

INVARIANTS OF FINITE GROUPS ACTING ON (FREE) SKEW FIELDS

HARM DERKSEN* AND JURIJ VOLČIČ†

ABSTRACT. Let M be a finitely generated skew field over a ground field $\mathbb{k}$, and let G be a finite group of $\mathbb{k}$ -linear automorphisms of M . This paper investigates finite generation of the skew subfield M^G of G -invariants in M , and relations between the generators. The first main result shows that M^G is finitely generated. Stronger conclusions hold when M is a free skew field, i.e., the universal skew field of fractions of a free algebra. The second main result is the solution of the free Noether problem for non-modular linear group actions: if G acts linearly on the free skew field M on m generators and $\text{char } \mathbb{k}$ does not divide $|G|$, then M^G is the free skew field on $|G|(m - 1) + 1$ generators. In contrast, a nonlinear action of $\mathbb{Z}_2$ on the free skew field M on two generators is presented such that $M^{\mathbb{Z}_2}$ is not a free skew field, resolving the free Lüroth problem. This action also exposes a non-scalar element of M whose centralizer is not a rational field, refuting a conjecture of P. M. Cohn from 1978.

CONTENTS

1. Introduction	2
2. Preliminaries	3
3. Finite skew field extensions	5
3.1. General finite generation	6
3.2. Linear group actions	8
4. Skew subfields of free skew fields	9
4.1. Fundamental relations	9
4.2. Invariants in free skew fields	11
4.3. Linear group actions on free skew fields	14
5. Non-free invariant skew subfields of a free skew field	17
5.1. Free de Jonquières involutions	17
5.2. Centralizers in free skew fields	21
6. Algorithms	22
References	25

Date: December 2, 2025.

2020 Mathematics Subject Classification. 16W22, 16S15, 14E08, 16K40.

Key words and phrases. Invariant skew subfield, free skew field, free Noether's problem, free Lüroth's problem, finite skew field extension.

*Partially supported by NSF grant DMS-2147769 and a Simons Foundation Fellowship.

†Partially supported by NSF grant DMS-2348720.

1. INTRODUCTION

Invariant theory studies group actions on algebraic varieties in terms of functions on them [PV94, O99, DK02]. Its classical problems focus on identifying generators and relations for polynomial and rational invariants of a group acting on an affine space. In particular, given a finite group acting on a field of multivariate rational functions, Noether’s problem asks whether the invariant subfield is itself rational [N17, S69, S83]. Emmy Noether originally considered permutation actions, but the problem has also been studied for linear and non-linear actions of finite groups. Negative answers to this question in particular resolved Lüroth’s problem on existence of non-rational subfields in a rational field [CG72, AM72, S84]. These developments inspired analogous problems in noncommutative rings, such as the Noether problem for rings of differential operators [AD06, FS20].

This paper investigates rational invariants in freely noncommutative variables (i.e., not satisfying any relations). Let $\mathbb{k}$ be a ground field, and let G be a finite group of automorphisms acting on the free algebra of noncommutative polynomials $\mathbb{k}\langle x_1, \dots, x_m \rangle$. The first structural result about the subalgebra of G -invariants $\mathbb{k}\langle x_1, \dots, x_m \rangle^G$ when G is the full symmetric group permuting the variables x_j dates back to [W36]. In general, when G acts linearly on $x_1, \dots, x_m$, the algebra $\mathbb{k}\langle x_1, \dots, x_m \rangle^G$ is free on infinitely many generators, unless G simply scales $x_1, \dots, x_m$ by the same root of unity, in which case it is free and finitely generated [DF82, K84]. Although this result conclusively describes the ring structure of noncommutative polynomial invariants, several further advances were made on their combinatorial [GKLLRT95, RS06] and analytic aspects [AY14, CPT-D18].

In contrast, noncommutative rational invariants have been less studied. The free algebra $\mathbb{k}\langle x_1, \dots, x_m \rangle$ admits the universal skew field of fractions $\mathbb{k}\langle\!\langle x_1, \dots, x_m \rangle\!\rangle$, also called the *free skew field* on m generators [A66]. Beyond its universal role among division rings [C95, S85^b], the free skew field appears in automata theory [BR11], control systems [BGM05] and computational complexity [HW14, GGOW16]. Furthermore, its elements can be viewed as noncommutative rational functions in several matrix variables [K-VV12]; this analytic perspective connects the free skew field to free analysis [K-VV14, AMY18] and free probability [HMS18, CMMPY24].

If a finite group G acts on $\mathbb{k}\langle x_1, \dots, x_m \rangle$, its action naturally extends to $\mathbb{k}\langle\!\langle x_1, \dots, x_m \rangle\!\rangle$. Although $\mathbb{k}\langle x_1, \dots, x_m \rangle^G$ is almost never finitely generated as an algebra as explained above, it was observed in [AMY18, CPT-D18] that when G is abelian and acts linearly, there are *finitely* many G -invariant noncommutative rational functions such that every element of $\mathbb{k}\langle x_1, \dots, x_m \rangle^G$ is a *rational* function in them. In the first systematic study of the structure of noncommutative rational invariants, [KPPV20] considered linear actions of finite solvable groups G on $\mathbb{k}\langle\!\langle x_1, \dots, x_m \rangle\!\rangle$. It was shown that $\mathbb{k}\langle\!\langle x_1, \dots, x_m \rangle\!\rangle^G$ is a finitely generated skew field in this case, and is free on $|G|(m-1) + 1$ generators for certain linear actions of G satisfying a cohomological condition [P23] (which is always satisfied for finite abelian groups).

This paper explores finite generation and freeness of $\mathbb{k}\langle\!\langle x_1, \dots, x_m \rangle\!\rangle^G$ for a general action of a finite group G . Our methods are independent of the preceding results mentioned above, and arise from finite extensions of skew fields. In fact, the scope of the first main result

(Theorem 3.3 below) on finite generation extends well beyond free skew fields. If $L \subseteq M$ are skew fields, then M is both a free left L -module and a free right L -module. The left L -dimension (resp. right L -dimension) of M is the number of free generators of M as a left (resp. right) L -module. The left and right dimension do not have to be the same, and one could even be infinite while the other is finite (see [C95, Section 5.9], [C77, Chapter 5] or [S85^a]).

Theorem 3.3. *Let $L \subseteq M$ be skew fields containing a field $\mathbb{k}$. If M is generated by m elements over $\mathbb{k}$ and the left or right L -dimension of M is d , then L is generated by at most $d^2(m-1) + d$ elements over $\mathbb{k}$.*

If $L = M^G$ for a finite group $|G|$, then M has (left or right) dimension at most $|G|$ over L , so Theorem 3.3 applies to invariant skew subfields. When M is a finitely generated free skew field, we obtain the generators of L in a constructive manner, as well as a finite set of relations between them that are fundamental in a certain sense (Proposition 4.1). Furthermore, these relations can be resolved if the action of G is linear; that is, we obtain an affirmative answer to the free Noether problem in this case.

Theorem 4.8. *If G is a finite group of linear automorphisms on $\mathbb{k}\langle x_1, \dots, x_m \rangle$ and $\text{char } \mathbb{k}$ does not divide $|G|$, then $\mathbb{k}\langle x_1, \dots, x_m \rangle^G$ is the free skew field on $|G|(m-1) + 1$ generators.*

At this point, it is worth mentioning that to date it has been unknown whether every skew subfield of a free skew field is free [S85^b, pages 183 and 206]. We show that this free Lüroth problem has a negative resolution by demonstrating that the conclusion of Theorem 4.8 fails for nonlinear group actions. More concretely, Theorem 5.2 presents an action of $\mathbb{Z}_2$ on $\mathbb{k}\langle x, y \rangle$ such that $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ is not free.

A special case of the free Lüroth problem is related to the rationality of centralizers in free skew fields. In [C78, Conjecture], Cohn conjectured that the centralizer of a non-scalar element in a free skew field is isomorphic to $\mathbb{k}(t)$; see also [S85^b, page 183], [L02, page 329] and [B-KRZ23, Problem 4.1] for other reappearances. However, our example of a non-free skew subfield of $\mathbb{k}\langle x, y \rangle$ leads to a counter-example to this conjecture.

Corollary 5.3. *Let $\text{char } \mathbb{k} \neq 2$. There exists $r \in \mathbb{k}\langle x, y \rangle \setminus \mathbb{k}$ with a non-rational centralizer.*

2. PRELIMINARIES

Throughout this paper let $\mathbb{k}$ be a fixed ground field. All rings and skew fields are considered to be unital $\mathbb{k}$ -algebras, and homomorphisms between them are unital and $\mathbb{k}$ -linear. Given two subsets A, B of an algebra, let AB denote the span of all products ab for $a \in A$ and $b \in B$. When discussing a group action on an algebra, we mean an action by $\mathbb{k}$ -linear automorphisms (i.e., an action that is compatible with the $\mathbb{k}$ -algebra structure), and we write it using the exponential notation. Given an algebra R and a group G acting on R , let R^G denote the subalgebra of G -invariant elements.

Let $\mathbb{k}\langle x_1, \dots, x_m \rangle$ be the free associative algebra generated by freely noncommuting variables $x_1, \dots, x_m$. We say that $\mathbb{k}\langle x_1, \dots, x_m \rangle$ is free of rank m . Let $\mathbb{k}\langle x_1, \dots, x_m \rangle$ denote the universal skew field of fractions of $\mathbb{k}\langle x_1, \dots, x_m \rangle$; see [C95, Corollary 4.5.9

and Theorem 5.4.1] or [C06, Corollaries 2.5.2 and 7.5.14] for uniqueness and universality. Informally, $\mathbb{k}\langle x_1, \dots, x_m \rangle$ is a skew field where the only relations between $x_1, \dots, x_m$ are consequences of division ring axioms, such as

$$(1) \quad (x_1 - x_2 x_4^{-1} x_3)^{-1} = x_1^{-1} + x_1^{-1} x_2 (x_4 - x_3 x_1^{-1} x_2)^{-1} x_3 x_1^{-1}.$$

Therefore, $\mathbb{k}\langle x_1, \dots, x_m \rangle$ is called the *free skew field* of rank m . For the reader's convenience, we collect some facts about free skew fields.

- (a) Consider the set of formal rational expressions in $x_1, \dots, x_m$ and scalars from $\mathbb{k}$ that are well-defined at some m -tuple of square matrices over $\mathbb{k}$. Two such expressions are equivalent if their evaluations agree on all matrix tuples over $\mathbb{k}$ at which both expressions are well-defined. By [A66, Theorem 16 and Section II.1] or [K-VV12, Section 2], one can view elements of $\mathbb{k}\langle x_1, \dots, x_m \rangle$ as equivalence classes of such formal rational expressions.
- (b) By [L74], another way to realize $\mathbb{k}\langle x_1, \dots, x_m \rangle$ is as the skew subfield generated by $\mathbb{k}\langle x_1, \dots, x_m \rangle$ within the skew field of Malcev-Neumann series over the free group generated by $x_1, \dots, x_m$.
- (c) A square matrix A over $\mathbb{k}\langle x_1, \dots, x_m \rangle$ is full if in any factorization $A = BC$ over $\mathbb{k}\langle x_1, \dots, x_m \rangle$, B has at least as many columns as A . By [C06, Corollary 7.5.14], a square matrix over $\mathbb{k}\langle x_1, \dots, x_m \rangle$ is invertible over $\mathbb{k}\langle x_1, \dots, x_m \rangle$ if and only if it is full.
- (d) By [C95, Theorem 5.8.11 and Corollary 5.8.14], free algebras and free skew fields are determined by their ranks up to isomorphism.

Let $a_1, \dots, a_m$ be elements of a skew field D , and let $r \in \mathbb{k}\langle x_1, \dots, x_m \rangle$. If a formal rational expression representing r is well-defined at $(a_1, \dots, a_m)$, in the sense that all nested inverses in the expression exist in D when the x_i are replaced by the a_i , then we say that $(a_1, \dots, a_m)$ is in the domain of r . If two expressions representing r (e.g., as in (1)) are well-defined at $(a_1, \dots, a_m)$, their evaluations at it coincide [C95, Section 7.3], and are denoted $r(a_1, \dots, a_m) \in D$. In particular, whenever referring to the value $r(a_1, \dots, a_m)$, we tacitly assume that $(a_1, \dots, a_m)$ is in the domain of r . More generally, if A is a matrix over $\mathbb{k}\langle x_1, \dots, x_m \rangle$ such that $(a_1, \dots, a_m)$ lies in the domains of all its entries, then $A(a_1, \dots, a_m)$ is a well-defined matrix over D .

Since (unital) homomorphisms between skew fields are necessarily embeddings, we also use more general maps between them. Let D and E be skew fields. A *local homomorphism* from D to E [C95, Section 4.1] is a unital homomorphism from a subring D_0 of D to E that maps non-invertible elements in D_0 to zero.

Lemma 2.1 ([C95, Theorem 4.4.1]). *Let D be a skew field generated by $a_1, \dots, a_m$, and let E be a skew field containing $b_1, \dots, b_m$. The following are equivalent:*

- (1) *there exists a local homomorphism from D to E such that $a_i \mapsto b_i$ for $i = 1, \dots, m$;*
- (2) *for every square matrix A over $\mathbb{k}\langle x_1, \dots, x_m \rangle$, if $A(b_1, \dots, b_m)$ is invertible over E then $A(a_1, \dots, a_m)$ is invertible over D .*

The universal property of $\mathbb{k}\langle x_1, \dots, x_m \rangle$ then states that for every skew field E with elements $b_1, \dots, b_m$, there is a local homomorphism from $\mathbb{k}\langle x_1, \dots, x_m \rangle$ to E mapping x_i to b_i ;

equivalently, invertibility of $A(b_1, \dots, b_m)$ over E (where A is a matrix over $\mathbb{k}\langle x_1, \dots, x_m \rangle$) implies invertibility of $A(x_1, \dots, x_m)$ over $\mathbb{k}\langle x_1, \dots, x_m \rangle$. This universal property is a consequence of the property of full matrices in item (c) above.

3. FINITE SKEW FIELD EXTENSIONS

In this section we establish finite generation of skew fields whose finite extensions are finitely generated (Theorem 3.3). For a comprehensive study of skew field extensions and the corresponding Galois theory, see [C95, Section 3] and [D95].

