)(x-y)$. What is perhaps less clear, and follows from our Theorem 4.1, is that

$$\begin{aligned}\mathbb{F}\langle\!\!\langle x,y\rangle\!\!\rangle^{S_2} &= \mathbb{F}\langle\!\!\langle x+y,(x-y)^2,(x-y)(x+y)(x-y)\rangle\!\!\rangle\\ &\cong \mathbb{F}\langle\!\!\langle a,b,c\rangle\!\!\rangle.\end{aligned}$$

Moreover, the isomorphism $\varphi:\mathbb{F}\langle\!\!\langle a,b,c\rangle\!\!\rangle \to \mathbb{F}\langle\!\!\langle x,y\rangle\!\!\rangle^{S_2}$ satisfies $\varphi(a)=x+y$, $\varphi(b)=(x-y)^2$, and $\varphi(c)=(x-y)(x+y)(x-y)$.

The equality and further isomorphism are remarkable for a few reasons. First, in the noncommutative case, it is nontrivial to show that the set of symmetric noncommutative polynomials generate the free skew field of symmetric rational functions. For example, expressions for relatively simple symmetric rational functions may require complicated expressions in terms of the generators, as is shown by the equalities expressing $x^{-1}+y^{-1}$:

$$\begin{aligned}x^{-1}+y^{-1} &= 4(x+y-(x-y)^2((x-y)(x+y)(x-y))^{-1}(x-y)^2)^{-1}\\ &= \varphi((a-bc^{-1}b)^{-1})\end{aligned}$$

(It is somewhat hard to even find an elementary way of showing the equality; we manufactured it using realization theory which will be a key ingredient of the proof of our main result.) Secondly, it is interesting that $x+y,(x-y)^2,(x-y)(x+y)(x-y)$ satisfy no hidden rational relations, which follows from a result of Lewin [Lew74, Theorem 1]. Unlike in the commutative case, it does not suffice to test only polynomial relations; for example, x, xy, xy^2 satisfy no polynomial relations and generate a proper free subalgebra in $\mathbb{F}\langle x,y\rangle$, while they satisfy a rational relation and the skew field they generate in $\mathbb{F}\langle\!\!\langle x,y\rangle\!\!\rangle$ is $\mathbb{F}\langle\!\!\langle x,y\rangle\!\!\rangle$ itself. The theory of symmetric noncommutative functions was first initiated through quasideterminants in [GKL+95], and their combinatorial aspects were further studied in [RS06, BRRZ08]. For the construction of a noncommutative manifold corresponding to symmetric analytic noncommutative functions, and associated Waring–Lagrange theorems and Newton–Girard formulae, see [AMY18].

There are also potential applications of understanding invariant subfields of the free skew field in theoretical control theory. Noncommutative rational functions naturally arise as transfer functions of linear systems that evolve along free semigroups [BGM05, BGM06]. When such a system admits additional symmetries (described by a group action), so does its associated transfer function. If the generators for this group action are known, then the transfer function can be expressed in terms of invariant building blocks. Thus it is likely that, as with classical discrete-time linear systems, this decomposition of the transfer function leads to a decomposition of the linear system into lower-dimensional subsystems, which make for a simpler analysis.

1.1. **Main results.** Let $G \subseteq \mathrm{GL}_d(\mathbb{F})$ be a finite group. The **skew field of rational invariants**, denoted by $\mathbb{F}\langle\!\!\langle x_1,\dots,x_d \rangle\!\!\rangle^G$, is the skew field of elements of $\mathbb{F}\langle\!\!\langle x_1,\dots,x_d \rangle\!\!\rangle$ that are invariant under the action of G, that is,

$$\mathbb{F}\langle\!\!\langle x_1,\dots,x_d \rangle\!\!\rangle^G = \{r \in \mathbb{F}\langle\!\!\langle x_1,\dots,x_d \rangle\!\!\rangle : r(g\cdot x) = r(x) \text{ for all } g \in G\}.$$

Our first main result states that for solvable groups the skew field of rational invariants is always finitely generated:

Theorem 1.1. *Let $G \subseteq \mathrm{GL}_d(\mathbb{F})$ be a finite solvable group. Then the skew field of invariants $\mathbb{F}\langle\!\!\langle x_1,\dots,x_d \rangle\!\!\rangle^G$ is finitely generated.*

For solvable groups G with a well-behaved representation theory we can give a finer structure of the invariant skew field $\mathbb{F}\langle\!\!\langle x_1,\dots,x_d \rangle\!\!\rangle^G$.

Definition 1.2. Let G be a finite group.

(1) Let N be a nontrivial normal abelian subgroup. We say that G is **unramified** over N if for every irreducible representation π of G, $\pi|_N$ is trivial or $\pi|_N$ splits into distinct irreducible representations of N.

(2) We say a group G is **totally unramified** if either G is the trivial group or there exists a nontrivial normal abelian subgroup N such that G is unramified over N and G/N is totally unramified.

Theorem 1.3. *Let G be a totally unramified group acting on $\mathbb{F}^G$ via the left regular representation. Then*

$$\mathbb{F}\langle\!\!\langle x_1,\dots,x_{|G|} \rangle\!\!\rangle^G \cong \mathbb{F}\langle\!\!\langle u_1,\dots,u_{|G|(|G|-1)+1} \rangle\!\!\rangle.$$

Examples of totally unramified groups include abelian groups, S_3, S_4, and dihedral groups; furthermore, all groups of order < 24 are totally unramified. For these, noncommutative Noether's problem is tractable in the sense that for left regular representations the answer is affirmative. In fact, we conjecture that invariant skew fields of finite groups are always free.

The smallest non-example of a totally unramified group is the group $\mathrm{SL}_2(\mathbb{F}_3)$ of order 24. The next non-examples are given by eight groups of order 48: the four groups in the isoclinism class of $(\mathbb{Z}_4 \times D_4) \rtimes \mathbb{Z}_2$, the isoclinism class of $\mathrm{GL}_2(\mathbb{F}_3)$ with two groups, and the isoclinism class of $\mathbb{Z}_2 \times \mathrm{SL}_2(\mathbb{F}_3)$ again containing two groups. Then we find 32 groups that are not totally unramified among the 267 groups of order 64. The smallest odd order examples are found among groups with 243 elements.

Finally, we present applications of the above results (for $\mathbb{F} = \mathbb{C}$) to real algebraic geometry. We provide positivity certificates for invariant noncommutative rational functions in terms of invariant weighted sums of squares. We say that $r \in \mathbb{C}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle$ is **positive** if for every $n \in \mathbb{N}$ and a tuple of hermitian matrices $X \in \mathrm{M}_n(\mathbb{C})^d$, r is defined at X and $r(X)$ is a positive semidefinite matrix. The following is a solution of the invariant free rational Hilbert's 17th problem.

Theorem 1.4. *Let $G \subset \mathrm{U}_d(\mathbb{C})$ be a finite solvable group. Then there are $q_1, \dots, q_N \in \mathbb{C}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^G$ such that every positive rational function $r \in \mathbb{C}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^G$ is of the form*

$$r = \sum_j \tilde{s}_j^* q_{n_j} \tilde{s}_j$$

for some $\tilde{s}_j \in \mathbb{C}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^G$.

Furthermore, we establish Positivstellensätze for invariant semialgebraic sets of bounded operators on a separable Hilbert space. Corollary 6.5 treats strict positivity when the invariant constraints satisfy an Archimedean condition, and Corollary 6.6 certifies positivity on convex domains (i.e., those given by linear matrix inequalities).

