Inverse problem in difference Galois theory

Detailed research manuscript

20 September 2026

Abstract

Let C be an algebraically closed field of characteristic zero and let $K = C(x)$ with $\sigma(x) = x + 1$. We give an algebraic construction which, for a closed subgroup $G \subseteq \mathrm{GL}_n(C)$ such that the quotient G/G° is cyclic, produces a system $\sigma Y = AY$ whose Picard–Vessiot group is the prescribed copy of G. Here G° denotes the identity component of G.

The principal criterion is the following. Suppose that $A = h + O(x^{-2})$, where h is semisimple, and that the finite poles of A and A^{-1} form a set S with $1 \notin \mathrm{span}_{\mathbb{Q}} S$. In every algebraic representation ρ, a rational difference-invariant line then has a constant generator. Indeed, choose a primitive polynomial generator $v = (v_i)$, whose coordinates have no common nonconstant factor, and write $v(x+1) = c(x)\rho(A(x))v(x)$ with $c \in C(x)^*$. Let $d = \max_{v_i \neq 0} \deg v_i$ be the degree of v, and let $k_s = \mathrm{ord}_{x=s}(c) \in \mathbb{Z}$ be the order of vanishing of the multiplier c at s (negative for a pole). All finite zeros and poles of c lie in S. Comparison at infinity gives $d + \sum_{s \in S} k_s s = 0$; the hypothesis $1 \notin \mathrm{span}_{\mathbb{Q}} S$ therefore forces $d = 0$. Chevalley's theorem and a descent argument in the total quotient ring identify the Galois group with the group generated by the coefficient values. Rational interpolation and a purely algebraic dilation supply all hypotheses.

The construction builds on the coefficient-group and interpolation methods of van der Put and Singer, together with classical Picard–Vessiot descent and Chevalley's line-stabilizer theorem. The additional argument developed here is the uniform invariant-line criterion obtained from the displayed degree identity and its application after arithmetic dilation. Precise attributions and the scope of the earlier inverse results are given below.

Contents

1 Statement, conventions, and dependencies 3

2 Finite singularities and change of representation 4

3 Rigidity of rational difference-invariant lines 5

4 Picard–Vessiot foundations with zero divisors 7

5 Chevalley detection and the coefficient-group criterion 11

6 An explicit rational curve generating the identity component 12

7 Arithmetic dilation and realization of the full group 15

8 Explicit realizations 17

9 Counterexamples and sharpness of the hypotheses 18

10 An alternative interpolation construction 19

A Earlier contributions and the scope of the present argument 20

1 Statement, conventions, and dependencies

Throughout, C is algebraically closed of characteristic zero, $K = C(x)$, and $\sigma(f(x)) = f(x+1)$. The prime field is identified with $\mathbb{Q} \subset C$. In particular $K^\sigma = C$: a shift-invariant rational function cannot have a finite pole, since such a pole would produce infinitely many integer translates; a nonconstant polynomial cannot be shift-invariant, since its difference has a nonzero leading coefficient in characteristic zero.

An algebraic group means a reduced closed subgroup of a general linear group over C. We write G° for the connected component of G containing the identity. Such groups and their closed subgroups are smooth in characteristic zero. A rational representation of G means a *regular homomorphism of algebraic groups* $\rho : G \to \mathrm{GL}(V)$ on a finite-dimensional C-vector space; it does not mean a partially defined rational map. We use the same symbol for the induced map on points over any commutative C-algebra.

Theorem 1.1 (Inverse realization in the prescribed representation)**.** *Let $G \subseteq \mathrm{GL}_n(C)$, $n \geq 1$, be a closed algebraic subgroup. Assume that G/G° is cyclic. There exist $A(x) \in G(K)$, a Picard–Vessiot ring R for $\sigma Y = AY$, and a fundamental matrix $Z \in G(R)$ such that*

$$\mathrm{Aut}_\sigma(R/K) \longrightarrow \mathrm{GL}_n(C), \qquad \tau \longmapsto Z^{-1}\tau(Z)$$

has image exactly $G(C)$, and identifies the algebraic Galois group with the given subgroup G.