Let $L \subseteq M$ be skew fields. To emphasize the left L -module and right L -module structure of M , we write ${}_L M$ respectively M_L . Then $\text{End}(M)$, $\text{End}({}_L M)$ and $\text{End}(M_L)$ are the algebras of $\mathbb{k}$ -vector space endomorphisms, left L -module endomorphisms and right L -module endomorphisms respectively. Similarly, $\dim M$, $\dim {}_L M$, $\dim M_L$ are the dimensions of M as a $\mathbb{k}$ -vector space, left L -module and right L -module respectively. In general, $\dim M_L \neq \dim {}_L M$ (see [C95, Section 5.9] for an example). We start with a technical lemma.

Lemma 3.1. *Let $A_1, \dots, A_r, B$ be modules over a ring, and assume $A_1, \dots, A_r$ are simple. Then, there exists a subset $I \subseteq \{1, \dots, r\}$ such that $B + \sum_{i=1}^r A_i = B \oplus \bigoplus_{i \in I} A_i$.*

Proof. We prove the statement by induction on i . The case $i = 0$ is obvious. If $A_r \cap B = \{0\}$ then we have $B + \sum_{i=1}^r A_i = A_r \oplus B + \sum_{i=1}^{r-1} A_i$ and we use induction. Otherwise, $A_r \cap B = A_r$ because A_r is simple. In this case, $A_r \subseteq B$ and we have $B + \sum_{i=1}^r A_i = B + \sum_{i=1}^{r-1} A_i$. Again, the lemma follows by induction. $\square$

Suppose that L and M are skew fields with $L \subseteq M$, and V is an m -dimensional $\mathbb{k}$ -subspace of M that generates M as a skew field over $\mathbb{k}$. If we set $V_+ = \mathbb{k} + V$, then $\mathbb{k}\langle V \rangle = \bigcup_{i=0}^{\infty} V_+^i$ is the associative algebra generated by V . In the case where $\dim M_L$ is finite, the proposition below constructs a $\mathbb{k}$ -subspace $W \subseteq \mathbb{k}\langle V \rangle$ such that $WL = M$ and $\dim W = \dim M_L$. This means that any $\mathbb{k}$ -basis of W is a basis of M as a right L -module. The subspace W is constructed inductively and greedily as a direct sum $W = W_1 \oplus W_2 \oplus \dots$ such that $W \cap V_+^k = W_1 \oplus W_2 \oplus \dots \oplus W_k$ contains an L -basis of $V_+^k L$ for all k . This proposition will be useful for finding small generating sets.

Proposition 3.2. *Let $L \subseteq M$ be skew fields. Suppose an m -dimensional $\mathbb{k}$ -subspace $V \subseteq M$ generates the skew field M over $\mathbb{k}$, and $\dim M_L$ is finite. There exists a $\mathbb{k}$ -subspace W of M with the following properties:*

- (1) $WL = M$ and $\dim W = \dim M_L$;
- (2) $\mathbb{k} \subseteq W \subseteq \mathbb{k} + VW$.

Proof. Denote $V_+ = V + \mathbb{k} \subseteq M$. Below we use the conventions $V^0 = V_+^0 = \mathbb{k}$. We inductively construct $\mathbb{k}$ -subspaces $W_i \subseteq M$ for $i \geq 0$ such that $W_0 = \mathbb{k}$ and the following properties hold:

- (1) $\dim W_i = \dim(W_i L)_L$ for $i \geq 0$;
- (2) $V_+^i L + VW_i L = V_+^{i+1} L$ for $i \geq 0$;
- (3) $W_i \subseteq VW_{i-1} \subseteq V^i$ for $i \geq 1$;
- (4) $V_+^{i-1} L \oplus W_i L = V_+^i L$ for $i \geq 1$.

It is clear that (1) and (2) hold for $i = 0$. Suppose that $i \geq 0$ and we have already constructed the spaces $W_0, W_1, \dots, W_i$. We will construct W_{i+1} with properties (1)–(4).

Choose a basis $a_1, \dots, a_r$ in VW_i and let $A_i = a_i L$. Then we have $V_+^i L + \sum_{j=1}^r A_j = V_+^{i+1} L$. By Lemma 3.1, there exists a subset $I \subseteq \{1, \dots, r\}$ such that $V_+^i L \oplus \bigoplus_{j \in I} A_j = V_+^{i+1} L$. Let W_{i+1} be the $\mathbb{k}$ -span of a_j for $j \in I$. Then, we have $V_+^i L \oplus W_{i+1} L = V_+^{i+1} L$ and $\dim W_{i+1} = |I| = \dim(W_{i+1} L)_L$. Thus, W_{i+1} has properties (1), (3) and (4). By (3), we have $W_{i+1} \subseteq V_+^{i+1}$, so

$$\begin{aligned} V_+^{i+1} L + VW_{i+1} L &= (V_+^{i+1} + W_{i+1}) L + VW_{i+1} L = V_+^{i+1} L + (\mathbb{k} + V) W_{i+1} L = \\ &= V_+^{i+1} L + V_+ W_{i+1} L = V_+ (V_+^i L \oplus W_{i+1} L) = V_+ V_+^{i+1} L = V_+^{i+2} L. \end{aligned}$$

By induction it is clear that $V_+^j L = \bigoplus_{i=0}^j W_i L$ and

$$\dim M_L \geq \dim(V_+^j L)_L = \sum_{i=0}^j \dim(W_i L)_L = \sum_{i=0}^j \dim W_i = \dim \bigoplus_{i=0}^j W_i.$$

This shows that for some $s \in \mathbb{N}$, we have $0 = W_{s+1} = W_{s+2} = \dots$. Define $W = \bigoplus_{i=0}^s W_i$. Consider the set $N = \{x \in M : xWL \subseteq WL\}$. It is clear that N is a subalgebra of M . If $x \in N$ is nonzero, then left multiplication by x gives an isomorphism between xWL and WL as right L -modules. So $(xWL)_L$ is a right L -submodule of $(WL)_L$ of the same dimension. It follows that $xWL = WL$. But then $x^{-1}WL \subseteq WL$, and so $x^{-1} \in N$. This shows that N is a skew subfield of M . It also contains the space V that generates M , so $N = M$. Now we have $(WL)_L = M_L$ and $\dim W = \sum_{i=0}^s \dim W_i = \sum_{i=0}^s \dim(W_i L)_L = \dim(WL)_L = \dim M_L$. Finally, we have $\mathbb{k} = W_0 \subseteq W = \mathbb{k} + (\sum_{i=1}^s W_i) \subseteq \mathbb{k} + \sum_{i=1}^s VW_{i-1} \subseteq \mathbb{k} + VW$. $\square$

3.1. General finite generation. Our first main result shows that skew fields with finitely generated finite extensions are themselves finitely generated.

Theorem 3.3. *Let $L \subseteq M$ be skew fields. Suppose M is generated by m elements over $\mathbb{k}$, and $d = \dim M_L$ is finite. Then, L is generated over $\mathbb{k}$ by at most $d^2(m-1) + d$ elements.*

Proof. Let V be the $\mathbb{k}$ -linear span of the m generators of M over $\mathbb{k}$. We use Proposition 3.2 to construct a subspace W of M with $WL = M$, $\dim W = \dim M_L = d$ and $\mathbb{k} \subseteq W \subseteq \mathbb{k} + VW$. As right L -modules we have $M_L = (WL)_L \cong (W \otimes L)_L$. This gives an isomorphism $\text{End}(M_L) \cong \text{End}((W \otimes L)_L) = \text{End}(W) \otimes L$. For $x \in M$, let $\lambda_x \in \text{End}(M_L)$ be left multiplication by x . Define $\rho : M \rightarrow \text{End}(W) \otimes L$ by $\rho(x) = \lambda_x$. It is clear that ρ is a $\mathbb{k}$ -algebra homomorphism and ρ is injective because M is a skew field and $\rho(1) \neq 0$.

We have isomorphisms

$$\text{Hom}(M, \text{End}(W) \otimes L) \cong \text{Hom}(M \otimes W, W \otimes L) \cong \text{Hom}(M \otimes W \otimes W^*, L).$$

Thus, we can view ρ in 3 different ways, namely

$$\begin{aligned} \rho : M &\rightarrow \text{End}(W) \otimes L, \\ \rho' : M \otimes W &\rightarrow W \otimes L \\ \rho'' : M \otimes W \otimes W^* &\rightarrow L. \end{aligned}$$

Since $W \subseteq \mathbb{k} + VW$, the subspace $W \cap VW$ has dimension at least $d - 1$. Note that $(VW \cap W) \otimes \mathbb{k}$ is contained in $\rho'(V \otimes W)$. So there exists a subspace $T \subseteq V \otimes W$ with $\dim T = \dim(W \cap VW)$ for which $\rho'(T) = (W \cap VW) \otimes \mathbb{k}$. This means that $\rho''(T \otimes W^*) = \mathbb{k}$. Let $T^\perp$ be a complement of T in $V \otimes W$; its dimension is at most $dm - (d - 1)$. Let $Z = \rho''(T^\perp \otimes W^*)$. Then,

$$\dim Z \leq \dim T^\perp \otimes W^* \leq (dm - d + 1)d = d^2(m - 1) + d.$$

We have $\rho'(V \otimes W) = \rho'(T \oplus T^\perp) = \rho'(T) + \rho'(T^\perp) \subseteq W \otimes \mathbb{k} + W \otimes Z$ and $\rho(V) \subseteq \text{End}(W) \otimes (\mathbb{k} + Z)$. Since $\rho(V)$ is contained in the algebra $\text{End}(W) \otimes \mathbb{k}(Z)$ and V generates M , we get $\rho(M) \subseteq \text{End}(W) \otimes \mathbb{k}(Z)$. If $x \in L$, then we have $x = \lambda_x(1) = \rho(x)(1 \otimes 1) \in \mathbb{k}(Z)$ because $\rho(x) \in \text{End}(W) \otimes \mathbb{k}(Z)$. Since $L \subseteq \mathbb{k}(Z)$ and Z is contained in L , we have $L = \mathbb{k}(Z)$. This shows that L is generated by at most $d^2(m - 1) + d$ elements. $\square$

Corollary 3.4. *Suppose M is generated by m elements over $\mathbb{k}$, and $d = \dim_L M$ is finite. Then, L is generated over $\mathbb{k}$ by at most $d^2(m - 1) + d$ elements.*

Proof. Taking the opposite rings, we have $\mathbb{k} \subseteq L^{\text{op}} \subseteq M^{\text{op}}$ and $\dim M_{L^{\text{op}}}^{\text{op}} = \dim_L M = d < \infty$. By the previous theorem, M^{op} is generated by at most $d^2(m - 1) + d$ generators, so the same is true for M . $\square$

A natural source of finite skew field extensions are invariants of finite groups. To see this, we first record a weak noncommutative version of Dedekind's lemma (for a different generalization, see [D95, Theorem 4] or [C95, Theorem 3.3.2]).

Lemma 3.5. *Let $\varphi_1, \dots, \varphi_d$ be distinct automorphisms of a skew field M , and let L be their fixed skew subfield in M . Then, $\varphi_1, \dots, \varphi_d$ are L -linearly independent in $\text{End}(M_L)$.*

Proof. Let $W = \text{span}_L\{\varphi_1, \dots, \varphi_d\} \subseteq \text{End}(M_L)$. It suffices to find $x_1, \dots, x_d \in M$ such that $W_k = \{\varphi \in W : \varphi(x_1) = \dots = \varphi(x_k) = 0\}$ for $k = 1, \dots, d$ has dimension $d - k$ as a right L -module ($k = d$ then implies the desired statement). We find the x_j by induction on k . For $k = 1$ take any nonzero $x_1 \in M$. Now suppose that $\dim(W_{k-1})_L = d - (k - 1)$. Choose a nonzero $\psi \in W_{k-1}$; its kernel is a proper L -submodule of M , so there exists $x_k \in M \setminus \ker \psi$. Then, $W_k = \{\varphi \in W_{k-1} : \varphi(x_k) = 0\}$ has dimension $d - k$ over L . $\square$

For a finite group G , we denote the group algebra of G over a skew field L by $L[G]$. Suppose a finite group G acts on a skew field M by automorphisms. If we apply an automorphism $g \in G$ to an element $y \in M$ then we may write y^g for the result instead of $g(y)$ to ease the notation. The set M^G of all elements of M that are fixed by the group is again a skew field.

For later refinements, we require the following noncommutative analogs of Artin's theorem and the normal basis theorem. We say that a group G of automorphisms on a skew field M consists of outer automorphisms if the identity is the only inner automorphism of M in G .

Lemma 3.6. *Let G be a finite group of automorphisms on a skew field M , and $L = M^G$.*

- (1) $\dim M_L, \dim_L M \leq |G|$.
- (2) *If G is a group of outer automorphisms, then $M \cong \mathbb{k}[G] \otimes L$ as an L -module and a G -space, and in particular $\dim M_L = \dim_L M = |G|$.*

(3) If M is a free skew field, then G is a group of outer automorphisms.

Proof. (1) By Lemma 3.5, the automorphisms $g \in G$ are L -independent. In particular, their sum is a nonzero endomorphism of M , so there exists $y \in M$ such that $\bar{y} = \sum_{g \in G} y^g \neq 0$. Let $d = |G|$, and let $f_1, \dots, f_{d+1} \in M$ be arbitrary. The set of functions from G to M is a free right M -module of rank d . Define functions $F_i : G \rightarrow M$ by $F_i(g) = f_i^g$. Then $F_1, \dots, F_{d+1}$ are dependent. After reordering we may assume that $F_{d+1} = \sum_{i=1}^d F_i a_i$ for some $a_1, a_2, \dots, a_\ell \in M$. That is, $f_{d+1}^g y = \sum_{i=1}^d f_i^g a_i y$ for every $g \in G$. Therefore $f_{d+1} y^{g^{-1}} = \sum_{i=1}^\ell f_i(a_i y)^{g^{-1}}$ for all $g \in G$, and so

$$f_{d+1} \bar{y} = \sum_{i=1}^d f_i \bar{a}_i, \quad \text{where} \quad \bar{a}_i = \sum_{g \in G} (a_i y)^g \in L.$$

Since $\bar{y} \in L$ is nonzero, we conclude that $f_1, \dots, f_{d+1}$ are linearly dependent over L . Hence, $\dim M_L \leq d$. The inequality $\dim_L M \leq d$ is proved analogously.