1.2. **Reader's guide.** The paper is organized as follows. After Section 2 with preliminaries we establish Theorem 1.1 in Section 3. Theorem 1.3 for abelian groups G is proved in Section 4, followed by the proof of the theorem itself, and a strengthening thereof (Theorem 5.1) in Section 5. Finally, Section 6 discusses relationships with real algebraic geometry; positivity certificates for invariant positive rational functions can be chosen to be invariant themselves.

Acknowledgment. The authors thank Primož Moravec and John Shareshian for insightful discussions on finite groups, and the anonymous referee for suggestions that vastly improved the presentation of the paper.

2. Preliminaries on group representations

In this section we give some background and introduce notions which will be necessary for the sequel.

2.1. **Pontryagin duality.** Let N be a finite abelian group. Define N^* to be the group of multiplicative homomorphisms $\chi : N \to \mathbb{F}^*$. The group N^* is non-canonically isomorphic to N. Every representation π of N decomposes into a direct sum of elements of N^*, that is, N^* consists of all the irreducible representations of N. For more details see [Ser77, Rud90].

2.2. **Complete representations.** A faithful representation π of a group G is **complete** if there is a direct summand π_B of π (i.e., π decomposes as $\pi_B \oplus \pi_J$ for some subrepresentation π_J) and there is a nontrivial normal abelian subgroup $N \subseteq G$ such that:

(1) $\pi_B|_N$ contains exactly the nontrivial representations of N as direct summands with multiplicity 1;
(2) The representation

$$\pi_{N^\tau} \oplus (\pi_B \otimes \pi \oplus \pi \otimes \pi_B)_{N^\tau} \oplus (\pi_B \otimes \pi \otimes \pi_B)_{N^\tau}$$

is a complete representation of G/N. Here, for a representation ϱ, ϱ_{N^τ} denotes the summands of ϱ which are trivial on N and thus naturally gives rise to a representation of G/N.

The notion of a complete representation is rather technical; the proper motivation is unveiled in Lemma 5.2, where completeness ensures linearity of certain induced group actions. In any case, complete representations should be viewed as a companion concept to the more natural definition of an unramified group. Namely, as seen in the proof of Theorem 1.3 below, the left regular representation of a totally unramified group is complete.

2.3. **Unramified groups.** The interplay between subgroups and representations is the subject of Clifford theory, see e.g. [Isa76]. We now give a reinterpretation of what it means for G to be unramified over a normal abelian subgroup N. There is a natural action of G/N on N^* given by

$$gN : \chi \mapsto (n \mapsto \chi(g^{-1}ng)) = \chi^g.$$

Let π an irreducible representation of G, such that $\pi|_N$ decomposes as $\bigoplus_i \chi_i$. For any $gN \in \text{Stab}\, \chi_i$, we have that $\pi(g)e_i \in \text{span}\, e_i$, where e_i form the basis corresponding to the decomposition of $\pi|_N$ into one-dimensional representations $\bigoplus_i \chi_i$. That is, G/N acts on the characters composing π, so if they are all distinct, as in the case of a totally unramified group, it permutes them.

Example 2.1. We show that S_4 is totally unramified. The maximal abelian normal subgroup is given by $\{e, (12)(34), (13)(24), (14)(23)\}$ which is an isomorphic copy of the Klein four group $V = \mathbb{Z}_2 \times \mathbb{Z}_2$. The character tables of the representations of V and S_4 are given by:

π_1	1	1	1	1
π_2	1	-1	1	-1
π_3	1	1	-1	-1
π_4	1	-1	-1	1

V

	{}	{2}	{2,2}	{3}	{4}
τ_1	1	1	1	1	1
τ_2	1	-1	1	1	-1
τ_3	3	1	-1	0	-1
τ_4	3	-1	-1	0	1
τ_5	2	0	2	-1	0

S_4

The only irreducible characters of S_4 that are nontrivial on V are τ_3 and τ_4. From the tables we see $\tau_3|_V = \tau_4|_V = \pi_2 + \pi_3 + \pi_4$. Therefore S_4 is unramified over V.

Now it remains to see that $S_4/V \cong S_3$ is totally unramified. The group S_3 has three irreducible representations, two of which are one-dimensional. The two-dimensional representation restricted to the $\mathbb{Z}_3$ subgroup has two distinct characters on the diagonal.

Example 2.2. The dihedral groups $D_n = \langle a, b \colon a^n = b^2 = abab = e\rangle$ are totally unramified. The irreducible two-dimensional representations π are given by

$$\pi \colon a \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \; b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where ω is a primitive n-th root of unity. The restriction of π to $\langle a \rangle$ splits into two distinct irreducible representations. For $n \geq 4$ such a representation is clearly not complete.

3. Solvable groups and their invariants

In this section we prove Theorem 1.1. A main technical ingredient are realizations of noncommutative rational functions, i.e., a canonical-type forms for them.

3.1. **Realizations.** Each rational function can be written in the form

$$r = c^* L^{-1} b \tag{3.1}$$

where $b, c \in \mathbb{F}^n$, and

$$L = A_0 + \sum_{i=1}^{d} A_i x_i$$

for some $A_i \in \mathrm{M}_n(\mathbb{F})$. This formula is nondegenerate if and only if L admits an invertible matrix evaluation. For a comprehensive study of noncommutative rational functions we refer to [Coh06, BR11] or [BGM05, KVV12]. We will need the realization formula in (3.1) to prove for abelian groups (and thus for solvable groups via a later inductive argument) that the noncommutative polynomial invariants generate the rational invariants.

3.2. **Proof of Theorem 1.1.** We prove that if G/H is abelian and $\mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^H$ is finitely generated, then $\mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^G$ is finitely generated. Note that this suffices for proving Theorem 1.1 by a simple inductive argument.

Lemma 3.1. *Let H be a normal subgroup of G such that $G/H = N$ is abelian. Suppose there are finitely many $q_i \in \mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^H$ such that every $r \in \mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^H$ is of the form*

$$r(x) = c^* \left(A_0 + \sum_i A_i q_i(x) \right)^{-1} b, \tag{3.2}$$

where the formula on the right-hand side is nondegenerate. Then, there exist finitely many $\tilde{q}_j \in \mathbb{F}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$ *such that for every* $\tilde{r} \in \mathbb{F}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$ *we have*

$$\tilde{r}(x) = \tilde{c}^* \left(\tilde{A}_0 + \sum_j \tilde{A}_j \tilde{q}_j(x)\right)^{-1} \tilde{b}, \tag{3.3}$$

and the formula on the right-hand side is nondegenerate.

Proof. Let $V = \operatorname{span}\{n \cdot q_i(x) \colon n \in N\}$. By Pontryagin duality there exists a basis $\{v_i\}_i$ for V such that $n \cdot v_i = \chi_i(n) v_i$. Without loss of generality, $q_i = v_i$. For each nontrivial χ in the subgroup of N^* generated by the χ_i, pick a monomial m_χ in the q_i such that $n \cdot m_\chi = \chi(n) m_\chi$. Without loss of generality, the subgroup generated by the χ_i is the whole of N^*.

The representation $\chi_i \mapsto \oplus_{n\in N}\chi_i(n)$ is conjugate to the left regular representation of N^*. Denote $\tilde{\chi}_i = P(\oplus_{n\in N}\chi_i(n))P^{-1}$ where $\tilde{\chi}_i$ is the permutation matrix that maps e_ν to $e_{\chi_i\nu}$. Define vectors

$$s^* = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} P \quad \text{and} \quad t = P^{-1} \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^*.$$

Index the rows of vectors s, t with elements of N. Observe that $s^* t = \sum_{n\in N} s_n t_n = 1$.