The theorem is the sufficient direction of the usual inverse problem. No necessity statement is required in its proof. The field C may be $\overline{\mathbb{Q}}$; no assumption of uncountability or analytic topology is made. All expansions at infinity are formal expansions in $u = x^{-1}$.

For reference, the proof uses these classical foundations:

(i) a finite-type, simple difference K-algebra has constants C;

(ii) a Picard–Vessiot ring in characteristic zero is the coordinate ring of a torsor for its algebraic Galois group;

(iii) multiplicative Jordan decomposition is internal to an algebraic group and is preserved by algebraic representations;

(iv) a semisimple element of a connected linear algebraic group over C belongs to a torus, and every torus over C is split.

Precise sources for (i) and (ii) are [1, Lemma 1.8 and Theorem 1.13]. For (iii) and (iv), see [2, Theorem 9.18 and Corollary 17.36]. We prove the required constant lemma below, give the consequences of the torsor theorem explicitly, and prove all subsequent deductions specific to the inverse problem. These foundations contain no inverse realization result. In particular no analytic connection-matrix realization or specialization theorem is used.

1.1 Origins and contribution of the argument

The inverse problem in Theorem 1.1 is the conjecture formulated in Chapter 3 of van der Put and Singer's monograph [1]; it is not a newly formulated problem. Their Proposition 1.20 proves that G/G° is cyclic whenever G is the Galois group of a system over $C(x)$. Their Proposition 3.2(1) introduces the coefficient group T_A, and Proposition 3.3(2) constructs $A \in G(C(x))$ with $T_A = G$ by interpolating a rational curve through generating points and multiplying by an element whose image generates G/G°. These are direct antecedents of the construction used here. They establish coefficient-group generation, which by itself does not establish the Galois group.

Our approach to identifying the Galois group is to detect a hypothetical proper PV subgroup by a line in an auxiliary representation. The subgroup-to-line step is Chevalley's classical theorem; the passage from that line to a rational difference-invariant line is standard PV descent, here written explicitly for rings with zero divisors. Rational invariant lines and degree obstructions already occur in [1, Lemma 3.9], and pole-orbit obstructions occur in [1, Lemma 3.4]. The specific step proved in Theorem 3.1 is that the coefficient identity

$$d + \sum_{s \in S(A)} k_s s = 0$$

forces every such rational line to have a constant generator, in every algebraic representation, under one common hypothesis on A. Theorem 5.2 combines this step with classical descent and Chevalley's theorem to obtain equality with T_A.

The ingredients of the final construction also have distinct origins. Jordan decomposition and one-parameter subgroups are standard algebraic-group theory. Rational interpolation through generators is the method of [1, Proposition 3.3(2)]. Interpolation together with high-order normalization at distinguished points already appears in their analytic construction [1, proof of Theorem 8.11]. Here we impose $A(x) = h + O(x^{-2})$ on the coefficient matrix itself and then dilate its finite singularities so that the degree identity is an obstruction. This combination, including its precise uniform hypotheses, is proved in the present text. The attributions describe the dependence of the argument and its identifiable antecedents; they do not assert bibliographical priority for the criterion or the resulting synthesis.

2 Finite singularities and change of representation

Definition 2.1. For $A \in \mathrm{GL}_n(K)$, let

$$S(A) = \{s \in C : \text{some entry of } A \text{ or } A^{-1} \text{ has a pole at } s\}.$$

Let T_A be the smallest closed C-subgroup of GL_n for which $A \in T_A(K)$. Equivalently, T_A is the algebraic subgroup generated by the values $A(a)$ for $a \in C \setminus S(A)$.

The definition and the value-generation characterization of T_A are [1, Proposition 3.2(1)]. We recall the short proof. To verify the equivalence, suppose a closed subgroup T contains all these values. For $f \in I(T) \subset C[X_{ij}, \det(X)^{-1}]$, the rational function $f(A(x))$ vanishes at infinitely many points and hence is zero. Thus $A \in T(K)$. The converse follows by evaluation of the same equations. The closure of a subgroup is an algebraic subgroup, so the indicated smallest group exists. The poles of A^{-1} are indispensable in this definition.