(2) This is a consequence of the normal basis theorem for finite groups of outer automorphisms [D95, Section 4.1], which states that there is $x \in M$ such that $\{x^g : g \in G\}$ has size $|G|$ and is a basis of M as a right (or left) L -module. Such an x then gives rise to an isomorphism $\mathbb{k}[G] \otimes L \rightarrow M$ given by $g \otimes \ell \mapsto x^g \ell$.

(3) By [C95, Exercise 6.2.4], no element in $M \setminus \mathbb{k}$ is algebraic over $\mathbb{k}$. Also, M is commutative if its rank is 1, and otherwise has center equal to $\mathbb{k}$ by [C06, Corollary 7.9.7]. Consequently, an inner automorphism of M is either the identity or has infinite order. Therefore, the identity is the only inner automorphism of M in G . $\square$

In general, the inequality in Lemma 3.6(1) is strict (see the example after [C95, Theorem 3.3.7]).

3.2. Linear group actions. In this section we will assume that G is a finite group such that $\text{char}(\mathbb{k}) \nmid |G|$. This implies that G is linearly reductive. We summarize some consequences of this. Whenever X is a subrepresentation of a finite dimensional representation Y , it has a G -stable complement $X^\perp$, so $Y = X \oplus X^\perp$. Every representation of G is a direct sum of irreducible representations. A linear map between representations $\phi : X \rightarrow Y$ is G -equivariant if $\phi(x^g) = \phi(x)^g$ for all $x \in X$ and $g \in G$. In that case we have $\phi(X^G) = Y^G$.

We can strengthen Theorem 3.3 for skew subfields of invariants for finite linear groups. We start by refining Proposition 3.2.

Proposition 3.7. *Let G be a finite outer group of automorphisms on a skew field M , and $\text{char } \mathbb{k} \nmid |G|$. Suppose there is an m -dimensional G -stable $\mathbb{k}$ -subspace of M that generates M over $\mathbb{k}$. Then, there exists a G -stable $\mathbb{k}$ -subspace W of the subalgebra in M generated by V , with the following properties:*

- (1) $WM^G = M$ and $\dim W = \dim M_{M^G}$;
- (2) $\mathbb{k} \subseteq W \subseteq \mathbb{k} + VW$;
- (3) $W^\star \cong \mathbb{k}[G]$ as G -spaces.

Proof. Let $L = M^G$; by Lemma 3.6 we have $\dim M_L = |G|$. Let $L[G]$ be the group algebra of G over L , where elements of L commute with group elements in G . Since $\text{char } \mathbb{k} \nmid |G|$, the group G is linearly reductive and $L[G]$ is semisimple.

We follow the proof of Proposition 3.2 to construct a space W with $WL = M$, $\dim W = \dim M_L$ and $\mathbb{k} \subseteq W \subseteq \mathbb{k} + VW$. However, we claim that we can choose W such that it is stable under the action of G . Since G is linearly reductive, any G -stable subspace in a representation of G over $\mathbb{k}$ has a complement. In the proof of Proposition 3.2, we construct subspaces W_i for $i \geq 0$. We claim that we can choose each W_i to be G -stable. The space $W_0 = \mathbb{k}$ it is clearly G -stable. By induction we may assume that W_i has been constructed, is G -stable and $V_+^i L + VW_i L = V_+^{i+1} L$. Since VW_i is also G -stable, we can write $VW_i = A_1 \oplus \cdots \oplus A_r$ where $A_1, \dots, A_r$ are irreducible representations of G . Now $A_i L \cong A_i \otimes L$ is a simple right $L[G]$ -module for all i . By Lemma 3.1, we can take some subset $I \subseteq \{1, \dots, r\}$ such that $V_+^i L \oplus \bigoplus_{j \in I} A_j L = V_+^{i+1} L$. Now take $W_{i+1} = \bigoplus_{j \in I} A_j$. Then we have $V_+^i L \oplus W_{i+1} L = V_+^{i+1} L$ and $W_{i+1} L = \bigoplus_{j=1}^r A_j L \cong \bigoplus_{j \in I} A_j \otimes L$, so $\dim(W_{i+1} L)_L = \sum_{j \in I} \dim(A_j \otimes L)_L = \sum_{i \in I} \dim(A_j) = \dim(W_{i+1})$. Now W_{i+1} is G -stable because it is a right $L[G]$ -module.

By the construction, $W = \bigoplus_i W_i$ is a G -stable subspace of the subalgebra in M generated by V , and satisfies (1) and (2) as in Proposition 3.2. Since $W \otimes L \cong M \cong \mathbb{k}[G] \otimes L$ as G -spaces and L -modules by Lemma 3.6, it follows that $W \cong \mathbb{k}[G]$. Therefore, $W^* \cong \mathbb{k}[G]$, and (3) holds. $\square$

Theorem 3.8. *Let G be a finite group of outer automorphisms on a skew field M , and $\text{char } \mathbb{k} \nmid |G|$. If V is an m -dimensional G -stable $\mathbb{k}$ -subspace of M that generates M over $\mathbb{k}$, then M^G is generated by at most $|G|(m-1) + 1$ generators.*

Proof. We follow the proof of Theorem 3.3 with $L = M^G$ by taking the group action into account. Let W be as in Proposition 3.7. Let $d = \dim W = \dim M_L$; by Lemma 3.6 we have $d = |G|$. Let $\rho : M \rightarrow \text{End}(W) \otimes L$, $\rho' : M \otimes W \rightarrow W \otimes L$ and $\rho'' : M \otimes W \otimes W^* \rightarrow L$ be as in the proof of Theorem 3.3. The subspace $W \cap VW$ is G -stable. We can find a G -stable subspace $T \subseteq V \otimes W$ with $\rho'(T) = (W \cap VW) \otimes \mathbb{k}$. We can also choose a G -stable complement $T^\perp$ of T in $V \otimes W$. Since G acts by automorphisms on M and trivially on $L = M^G$, the map $\rho'' : V \otimes W \otimes W^* \rightarrow L$ is G -invariant. In particular, we have $Z = Z^G = \rho''(T^\perp \otimes W^*)^G = \rho''((T^\perp \otimes W^*)^G)$. Since $W^* \cong \mathbb{k}[G]$ and $(U \otimes \mathbb{k}[G])^G \cong U$ for every G -space U , it follows that $\dim Z \leq \dim(T^\perp \otimes W^*)^G = \dim(T^\perp \otimes \mathbb{k}[G])^G = \dim T^\perp \leq md - (d-1)$. $\square$

4. SKEW SUBFIELDS OF FREE SKEW FIELDS

We can enhance the results of Section 3 in the context of free skew fields. Throughout the section let $M = \mathbb{k}\langle x_1, \dots, x_m \rangle$ be the free skew field over $\mathbb{k}$ generated by free variables $x_1, \dots, x_m$.

4.1. Fundamental relations. Let L be a skew subfield of M with $\dim M_L = d$. Let $W \subseteq M$, $\rho : M \rightarrow \text{End}(W) \otimes L$ and $Z \subseteq L$ be as in Proposition 3.2 and the proof of Theorem 3.3. Let us choose a basis of W that starts with 1, and let $X_i \in L^{d \times d}$ be the

matrix representing $\rho(x_i)$ relative to the chosen basis. Then $\mathbb{k}1 + Z$ is the $\mathbb{k}$ -linear span of the entries of $X_1, \dots, X_m$.

Let $z_1, \dots, z_t$ span Z . Then, there exist $d \times d$ matrices $A_{i0}, \dots, A_{it}$ over $\mathbb{k}$ such that

$$(2) \quad X_i = A_{i0} + z_1 A_{i1} + \dots + z_t A_{it}.$$

Let $\mathfrak{z}_1, \dots, \mathfrak{z}_t$ be auxiliary free variables, and denote

$$(3) \quad \mathfrak{X}_i := A_{i0} + \mathfrak{z}_1 A_{i1} + \dots + \mathfrak{z}_t A_{it},$$

viewed as a $d \times d$ matrix over $\mathbb{k}\langle \mathfrak{z}_1, \dots, \mathfrak{z}_t \rangle \subset \mathbb{k}\langle \mathfrak{z}_1, \dots, \mathfrak{z}_t \rangle$. If $z_1, \dots, z_t$ form a basis of Z , the matrices $\mathfrak{X}_i$ are uniquely determined by this basis (which is typically the case one is interested in, but for the sake of a later use we only assume that $z_1, \dots, z_t$ span Z). Using matrices (3), we provide an explicit finite collection of relations for L that are in a certain sense fundamental for L .

Proposition 4.1. *With the notation as above, denote*

$$\begin{aligned} \mathcal{R} = & \left\{ z_j(\mathfrak{X}_1, \dots, \mathfrak{X}_m)_{11} - \mathfrak{z}_j : j = 1, \dots, t \right\} \\ & \cup \left\{ (z_j(\mathfrak{X}_1, \dots, \mathfrak{X}_m)_{\ell 1} : j = 1, \dots, t, \ell = 2, \dots, d) \right\}. \end{aligned}$$

Let D be a skew field generated by $a_1, \dots, a_t$ such that $r(a_1, \dots, a_t) = 0$ for all $r \in \mathcal{R}$. If there is a local homomorphism from D to L such that $a_j \mapsto z_j$ for $j = 1, \dots, t$, then $D \cong L$.

In particular, if $\mathcal{R} = \{0\}$, then L is the free skew field of rank t .

Proof. Note that the first column of $z_j(X_1, \dots, X_m)$ equals $z_j e_1$, where e_1 is the first standard basis vector in $\mathbb{k}^d$. Indeed, ρ is a homomorphism and thus $z_j(\rho(x_1), \dots, \rho(x_m)) = \rho(z_j)$, and $z_j \in L$ as an element of the free L -module $M = WL$ is simply the z_j -multiple of the first basis vector.

Next, we claim that the homomorphism $\phi : \mathbb{k}\langle x_1, \dots, x_m \rangle \rightarrow D^{d \times d}$ defined by $x_i \mapsto \mathfrak{X}_i(a_1, \dots, a_t)$ extends to an embedding $\Phi : M \rightarrow D^{d \times d}$. Since M is the universal skew field of fractions of $\mathbb{k}\langle x_1, \dots, x_m \rangle$, its elements are entries of inverses of matrices over $\mathbb{k}\langle x_1, \dots, x_m \rangle$ by [C95, Theorem 4.2.1]. Thus, it suffices to see the following for a square matrix A over $\mathbb{k}\langle x_1, \dots, x_m \rangle$: if A is invertible over M , then the entry-wise application of ϕ maps it to an invertible matrix over D . Since A is invertible over M and $\rho : M \rightarrow L^{d \times d}$ is an embedding of a skew field, the matrix $A(X_1, \dots, X_m)$ is invertible over L . Consider the matrix $B = A(\mathfrak{X}_1, \dots, \mathfrak{X}_m)$ over $\mathbb{k}\langle \mathfrak{z}_1, \dots, \mathfrak{z}_t \rangle$. Since $B(z_1, \dots, z_t) = A(X_1, \dots, X_m)$ is invertible over L , the matrix $B(a_1, \dots, a_t)$ is invertible over D by Lemma 2.1, as desired.

Finally, consider the restricted homomorphism of $\Phi|_L : L \rightarrow D^{d \times d}$. For every $j = 1, \dots, t$, the first column of $\Phi(z_j)$ equals $a_j e_1$ by the definition of $\mathcal{R}$. Therefore, the map $L \rightarrow D$ given by $u \mapsto \Phi(u)_{11}$ is a surjective homomorphism of skew fields, and thus an isomorphism. $\square$

More generally, the conclusion of Proposition 4.1 holds even if the entries of X_i are not affine in the generators of L , but rational in the generators of L . Note that Proposition 4.1 reduces freeness of generators $z_1, \dots, z_t$ to noncommutative rational identity testing, which can be done efficiently [GGOW16, DM17, IQS18]. In general, freeness translates to checking linear independence over the enveloping algebra $M \otimes M^{\text{op}}$ via universal derivation modules

(see [C95, Section 5.8] or [S85^b, Section 10]); however, this does not evidently yield an effective algorithm for deciding freeness.

4.2. Invariants in free skew fields. Theorem 3.3 and Lemma 3.6 imply the following.

Corollary 4.2. *If G is a finite group of automorphisms on $\mathbb{k}\langle x_1, \dots, x_m \rangle$, then the skew subfield $\mathbb{k}\langle x_1, \dots, x_m \rangle^G$ is generated over $\mathbb{k}$ by at most $|G|^2(m-1) + |G|$ elements.*

Let us further simplify the presentation of generators and their relations from Corollary 4.2. Denote $M = \mathbb{k}\langle x_1, \dots, x_m \rangle$ and $L = M^G$. Let $1 = w_1, w_2, \dots, w_d$ be a basis of the vector space W as in Proposition 3.2; note that $d = |G|$ by Lemma 3.6. If $X_i \in L^{d \times d}$ is the matrix representing $\rho(x_i)$ relative to this basis, then

$$(4) \quad x_i w_j = \sum_{k=1}^d w_k \cdot (X_i)_{kj} \quad \text{for } i = 1, \dots, m, \quad j = 1, \dots, d.$$

Applying an automorphism $g \in G$ to (4) gives

$$(5) \quad x_i^g w_j^g = \sum_{k=1}^d w_k^g \cdot (X_i)_{kj} \quad \text{for all } i, j \text{ and } g \in G.$$

For $i = 1, \dots, m$ let $\mathbf{D}_i$ be the diagonal $d \times d$ matrix indexed by $g \in G$ whose g^{th} diagonal entry equals x_i^g . Consider the $d \times d$ matrix $\mathbf{W} = (w_j^g)_{g,j}$, whose rows are indexed by $g \in G$, and columns are indexed by $j = 1, \dots, d$.