Let $\tilde{r}(x)$ be a G-invariant rational function. Then it is in particular H-invariant, and by assumption it admits a realization as in (3.2). From it one derives a new realization of $\tilde{r}(x)$,

$$\begin{aligned}
\tilde{r}(x) &= \sum_{n\in N} s_n t_n c^* \left(A_0 + \sum_i A_i q_i(n\cdot x)\right)^{-1} b \\
&= (s\otimes c)^* \left(I\otimes A_0 + \oplus_{n\in N} \sum_i A_i q_i(n\cdot x)\right)^{-1} (t\otimes b) \\
&= (s\otimes c)^* \left(I\otimes A_0 + \oplus_{n\in N} \sum_i A_i \chi_i(n) q_i(x)\right)^{-1} (t\otimes b) \\
&= \begin{pmatrix} c \\ 0 \\ \vdots \\ 0 \end{pmatrix}^* \left(I\otimes A_0 + \sum_i \tilde{\chi}_i \otimes A_i q_i(x)\right)^{-1} \begin{pmatrix} b \\ 0 \\ \vdots \\ 0 \end{pmatrix} \\
&=: \tilde{c}^* \left(I\otimes A_0 + \sum_i \tilde{\chi}_i \otimes A_i q_i(x)\right)^{-1} \tilde{b}.
\end{aligned}$$

Let M be a diagonal matrix with columns indexed by elements of N^* (starting with the identity) such that the diagonal entries are m_χ for nontrivial χ and 1 otherwise. Similarly, let $\hat{M}$ be diagonal with diagonal entries $m_{\chi^{-1}}$ for nontrivial χ and 1 otherwise. Observe that $\tilde{c}^*(M\otimes I) = \tilde{c}^*$ and $(\hat{M}\otimes I)\tilde{b} = \tilde{b}$

Then,

$$\begin{aligned} r(x) &= \tilde{c}^* \left(I \otimes A_0 + \sum_i \tilde{\chi}_i \otimes A_i q_i(x) \right)^{-1} \tilde{b} \\ &= \tilde{c}^* (M M^{-1} \otimes I) \left(A_0^{\oplus |N|} + \sum_i \tilde{\chi}_i \otimes A_i q_i(x) \right)^{-1} (\hat{M}^{-1} \hat{M} \otimes I) \tilde{b} \\ &= \tilde{c}^* \left(\hat{M} M \otimes A_0 + \sum_i \hat{M} \tilde{\chi}_i M q_i(x) \otimes A_i \right)^{-1} \tilde{b}. \end{aligned}$$

Note that $\hat{M}M$ is invariant. Now we need to show that $\hat{M}\tilde{\chi}_i q_i(x) M$ is invariant. The nonzero elements of $\hat{M}\tilde{\chi}_i q_i(x) M$ are $m_{(\chi_i \nu)^{-1}} q_i(x) m_\nu$ which are clearly invariant by the choice of q_i and m_χ. Let $\tilde{q}_j \in \mathbb{F}\langle\!\!\!\!<\! x_1, \ldots, x_d \!>\!\!\!\!\rangle^G$ be the nonconstant entries of matrices $\hat{M}M$ and $\hat{M}\tilde{\chi}_i q_i(x) M$ (they do not depend on b, c, A_i from (3.2)). So there are constant matrices $\tilde{A}_j$ such that

$$\hat{M} M \otimes A_0 + \sum_i \hat{M} \tilde{\chi}_i M q_i(x) \otimes A_i = \tilde{A}_0 + \sum_j \tilde{A}_j \tilde{q}_j(x).$$

This concludes the proof since the new form (3.3) is defined wherever M was invertible, and thus non-degenerate. ☐

4. The abelian case

The next theorem shows that the invariant fields for abelian groups are free and can be explicitly described.

Theorem 4.1. *Let $G \subset \mathrm{GL}_d(\mathbb{F})$ be abelian. Then*

$$\mathbb{F}\langle\!\!\!\!<\! x_1, \ldots, x_d \!>\!\!\!\!\rangle^G \cong \mathbb{F}\langle\!\!\!\!<\! u_1, \ldots, u_{|G|(d-1)+1} \!>\!\!\!\!\rangle.$$

If G is diagonal, that is $G = \oplus \chi_i$ where $\chi_i \in G^*$, then any minimal set of generators for the subgroup of the free group on d generators given by the words $x_{i_1}^{j_1} \ldots x_{i_k}^{j_k}$ with $\chi_{i_1}^{j_1} \ldots \chi_{i_k}^{j_k} = 1$ can serve as the preimage of the u_j.

Proof. We note that every linear action of an abelian group G can be diagonalized with an appropriate linear change of coordinates. Hence there exist linear polynomials $w_1, \ldots, w_d$ such that

$$g \cdot w_i = \chi_i(g) w_i,$$

where χ_i belongs to the character group of G, denoted $\hat{G}$, and w_i form an orthonormal basis (in the sense that the coefficients are orthogonal) for the space of all linear polynomials in $\mathbb{F}<x_1, \ldots, x_d>$. By [CPTD18, Theorem 7.4] the elements of $\mathbb{F}<x_1, \ldots, x_d>^G$ are spanned by monomials of the form $w_{i_1} \ldots w_{i_k}$ such that $\chi_{i_1} \ldots \chi_{i_k} = 1$. By embedding $\mathbb{F}<x_1, \ldots, x_d>$ into the group algebra of the free group on d generators by mapping the w_i to the said group generators, one obtains that the invariants in the free group algebra (of noncommutative Laurent polynomials) are generated by $|G|(d-1)+1$ elements via the Nielsen-Schreier theorem [LS01, Section I.3] as in [CPTD18, Theorem 7.5]. Concretely, we have a surjective homomorphism from the free group with d generators to $\hat{G}$ which is itself non-canonically isomorphic to G. The kernel of this homomorphism is a subgroup of the free group with d generators, which must be free and have $|G|(d-1)+1$ generators via the Nielsen-Schreier formula. The generating elements can satisfy no rational relations by [Lew74] (see also [Lin00]), that is, their rational closure is a free skew field on these generators.

Therefore it suffices to show that polynomial invariants $\mathbb{F}\langle x_1,\dots,x_d\rangle^G$ generate the skew field of rational invariants $\mathbb{F}(\!\langle x_1,\dots,x_d\rangle\!)^G$. This follows a similar line of reasoning as used in the proof of Lemma 3.1. Let $r\in\mathbb{F}(\!\langle x_1,\dots,x_d\rangle\!)^G$. By the realization theory, one can write any element of the free skew field as $r=c^*(A_0+\sum_i A_iw_i)^{-1}b$. Now $g\cdot r=r$, so as in the proof of Lemma 3.1, we have

$$r=c^*\left(A_0+\sum_i A_i\chi_i(g)w_i\right)^{-1}b=\begin{pmatrix}c\\0\\\vdots\\0\end{pmatrix}^*\left(I\otimes A_0+\sum_i\tilde{\chi}_i\otimes A_iw_i\right)^{-1}\begin{pmatrix}b\\0\\\vdots\\0\end{pmatrix},$$

where $\tilde{\chi}_i$ is the permutation matrix that maps e_ν to $e_{\chi_i\nu}$.