Lemma 2.2 (Functorial control of singularities and the first jet)**.** *Let $A \in G(K)$ and let $\rho : G \to \mathrm{GL}(V)$ be an algebraic representation. Then*

$$S(\rho(A)) \subseteq S(A).$$

If $A(x) = h + O(x^{-2})$ with $h \in G(C)$, then

$$\rho(A(x)) = \rho(h) + O(x^{-2}).$$

If h is semisimple, so is $\rho(h)$.

Proof. For $s \notin S(A)$ set $\mathcal{O}_s = C[x]_{(x-s)}$. Both A and A^{-1} have entries in $\mathcal{O}_s$, so $A \in \mathrm{GL}_n(\mathcal{O}_s)$. The defining equations of G vanish on A in K and therefore in $\mathcal{O}_s$. Consequently $A \in G(\mathcal{O}_s)$. Applying the morphism ρ gives $\rho(A) \in \mathrm{GL}(V)(\mathcal{O}_s)$, including regularity of its inverse.

At infinity, A and h are $G(C[[u]])$-points with identical reductions in $G(C[[u]]/(u^2))$. A morphism of schemes preserves this equality after reduction, giving the second assertion. The third assertion follows from functoriality of Jordan decomposition. Alternatively, the closure of the cyclic group generated by a semisimple h is a subgroup of a diagonal torus after conjugation; it is diagonalizable, so every representation of it is a sum of character spaces. □

Lemma 2.3 (Local primitivity)**.** *Let $\mathcal{O}$ be a discrete valuation ring with fraction field F and valuation ν. For a nonzero vector $w \in F^m$, put $\nu(w) = \min_i \nu(w_i)$, with $\nu(0) = +\infty$. If $B \in \mathrm{GL}_m(\mathcal{O})$, then $\nu(Bw) = \nu(w)$.*

Every K-line in K^m has a representative $v \in C[x]^m$ whose coordinates have greatest common divisor 1*. Such a representative satisfies $\mathrm{ord}_s(v) = \mathrm{ord}_s(\sigma v) = 0$ at every $s \in C$, and is unique up to a nonzero scalar in C.*

Proof. Integrality of the matrix entries gives $\nu(Bw) \geq \nu(w)$. Apply the same inequality to B^{-1} to obtain the reverse inequality.

For the second assertion, clear denominators and divide by the greatest common divisor in the principal ideal domain $C[x]$. Coprimeness is equivalent to the coordinates generating the unit ideal, and hence to their not all vanishing at any point of the algebraically closed field C. Translation preserves the unit ideal. If two primitive representatives differ by $f \in K^*$, then at every finite point the minimum-valuation identity gives $\mathrm{ord}_s(f) = 0$. A rational function with no finite zero or pole is constant, which proves uniqueness. □

3 Rigidity of rational difference-invariant lines

The proof below combines finite-point valuations with comparison of two coefficients at infinity. Its rational-solution viewpoint has precedents in the pole and degree calculations of [1, Lemmas 3.4 and 3.9]. A related general method for bounding polynomial-solution degrees by an indicial polynomial is described in [3, Section 4.1, Definition 4.12, Remark 4.13, and Lemma 4.14]. That is a methodological comparison: those results do not state the representation-uniform rigidity theorem below. Here the missing x^{-1} term and semisimplicity turn the degree comparison into an exact identity involving the singularity locations.

Throughout this section, V is an abstract finite-dimensional C-vector space, and $\rho : G \to \mathrm{GL}(V)$ is an algebraic representation on it. The space V is not defined as a space of solutions of a difference equation. Set $V_K = K \otimes_C V$ and identify V with its image under $v \mapsto 1 \otimes v$. The automorphism σ of K induces an additive bijection on V_K, also denoted by σ, by the rule

$$\sigma\Big(\sum_i f_i \otimes v_i\Big) = \sum_i \sigma(f_i) \otimes v_i = \sum_i f_i(x+1) \otimes v_i.$$

This definition is independent of the tensor expression: since σ fixes C, it respects the relations $fa \otimes v = f \otimes av$ for $a \in C$. It is σ-semilinear, meaning that $\sigma(fu) = \sigma(f)\sigma(u)$ for $f \in K$ and $u \in V_K$, and fixes every vector $1 \otimes v$ with $v \in V$. In a C-basis $e_1, \ldots, e_m$ of V, this says

$$\sigma\Big(\sum_{i=1}^m f_i(x) e_i\Big) = \sum_{i=1}^m f_i(x+1) e_i, \qquad f_i \in K.$$

Since $K^\sigma = C$, the fixed vectors of V_K are exactly the embedded copy of V. Thus a *constant vector* means an element of this copy; equivalently, its coordinates in any C-basis of V belong to C.