Lemma 4.3. *The matrix $\mathbf{W}$ is invertible over M .*

Proof. By Lemma 3.5, there exists $y \in M$ such that $\sum_{g \in G} y^g \neq 0$. Suppose $\mathbf{W}$ is not invertible over M . Then there is a vector $u = (u_j)_j$ over M such that $\mathbf{W}u = 0$ and $u_{j_0} = y$ for some j_0 . Since $\mathbf{W}u = 0$ implies $\sum_j w_j^g u_j = 0$ for all $g \in G$, we get $\sum_j w_j u_j^{g^{-1}} = \sum_j (w_j^g u_j)^{g^{-1}} = 0$. Summing over all $g \in G$ gives $\sum_j w_j \bar{u}_j = 0$ where $\bar{u}_j = \sum_{g \in G} u_j^g$. Since $\bar{u}_j \in L$ for all j , and $\bar{u}_{j_0} = \sum_{g \in G} y^g \neq 0$, it follows that $w_1, \dots, w_d$ are linearly dependent over L , a contradiction. $\square$

Since $\mathbf{W}$ is invertible, (5) can be rewritten as

$$(6) \quad \mathbf{D}_i \mathbf{W} = \mathbf{W} X_i \quad \text{or} \quad X_i = \mathbf{W}^{-1} \mathbf{D}_i \mathbf{W} \quad \text{for } i = 1, \dots, m,$$

which is a convenient way of obtaining the generators $(X_i)_{kj}$ of L . Furthermore, Proposition 4.1 shows that

$$(7) \quad z_j(\mathfrak{X}_1, \dots, \mathfrak{X}_m) e_1 - \mathfrak{z}_j e_1 \quad \text{for } j = 1, \dots, t, \quad \ell = 1, \dots, d$$

(where e_1 is the first standard unit vector) vanish (are constantly zero) when evaluated on $z_1, \dots, z_t$ forming a basis of Z , and are the fundamental relations satisfied by these generators.

There is a convenient way to reformulate the relations (7) using a block matrix equation that does not involve choosing a basis of Z . Let $X_i(\mathfrak{X}_1, \dots, \mathfrak{X}_m)$ be the block matrix obtained by replacing x_k by $\mathfrak{X}_k$ for $i = 1, \dots, m$ in the matrix X_i . Using (2), this is equal to

$$A_{i0} \otimes I + A_{i1} \otimes z_1(\mathfrak{X}_1, \dots, \mathfrak{X}_m) + \dots + A_{it} \otimes z_t(\mathfrak{X}_1, \dots, \mathfrak{X}_m),$$

where $\otimes$ is the Kronecker tensor product of matrices. After multiplying on the right by $I \otimes e_1$, we get

$$\begin{aligned} & X_i(\mathfrak{X}_1, \dots, \mathfrak{X}_m)(I \otimes e_1) - \mathfrak{X}_i \otimes e_1 \\ &= A_{i0} \otimes e_1 + A_{i1} \otimes z_1(\mathfrak{X}_1, \dots, \mathfrak{X}_m)e_1 + \dots + A_{it} \otimes z_t(\mathfrak{X}_1, \dots, \mathfrak{X}_m)e_1 \\ &\quad - (A_{i0} + \mathfrak{z}_1 A_{i1} + \dots + \mathfrak{z}_t A_{it}) \otimes e_1 \\ &= A_{i1} \otimes (z_1(\mathfrak{X}_1, \dots, \mathfrak{X}_m)e_1 - \mathfrak{z}_1 e_1) + \dots + A_{it} \otimes (z_t(\mathfrak{X}_1, \dots, \mathfrak{X}_m)e_1 - \mathfrak{z}_t e_1) \end{aligned}$$

by (3). Combining this equation with (6) shows that vanishing of (7) implies vanishing of (8) $\mathbf{D}_i(\mathfrak{X}_1, \dots, \mathfrak{X}_m)\mathbf{W}(\mathfrak{X}_1, \dots, \mathfrak{X}_m)(I \otimes e_1) - \mathbf{W}(\mathfrak{X}_1, \dots, \mathfrak{X}_m)(\mathfrak{X}_i \otimes e_1)$ for $i = 1, \dots, m$.

But because the span of the entries of the X_i 's equals the span of $z_1, \dots, z_t$, vanishing of (8) also implies vanishing of (7). The benefit of (8) is that these equations do not depend on the choice of a basis of Z (as opposed to the relations in Proposition 4.1).

4.2.1. Bivariate invariants of involutions. Let us demonstrate the findings of this section on faithful actions of $\mathbb{Z}_2$ on $\mathbb{k}\langle x, y \rangle$. Such an action is given by an involution $\phi : \mathbb{k}\langle x, y \rangle \rightarrow \mathbb{k}\langle x, y \rangle$, a $\mathbb{k}$ -linear automorphism of order two. Without loss of generality let $x^\phi \neq x$. Then, the subspace $W = \text{span}_{\mathbb{k}}\{1, x\}$ satisfies the conclusions of Proposition 3.2. The corresponding matrices $\mathbf{D}_i$ and $\mathbf{W}$ are

$$\mathbf{D}_1 = \begin{pmatrix} x & 0 \\ 0 & x^\phi \end{pmatrix}, \quad \mathbf{D}_2 = \begin{pmatrix} y & 0 \\ 0 & y^\phi \end{pmatrix}, \quad \mathbf{W} = \begin{pmatrix} 1 & x \\ 1 & x^\phi \end{pmatrix}.$$

Next, we calculate

$$\mathbf{W}^{-1} = \begin{pmatrix} 1 + x(x^\phi - x)^{-1}x^\phi & -x(x^\phi - x)^{-1} \\ -(x^\phi - x)^{-1}x^\phi & (x^\phi - x)^{-1} \end{pmatrix}.$$

The matrices $X = \mathbf{W}^{-1}\mathbf{D}_1\mathbf{W}$ and $Y = \mathbf{W}^{-1}\mathbf{D}_2\mathbf{W}$ as in (6) are then equal to

$$(9) \quad X = \begin{pmatrix} 0 & z_1 \\ 1 & z_2 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} z_3 & z_5 \\ z_4 & z_6 \end{pmatrix}, \quad \text{where}$$

$$\begin{aligned} (10) \quad z_1 &= x^\phi(x^\phi - x)^{-1}x^2 - x(x^\phi - x)^{-1}(x^\phi)^2 \\ z_2 &= (x^\phi - x)^{-1}((x^\phi)^2 - x^2) \\ z_3 &= x^\phi(x^\phi - x)^{-1}y - x(x^\phi - x)^{-1}y^\phi \\ z_4 &= (x^\phi - x)^{-1}(y^\phi - y) \\ z_5 &= x^\phi(x^\phi - x)^{-1}yx - x(x^\phi - x)^{-1}y^\phi x^\phi \\ z_6 &= (x^\phi - x)^{-1}(y^\phi x^\phi - yx). \end{aligned}$$

The six not-obviously-scalar entries $z_1, \dots, z_6$ of X, Y generate $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ by Corollary 4.2. By Proposition 4.1, all relations between these generators are captured by the $6 \cdot 2 = 12$ equations as in (8). In Section 5 below we further investigate these equations for a specific nonlinear involution on $\mathbb{k}\langle x, y \rangle$, where we see that $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ is not necessarily free, nor can it be generated by three generators in general. But first, we analyze $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ for a

linear action of $\mathbb{Z}_2$ on $\mathbb{k}\langle x, y \rangle$; that is, we assume that x^ϕ, y^ϕ are linear combinations of x, y . If $\text{char } \mathbb{k} \neq 2$, then there are, up to isomorphism, only the following two examples of nontrivial 2-dimensional representations of $\mathbb{Z}_2$:

Example 4.4. Let $\text{char } \mathbb{k} \neq 2$; and assume that $x^\phi = -x$ and $y^\phi = y$. Then, the equations (9) and (10) simplify to

$$X = \begin{pmatrix} 0 & x^2 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} y & 0 \\ 0 & x^{-1}yx \end{pmatrix}.$$

In this case, $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ is generated by three generators: $x^2, y, x^{-1}yx$ or $x^2, yx, x^{-1}y$. Furthermore, these generators are free; since $\mathbb{Z}_2$ is abelian and $\text{char } \mathbb{k} \neq 2$, this holds by [KPPV20, Theorem 4.1], or by Theorem 4.8 below for general finite linear groups. Alternatively, one can directly check that the six relations (two per generator of $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$) in Proposition 4.1 are trivial; for example, if $y^\phi = y$, the generators are $z_1 = x^2, z_2 = y, z_3 = x^{-1}yx$, and the first columns of

$$\begin{aligned} \begin{pmatrix} 0 & \mathfrak{z}_1 \\ 1 & 0 \end{pmatrix}^2 &= \begin{pmatrix} \mathfrak{z}_1 & 0 \\ 0 & \mathfrak{z}_1 \end{pmatrix}, \quad \begin{pmatrix} \mathfrak{z}_2 & 0 \\ 0 & \mathfrak{z}_3 \end{pmatrix} = \begin{pmatrix} \mathfrak{z}_2 & 0 \\ 0 & \mathfrak{z}_3 \end{pmatrix}, \\ \begin{pmatrix} 0 & \mathfrak{z}_1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{z}_2 & 0 \\ 0 & \mathfrak{z}_3 \end{pmatrix} \begin{pmatrix} 0 & \mathfrak{z}_1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} \mathfrak{z}_3 & 0 \\ 0 & \mathfrak{z}_1^{-1}\mathfrak{z}_2\mathfrak{z}_1 \end{pmatrix} \end{aligned}$$

equal $\mathfrak{z}_j$ times e_1 , implying that there are no relations between z_1, z_2, z_3 .

Example 4.5. Let $\text{char } \mathbb{k} \neq 2$ and assume that $x^\phi = -x$ and $y^\phi = -y$ after a linear change of coordinates. Then, from (9) and (10) follows that

$$X = \begin{pmatrix} 0 & x^2 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & yx \\ x^{-1}y & 0 \end{pmatrix}.$$

In this case, $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ is generated by $x^2, yx, x^{-1}y$. The reader may verify, as in the previous example, that these are free generators.

If $\text{char } \mathbb{k} = 2$, then there is a unique nontrivial 2-dimensional representation of $\mathbb{Z}_2$ up to isomorphism.

Example 4.6. Let $\text{char } \mathbb{k} = 2$ and can assume that $x^\phi = y$ and $y^\phi = x$. Then, it follows from (9) and (10) that

$$X = \begin{pmatrix} 0 & x(x+y)^{-1}y(x+y) \\ 1 & (x+y)^{-1}(x^2+y^2) \end{pmatrix}, \quad Y = \begin{pmatrix} x+y & xy+yx+x(x+y)^{-1}y(x+y) \\ 1 & (x+y)^{-1}(xy+yx) \end{pmatrix}.$$

The entries of these two matrices generate $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$; a short calculation shows that the diagonal entries of Y and the top right entry of X generate the remaining entries. Thus, $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ is generated by $z_1 = x + y, z_2 = xy + yx, z_3 = x^{-1} + y^{-1}$ (note that z_3 is the inverse of $x(x+y)^{-1}y$), and these are free by Proposition 4.1 (more precisely, the sentence

after it) because

$$\begin{aligned} & \left(\begin{pmatrix} 0 & \mathfrak{z}_3^{-1} \mathfrak{z}_1 \\ 1 & \mathfrak{z}_1 + \mathfrak{z}_1^{-1} \mathfrak{z}_2 \end{pmatrix} + \begin{pmatrix} \mathfrak{z}_1 & \mathfrak{z}_2 + \mathfrak{z}_3^{-1} \mathfrak{z}_1 \\ 1 & \mathfrak{z}_1^{-1} \mathfrak{z}_2 \end{pmatrix} \right) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathfrak{z}_1 \\ 0 \end{pmatrix}, \\ & \left(\begin{pmatrix} 0 & \mathfrak{z}_3^{-1} \mathfrak{z}_1 \\ 1 & \mathfrak{z}_1 + \mathfrak{z}_1^{-1} \mathfrak{z}_2 \end{pmatrix} \begin{pmatrix} \mathfrak{z}_1 & \mathfrak{z}_2 + \mathfrak{z}_3^{-1} \mathfrak{z}_1 \\ 1 & \mathfrak{z}_1^{-1} \mathfrak{z}_2 \end{pmatrix} + \begin{pmatrix} \mathfrak{z}_1 & \mathfrak{z}_2 + \mathfrak{z}_3^{-1} \mathfrak{z}_1 \\ 1 & \mathfrak{z}_1^{-1} \mathfrak{z}_2 \end{pmatrix} \begin{pmatrix} 0 & \mathfrak{z}_3^{-1} \mathfrak{z}_1 \\ 1 & \mathfrak{z}_1 + \mathfrak{z}_1^{-1} \mathfrak{z}_2 \end{pmatrix} \right) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathfrak{z}_2 \\ 0 \end{pmatrix}, \\ & \left(\begin{pmatrix} 0 & \mathfrak{z}_3^{-1} \mathfrak{z}_1 \\ 1 & \mathfrak{z}_1 + \mathfrak{z}_1^{-1} \mathfrak{z}_2 \end{pmatrix}^{-1} + \begin{pmatrix} \mathfrak{z}_1 & \mathfrak{z}_2 + \mathfrak{z}_3^{-1} \mathfrak{z}_1 \\ 1 & \mathfrak{z}_1^{-1} \mathfrak{z}_2 \end{pmatrix}^{-1} \right) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathfrak{z}_3 \\ 0 \end{pmatrix}. \end{aligned}$$

4.3. Linear group actions on free skew fields. In this section we show that the generators $z_1, \dots, z_t$ obtained in the proof of Theorem 3.8 are free when G is a finite group of linear automorphisms on $M = \mathbb{k}\langle x_1, \dots, x_m \rangle$. This is achieved using Proposition 4.1; the following construction will help us show that the relations in Proposition 4.1 are trivial (i.e., the zero functions in $\mathfrak{z}_1, \dots, \mathfrak{z}_t$).