Fix polynomials v_χ such that $g\cdot v_\chi=\chi(g)v_\chi$ and $v_\tau=1$, where τ is the trivial representation. Let V be a diagonal matrix whose diagonal entries are the v_χ. Similarly, let $\hat{V}$ be diagonal with diagonal entries $v_{\chi^{-1}}$. Now

$$\begin{aligned}r&=\begin{pmatrix}c\\0\\\vdots\\0\end{pmatrix}^*\left(I\otimes A_0+\sum_i\tilde{\chi}_i\otimes A_iw_i\right)^{-1}\begin{pmatrix}b\\0\\\vdots\\0\end{pmatrix}\\&=\begin{pmatrix}c\\0\\\vdots\\0\end{pmatrix}^*(VV^{-1}\otimes I)\left(I\otimes A_0+\sum_i\tilde{\chi}_i\otimes A_iw_i\right)^{-1}(\hat{V}^{-1}\hat{V}\otimes I)\begin{pmatrix}b\\0\\\vdots\\0\end{pmatrix}\\&=\begin{pmatrix}c\\0\\\vdots\\0\end{pmatrix}^*\left(\hat{V}V\otimes A_0+\sum_i(\hat{V}\tilde{\chi}_iw_iV)\otimes A_i\right)^{-1}\begin{pmatrix}b\\0\\\vdots\\0\end{pmatrix}.\end{aligned}$$

As in the proof of Lemma 3.1, $\hat{V}V$ and $\hat{V}\tilde{\chi}_iw_iV$ are invariant under the action of G. We get $(\tilde{\chi}_i)_{\eta,\nu}=1$ if $\eta=\chi_i\nu$ and 0 otherwise. Now, $(\hat{V}\tilde{\chi}_iw_iV)_{\chi_i\nu,\nu}=v_{\chi_i^{-1}\nu^{-1}}w_iv_\nu$ is clearly invariant, so we are done. □

Corollary 4.2. *Let G be an abelian group acting on $\mathbb{F}^d$ via a complete representation $\pi=\pi_B\oplus\pi_J$, where π_B acts on $\mathbb{F}^{G^*\setminus\{\tau\}}$ and τ denotes the trivial representation. Let b_χ and j_i diagonalize π_B and π_J, respectively. Then*

$$\mathbb{F}(\!\langle x_1,\dots,x_d\rangle\!)^G\cong\mathbb{F}(\!\langle u_1,\dots,u_{|G|(d-1)+1}\rangle\!),$$

and preimages of the u_j are of the form $b_\chi b_\eta b_{(\chi\eta)^{-1}}, b_\chi j_i b_{(\chi\eta_i)^{-1}}$, where $b_\tau=1$.

Proof. For v_χ from the proof of Theorem 4.1 we take b_χ, while for w_i we take b_χ and j_i for $i = 1, \dots, d - |G| + 1$, where $d - |G| + 1$ is the dimension of π_J. Clearly

$$\left\{b_\eta b_{\eta^{-1}},\ b_\chi b_\eta b_{(\chi\eta)^{-1}},\ b_\chi j_i b_{(\chi\eta_i)^{-1}} \colon \chi \in G^*,\ \eta \in G^* \setminus \{\tau\},\ 1 \le i \le t\right\} \setminus \{1\}$$

generate $\mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^G$. Since $b_\eta b_{\eta^{-1}} = b_\tau b_\eta b_{\eta^{-1}} = b_\eta b_{\eta^{-1}} b_\tau$, there are

$$(|G| - 1) + (|G| - 1)(|G| - 2) + |G|(d - |G| + 1) = |G|(d - 1) + 1$$

generators. By [Coh95, Corollary 5.8.14] they are free generators of the free skew field of invariants. □

Example 4.3. Let ω be a third root of unity and c a generator of $\mathbb{Z}_3$. Define a representation of $\mathbb{Z}_3$ on $\mathbb{F}^2$ by $cx = \omega x$ and $cy = \omega^2 y$. Then we have

$$\mathbb{F}\langle\!\langle x, y \rangle\!\rangle^{\mathbb{Z}_3} = \mathbb{F}\langle\!\langle x^3, xy, yx, y^3 \rangle\!\rangle.$$

5. Unramified groups and their invariants

The following is our main structure theorem for invariant fields of solvable groups.

Theorem 5.1. *Let $G \subset \mathrm{GL}_d(\mathbb{F})$ be a finite group acting on $\mathbb{F}^d$ via a complete representation. Then*

$$\mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^G \cong \mathbb{F}\langle\!\langle u_1, \dots, u_{|G|(d-1)+1} \rangle\!\rangle.$$

A key step in the proof of Theorem 5.1 will be the following lemma.

Lemma 5.2. *Let $\pi = \pi_B \oplus \pi_J$ be a complete representation of G on $\mathbb{F}^d$ and let N be a normal abelian subgroup as in the definition of complete representation in Section 2.2. Then G/N acts linearly on the free generators of $\mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^N$ constructed in Corollary 4.2 (when applied to the abelian group N).*

Proof. Let b_χ and j_k diagonalize $\pi_B|_N$ and $\pi_J|_N$, respectively. Here b_χ are indexed by $N^* \backslash \{\tau\}$. Then $ng \cdot b_\chi = \chi(g^{-1}ng)(g \cdot b_\chi) = \chi^g(n)(g \cdot b_\chi)$, so $g \cdot b_\chi$ is a scalar multiple of b_{χ^g}.

Denote $V_\chi = \operatorname{span}\{j_i \colon n \cdot j_i = \chi(n) j_i\}$. Since $ng \cdot j_i = \chi(g^{-1}ng)(g \cdot j_i) = \chi^g(n)(g \cdot j_i)$, $v \in V_\chi$ implies $g \cdot v \in V_{\chi^g}$. □

Proof of Theorem 5.1. Let π be a complete representation of G and N a nontrivial abelian normal subgroup corresponding to it. Then G/N acts linearly on

$$\mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^N \cong \mathbb{F}\langle\!\langle u_1, \dots, u_{|N|(d-1)+1} \rangle\!\rangle$$

by Lemma 5.2; furthermore, by the description of the generators u_j in Corollary 4.2, this action is precisely the representation

$$\pi_{N^\tau} \oplus (\pi_B \otimes \pi \oplus \pi \otimes \pi_B)_{N^\tau} \oplus (\pi_B \otimes \pi \otimes \pi_B)_{N^\tau}.$$

Since it is a complete representation of G/N by assumption, induction implies

$$\mathbb{F}\langle\!\langle x_1, \dots, x_d \rangle\!\rangle^G \cong \mathbb{F}\langle\!\langle u_1, \dots, u_{|N|(d-1)+1} \rangle\!\rangle^{G/N} \cong \mathbb{F}\langle\!\langle \tilde{u}_1, \dots, \tilde{u}_{|G|(d-1)+1} \rangle\!\rangle. \qquad \square$$

Proof of Theorem 1.3. We prove that the left regular representation of a totally unramified group is complete. Let G be unramified over N. By Clifford's theorem [Isa76, Theorem 6.2], irreducible representations of N partition into orbits and each orbit is represented by an irreducible representation of G. Take the nontrivial representatives and define π_B as their sum. The left regular representation of G/N is then contained in π_{N^τ} and we are done by recursion. □

Example 5.3. Define a representation of S_3 on $\mathbb{F}^3$ via $\sigma x_i = x_{\sigma(i)}$. The representation of the normal subgroup N generated by $(1\ 2\ 3)$ is diagonalized in the basis $v_1 = x_1 + x_2 + x_3$, $v_2 = x_1 + \omega x_2 + \omega^2 x_3$, $v_3 = x_1 + \omega^2 x_2 + \omega x_3$, where ω is the third root of unity. By Corollary 4.2, we obtain the invariant skew field $\mathbb{F}\langle\!\!\langle x_1, x_2, x_3\rangle\!\!\rangle^N = \mathbb{F}\langle\!\!\langle v_1, v_2v_3, v_3v_2, v_2v_1v_3, v_3v_1v_2, v_2^3, v_3^3\rangle\!\!\rangle = \mathbb{F}\langle\!\!\langle z_1, \dots, z_7\rangle\!\!\rangle$.