The notation $\rho(A)$ denotes the invertible K-linear map on V_K obtained by evaluating the scalar extension of ρ at $A \in G(K)$. The difference structure associated with A and ρ is the

semilinear automorphism $\Phi_\rho = \rho(A)^{-1}\sigma$ of V_K. We call a K-line $L \subset V_K$ difference-invariant if $\Phi_\rho(L) = L$. Equivalently, for any nonzero generator v there is $c \in K^*$ such that

$$\sigma(v) = c\rho(A)v. \tag{3.1}$$

Replacing v by fv, $f \in K^*$, replaces c by $c\sigma(f)/f$.

Theorem 3.1 (Invariant-line rigidity)**.** *Suppose that $A \in G(K)$ satisfies*

$$A(x) = h + O(x^{-2}), \qquad h \in G(C) \text{ semisimple}, \qquad 1 \notin \operatorname{span}_{\mathbb{Q}} S(A). \tag{3.2}$$

For every finite-dimensional algebraic representation ρ of G, each difference-invariant K-line in $K \otimes_C V$ is the scalar extension of a C-line.

Proof. Choose a C-basis of V, put $m = \dim_C V$, and identify $K \otimes_C V$ with K^m. By Lemma 2.3, the line has a primitive polynomial generator

$$v = (v_1, \dots, v_m)^{\mathsf{T}} \in C[x]^m, \qquad \gcd(v_1, \dots, v_m) = 1.$$

Rescale the multiplier c so that (3.1) holds for this generator. For $s \in C$ write $\nu_s(f) = \operatorname{ord}_{x=s}(f)$, normalized by $\nu_s(x - s) = 1$, and put $\nu_s(0) = +\infty$. For a nonzero vector $w = (w_i) \in K^m$ define

$$\nu_s(w) := \min_{1 \le i \le m} \nu_s(w_i).$$

Thus $\nu_s(w) = 0$ for $w \in \mathcal{O}_s^m$ precisely when at least one coordinate is a unit in the local ring $\mathcal{O}_s = C[x]_{(x-s)}$.

Primitivity gives polynomials $a_1, \dots, a_m \in C[x]$ with

$$\sum_{i=1}^{m} a_i(x)v_i(x) = 1, \qquad \sum_{i=1}^{m} a_i(x+1)v_i(x+1) = 1.$$

At every $s \in C$, the coordinates of v and of $\sigma v = (v_i(x+1))_i$ are integral in $\mathcal{O}_s$ and cannot all belong to its maximal ideal. Consequently

$$\nu_s(v) = 0, \qquad \nu_s(\sigma v) = 0 \quad (s \in C). \tag{3.3}$$

Equivalently, the second equality is $\min_i \operatorname{ord}_{x=s+1}(v_i) = 0$. Individual coordinates may vanish at s; it is their minimum valuation that is zero.

Now put $S = S(A)$ and fix $s \notin S$. By Lemma 2.2, the matrix $B = \rho(A)$ and its inverse have entries in $\mathcal{O}_s$. For any $0 \neq w \in K^m$, the valuation inequality for a sum gives, for each i,

$$\nu_s\big((Bw)_i\big) = \nu_s\Big(\sum_{j=1}^{m} B_{ij}w_j\Big) \ge \min_j\big(\nu_s(B_{ij}) + \nu_s(w_j)\big) \ge \nu_s(w).$$

Taking the minimum over i yields $\nu_s(Bw) \ge \nu_s(w)$. Applying the same inequality to B^{-1} and Bw gives

$$\nu_s(w) = \nu_s\big(B^{-1}(Bw)\big) \ge \nu_s(Bw), \qquad \text{hence} \qquad \nu_s(Bw) = \nu_s(w).$$