Given a vector space U over $\mathbb{k}$, let $\mathbb{k}\langle U \rangle$ be the tensor algebra over U (which is isomorphic to the free algebra of rank $\dim U$, justifying the notation). Let $V = \text{span}_{\mathbb{k}}\{x_1, \dots, x_m\}$. Suppose G is a finite group of automorphisms on M with $\text{char } \mathbb{k} \nmid |G|$, and V is G -stable. Let $W \subset \mathbb{k}\langle V \rangle$ be as in Proposition 3.7. We endow $V \otimes W$ and $V \otimes W \otimes W^*$ with the diagonal action of G . Choose a G -stable complement $(W \cap VW)^\perp$ of $W \cap VW$ in $VW \equiv V \otimes W$ (this identification is merited because V and W are subspaces of a free algebra, and V is homogeneous). Denote the vector space $\mathfrak{Z} = ((W \cap VW)^\perp \otimes W^*)^G$, and consider the surjective map

$$\pi'' : V \otimes W \otimes W^* = ((W \cap VW) \otimes W^*) \oplus ((W \cap VW)^\perp \otimes W^*) \xrightarrow{\text{tr} \oplus \mathcal{R}} \mathbb{k} \oplus \mathfrak{Z},$$

where $\text{tr} : W \otimes W^* \rightarrow \mathbb{k}$ is the trace $\text{tr}(w \otimes \varphi) = \varphi(w)$ and $\mathcal{R} : (W \cap VW)^\perp \otimes W^* \rightarrow \mathfrak{Z}$ is the Reynolds operator $\mathcal{R}(u) = \frac{1}{|G|} \sum_{g \in G} u^g$. Then π'' is a G -invariant linear map. We can view π'' as a G -equivariant map in 3 different ways:

$$\begin{aligned} \pi : V &\rightarrow W^* \otimes W \otimes (\mathbb{k} \oplus \mathfrak{Z}) \\ \pi' : V \otimes W &\rightarrow W \otimes (\mathbb{k} \oplus \mathfrak{Z}) \\ \pi'' : V \otimes W \otimes W^* &\rightarrow \mathbb{k} \oplus \mathfrak{Z}. \end{aligned}$$

Now

$$\pi : V \rightarrow W^* \otimes W \otimes (\mathbb{k} \oplus \mathfrak{Z}) \cong \text{End}(W) \otimes (\mathbb{k} \oplus \mathfrak{Z}) \subseteq \text{End}(W) \otimes \mathbb{k}\langle \mathfrak{Z} \rangle$$

extends to a G -equivariant algebra homomorphism

$$\Pi : \mathbb{k}\langle V \rangle \rightarrow \text{End}(W) \otimes \mathbb{k}\langle \mathfrak{Z} \rangle.$$

Lemma 4.7. *Assume the notation from the preceding paragraph. Let $\{w_j\}_j$ be a basis of W , and let $\{w_j^*\}_j$ be its dual basis of W^* . Then,*

$$(11) \quad \Pi(vw)(1 \otimes 1) = \sum_{k=1}^d \Pi(w_k)(1 \otimes \pi''(v \otimes w \otimes w_k^*))$$

for all $v \in V$ and $w \in W$ (where $\Pi(vw), \Pi(w_k)$ act on $W \otimes \mathbb{k}\langle \mathfrak{Z} \rangle$).

Proof. First, we show that

$$(12) \quad \Pi(w)(1 \otimes 1) = w \otimes 1 \quad \text{for } w \in W.$$

We prove (12) by induction on $\deg w$, using $W \subseteq \mathbb{k} + VW$. Clearly, (12) holds for $w \in \mathbb{k}$. Now let $w = \alpha + \sum_j \ell_j w_j$ where $\ell_j \in V$ and $w_j \in W$ satisfy $\Pi(w_j)(1 \otimes 1) = w_j \otimes 1$. Then

$$\begin{aligned} \Pi(w)(1 \otimes 1) &= \alpha \otimes 1 + \sum_j \Pi(\ell_j) \Pi(w_j)(1 \otimes 1) = \alpha \otimes 1 + \sum_j \pi(\ell_j)(w_j \otimes 1) \\ &= \alpha \otimes 1 + \sum_j \pi'(\ell_j \otimes w_j) \in W \otimes (\mathbb{k} \oplus \mathfrak{Z}), \end{aligned}$$

and hence

$$\begin{aligned} (w_k^* \otimes \text{id})(\Pi(w)(1 \otimes 1)) &= \alpha w_k^*(1) + \sum_j (w_k^* \otimes \text{id})(\pi'(\ell_j \otimes w_j)) \\ &= \alpha w_k^*(1) + \sum_j \pi''(\ell_j \otimes w_j \otimes w_k^*) \\ &= \pi'' \left(\left(\alpha \otimes 1 + \sum_j \ell_j \otimes w_j \right) \otimes w_k^* \right) = w_k^*(w) \end{aligned}$$

for all k , which implies $\Pi(w)(1 \otimes 1) = w \otimes 1$. Now, consider both sides of (11). Using (12), they simplify to

$$(13) \quad \Pi(vw)(1 \otimes 1) = \Pi(v)\Pi(w)(1 \otimes 1) = \pi(v)(w \otimes 1) = \pi'(v \otimes w) \in W \otimes (\mathbb{k} \oplus \mathfrak{Z}),$$

$$(14) \quad \sum_k \Pi(w_k)(1 \otimes \pi''(v \otimes w \otimes w_k^*)) = \sum_k w_k \otimes \pi''(v \otimes w \otimes w_k^*) \in W \otimes (\mathbb{k} \oplus \mathfrak{Z}).$$

Applying $w_{k'}^* \otimes \text{id}$ to (13) results in

$$(w_{k'}^* \otimes \text{id})(\pi'(v \otimes w)) = \pi''(v \otimes w \otimes w_{k'}^*),$$

while applying it to (14) results in

$$\sum_k w_{k'}^*(w_k) \pi''(v \otimes w \otimes w_k^*) = \pi''(v \otimes w \otimes w_{k'}^*).$$

Since this is true for all k' , it follows that (13) and (14) are equal, and so (11) holds. $\square$

The system (11) of polynomial identities in $\mathbb{k}\langle \mathfrak{Z} \rangle$ is the last ingredient for the proof of the next main result.

Theorem 4.8. *Let G be a finite group of linear automorphisms on $\mathbb{k}\langle x_1, \dots, x_m \rangle$, and $\text{char } \mathbb{k} \nmid |G|$. Then, $\mathbb{k}\langle x_1, \dots, x_m \rangle^G$ is the free skew field of rank $|G|(m-1)+1$.*

Proof. Let $M = \mathbb{k}\langle x_1, \dots, x_m \rangle$ and $V = \text{span}_{\mathbb{k}}\{x_1, \dots, x_m\}$. Note that G consists of outer automorphisms. Let W be as in Proposition 3.7, and $d = \dim W = \dim M_{M^G} = |G|$.

We mimic the proof of Theorem 3.8; let $\rho : M \rightarrow \text{End}(W) \otimes L$ and $\rho'' : M \otimes W \otimes W^* \rightarrow L$ be as therein. Since W is a subspace of the free algebra $\mathbb{k}\langle V \rangle$ and $W \subseteq \mathbb{k} + VW$, it follows that the G -stable subspace $W \cap VW \subseteq VW$ has dimension $d-1$. Since $VW = V \otimes W$ in the tensor algebra $\mathbb{k}\langle V \rangle$, we can view $W \cap VW$ as a subspace of $V \otimes W$ (that plays

the role of T from the proofs of Theorems 3.3 and 3.8). Choose a G -stable complement $(W \cap VW)^\perp$ of $W \cap VW$ in $V \otimes W$, and denote $\mathfrak{Z} = ((W \cap VW)^\perp \otimes W^*)^G \subseteq V \otimes W \otimes W^*$. Since $W^* \cong \mathbb{k}[G]$, we have $\dim \mathfrak{Z} = \dim ((W \cap VW)^\perp \otimes W^*)^G = \dim(W \cap VW)^\perp$. The map $\rho'' : V \otimes W \otimes W^* \rightarrow L$ is G -invariant, and consequently $Z = \rho''((W \cap VW)^\perp \otimes W^*) = \rho''(\mathfrak{Z})$. Recall that L is then generated by a basis of Z by the proof of Theorem 3.3.

Let $\pi'' : V \otimes W \otimes W^* \rightarrow \mathbb{k} \oplus \mathfrak{Z}$ and $\Pi : \mathbb{k}\langle V \rangle \rightarrow \text{End}(W) \otimes \mathbb{k}\langle \mathfrak{Z} \rangle$ be as in Lemma 4.7. Fix a basis $1 = w_1, \dots, w_d$ of W , and its dual basis $w_1^*, \dots, w_d^*$ in W^* . Then,

$$(15) \quad \Pi(x_i^g w_j^g)(1 \otimes 1) - \sum_{k=1}^d \Pi(w_k^g)(1 \otimes \pi''(v \otimes w_j \otimes w_k^*)) = 0 \quad \text{for all } i, j, g$$

by (11) because Π is G -equivariant. By the construction of ρ, ρ'' and Π, π'' , the diagrams

$$(16) \quad \begin{array}{ccc} V \otimes W \otimes W^* & \xrightarrow{\pi''} & \mathbb{k} \oplus \mathfrak{Z} \\ & \searrow \rho'' & \downarrow \rho'' \\ & & \mathbb{k} \oplus Z \end{array} \quad \begin{array}{ccc} \mathbb{k}\langle V \rangle & \xrightarrow{\Pi} & \text{End}(W) \otimes \mathbb{k}\langle \mathfrak{Z} \rangle \\ & \searrow \rho & \downarrow \\ & & \text{End}(W) \otimes L \end{array}$$

commute; here, the vertical map in the second diagram in (16) is the unique algebra homomorphism that restricts to the identity on $\text{End}(W)$ and whose restriction to $\mathfrak{Z}$ agrees with ρ'' . Let $\mathfrak{z}_1, \dots, \mathfrak{z}_t$ form a basis of $\mathfrak{Z}$; then $z_1 = \rho''(\mathfrak{z}_1), \dots, z_t = \rho''(\mathfrak{z}_t)$ span Z , and our goal is to show that they are free in M . Since $\mathfrak{z}_1, \dots, \mathfrak{z}_t$ span $\mathfrak{Z}$, there are matrices $A_{i0}, \dots, A_{it}$ over $\mathbb{k}$ (for $i = 1, \dots, m$) such that

$$(17) \quad \left(\pi''(x_i \otimes w_j \otimes w_k^*) \right)_{j,k=1}^d = A_{i0} + \mathfrak{z}_1 A_{i1} + \dots + \mathfrak{z}_t A_{it}.$$

Since the first diagram in (16) commutes, the matrices X_i representing $\rho(x_i)$ relative to the basis $w_1, \dots, w_d$ satisfy

$$X_i = A_{i0} + z_1 A_{i1} + \dots + z_t A_{it}.$$

Thus, we view (17) as affine matrices over $\mathbb{k}\langle \mathfrak{z}_1, \dots, \mathfrak{z}_t \rangle = \mathbb{k}\langle \mathfrak{Z} \rangle$ and denote them $\mathfrak{X}_i$ as in (3). By Proposition 4.1 and (8) (see also (5)), the fundamental relations between $z_1, \dots, z_t$ are

$$(18) \quad (x_i^g w_j^g)(\mathfrak{X})e_1 - \sum_{k=1}^d (w_k^g)(\mathfrak{X})e_1 \cdot (\mathfrak{X}_i)_{kj} \quad \text{for all } i, j, g.$$

Expressions (18) are vectors of noncommutative polynomials in $\mathfrak{z}_1, \dots, \mathfrak{z}_t$; we claim that they are zero (i.e., they are trivial relations between $z_1, \dots, z_t$). By the definition of $\mathfrak{X}_i$ we have $(\mathfrak{X}_i)_{kj} = \pi''(v \otimes w_j \otimes w_k^*)$. Since the diagrams (16) commute, $(w_k^g)(\mathfrak{X})e_1$ and $(x_i^g w_j^g)(\mathfrak{X})e_1$ are precisely the vectors representing $\Pi(w_k^g)(1 \otimes 1)$ and $\Pi(x_i^g w_j^g)(1 \otimes 1)$, respectively, relative to the basis $w_1, \dots, w_d$ of W . Thus, the expressions (18) are vector representations of the left-hand-side expressions in (15). The equations (15) then imply that (18) are zero. Hence, the fundamental relations between $z_1, \dots, z_t$ are trivial, so $z_1, \dots, z_t$ are free in M by Proposition 4.1. In particular, they are also linearly independent, so

$$\dim Z = \dim S = \dim(W \cap VW)^\perp = md - (d - 1).$$

Hence, $t = md - (d - 1)$ and $z_1, \dots, z_t$ are free generators of L . $\square$

Theorem 4.8 bears resemblance to the renowned Nielsen–Schreier index formula for subgroups of free groups. While the proof of Theorem 4.8 does not rely on free groups (as opposed to its earlier special case [KPPV20, Theorem 5.1]), an expert may nevertheless recognize analogies in the proof. For another manifestation of the index formula, see the Schreier–Lewin formula for ranks of free modules over free algebras [L69, Theorem 4].

It is not surprising that invariants of infinite linear groups may not be finitely generated. The techniques developed in this paper do not readily apply to this case (which is left to later studies). Nevertheless, let us show that the freeness conclusion still holds in the simplest nontrivial example.

Example 4.9. Suppose $\mathbb{k}$ is infinite, and let G be an infinite multiplicative subgroup of $\mathbb{k} \setminus \{0\}$. Consider the linear action of G on $\mathbb{k}\langle x, y \rangle$ given by $x^\alpha = \alpha x$ and $y^\alpha = y$ for $\alpha \in G$. We claim that $\mathbb{k}\langle x, y \rangle^G$ is a free skew field on infinitely many generators. Let L be the skew subfield of $\mathbb{k}\langle x, y \rangle$ generated by $\{x^{-n}yx^n : n \in \mathbb{Z}\}$, and consider the automorphism $\sigma : L \rightarrow L$ given by $\sigma(\ell) = x^{-1}\ell x$. By [C95, Lemma 5.5.6], the generators $x^{-n}yx^n$ for $n \in \mathbb{Z}$ are free in L , and $\mathbb{k}\langle x, y \rangle = L(x; \sigma)$ (the classical ring of right fractions of the skew polynomial ring $L[x; \sigma]$). We claim that $L = \mathbb{k}\langle x, y \rangle^G$. Clearly, $L \subseteq \mathbb{k}\langle x, y \rangle^G$. Conversely, if $r \in \mathbb{k}\langle x, y \rangle^G \subseteq L(x; \sigma)$, we can write $r = pq^{-1}$ for $p, q \in L[x; \sigma]$ of minimal total degree in x . Since $L[x; \sigma]$ is a principal right ideal domain [C95, Proposition 2.1.1], p and q are uniquely determined up to a right multiple from L . Since

$$p(x)q(x)^{-1} = r = r^\alpha = p(\alpha x)q(\alpha x)^{-1}$$

for infinitely many $\alpha \in G$, uniqueness implies $p, q \in L$, and therefore $r \in L$.

5. NON-FREE INVARIANT SKEW SUBFIELDS OF A FREE SKEW FIELD

The aim of this section is threefold. First, it demonstrates that there exist non-free invariant skew subfields in the free skew field, resolving a Lüroth-like question of Schofield [S85^b]. Second, the number of required generators does not depend just on the group, but on its action (cf. Corollary 4.2 and Theorem 3.8). Third, we disprove the conjecture of Cohn [C78] on centralizers in free skew fields.