The action of $G/N \cong \mathbb{Z}_2$ on $\mathbb{F}\langle\!\!\langle z_1, \dots, z_7\rangle\!\!\rangle$ is given by the action of $(2\ 3)$ (or any other transposition) on the initial variables. We get a representation given by

$$z_1 \mapsto z_1, z_2 \mapsto z_3, z_3 \mapsto z_2, z_4 \mapsto z_5, z_5 \mapsto z_4, z_6 \mapsto z_7, z_7 \mapsto z_6,$$

which is diagonalized by

$$w_1 = z_1, w_2 = z_2 + z_3, w_3 = z_2 - z_3, w_4 = z_4 + z_5, w_5 = z_4 - z_5, w_6 = z_6 + z_7, w_7 = z_6 - z_7.$$

Finally, applying Corollary 4.2 again, the obtained free generators of $\mathbb{F}\langle\!\!\langle x_1, x_2, x_3\rangle\!\!\rangle^{S_3}$ are

$$w_1,\ w_2,\ w_4,\ w_6,\ w_3^2,\ w_3w_5,\ w_3w_7,\ w_5w_3,\ w_7w_3,\ w_3w_1w_3,\ w_3w_2w_3,\ w_3w_4w_3,\ w_3w_6w_3.$$

Example 5.4. Even though the standard two-dimensional representation of $D_4 = \mathbb{Z}_4 \rtimes \mathbb{Z}_2$ given by $a \cdot x = ix,\ a \cdot y = -iy,\ b \cdot x = y$ and $b \cdot y = x$ is not complete, we can still compute its invariants. The invariants of $N = \langle a\rangle \cong \mathbb{Z}_4$ are freely generated by $z_1 = xy,\ z_2 = yx,\ z_3 = x^2y^2,\ z_4 = y^2x^2$ and $z_5' = x^4$. Then we replace z_5' by $z_5 = z_5' z_4^{-1} = x^2y^{-2}$. The action of $D_4/N \cong \mathbb{Z}_2$ on these generators is

$$z_1 \mapsto z_2,\ z_2 \mapsto z_1,\ z_3 \mapsto z_4,\ z_4 \mapsto z_3,\ z_5 \mapsto z_5^{-1}.$$

Observe that this action is linearized and diagonalized with respect to

$$w_1 = z_1 + z_2,\ w_2 = z_1 - z_2,\ w_3 = z_3 + z_4,\ w_4 = z_3 - z_4,\ w_5 = (1 + z_5)(1 - z_5)^{-1}.$$

Finally we get nine free generators of the rational invariants of D_4:

$$w_1,\ w_2^2,\ w_2w_1w_2,\ w_2w_3w_2,\ w_2w_4w,\ w_2w_5,\ w_3,\ w_4w_2,\ w_5w_2.$$

Example 5.5. The smallest example of a not totally unramified group is $\mathrm{SL}_2(\mathbb{F}_3)$. It has only one nontrivial normal abelian subgroup $N \cong \mathbb{Z}_2$; it is generated by $\mathrm{diag}(2, 2)$. Every irreducible representation restricted to N is trivial or contains two copies of the sign representation.

Let us describe problems arising in the computation of a generating set for the skew field of invariants. We start with a two-dimensional irreducible representation of

$\mathrm{SL}_2(\mathbb{F}_3)$ on $\mathbb{F}^2$, for instance defined by

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\mapsto\begin{pmatrix}0&\omega^2\\-\omega&-1\end{pmatrix},\quad \begin{pmatrix}0&1\\2&0\end{pmatrix}\mapsto\begin{pmatrix}0&-\omega\\\omega^2&0\end{pmatrix}.$$

The generator of N is mapped to $\mathrm{diag}(-1,-1)$. Hence the free generators of N-invariants are x^2, xy and yx.

The group G/N has one abelian normal subgroup $\tilde{N}/N$; it is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2$. Representatives of its generators are mapped to

$$\begin{pmatrix}0&\omega\\-\omega^2&0\end{pmatrix}\quad\text{and}\quad\begin{pmatrix}-\omega&-1\\\omega&\omega\end{pmatrix}.$$

The action of these two on N-invariants is given by

$$x^2\mapsto\omega y^2=\omega(yx)(x^2)^{-1}(xy),\ xy\mapsto -yx,\ yx\mapsto -xy, \tag{5.1}$$

and

$$x^2\mapsto\omega(x+y)^2,\ xy\mapsto-\omega(x+y)(\omega y-x),\ yx\mapsto-\omega(\omega y-x)(x+y). \tag{5.2}$$

Now the problem is to find a set of free generators of N-invariants that simultaneously linearizes and diagonalizes both mappings as we have done in Example 5.4. It is straightforward to linearize (5.1) by using a linear fractional transformation in $xy^{-1}=x^2(yx)^{-1}$ (cf. Example 5.4), but then the action (5.2) becomes unwieldy. We have been unable to determine if $\mathbb{F}\langle\!\langle x,y\rangle\!\rangle^{\mathrm{SL}_2(\mathbb{F}_3)}$ is free (on 25 generators).

6. Positivity of invariant rational functions

In this section we investigate positive invariant noncommutative rational functions and prove an invariant rational Positivstellensatz in Theorem 6.2 for solvable groups G. A finer structure of constraint positivity is proved in Subsection 6.1. Positivity certificates for invariants are ubiquitous in real algebraic geometry literature, see e.g. [PS85, CKS09, Rie16, Bro98]. Throughout this section let $\mathbb{F}=\mathbb{C}$ be the field of complex numbers. We endow $\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle$ with the natural involution fixing the x_j and extending the complex conjugation on $\mathbb{C}$.

Lemma 6.1. *Let $G\subset\mathrm{U}_d(\mathbb{C})$ be a finite solvable group, H its normal subgroup, and assume that $N=G/H$ is abelian. There exists an invertible matrix $R_N\in\mathrm{M}_{|N|}(\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^H)$ such that for every $Q_H\in\mathrm{M}_n(\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^H)$,*

$$Q_G=(R_N\otimes I)^*\left(\bigoplus_{n\in N}n\cdot Q_H\right)(R_N\otimes I)\in\mathrm{M}_{|N|n}(\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G)$$

and every $r\in\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$ of the form

$$r(x)=c^*\left(\left(A_0+\sum_i A_iq_i(x)\right)^{-1}\right)^*Q_H\left(A_0+\sum_i A_iq_i(x)\right)^{-1}c, \tag{6.1}$$

where the $q_i \in \mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^H$, *can be rewritten as*

$$r(x) = \tilde{c}^* \left(\left(\tilde{A}_0 + \sum_j \tilde{A}_j \tilde{q}_j(x)\right)^{-1}\right)^* Q_G \left(\tilde{A}_0 + \sum_j \tilde{A}_j \tilde{q}_j(x)\right)^{-1} \tilde{c}$$

with $\tilde{q}_j \in \mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$.