In particular $\nu_s(Bv) = 0$. Moreover, for any $a \in K^*$,

$$\nu_s(aw) = \min_i\big(\nu_s(a) + \nu_s(w_i)\big) = \nu_s(a) + \nu_s(w).$$

Applying this scalar rule to the vector identity (3.1), and using (3.3), proves explicitly that

$$0 = \nu_s(\sigma v) = \nu_s(cBv) = \nu_s(c) + \nu_s(Bv) = \nu_s(c) \qquad (s \notin S). \tag{3.4}$$

Thus every finite zero or pole of c belongs to S. Since C is algebraically closed, factorization of rational functions yields

$$c(x) = \gamma \prod_{s\in S} (x-s)^{k_s}, \qquad \gamma \in C^*, \quad k_s \in \mathbb{Z}. \tag{3.5}$$

Let $d = \max_i \deg v_i \geq 0$ and write

$$v(x) = x^d\big(v_d + x^{-1}v_{d-1} + O(x^{-2})\big), \qquad v_d \neq 0.$$

For $d = 0$ set $v_{-1} = 0$. Put $e = \sum_s k_s$. The highest powers of x on the two sides of (3.1) are d and $d+e$. The coefficient on the right is nonzero, since $\gamma \neq 0$ and $\rho(h)$ is invertible. It follows that

$$e = \sum_s k_s = 0. \tag{3.6}$$

Set $q = \sum_s k_s s$ and $M = \gamma\rho(h)$. Factoring out the powers of x in (3.5) and expanding formally, including for negative integers k_s, gives

$$c(x) = \gamma(1 - qx^{-1} + O(x^{-2})).$$

Consequently

$$\begin{aligned} v(x+1) &= x^d\big(v_d + x^{-1}(dv_d + v_{d-1}) + O(x^{-2})\big), \\ c\rho(A)v &= x^d\big(Mv_d + x^{-1}(Mv_{d-1} - qMv_d) + O(x^{-2})\big). \end{aligned}$$

Equality of coefficients gives

$$Mv_d = v_d, \qquad (d+q)v_d = (M-I)v_{d-1}. \tag{3.7}$$

The matrix M is semisimple by Lemma 2.2. Its 1-eigenspace is therefore disjoint from $\mathrm{im}(M-I)$. The two sides of the second identity in (3.7) belong to these two spaces. As $v_d \neq 0$, we obtain

$$\boxed{d + \sum_{s\in S} k_s s = 0.} \tag{3.8}$$

If $d > 0$, division by the nonzero integer d would put 1 in $\mathrm{span}_{\mathbb{Q}} S$. Thus $d = 0$ and v is a nonzero constant vector. □

Remark 3.2 (Uniformity and the exact conclusion)**.** The conditions on A are chosen once and do not depend on ρ. All representations have the same upper bound $S(A)$ on their finite singularities and inherit the same vanishing first jet. The conclusion is constancy of the *line*, not of c. The integers k_s need not vanish individually. For a constant representative v_0, equation (3.1) says that $\rho(A)$ preserves Kv_0, equivalently $A \in \mathrm{Stab}_G(Cv_0)(K)$; it need not fix v_0.

Remark 3.3 (A translation-invariant weakening)**.** For nonempty S one can replace the last condition in (3.2) by

$$1 \notin \mathrm{span}_{\mathbb{Q}}\{s - s_0 : s \in S\}, \qquad s_0 \in S.$$

Indeed, (3.6) implies $\sum_s k_s s = \sum_s k_s(s - s_0)$. The condition is independent of s_0. Equivalently, the group $\{\sum_s k_s s : k_s \in \mathbb{Z},\ \sum_s k_s = 0\}$ meets $\mathbb{Z}$ only in 0: clearing denominators proves one implication and dividing by a nonzero integer proves the other. The stronger condition in (3.2) is sufficient for our construction.

4 Picard–Vessiot foundations with zero divisors

We include the details needed to descend a line without assuming that the PV ring is a domain or that the PV torsor has a K-rational point.

4.1 The constant lemma and a PV quotient of the coordinate ring

The next result is [1, Lemma 1.8]. Its proof follows their constructible-image argument, with the algebraicity and scalar-extension steps made explicit; neither the lemma nor its underlying argument is claimed as a new result.