5.1. Free de Jonquières involutions. To establish the above claims, we advance the calculations from Section 4.2.1 for a special kind of involution on $\mathbb{k}\langle x, y \rangle$. Let $f \in \mathbb{k}(x) \setminus \{0\}$. Then,

$$x^\phi = y^{-1}xy, \quad y^\phi = y^{-1}f$$

determines an involution ϕ of $\mathbb{k}\langle x, y \rangle$, since

$$(x^\phi)^\phi = (y^\phi)^{-1}x^\phi y^\phi = f^{-1}y \cdot y^{-1}xy \cdot y^{-1}f = x, \quad (y^\phi)^\phi = (y^\phi)^{-1}f(x^\phi) = f^{-1}y \cdot y^{-1}fy = y.$$

This involution is a noncommutative analog of a de Jonquières involution of the plane [BB00]. If $\mathbb{k}$ is algebraically closed, one can restrict to $f \in \mathbb{k}[x]$ with simple roots after a change of variables $y \mapsto qy$ for a suitable $q \in \mathbb{k}(x)$. If f is a polynomial of degree at least three with pairwise distinct roots, the commutative specialization of ϕ is not conjugated to a linear automorphism (see [BB00]); thus, this involution is a natural candidate for seeking non-free skew subfields of $\mathbb{k}\langle x, y \rangle$. We assume $\text{char } \mathbb{k} \neq 2$ for the rest of this section.

As in Section 4.2.1 we take $W = \text{span}_{\mathbb{k}}\{1, x\}$, and write

$$\mathbf{D}_1 = \begin{pmatrix} x & 0 \\ 0 & y^{-1}xy \end{pmatrix}, \quad \mathbf{D}_2 = \begin{pmatrix} y & 0 \\ 0 & y^{-1}f \end{pmatrix}, \quad \mathbf{W} = \begin{pmatrix} 1 & x \\ 1 & y^{-1}xy \end{pmatrix}.$$

Denote

$$X := \begin{pmatrix} 0 & z_1 \\ 1 & z_2 \end{pmatrix} = \mathbf{W}^{-1}\mathbf{D}_1\mathbf{W}, \quad Y := \begin{pmatrix} z_3 & z_5 \\ z_4 & z_6 \end{pmatrix} = \mathbf{W}^{-1}\mathbf{D}_2\mathbf{W}, \quad E = I \otimes e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Then, $z_1, \dots, z_6$ generate $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$, and the fundamental relations between these generators come from (8) by Proposition 4.1. One can check that all six generators are nonzero by inspecting the formula (10) (we point this out because the calculations below involve multiplying equations by the generators or their inverses). The fundamental relations between $z_1, \dots, z_6$ as in (8) specialize to

$$\begin{pmatrix} X & 0 \\ 0 & Y^{-1}XY \end{pmatrix} \begin{pmatrix} I & X \\ I & Y^{-1}XY \end{pmatrix} E = \begin{pmatrix} I & X \\ I & Y^{-1}XY \end{pmatrix} EX, \\ \begin{pmatrix} Y & 0 \\ 0 & Y^{-1}f(X) \end{pmatrix} \begin{pmatrix} I & X \\ I & Y^{-1}XY \end{pmatrix} E = \begin{pmatrix} I & X \\ I & Y^{-1}XY \end{pmatrix} EY,$$

which simplify to

$$(19) \quad \begin{pmatrix} X & X^2 \\ XY & X^2Y \end{pmatrix} E = \begin{pmatrix} I & X \\ Y & XY \end{pmatrix} EX, \\ \begin{pmatrix} Y & YX \\ f(X) & f(X)Y^{-1}XY \end{pmatrix} E = \begin{pmatrix} I & X \\ Y & XY \end{pmatrix} EY.$$

A direct calculation shows that the first block rows of both equations in (19) trivially hold; that is, they do not store any information about the relations between $z_1, \dots, z_6$. Thus, (19) simplifies to

$$(20) \quad XC = CX, \quad f(X)Y^{-1}C = CY, \quad \text{where } C := (Y \quad XY)E = \begin{pmatrix} z_3 & z_1z_4 \\ z_4 & z_3 + z_2z_4 \end{pmatrix}.$$

Since Y and C have the same first column, we can write

$$Y^{-1}C = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}.$$

Because x and y do not commute, $\mathbf{D}_1$ and $\mathbf{D}_2$ do not commute, and therefore X and Y do not commute. We have $Y^{-1}C \neq I$, because otherwise the first equation in (20) would imply that X commutes with $Y = C$. Since C commutes with X and $(Y^{-1}C)^2 = f(X)^{-1}C^2$ by (20), it follows that $(Y^{-1}C)^2X = X(Y^{-1}C)^2$. The first columns of this matrix equation imply $a + ab = 0$ and $b^2 = 1$. Hence, $(Y^{-1}C)^2 = I$, and so $C^2 = f(X)$ by (20). Furthermore, we have $b = 1$ and $a = 0$ (because $\text{char } \mathbb{k} \neq 2$) or $b = -1$; the first option contradicts $Y^{-1}C \neq I$, and so $b = -1$.

Let $f(X) = \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix}$. The first columns in XC and CX are trivially equal, and do not contribute any information. The equations $b = -1$ (i.e., the last piece of information from $(Y^{-1}C)^2 = I$), $XC = CX$ and $C^2 = f(X)$ are then equivalent to

$$(21) \quad (z_6 - z_4 z_3^{-1} z_5)^{-1} (z_3 + z_2 z_4 - z_4 z_3^{-1} z_1 z_4) = -1,$$

$$(22) \quad z_1 z_3 + z_1 z_2 z_4 = z_3 z_1 + z_1 z_4 z_2,$$

$$(23) \quad z_1 z_4 + z_2 z_3 + z_2^2 z_4 = z_4 z_1 + z_3 z_2 + z_2 z_4 z_2,$$

$$(24) \quad z_3^2 + z_1 z_4^2 = f_{11},$$

$$(25) \quad z_4 z_3 + z_3 z_4 + z_2 z_4^2 = f_{21},$$

$$(26) \quad z_3 z_1 z_4 + z_1 z_4 z_3 + z_1 z_4 z_2 z_4 = f_{12},$$

$$(27) \quad z_4 z_1 z_4 + (z_3 + z_2 z_4)^2 = f_{22}.$$

Since $f(X)$ commutes with X , we have $f_{12} = z_1 f_{21}$ and $f_{22} - f_{11} = z_2 f_{21}$. Then, (26) is a consequence of $f_{12} = z_1 f_{21}$, (25) and (22) (right-multiplied by z_4); (27) is a consequence of $f_{22} - f_{11} = z_2 f_{21}$, (24), (25) and (23) (right-multiplied by z_4). Observe that z_6 is a noncommutative rational function in $z_1, \dots, z_5$ by (21), and that z_5 does not appear in any other relation. Thus, $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ is generated by $z_1, \dots, z_5$ where $z_1, \dots, z_4$ satisfy relations (22), (23), (24) and (25).

From here on, we restrict to a cubic polynomial $f = x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0$ with $\alpha_i \in \mathbb{k}$. In this case, $f_{11} = z_1 z_2 + \alpha_2 z_1 + \alpha_0$ and $f_{21} = z_1 + z_2^2 + \alpha_2 z_2 + \alpha_1$. We can express $z_1 = z_4 z_3 + z_3 z_4 + z_2 z_4^2 - z_2^2 - \alpha_2 z_2 - \alpha_1$ from (25) – this is the main reason for restricting to a cubic f . After inserting z_1 in (23) and rearranging, we obtain

$$(z_3 + z_4(z_4^2 - z_2 - \alpha_2)) \cdot (z_4^2 - z_2) = (z_4^2 - z_2) \cdot (z_3 + z_4(z_4^2 - z_2 - \alpha_2)).$$

Denote $r = z_4^2 - z_2 - \alpha_2$ and $s = z_3 + z_4(z_4^2 - z_2 - \alpha_2)$. Then, r and s commute, and r, s, z_4 generate the same subfield of $\mathbb{k}\langle x, y \rangle$ as z_2, z_3, z_4 :

$$z_2 = z_4^2 - \alpha_2 - r, \quad z_3 = s - z_4 r, \quad z_1 = z_4 s + s z_4 - z_4 r z_4 - (r^2 + \alpha_2 r + \alpha_1).$$

Next, we express the remaining two equations (24) and (22) in terms of r, s, z_4 . After a tedious yet straightforward calculation (using $rs = sr$), we simplify them to

$$(28) \quad s^2 = r^3 + \alpha_2 r^2 + \alpha_1 r + \alpha_0,$$

$$(29) \quad z_4(s^2 - r^3 - \alpha_2 r^2 - \alpha_1 r) = (s^2 - r^3 - \alpha_2 r^2 - \alpha_1 r)z_4.$$

Note that (29) is a direct consequence of (28).

Let us summarize our findings: z_6, z_1 are noncommutative rational functions in $z_2, \dots, z_5$, and z_2, z_3 can be further replaced by r, s . Thus, L is generated by z_4, z_5, r, s and in terms of these generators, the fundamental relations reduce to $rs = sr$ and $s^2 = f(r)$. Using the formulae (10), it is easy to verify that r and s are nonconstant (and thus transcendental) elements of $\mathbb{k}\langle x, y \rangle$ (for their simplified explicit forms, see Corollary 5.3 below). Hence, they generate the function field of the plane cubic curve $\mathcal{C} = \{(u, v) : v^2 = f(u)\}$.

Given a $\mathbb{k}$ -algebra A , its universal derivation bimodule $\Omega_{\mathbb{k}}(A)$ is the A -subbimodule in $A \otimes_{\mathbb{k}} A^{\text{op}}$ generated by $\{da : a \in A\}$, where $da = a \otimes 1 - 1 \otimes a$. If A is a skew field generated by $a_1, \dots, a_m$, then $\Omega_{\mathbb{k}}(A)$ is generated by $da_1, \dots, da_m$ since $d : A \rightarrow \Omega_{\mathbb{k}}(A)$ is a derivation.

For the free skew field $M = \mathbb{k}\langle x_1, x_2, \dots, x_m \rangle$, the bimodule $\Omega_{\mathbb{k}}(M)$ is freely generated by $dx_1, dx_2, \dots, dx_m$ [C95, Proposition 5.8.7 and Theorem 5.8.10]. The universal derivation bimodule can be used to test freeness.

Assume that f has simple roots and $\text{char } \mathbb{k} \neq 2$, so that this curve $\mathcal{C} = \{(u, v) : v^2 = f(u)\}$ is smooth (in other words, its completion is an elliptic curve). Then the function field F of $\mathcal{C}$ is not rational over $\mathbb{k}$ [H77, Example II.8.20.3] (which implies that it is not a free skew field). We will need the following lemma later (even though we already know that F is not a free skew field):

Lemma 5.1. *The F -bimodule $\Omega_{\mathbb{k}}(F)$ is not cyclic.*

Proof. The projective closure $\overline{\mathcal{C}}$ of $\mathcal{C}$ with the point at infinity ∞ is an elliptic curve. Let $R = \mathbb{k}[u, v]/(v^2 - f(u))$ be the coordinate ring of $\mathcal{C}$ (with F as its field of fractions). Suppose $\Omega_{\mathbb{k}}(F)$ is a cyclic F -bimodule, in other words, a principal ideal in $F \otimes_{\mathbb{k}} F$. Then, it is generated by some $c \in F \otimes_{\mathbb{k}} R$. Note that $\Omega_{\mathbb{k}}(F)$ is the localization (at $1 \otimes R \setminus \{0\}$) of the maximal ideal $(u - r, v - s)$ in $F \otimes_{\mathbb{k}} R$ corresponding to the F -rational point $P = (r, s)$ on $\mathcal{C}$. The principal divisor of c is then of the form $\text{div}(c) = (P) + (Q_1) + \dots + (Q_m) - (m+1)(\infty)$, where $Q_1, \dots, Q_m$ are $\mathbb{k}$ -rational points on $\mathcal{C}$. Because $Q \mapsto (Q) - (\infty)$ induces a one-to-one correspondence between the points on $\overline{\mathcal{C}}$ and the equivalence classes of degree-zero divisors on $\overline{\mathcal{C}}$ [H77, Example IV.1.3.7], there is a $\mathbb{k}$ -rational point Q on $\mathcal{C}$ and $d \in F \setminus \{0\}$ (viewed as the function field of $\mathcal{C}$) such that $m(\infty) - (Q_1) - \dots - (Q_m) = (Q) - (\infty) + \text{div}(d)$. Then, $\text{div}(cd) = (P) - (Q)$; note that $P \neq Q$ since Q is $\mathbb{k}$ -rational and P is not. But distinct points on a non-rational smooth complete curve are not linearly equivalent [H77, Example II.6.10.1], so $(P) - (Q)$ cannot be a principal divisor, a contradiction. Thus, $\Omega_{\mathbb{k}}(F)$ is not a cyclic F -bimodule. $\square$

The following Theorem gives us an example of an invariant subfield of a free skew field that is *not* free.

Theorem 5.2. *Assume $\text{char } \mathbb{k} \neq 2$ and let $f \in \mathbb{k}[x]$ be a monic cubic polynomial with simple roots. If $\mathbb{Z}_2$ acts on $\mathbb{k}\langle x, y \rangle$ via the involution*

$$x \mapsto y^{-1}xy, \quad y \mapsto y^{-1}f,$$

then the skew field $\mathbb{k}\langle x, y \rangle^{\mathbb{Z}_2}$ is generated by four (but not three) elements, and is not free.

Proof. Let $K = \mathbb{k}\langle z_4, z_5 \rangle$, and let F be field generated by r, s satisfying $s^2 = f(r)$. Let D be the skew field coproduct of K and F over $\mathbb{k}$; that is, D is the universal skew field of fractions of the ring coproduct of K and F over $\mathbb{k}$ (since the ring coproduct of K and F is a free ideal ring [C95, Theorem 5.3.9]). Thus, D is generated by z_4, z_5, r, s . The preceding calculations in this section show that L is also generated by z_4, z_5, r, s , and all the relations between these generators in D also hold in L (and a priori, they may satisfy further relations in L). Thus, there is a local homomorphism from D to L . However, all the preceding calculations are reversible (i.e., no information was lost in manipulating the equations), so D satisfies the fundamental relations of L (when we choose the generators of D in the same way as r, s express with z_1, z_2, z_3, z_4 in L). Thus, $D \cong L$ by Proposition 4.1.