Proof. Consider $r(x)$ as in (6.1). Tracing through the proof of Theorem 1.1 we see that $r(x)$ admits a realization

$$\tilde{c}^* \left(\left(\tilde{A}_0 + \textstyle\sum_j \tilde{A}_j \tilde{q}_j(x)\right)^{-1}\right)^* ((\hat{M}\Gamma^*)\otimes I)\left(\textstyle\bigoplus_{n\in N} n\cdot Q_H\right)((\Gamma M)\otimes I)\left(\tilde{A}_0 + \textstyle\sum_j \tilde{A}_j \tilde{q}_j(x)\right)^{-1}\tilde{c},$$

where Γ is a unitary change of basis matrix (more precisely, columns of Γ^* are eigenvectors for the left regular representation of N^*). Note that we can take $\hat{M} = M^*$. Hence $R_N = \Gamma M$ is the desired matrix. □

Theorem 6.2. *Let* $G \subset \mathrm{U}_d(\mathbb{C})$ *be a finite solvable group. There exists an invertible matrix* $R_G \in \mathrm{M}_{|G|}(\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle)$ *such that for every* $Q \in \mathrm{M}_n(\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle)$,

$$Q_G = (R_G \otimes I)^* \left(\bigoplus_{g\in G} g\cdot Q\right)(R_G\otimes I) \in \mathrm{M}_{|G|n}(\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G)$$

and every $r \in \mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$ *of the form*

$$r(x) = c^* \left(\left(A_0 + \sum_i A_i q_i(x)\right)^{-1}\right)^* Q \left(A_0 + \sum_i A_i q_i(x)\right)^{-1} c, \tag{6.2}$$

where the $q_i \in \mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle$, *can be rewritten as*

$$r(x) = \tilde{c}^* \left(\left(\tilde{A}_0 + \sum_j \tilde{A}_j \tilde{q}_j(x)\right)^{-1}\right)^* Q_G \left(\tilde{A}_0 + \sum_j \tilde{A}_j \tilde{q}_j(x)\right)^{-1} \tilde{c} \tag{6.3}$$

with $\tilde{q}_j \in \mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$.

Proof. Apply Lemma 6.1 and induction on the derived series of G. □

Corollary 6.3. *Let* $G \subset \mathrm{U}_d(\mathbb{C})$ *be a finite solvable group. Then there are* $q_1,\dots,q_N \in \mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$ *such that for every* $r \in \mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$, *if* $r = \sum_i s_i^* s_i$, *then*

$$r = \sum_j \tilde{s}_j^* q_{n_j} \tilde{s}_j,$$

where $\tilde{s}_j \in \mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G$.

Proof. If $s_i = c_i^* L_i^{-1} b_i$ is a realization of s_i, then

$$s_i^* s_i = \begin{pmatrix} 0 & b_i^* \end{pmatrix} \begin{pmatrix} c_i c_i^* & L_i^* \\ -L_i & 0 \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ b_i \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 0 & b_i^* \end{pmatrix}\left(\begin{pmatrix} c_ic_i^* & L_i^* \\ -L_i & 0 \end{pmatrix}^{-1} + \begin{pmatrix} c_ic_i^* & -L_i^* \\ L_i & 0 \end{pmatrix}^{-1}\right)\begin{pmatrix} 0 \\ b_i \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 0 & b_i^* \end{pmatrix}\begin{pmatrix} c_ic_i^* & L_i^* \\ -L_i & 0 \end{pmatrix}^{-1}\left(\begin{pmatrix} c_ic_i^* & L_i^* \\ -L_i & 0 \end{pmatrix} + \begin{pmatrix} c_ic_i^* & -L_i^* \\ L_i & 0 \end{pmatrix}\right)\begin{pmatrix} c_ic_i^* & -L_i^* \\ L_i & 0 \end{pmatrix}^{-1}\begin{pmatrix} 0 \\ b_i \end{pmatrix}$$

$$= \begin{pmatrix} 0 & b_i^* \end{pmatrix}\begin{pmatrix} c_ic_i^* & L_i^* \\ -L_i & 0 \end{pmatrix}^{-1}\begin{pmatrix} c_ic_i^* & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c_ic_i^* & -L_i^* \\ L_i & 0 \end{pmatrix}^{-1}\begin{pmatrix} 0 \\ b_i \end{pmatrix}.$$

Therefore r can be written as in (6.2) for a constant positive semidefinite $Q = P^*P$. By Theorem 6.2, r can be written as in (6.3) with $Q_G = (R_G \otimes P)^*(R_G \otimes P)$, which then yields the desired G-invariant sum of hermitian squares presentation for r. □

Recall that a rational function r is **positive** if for every $n \in \mathbb{N}$ and $X = X^* \in \mathrm{M}_n(\mathbb{C})^d$, r is defined at X and $r(X)$ is positive semidefinite. We are now ready to prove Theorem 1.4.

Proof of Theorem 1.4. Since r is positive semidefinite, it is a sum of hermitian squares by [KPV17, Theorem 4.5]. The conclusion now follows from Corollary 6.3. □

6.1. **Quadratic modules and free semialgebraic sets.** The **quadratic module** associated to a symmetric matrix $Q \in \mathrm{M}_n(\mathbb{C}\langle x_1, \dots, x_d \rangle)$ is

$$\mathrm{QM}_{\mathbb{C}\langle x_1,\dots,x_d\rangle}(Q) = \left\{ \textstyle\sum_i u_i^* u_i + \sum_j v_j^* Q v_j \colon v_j \in \mathbb{C}\langle x_1, \dots, x_d \rangle^n,\ u_i \in \mathbb{C}\langle x_1, \dots, x_d \rangle \right\}.$$

It is called **Archimedean** if there is $N \in \mathbb{N}$ so that $N - \sum_j x_j^2 \in \mathrm{QM}_{\mathbb{C}\langle x_1,\dots,x_d\rangle}(Q)$. The associated **free semialgebraic set** is

$$\mathcal{D}_Q = \left\{ X = X^* \in B(\mathcal{H})^d \colon Q(X) \succeq 0 \right\},$$

where $\mathcal{H}$ is a separable Hilbert space.

Corollary 6.4. *Let $G \subset \mathrm{U}_d(\mathbb{C})$ be a finite solvable group. Then*

$$\mathrm{QM}_{\mathbb{C}\langle x_1,\dots,x_d\rangle}(Q) \cap \mathbb{C}\langle x_1, \dots, x_d \rangle^G = \mathrm{QM}_{\mathbb{C}\langle x_1,\dots,x_d\rangle^G}(Q_G).$$

Proof. Use Theorem 6.2. □

Let $\mathfrak{r}$ be a formal rational expression. We say that $\mathfrak{r}$ is **(strictly) positive** on $\mathcal{D}_Q$ if for every $X \in \mathcal{D}_Q$, $\mathfrak{r}$ is defined at X and $\mathfrak{r}(X)$ is a positive semidefinite (definite) operator. In this case we write $\mathfrak{r} \succeq 0$ ($\mathfrak{r} \succ 0$) on $\mathcal{D}_Q$.

The reason for using formal rational expressions is that rational functions (as elements of the free skew field) do not admit unambiguous evaluations on $B(\mathcal{H})^d$. For example, the expression $\mathfrak{r} = x_1(x_2x_1)^{-1}x_2 - 1$ represents the zero element of the free skew field, but admits nonzero evaluations on operators, namely $\mathfrak{r}(S, S^*) \neq 0$ where S is the unilateral shift on $\ell^2(\mathbb{N})$.

Corollary 6.5. *Let $G \subset \mathrm{U}_d(\mathbb{C})$ be a finite solvable group. Suppose $Q = Q^* \in \mathrm{M}_n(\mathbb{C}<x_1,\dots,x_d>)$ is such that $\mathrm{QM}_{\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle}(Q)$ is Archimedean. If $\mathfrak{r}$ is a formal rational expression such that $\mathfrak{r} \succ 0$ on $\mathcal{D}_Q$ and $\mathfrak{r}$ induces a G-invariant rational function r, then $r \in \mathrm{QM}_{\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G}(Q_G)$.*

Proof. By [Pas18, Theorem 2.1], $r \in \mathrm{QM}_{\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle}(Q)$. Now Corollary 6.4 finishes the proof. □

When the semialgebraic set $\mathcal{D}_Q$ is convex, in which case one can assume that Q is a symmetric affine matrix by the renowned Helton–McCullough theorem [HM12], one can certify (non-strict) positivity on $\mathcal{D}_Q$.