Lemma 4.1 (Constants in a simple finite-type difference algebra)**.** *Let (k, σ) be a difference field with algebraically closed constants $C = k^\sigma$, and let R be a nonzero finitely generated k-algebra with an automorphism extending σ. If R has no nonzero proper difference ideal, then $R^\sigma = C$.*

Proof. The constants of R form a field: for a nonzero constant b, the ideal bR is a nonzero difference ideal, hence is R; its inverse is again constant. Suppose $b \in R^\sigma \setminus C$. Algebraic closedness of C implies that b is transcendental over C, and every $b - c$, $c \in C$, is a unit of R.

Let $\bar{k}$ be an algebraic closure of k. The nonempty affine scheme $\mathrm{Spec}(\bar{k} \otimes_k R)$ has finite type over $\bar{k}$. By Chevalley's constructibility theorem, the image of the regular function b in $\mathbb{A}^1_{\bar{k}}$ is constructible and contains no point of C, since $b - c$ is invertible for each $c \in C$. An infinite constructible subset of the affine line over an algebraically closed field is cofinite, and a cofinite subset cannot avoid the infinite field C. Hence the image is a finite set of closed points $\{\beta_1, \dots, \beta_s\}$. The element $\prod_j (b - \beta_j)$ lies in the nilradical, so its Nth power is zero for some N. Thus finitely many powers of b become linearly dependent over $\bar{k}$. Faithful flatness, applied to the kernel of $k^{d+1} \to R$ sending (a_i) to $\sum_i a_i b^i$ for a sufficiently large d, descends this dependence to k. Consequently b is algebraic over k. No extension of σ to $\bar{k}$ has been used.

The kernel of $k[T] \to R$, $T \mapsto b$, is therefore generated by a unique monic polynomial $P(T)$ of least positive degree. Since b is fixed by σ, applying σ to its coefficients gives another monic annihilating polynomial of the same degree. Uniqueness gives $\sigma(P) = P$, so $P \in C[T]$, a contradiction. □

The following is the standard maximal-difference-ideal construction of a PV ring, applied to $K[G]$ instead of $K[\mathrm{GL}_n]$; compare [1, Section 1.1 and Proposition 1.21(1)]. The coordinate-ring formulation also appears at the beginning of the unsigned note [5].

Proposition 4.2 (A fundamental matrix valued in the target group)**.** *For $A \in G(K)$ there is a PV ring R with $Z \in G(R)$ satisfying $\sigma Z = AZ$. Relative to this Z, its Galois group J is a closed subgroup of the given G.*

Proof. Put $\mathcal{S} = K \otimes_C C[G]$ and let X denote the universal matrix. On $\mathcal{S}$ define a semilinear map by $\sigma X = AX$ and by the given action on K. This preserves the equations of G: applying σ to their coefficients fixes them, and left multiplication by A is an automorphism of G_K. Its inverse restricts to σ^{-1} on K and sends

$$X \longmapsto \sigma^{-1}(A^{-1})X.$$

Thus it is an automorphism.

By Zorn's lemma choose a maximal proper ideal I with $\sigma(I) \subseteq I$. The ideal $\sigma^{-1}(I)$ is proper, is a difference ideal, and contains I, so maximality implies $\sigma^{-1}(I) = I$. The quotient $R = \mathcal{S}/I$ therefore inherits an automorphism and is difference simple. Its nilradical is a proper difference ideal, so it is zero. Also $K \to R$ is injective, because a proper ideal cannot meet K^*.

Let Z be the image of X. Then $Z \in G(R)$, $\sigma Z = AZ$, and

$$R = K[Z_{ij}, \det(Z)^{-1}], \qquad R^\sigma = C$$

by Lemma 4.1. These are the defining properties of a PV ring. In particular, the construction does not assume that $K[G]$ was already difference simple.