The K -bimodule $\Omega_{\mathbb{k}}(K)$ is free of rank 2 with generators dz_4, dz_5 by [C95, Proposition 5.8.7 and Theorem 5.8.10]. The F -bimodule $\Omega_{\mathbb{k}}(F)$ is generated by dr, ds but it is not free of rank 1 by Lemma 5.1. By [C95, Theorems 5.8.8 and 5.8.10], the D -bimodule $\Omega_{\mathbb{k}}(D)$ is generated by dz_4, dz_5, dr, ds and the relations between these are precisely those from $\Omega_{\mathbb{k}}(K)$ and $\Omega_{\mathbb{k}}(F)$. Thus, $\Omega_{\mathbb{k}}(D)$ is not a free D -bimodule and cannot be generated by three elements. Thus, the skew field D cannot be generated by three elements, and is not free by [C95, Theorem 5.8.10]. $\square$

5.2. Centralizers in free skew fields. The invariant skew field in Section 5.1 is also significant for centralizers in free skew fields. The centralizer of a non-scalar element in a free skew field is commutative [C78, Corollaire 2], and furthermore finitely generated of transcendence degree 1 over $\mathbb{k}$ [S85^b, Theorem 11.6]. That is, every centralizer of a non-scalar element is isomorphic to the function field of a curve. It was conjectured in [C78, Conjecture] that the centralizer is rational, i.e., isomorphic to $\mathbb{k}(t)$. However, this is not the case, as demonstrated by the r, s constructed above that generate a non-rational field (and consequently their centralizer is not rational, since all subfields of $\mathbb{k}(t)$ containing $\mathbb{k}$ are rational by Lüroth's theorem [H77, Example 2.5.5]).

Corollary 5.3. *Assume $\text{char } \mathbb{k} \neq 2$ and let $f \in \mathbb{k}[x]$ be a monic cubic polynomial with simple roots and the quadratic coefficient α . Define $r, s \in \mathbb{k}\langle x, y \rangle \setminus \mathbb{k}$ as*

$$r = b_1^2 - b_2 - \alpha \quad \text{and} \quad s = y - xb_1 + b_1r,$$

$$\text{where} \quad b_1 = (xy - yx)^{-1}(f - y^2), \quad b_2 = (xy - yx)^{-1}(x^2y - yx^2).$$

Then, $rs = sr$ and $s^2 = f(r)$; the centralizer of r (and s) in $\mathbb{k}\langle x, y \rangle$ is not rational.

For a comparison, the centralizer of a non-scalar element in a free algebra is isomorphic to $\mathbb{k}[t]$ by Bergman's centralizer theorem [B69, Theorem 5.3]; moreover, its centralizer within the corresponding free skew field is isomorphic to $\mathbb{k}(t)$ by [C06, Theorem 7.9.8]. One can push this analogy further: [C06, Corollary 6.7.2] shows that the centralizer of a non-scalar element in the ring of formal power series in free variables is isomorphic to $\mathbb{k}[[t]]$; it is also not hard to see that the centralizer of a non-scalar element in the skew field of Malcev-Neumann series over a free group is isomorphic to the field of formal Laurent series $\mathbb{k}((t))$.

Corollary 5.3 shows that all function fields of curves of genus 1 (at least when $\mathbb{k}$ is algebraically closed and $\text{char } \mathbb{k} \neq 2$) embed into a free skew field; it is not known what happens for curves with higher genera. A remarkable result [S85^b, Theorem 11.10] states that two elements of a free skew field are either free or commute; this fact hints at a possibly special role of commutativity among non-trivial relations in a free skew field. Thus, we conclude the section with the following questions.

Question 5.4. *Let M be a noncommutative free skew field.*

- (a) *Does the function field of every curve embed into M ?*
- (b) *Is every skew subfield of M a skew field coproduct (over $\mathbb{k}$) of function fields of curves?*

A better understanding of invariants for the involution $x \mapsto y^{-1}xy, y \mapsto y^{-1}f$ for a general $f \in \mathbb{k}[x]$ would provide further insight into these questions. Yet at the moment, a conclusive procedure for reducing equations in free skew fields is lacking.

There is also a geometric explanation for why elements in the free skew field with centralizers of higher genera are rather atypical. Namely, a higher genus of the centralizer of $r \in \mathbb{k}\langle x_1, \dots, x_m \rangle$ implies a higher algebraic dependency of eigenvalues of r (as a multivariate matrix function), as follows.

Proposition 5.5. *Let $\mathbb{k}$ be an algebraically closed field of characteristic 0. Suppose that $r, s \in \mathbb{k}\langle x_1, \dots, x_m \rangle$ commute and generate the function field of a curve of genus g . If $n \geq g$ is such that r and s are defined at some point in $(\mathbb{k}^{n \times n})^m$, then the eigenvalues of r on $(\mathbb{k}^{n \times n})^m$ generate a field of transcendence degree at most $n - g$ over $\mathbb{k}$.*

Proof. The commuting variety $\mathcal{Z}$ is the set of all pairs $(A, B) \in (\mathbb{k}^{n \times n})^2$ with $AB = BA$. It is an irreducible variety of dimension $n^2 + n$.¹ The group $\mathrm{GL}_n(\mathbb{k})$ acts on $\mathcal{Z}$ by simultaneous conjugation, and S_n acts on $\mathcal{D} \times \mathcal{D}$ by simultaneously permuting the diagonal entries of the two matrices. There is an isomorphism between GIT quotients $\mathcal{Z} // \mathrm{GL}_n(\mathbb{k}) \cong (\mathcal{D} \times \mathcal{D}) // S_n$ by [GG06, Lemma 2.8.3]. We have a rational map $(r, s) : (\mathbb{k}^{n \times n})^m \dashrightarrow \mathcal{Z}$. Define the rational map $\sigma : (\mathbb{k}^{n \times n})^m \dashrightarrow (\mathcal{D} \times \mathcal{D}) // S_n$ as the composition

$$(\mathbb{k}^{n \times n})^m \dashrightarrow \mathcal{Z} \longrightarrow \mathcal{Z} // \mathrm{GL}_n(\mathbb{k}) \cong (\mathcal{D} \times \mathcal{D}) // S_n$$

Since $r(X)$ and $s(X)$ commute for every tuple of $n \times n$ matrices X where they are both defined, each pair of their corresponding eigenvalues give a point on $\mathcal{C}$. So the image of σ is contained in $\mathcal{C}^{(d)} = \mathcal{C}^d // S_d$, the d^{th} symmetric power of $\mathcal{C}$ (see [M86^b, Proposition 3.1]). There is a canonical map $\phi : \mathcal{C}^{(n)} \rightarrow J(\mathcal{C})$ by [M86^b, Section 5], where $J(\mathcal{C})$ is the Jacobian variety of $\mathcal{C}$, and ϕ is surjective since $n \geq g$. Note that $\dim \mathcal{C}^{(n)} = n$ and $\dim J(\mathcal{C}) = g$ by [M86^b, Proposition 2.1]. Since $J(\mathcal{C})$ is an abelian variety and every rational map from an affine space to an abelian variety is constant by [M86^a, Corollary 3.9], it follows that $\phi \circ \sigma$ is constant. Therefore, the image of σ has dimension at most $n - g$. The projection of $\mathcal{D} \times \mathcal{D} \rightarrow \mathcal{D}$ onto the first factor induces a morphism of quotients $\pi : (\mathcal{D} \times \mathcal{D}) // S_n \rightarrow \mathcal{D} // S_n$. The composition $\pi \circ \sigma$ sends an m -tuple $X \in (\mathbb{k}^{n \times n})^m$ to the set of eigenvalues of $r(X)$. The dimension of the image of $\pi \circ \sigma$ is at most the dimension of the image of σ , which is $n - g$. $\square$

Proposition 5.5 does not admit a converse; for instance, eigenvalues of $xy - yx$ add up to 0 and are thus linearly dependent, and the centralizer of $xy - yx$ in $\mathbb{k}\langle x, y \rangle$ equals $\mathbb{k}(xy - yx)$ by [C06, Theorem 7.9.8]. The authors do not know of an element in a free skew field whose eigenvalues (in the sense of matrix functions as above) satisfy more than a single relation.

6. ALGORITHMS

In this section we discuss computational aspects of finding generators for skew subfields of $M = \mathbb{k}\langle x_1, \dots, x_m \rangle$. Denote $R = \mathbb{k}\langle x_1, \dots, x_m \rangle$.

First, we outline some basics of computing and rational identity testing in M . For every $r \in M$ there exist $\delta \in \mathbb{N}$, $\delta \times \delta$ matrices $A_0, A_1, \dots, A_m \in \mathbb{k}^{\delta \times \delta}$ and row/column vectors u, v over $\mathbb{k}$ such that $r = uA^{-1}v$ and $A = A_0 + x_1A_1 + \dots + x_mA_m$ is full. The triple

¹Since we view $\mathcal{Z}$ as an algebraic set it is also reduced. It is not known whether the commuting variety, as a scheme, is reduced.

(u, A, v) is known as a *linear representation* of r of dimension δ . See [CR99, Section 1] for the construction of linear representations, and the arithmetic operations in M in terms of linear representations. Then, $r = 0$ in M if and only if the $(\delta + 1) \times (\delta + 1)$ matrix

$$\begin{pmatrix} 0 & u \\ v & A \end{pmatrix}$$

is not full over R . There is a polynomial-time deterministic algorithm for deciding non-fullness of such a matrix by [GGOW16, Theorem I.1] and [IQS18, Theorem 1.5]. If $\mathbb{k}$ is infinite, then a $(\delta + 1) \times (\delta + 1)$ affine matrix over R is full if and only if its evaluation at some tuple of matrices $X \in (\mathbb{k}^{\delta \times \delta})^m$ is invertible [DM17, Proposition 1.12]. In particular, this allows for a straightforward probabilistic test of $r \neq 0$: based on the number of operations in r one can estimate the dimension of a linear representation of r , and check if $r(X)$ is nonzero at a sufficiently large random matrix tuple X over $\mathbb{k}$.

The above algorithms for rational identity testing also extend to computing the rank of matrices over M . Given a rectangular matrix A over R , there is an algorithm for deciding whether A has full rank over M : pad A with zeros to a square matrix, linearize it, and then apply [IQS18, Theorem 1.5]. Furthermore, if $\mathbb{k}$ is infinite, then A has full rank over M if and only if $A(X)$ has full rank for some $X \in (\mathbb{k}^{N \times N})^m$, where $N \in \mathbb{N}$ is sufficiently large (and can be estimated using the number of operations in A and [DM17, Proposition 1.12]).

Let L be a skew subfield of M for which $d = \dim M_L$ is finite. Below we present an algorithm that finds a set of generators with at most $d^2(m - 1) + d$ elements. The algorithm finds a basis $\mathcal{B}$ of M as a right L -module with $1 \in \mathcal{B}$. Such a basis has $d = \dim M_L$ elements. If $\mathcal{B} = \{b_1, \dots, b_d\}$ with $b_1 = 1$, then the algorithm finds $d \times d$ matrices $X_1, \dots, X_m$ with entries $(X_\ell)_{i,j} \in L$ that satisfy $x_\ell b_j = \sum_i b_i (X_\ell)_{i,j}$. Because of the way the basis $\mathcal{B}$ is constructed in the algorithm, some of the coefficients $(X_\ell)_{i,j}$ will be 0 or 1. Let $\mathcal{L}$ be the set of all elements $(X_\ell)_{i,j}$ distinct from 0 and 1; then, $\mathcal{L}$ generates the skew field L .

The input of Algorithm 6.1 are the field $\mathbb{k}$, the number $m \in \mathbb{N}$ determining M , and the intermediate skew field L . The latter is given indirectly; we assume there is an algorithm for $w, b_1, \dots, b_r \in M$ that finds coefficients $c_1, \dots, c_r \in L$ with $w = b_1 c_1 + \dots + b_r c_r$ or decides that such coefficients do not exist. Note that the coefficients are unique if $b_1, \dots, b_r$ are independent as right L -module generators.

During the execution of Algorithm 6.1, $\mathcal{B}$ is always a set of elements of M that are linearly independent over L . This set consists of words in $x_1, \dots, x_m$. If $\mathcal{B} = \{b_1, \dots, b_r\}$ with $b_1 = 1$, then for every $i > 1$, b_i equals $x_\ell b_j$ for some ℓ and some $j < i$; therefore, $(X_\ell)_{i,j} = 1$ and $(X_\ell)_{t,j} = 0$ for $t \neq i$. At termination, $\mathcal{B}$ is a basis of M as a right L -module. At least $d(d - 1)$ entries $(X_\ell)_{i,j}$ are equal to 0 or 1. This implies that $\mathcal{L}$ has at most $d^2 m - d(d - 1) = d^2(m - 1) + d$ elements at termination. During execution, $\mathcal{T}$ consists of monomials that have to be checked whether they lie in the L -module generated by $\mathcal{B}$.

Algorithm 6.1.

- 1: $\mathcal{T} = \{1\}$
- 2: $\mathcal{L} = \{\}$
- 3: $\mathcal{B} = \{\}$
- 4: **while** $\mathcal{T} \neq \{\}$ **do**

```

5:   choose  $w \in \mathcal{T}$ 
6:    $\mathcal{T} = \mathcal{T} \setminus \{w\}$ 
7:   if  $w \in \mathcal{B}L$  then
8:     write  $w = \sum_{b \in \mathcal{B}} bc_b$  with  $c_b \in L$  for all  $b \in \mathcal{B}$ 
9:      $\mathcal{L} = \mathcal{L} \cup \{c_b : b \in \mathcal{B}\}$ 
10:  else
11:     $\mathcal{B} = \mathcal{B} \cup \{w\}$ 
12:     $\mathcal{T} = \mathcal{T} \cup \{x_1w, x_2w, \dots, x_mw\}$ 
13:  end if
14: end while

```

The correctness and termination of Algorithm 6.1 follows from the proofs of Proposition 3.2 and Theorem 3.3. Let us concretize lines 7–8 in the case where $L = M^G$ for a finite group G . Given $b_1, \dots, b_\ell \in M$ with $\ell \leq |G|$, let us call the $|G| \times \ell$ matrix over M

$$(b_j^g)_{g \in G, 1 \leq j \leq \ell}$$

the G -matrix of $b_1, \dots, b_\ell$ (determined up to ordering of G). Similarly to Lemma 4.3, we see that $b_1, \dots, b_\ell \in M$ are linearly independent over L if and only if the G -matrix of $b_1, \dots, b_\ell$ has full rank over M . Then, the equation $w = \sum_{b \in \mathcal{B}} bc_b$ for known $w \in \mathcal{T}$, $b \in \mathcal{B}$ and unknown $c_b \in L$ in line 8 is equivalent to

$$(30) \quad (w^g)_{g \in G} = (b_\ell^g)_{g \in G, b \in \mathcal{B}} \cdot (c_b)_{b \in \mathcal{B}}.$$

Note that (30) is solvable for $c_b \in L$ if and only if it is solvable for $c_b \in M$, since the G -matrix of $\mathcal{B}$ has full rank. Thus, (30) is an overdetermined right-linear system of equations over M , and can be solved via Gaussian elimination (using rational operations and identity testing in M).