Corollary 6.6. *Let $G \subset \mathrm{U}_d(\mathbb{C})$ be a finite solvable group. Assume $Q = Q^* \in \mathrm{M}_n(\mathbb{C}<x_1,\dots,x_d>)$ is linear with $Q(0) = I$. If $\mathfrak{r}$ is a formal rational expression such that $\mathfrak{r} \succeq 0$ on $\mathcal{D}_Q$ and $\mathfrak{r}$ induces a G-invariant rational function r, then $r \in \mathrm{QM}_{\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle^G}(Q_G)$.*

Proof. By [Pas18, Theorem 3.1], $r \in \mathrm{QM}_{\mathbb{C}\langle\!\langle x_1,\dots,x_d\rangle\!\rangle}(Q)$. Now apply Corollary 6.4. □

Example 6.7. Let $G = S_2$ act on $\mathbb{C}\langle\!\langle x,y\rangle\!\rangle$. Then

$$a = x + y, \quad b = (x-y)^2, \quad c = (x-y)(x+y)(x-y)$$

are free generators of $\mathbb{C}\langle\!\langle x,y\rangle\!\rangle^G$. The matrix R_G from Theorem 6.2 equals

$$R_G = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \operatorname{diag}(1, x-y) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & x-y \\ -1 & x-y \end{pmatrix}.$$

By computing the invariant middle matrix Q_G we obtain the following Positivstellensätze.

(1) (Entire space) If $Q = 1$ then $Q_G = \operatorname{diag}(1, b)$. By Theorem 1.4, every positive G-invariant rational function r is of the form

$$r = \sum_j u_j^* u_j + \sum_j v_j b v_j^*, \qquad u_j, v_j \in \mathbb{C}\langle\!\langle x,y\rangle\!\rangle^G.$$

(2) (Disk) If $Q = 1 - x^2 - y^2$ then

$$Q_G = \operatorname{diag}\left(1 - \tfrac{1}{2}(a^2 + b), b - \tfrac{1}{2}(cb^{-1}c + b^2)\right).$$

Since Q clearly generates an Archimedean quadratic module, every G-invariant rational expression strictly positive on the disk

$$\{(X,Y)\colon X^2 + Y^2 \preceq I\}$$

induces a rational function of the form

$$\sum_j u_j^* u_j + \sum_j v_j (1 - \tfrac{1}{2}(a^2+b)) v_j^* + \sum_j w_j (b - \tfrac{1}{2}(cb^{-1}c + b^2)) w_j^*$$

for $u_j, v_j, w_j \in \mathbb{C}\langle\!\langle x,y \rangle\!\rangle^G$ by Corollary 6.5. On the other hand, the disk also admits a linear matrix representation given by

$$Q' = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & y \\ x & y & 1 \end{pmatrix},$$

which yields

$$Q'_G = \frac{1}{2}\begin{pmatrix} 2 & 0 & a & 0 & 0 & b \\ 0 & 2 & a & 0 & 0 & -b \\ a & a & 2 & b & -b & 0 \\ 0 & 0 & b & 2b & 0 & c \\ 0 & 0 & -b & 0 & 2b & c \\ b & -b & 0 & c & c & 2b \end{pmatrix}.$$

Note that the free semialgebraic set associated with Q'_G as a matrix in variables a, b, c is also convex. By Corollary 6.6 we can use Q'_G to describe G-invariant positivity on the disk.

(3) (Bidisk) If $Q = \operatorname{diag}(1-x^2, 1-y^2)$ then

$$Q_G = \frac{1}{2}\begin{pmatrix} 2-\frac{1}{2}(a^2+b) & 0 & -\frac{1}{2}(c+ab) & 0 \\ 0 & 2-\frac{1}{2}(a^2+b) & 0 & \frac{1}{2}(c+ab) \\ -\frac{1}{2}(c+ba) & 0 & 2b-\frac{1}{2}(cb^{-1}c+b^2) & 0 \\ 0 & \frac{1}{2}(c+ba) & 0 & 2b-\frac{1}{2}(cb^{-1}c+b^2) \end{pmatrix}.$$

Note that $2Q_G$ is unitarily similar to a direct sum of two copies of

$$S = \begin{pmatrix} 2-\frac{1}{2}(a^2+b) & \frac{1}{2}(c+ab) \\ \frac{1}{2}(c+ba) & 2b-\frac{1}{2}(cb^{-1}c+b^2) \end{pmatrix}.$$

Every G-invariant rational expression strictly positive on the bidisk

$$\{(X,Y) \colon X^2 \preceq I \ \&\ Y^2 \preceq I\}$$

induces a rational function in $\mathrm{QM}_{\mathbb{C}\langle\!\langle x,y \rangle\!\rangle^G}(S)$ by Corollary 6.5. As in the case of the disk, bidisk can also be represented by a monic linear matrix inequality, which by Corollary 6.6 then gives a description of invariant expressions positive on the bidisk.

(4) (Positive orthant) If $Q = \operatorname{diag}(x, y)$ then $2Q_G$ is unitarily similar to a direct sum of two copies of

$$S = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

The positive orthant

$$\{(X,Y) \colon X \succeq 0 \ \&\ Y \succeq 0\}$$

is a convex semialgebraic set, and after a scalar shift it admits a monic linear matrix representation. Hence rational expressions positive on the orthant induce rational functions in $\mathrm{QM}_{\mathbb{C}\langle x,y\rangle}(Q)$ by [Pas18, Theorem 3.1]. The G-invariant rational functions among them then lie to $\mathrm{QM}_{\mathbb{C}\langle x,y\rangle^G}(S)$ by Corollary 6.4.

Example 6.8. Let $G = \mathbb{Z}_3$ act on $\mathbb{C}\langle x, y, z\rangle$. Let $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ and

$$q_1 = \omega x + \omega^2 y + z, \quad q_2 = \omega^2 x + \omega y + z.$$

Then

$$R_G = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega^2 & \omega & 1 \end{pmatrix} \operatorname{diag}(1, q_2, q_1).$$

For $Q = 1$ we get $Q_G = \operatorname{diag}(1, q_1 q_2, q_2 q_1)$. Therefore all positive semidefinite G-invariant rational functions in $\mathbb{C}\langle x, y, z\rangle$ are of the form

$$\sum_j u_j^* u_j + \sum_j v_j q_1 q_2 v_j^* + \sum_j w_j q_2 q_1 w_j^*, \qquad u_j, v_j, w_j \in \mathbb{C}\langle x, y, z\rangle^G.$$

References

[AM72] Michael Artin and David B. Mumford. Some elementary examples of unirational varieties which are not rational. *Proc. London Math. Soc. (3)*, 25:75–95, 1972. 2

[AMY18] Jim Agler, John E. McCarthy, and N. J. Young. Non-commutative manifolds, the free square root and symmetric functions in two non-commuting variables. *Trans. London Math. Soc.*, 5(1):132–183, 2018. 3

[AY14] Jim Agler and Nicholas J. Young. Symmetric functions of two noncommuting variables. *J. Funct. Anal.*, 266(9):5709–5732, 2014. 3