Now let G be a finite group acting faithfully and linearly on $V = \text{span}_{\mathbb{k}}\{x_1, \dots, x_m\}$, and $\text{char } \mathbb{k} \nmid |G|$. The skew field $L = M^G$ is free of rank $|G|(m-1) + 1$ by Theorem 4.8. In this setup, the key advantage in comparison with Theorem 3.3 is the existence of a G -stable subspace $W \subseteq R$ such that $M = WL$, $\dim W = |G|$ and $1 \in W \subseteq \mathbb{k} + VW$ (Proposition 3.7 and Section 4.3). Below we present an algorithm for finding a basis $\mathcal{B}$ of such W , consisting of homogeneous elements in R , and a set of free generators $\mathcal{L}$ of L . The input of Algorithm 6.2 below are the field $\mathbb{k}$, the number $m \in \mathbb{N}$ determining M , and the linear action of G on V (e.g., given as a collection of $|G|$ $m \times m$ matrices over $\mathbb{k}$).

Algorithm 6.2.

```

1:  $\mathcal{T} = \{1\}$ 
2:  $\mathcal{L} = \{\}$ 
3:  $\mathcal{B} = \{\}$ 
4: while  $\mathcal{T} \neq \{\}$  do
5:   extract a basis of  $\text{span}_{\mathbb{k}}\{x_iw : 1 \leq i \leq m, w \in \mathcal{T}\}$  as a disjoint union  $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_r$ 
   such that  $\text{span}_{\mathbb{k}} \mathcal{B}_j$  is an irreducible  $G$ -space for  $j = 1, \dots, r$ 
6:    $\mathcal{T} = \{\}$ 
7:   for  $j = 1, \dots, r$  do

```

```

8:      choose one  $w \in \mathcal{B}_j$ 
9:      if  $w \in \mathcal{B}L$  then
10:         write  $w = \sum_{b \in \mathcal{B}} bc_b$  with  $c_b \in L$  for all  $b \in \mathcal{B}$ 
11:          $\mathcal{L} = \mathcal{L} \cup \{c_b : b \in \mathcal{B}\}$ 
12:      else
13:          $\mathcal{B} = \mathcal{B} \cup \mathcal{B}_j$ 
14:          $\mathcal{T} = \mathcal{T} \cup \mathcal{B}_j$ 
15:      end if
16:  end for
17: end while
18: replace  $\mathcal{L}$  by its maximal  $\mathbb{k}$ -linearly independent subset

```

The correctness and termination of Algorithm 6.2 is established as in the case of Algorithm 6.1, with modifications according to the proof of Proposition 3.7. Let us highlight the main differences. First, $\text{span}_{\mathbb{k}}\{x_i w : 1 \leq i \leq m, w \in \mathcal{T}\}$ in line 5 is a G -space, since it is the tensor product of G -spaces V and $\text{span}_{\mathbb{k}} \mathcal{T}$ (and the latter is a G -space inductively). For finding its decomposition into irreducible G -spaces and extracting their bases, see [BR90, Theorem 1.2] and [HBO'B05, Section 7.4]. Second, lines 9–11 are applied to a single element of $w \in \mathcal{B}_j$; this is sufficient according to the system (30) since the $\mathbb{k}$ -span of $\mathcal{B}$ is G -stable. Third, Theorem 4.8 guarantees that line 18 results in a set of free generators of L ; let us thus comment on testing $\mathbb{k}$ -linear dependence in M . By [R80, Theorem 7.6.16], linear dependence of $r_1, \dots, r_\ell \in M$ is equivalent to vanishing of the Capelli polynomial in $r_1, \dots, r_\ell$ and $\ell - 1$ auxiliary variables, and thus reduces to rational identity testing as in the beginning of the section. Alternatively, $r_1, \dots, r_\ell$ are linearly dependent if and only if their evaluations are linearly dependent on all sufficiently large matrix tuples [V18, Theorem 6.5].

REFERENCES

- [AMY18] J. Agler, J. E. McCarthy, N. J. Young: *Non-commutative manifolds, the free square root and symmetric functions in two non-commuting variables*, Trans. London Math. Soc., 5 (2018) 132–183.
- [AY14] J. Agler, N. J. Young: *Symmetric functions of two noncommuting variables*, J. Funct. Anal. 266 (2014) 5709–5732.
- [A66] S. A. Amitsur: *Rational identities and applications to algebra and geometry*, J. Algebra 3 (1966) 304–359.
- [AD06] J. Alev, F. Dumas: *Opérateurs différentiels invariants et problème de Noether*, Studies in Lie theory, 21–50, Progr. Math. 243, Birkhäuser Boston, Inc., Boston MA, 2006.
- [AM72] M. Artin, D. Mumford: *Some elementary examples of unirational varieties which are not rational*, Proc. Lond. Math. Soc. 25 (1972) 75–95.
- [BR90] L. Babai, L. Rónyai: *Computing irreducible representations of finite groups*, Math. Comp. 55 (1990) 705–722.
- [BGM05] J. A. Ball, G. Groenewald, T. Malakorn: *Structured noncommutative multidimensional linear systems*, SIAM J. Control Optim. 44 (2005) 1474–1528.
- [BB00] L. Bayle, A. Beauville: *Birational involutions of $\mathbb{P}^2$* , Asian J. Math. 4 (2000) 11–17.
- [B-KRZ23] A. Belov-Kanel, F. Razavinia, W. Zhang: *Centralizers in free associative algebras and generic matrices*, Mediterr. J. Math. 20 (2023) paper no. 85.
- [B69] G. M. Bergman: *Centralizers in free associative algebras*, Trans. Amer. Math. Soc. 137 (1969) 327–344.

- [BR11] J. Berstel, C. Reutenauer: *Noncommutative rational series with applications*, Encyclopedia Math. Appl. 137, Cambridge University Press, Cambridge, 2011.
- [CG72] C. H. Clemens, P. A. Griffiths: *The intermediate Jacobian of the cubic threefold*, Ann. Math. 95 (1972) 281–356.
- [C77] P. M. Cohn: *Skew field constructions*, London Math. Soc. Lecture Series 27, Cambridge University Press, 1977.
- [C78] P. M. Cohn: *Centralisateurs dans les corps libres*, Séries formelles en variables non commutatives et applications, 45–54, École Nationale Supérieure de Techniques Avancées, Paris, 1978.
- [C95] P. M. Cohn: *Skew fields. Theory of general division rings*, Encyclopedia Math. Appl. 57, Cambridge University Press, Cambridge, 1995.
- [C06] P. M. Cohn: *Free ideal rings and localization in general rings*, New Mathematical Monographs 3, Cambridge University Press, Cambridge, 2006.
- [CR99] P. M. Cohn, C. Reutenauer: *On the construction of the free field*, Internat. J. Algebra Comput. 9 (1999) 307–323.
- [CMMPY24] B. Collins, T. Mai, A. Miyagawa, F. Parraud, S. Yin: *Convergence for noncommutative rational functions evaluated in random matrices*, Math. Ann. 388 (2024) 543–574.
- [CPT-D18] D. Cushing, J. E. Pascoe, R. Tully-Doyle: *Free functions with symmetry*, Math. Z. 289 (2018) 837–857.
- [DK02] H. Derksen, G. Kemper: *Computational invariant theory*, Encyclopaedia Math. Sci. 130, Springer-Verlag, Berlin, 2002.
- [DM17] H. Derksen, V. Makam: *Polynomial degree bounds for matrix semi-invariants*, Adv. Math. 310 (2017) 44–63.
- [DF82] W. Dicks, E. Formanek: *Poincaré series and a problem of S. Montgomery*, Lin. Multilin. Algebra 12 (1982) 21–30.
- [D95] A. W. M. Dress: *Basic noncommutative Galois theory*, Adv. Math. 110 (1995) 141–173.
- [FS20] V. Futorny, J. Schwarz: *Noncommutative Noether’s problem vs classic Noether’s problem*, Math. Z. 295 (2020) 1323–1335.
- [GGOW16] A. Garg, L. Gurvits, R. Oliveira, A. Wigderson: *A deterministic polynomial time algorithm for non-commutative rational identity testing*, 57th Annual IEEE Symposium on Foundations of Computer Science, 109–117, IEEE Computer Society, Los Alamitos CA, 2016.
- [GKLLRT95] I. M. Gelfand, D. Krob, A. Lascoux, B. Leclerc, V. S. Retakh, J.-Y. Thibon: *Noncommutative symmetric functions*, Adv. Math. 112 (1995) 218–348.
- [GG06] W. L. Gan, V. Ginzburg: *Almost-commuting variety, D-modules, and Cherednik algebras*, IMRP Int. Math. Res. Pap. (2006) 26439, 1–54.
- [H77] R. Hartshorne: *Algebraic geometry*, Grad. Texts in Math. 52, Springer-Verlag, New York-Heidelberg, 1977.
- [HMS18] J. W. Helton, T. Mai, R. Speicher: *Applications of realizations (aka linearizations) to free probability*, J. Funct. Anal. 274 (2018) 1–79.
- [HBO’B05] D. F. Holt, B. Eick, E. A. O’Brien: *Handbook of computational group theory*, Discrete Math. Appl., Chapman & Hall/CRC Press, Boca Raton FL, 2005.
- [HW14] P. Hrubeš, A. Wigderson, *Non-commutative arithmetic circuits with division*, in: Proceedings of the 5th conference on Innovations in theoretical computer science, 2014, 49–66.
- [IQS18] G. Ivanyos, Y. Qiao, K. V. Subrahmanyam: *Constructive non-commutative rank computation is in deterministic polynomial time*, Comput. Complex. 27 (2018) 561–593.
- [K-VV12] D. S. Kalyuzhnyi-Verbovetskiĭ, V. Vinnikov: *Noncommutative rational functions, their difference-differential calculus and realizations*, Multidimens. Syst. Signal Process. 23 (2012) 49–77.
- [K-VV14] D. S. Kalyuzhnyi-Verbovetskiĭ, V. Vinnikov: *Foundations of free noncommutative function theory*, Mathematical Surveys and Monographs 199, American Mathematical Society, Providence RI, 2014.

- [K84] V. K. Kharchenko: *Noncommutative invariants of finite groups and Noetherian varieties*, J. Pure Appl. Algebra 31 (1984) 83–90.
- [KPPV20] I. Klep, J. E. Pascoe, G. Podlogar, J. Volčič: *Noncommutative rational functions invariant under the action of a finite solvable group*, J. Math. Anal. Appl. 490 (2020) 124341.
- [L69] J. Lewin: *Free modules over free algebras and free group algebras: the Schreier technique*, Trans. Amer. Math. Soc. 145 (1969) 455–465.
- [L74] J. Lewin: *Fields of fractions for group algebras of free groups*, Trans. Amer. Math. Soc. 192 (1974) 339–346.
- [L02] M. Lothaire: *Centralizers of Noncommutative Series and Polynomials*, in Algebraic Combinatorics on Words, 312–329, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2002.
- [M86^a] J. S. Milne: *Abelian varieties*, in Arithmetic Geometry (Storrs CT, 1984), 103–150, Springer-Verlag, New York, 1986.
- [M86^b] J. S. Milne: *Jacobian varieties*, in Arithmetic Geometry (Storrs CT, 1984), 167–212, Springer-Verlag, New York, 1986.
- [N17] E. Noether: *Gleichungen mit vorgeschriebener Gruppe* Math. Annalen 78 (1917) 221–229.
- [O99] P. J. Olver: *Classical invariant theory*, London Math. Soc. Stud. Texts 44, Cambridge University Press, Cambridge, 1999.
- [P23] G. Podlogar: *Finite solvable groups with a rational skew-field of noncommutative real rational invariants*, Comm. Algebra 51 (2023) 2268–2292.
- [PV94] V. Popov, E. Vinberg: *Invariant theory*, in Algebraic geometry IV, Encyclopaedia Math. Sci. 55, Springer-Verlag, Berlin, 1994.
- [RS06] M. H. Rosas, B. E. Sagan: *Symmetric functions in noncommuting variables*, Trans. Amer. Math. Soc. 358 (2006) 215–232.
- [R80] L. H. Rowen: *Polynomial identities in ring theory*, Pure Appl. Math. 84, Academic Press, Inc., New York-London, 1980.
- [S84] D. J. Saltman: *Noether’s problem over an algebraically closed field*, Invent. Math. 77 (1984) 71–84.
- [S85^a] A. H. Schofield: *Artin’s problem for skew field extensions*, Math. Proc. Camb. Philos. Soc. 97 (1985) 1–6.
- [S85^b] A. H. Schofield: *Representations of rings over skew fields*, London Math. Soc. Lecture Notes Series 92, Cambridge University Press, Cambridge, 1985.
- [S69] R. G. Swan: *Invariant rational functions and a problem of Steenrod*, Invent. Math. 7 (1969) 148–158.
- [S83] R. G. Swan: *Noether’s problem in Galois theory*, in Emmy Noether in Bryn Mawr, 21–40, Springer-Verlag, New York-Berlin, 1983.
- [V18] J. Volčič: *Matrix coefficient realization theory of noncommutative rational functions*, J. Algebra 499 (2018) 397–437.
- [W36] M. C. Wolf: *Symmetric functions of noncommuting elements*, Duke Math. J. 2 (1936) 626–637.

DEPARTMENT OF MATHEMATICS, NORTHEASTERN UNIVERSITY, MASSACHUSETTS, USA

Email address: ha.derksen@northeastern.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF AUCKLAND, NEW ZEALAND

Email address: jurij.volcic@auckland.ac.nz