[AY17] Jim Agler and Nicholas J. Young. Realization of functions on the symmetrized bidisc. *J. Math. Anal. Appl.*, 453(1):227–240, 2017. 2

[BGM05] Joseph A. Ball, Gilbert Groenewald, and Tanit Malakorn. Structured noncommutative multidimensional linear systems. *SIAM J. Control Optim.*, 44(4):1474–1528, 2005. 2, 4, 7

[BGM06] Joseph A. Ball, Gilbert Groenewald, and Tanit Malakorn. Conservative structured noncommutative multidimensional linear systems. In *The state space method generalizations and applications*, volume 161 of *Oper. Theory Adv. Appl.*, pages 179–223. Birkhäuser, Basel, 2006. 4

[BR11] Jean Berstel and Christophe Reutenauer. *Noncommutative rational series with applications*, volume 137 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2011. 2, 7

[Bro98] Ludwig Broecker. On symmetric semialgebraic sets and orbit spaces. In *Singularities Symposium—Łojasiewicz 70 (Kraków, 1996; Warsaw, 1996)*, volume 44 of *Banach Center Publ.*, pages 37–50. Polish Acad. Sci. Inst. Math., Warsaw, 1998. 13

[BRRZ08] Nantel Bergeron, Christophe Reutenauer, Mercedes Rosas, and Mike Zabrocki. Invariants and coinvariants of the symmetric groups in noncommuting variables. *Canad. J. Math.*, 60(2):266–296, 2008. 3

[CHHK15] Huah Chu, Akinari Hoshi, Shou-Jen Hu, and Ming-chang Kang. Noether's problem for groups of order 243. *J. Algebra*, 442:233–259, 2015. 2

[CHKK10] Huah Chu, Shou-Jen Hu, Ming-chang Kang, and Boris E. Kunyavskii. Noether's problem and the unramified Brauer group for groups of order 64. *Int. Math. Res. Not. IMRN*, (12):2329–2366, 2010. 2

[CKS09] Jaka Cimprič, Salma Kuhlmann, and Claus Scheiderer. Sums of squares and moment problems in equivariant situations. *Trans. Amer. Math. Soc.*, 361(2):735–765, 2009. 13

[Coh95] Paul Moritz Cohn. *Skew Fields: Theory of General Division Rings*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1995. 11

[Coh06] Paul Moritz Cohn. *Free ideal rings and localization in general rings*, volume 3 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006. 2, 3, 7

[CPTD18] David Cushing, James E. Pascoe, and Ryan Tully-Doyle. Free functions with symmetry. *Math. Z.*, 289(3-4):837–857, 2018. 3, 9, 10

[CTS07] 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

[DK15] 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. 2

[GKL+95] Israel M. Gelfand, Daniel Krob, Alain Lascoux, Bernard Leclerc, Vladimir S. Retakh, and Jean-Yves Thibon. Noncommutative symmetric functions. *Adv. Math.*, 112(2):218–348, 1995. 3

[GM85] Jessy W. Grizzle and Steven I. Marcus. The structure of nonlinear control systems possessing symmetries. *IEEE Trans. Automat. Control*, 30(3):248–258, 1985. 2

[GR08] Bruce Gilligan and Guy J. Roos, editors. *Symmetries in complex analysis*, volume 468 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 2008. Lectures from the Workshop on Several Complex Variables, Analysis on Complex Lie Groups and Homogeneous Spaces held at Zhejiang University, Hangzhou, October 17–29, 2005. 2

[HM12] J. William Helton and Scott McCullough. Every convex free basic semi-algebraic set has an LMI representation. *Ann. of Math. (2)*, 176(2):979–1013, 2012. 16

[HMV06] J. William Helton, Scott A. McCullough, and Victor Vinnikov. Noncommutative convexity arises from linear matrix inequalities. *J. Funct. Anal.*, 240(1):105–191, 2006. 2

[Isa76] I. Martin Isaacs. *Character theory of finite groups*. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976. Pure and Applied Mathematics, No. 69. 6, 12

[JS] Urban Jezernik and Jonatan Sánchez. Irrationality of generic quotient varieties via Bogomolov multipliers. *preprint*, arXiv:1811.01851. 2

[KPV17] Igor Klep, James Eldred Pascoe, and Jurij Volčič. Regular and positive noncommutative rational functions. *J. Lond. Math. Soc. (2)*, 95(2):613–632, 2017. 15

[Kra84] Hanspeter Kraft. *Geometrische Methoden in der Invariantentheorie*. Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig, 1984. 2

[KVV12] Dmitry S. Kaliuzhnyi-Verbovetskyi and Victor Vinnikov. Noncommutative rational functions, their difference-differential calculus and realizations. *Multidimens. Syst. Signal Process.*, 23(1-2):49–77, 2012. 2, 7

[Kwa95] Huibert Kwakernaak. Symmetries in control system design. In *Trends in control (Rome, 1995)*, pages 17–51. Springer, Berlin, 1995. 2

[Lew74] Jacques Lewin. Fields of fractions for group algebras of free groups. *Trans. Amer. Math. Soc.*, 192:339–346, 1974. 3, 10

[Lin00] Peter A. Linnell. A rationality criterion for unbounded operators. *J. Funct. Anal.*, 171(1):115–123, 2000. 10

[LS01] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition. 10

[Mor12] Primož Moravec. Unramified Brauer groups of finite and infinite groups. *Amer. J. Math.*, 134(6):1679–1704, 2012. 2

[Pas18] James E. Pascoe. Positivstellensätze for noncommutative rational expressions. *Proc. Amer. Math. Soc.*, 146(3):933–937, 2018. 16, 18

[Pey08] Emmanuel Peyre. Unramified cohomology of degree 3 and Noether's problem. *Invent. Math.*, 171(1):191–225, 2008. 2

[PS85] Claudio Procesi and Gerald Schwarz. Inequalities defining orbit spaces. *Invent. Math.*, 81(3):539–554, 1985. 13

[Rie16] Cordian Riener. Symmetric semi-algebraic sets and non-negativity of symmetric polynomials. *J. Pure Appl. Algebra*, 220(8):2809–2815, 2016. 13

[RS06] Mercedes H. Rosas and Bruce E. Sagan. Symmetric functions in noncommuting variables. *Trans. Amer. Math. Soc.*, 358(1):215–232, 2006. 3

[Rud90] Walter Rudin. *Fourier analysis on groups*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1990. Reprint of the 1962 original, A Wiley-Interscience Publication. 5

[Sal84] David J. Saltman. Noether's problem over an algebraically closed field. *Invent. Math.*, 77(1):71–84, 1984. 2

[Sat14] Ichirô Satake. *Algebraic structures of symmetric domains*. Princeton University Press, 2014. 2

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. 5

[Stu08] Bernd Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, second edition, 2008. 2

[vdS87] A. J. van der Schaft. Symmetries in optimal control. *SIAM J. Control Optim.*, 25(2):245–259, 1987. 2

[Vol18] Jurij Volčič. Matrix coefficient realization theory of noncommutative rational functions. *J. Algebra*, 499:397–437, 2018. 2

Igor Klep, Department of Mathematics, Faculty of Mathematics and Physics, University of Ljubljana, Slovenia
E-mail address: igor.klep@fmf.uni-lj.si

James E. Pascoe, Department of Mathematics, University of Florida, USA
E-mail address: pascoej@ufl.edu

Gregor Podlogar, Institute of Mathematics, Physics and Mechanics, Ljubljana, Slovenia
E-mail address: gregor.podlogar@imfm.si

Jurij Volčič, Department of Mathematics, Texas A&M University, USA
E-mail address: volcic@math.tamu.edu