For $\tau \in \mathrm{Aut}_\sigma(R/K)$ put $g_\tau = Z^{-1}\tau(Z)$. Then

$$\sigma(g_\tau) = (AZ)^{-1}A\tau(Z) = g_\tau.$$

The entries of g_τ and its inverse lie in C. Moreover $Z, \tau(Z) \in G(R)$, so $g_\tau \in G(R)$. Since $C \hookrightarrow R$, the defining equations of G imply $g_\tau \in G(C)$. The standard PV group theorem gives a reduced algebraic group J with these C-points. Closedness and density of C-points imply $J \subseteq G$. □

4.2 The precise torsor input and total-quotient invariants

We use the PV torsor theorem in the following form. If R is a PV ring over K as above and J its algebraic group, the action induces an isomorphism

$$\theta : R \otimes_K R \xrightarrow{\sim} R \otimes_C C[J], \qquad \theta(a \otimes b) = (a \otimes 1)\delta(b), \tag{4.1}$$

where δ is the coaction for the right action $Z \mapsto Zg$. Equivalently, $\operatorname{Spec} R$ is a J_K-torsor. The separability hypothesis in [1, Theorem 1.13] holds: a reduced algebra of finite type over a characteristic-zero field is geometrically reduced. This theorem does not require R to be an integral domain.

The first two assertions below are [1, Corollary 1.15], and the third is [1, Lemma 1.28(1)]. We include the proofs to specify how invariance in the total quotient ring is used when R is not a domain.

Lemma 4.3 (Consequences of the torsor theorem)**.** *Let $Q(R)$ be the localization of R at its nonzerodivisors. Every automorphism of R preserves nonzerodivisors and therefore extends uniquely to $Q(R)$. Then*

(a) $R^{J(C)} = K$;

(b) *R has no nonzero proper ideal invariant under all $J(C)$;*

(c) $Q(R)^{J(C)} = K$.

Proof. We first explain why testing the C-points suffices. For any invariant ideal I, reduce $\delta(f)$ modulo I for $f \in I$. The resulting element of $(R/I) \otimes_C C[J]$ is a finite sum. Write its coefficients in a C-linearly independent finite set in R/I. Evaluating at each $g \in J(C)$ gives zero, so each coefficient function on the reduced group J vanishes on all C-points and is zero. Thus I is stable under the algebraic coaction, and remains so after field extension. The same reasoning applies to invariant elements.

After extending K to an algebraic closure $\bar{K}$, the torsor has a $\bar{K}$-point and hence is isomorphic to $J_{\bar{K}}$ with its right translation action. Its invariant regular functions are constants. If $f \in R^{J(C)}$, then $f \otimes 1$ is such a constant in $R \otimes_K \bar{K}$. A K-basis of R containing 1 shows that this is possible only when $f \in K$, proving (a).

Let $I \subset R$ be a nonzero proper invariant ideal. Faithful flatness ensures that $I \otimes_K \bar{K}$ is still nonzero and proper. Its zero set in $J_{\bar{K}}$ is nonempty and stable under all right translations, so is all of $J_{\bar{K}}$. Since $\bar{K}[J]$ is reduced, an ideal with that zero set is zero, a contradiction. This proves (b).

For (c), take $f \in Q(R)^{J(C)}$ and set

$$D_f = \{r \in R : rf \in R\}.$$

It is an ideal and contains a nonzerodivisor denominator of f, hence is nonzero. For $\tau \in J(C)$ and $r \in D_f$, $\tau(r)f = \tau(rf) \in R$, so D_f is invariant. By (b), $D_f = R$. Therefore $f \in R$ and (a) implies $f \in K$. □

4.3 Descending a semi-invariant line

The correspondence between algebraic representations and difference modules is part of classical PV theory; see [1, Theorem 1.32(4)]. The next lemma is an explicit form of its descent mechanism for a line. The choice of a common nonzerodivisor below makes that mechanism applicable to every component of the PV ring simultaneously.

Lemma 4.4 (Descent without an integral-domain assumption)**.** *Let R, Z, J be as in Proposition 4.2. Suppose that $\rho : G \to \mathrm{GL}(V)$ is an algebraic representation and that $\ell = Cw$ is a J-stable line, $w \neq 0$. Then there are $v \in K \otimes_C V$, $v \neq 0$, and $c \in K^*$ such that*

$$\sigma(v) = c\rho(A)v, \qquad Q(R)v = Q(R)\rho(Z)w.$$

Proof. Set $u = \rho(Z)w \in R \otimes_C V$. Choose $b \in V^*$ with $b(w) = 1$. The identity $b\rho(Z)^{-1}u = 1$ shows that the coordinates of u generate the unit ideal of R.

There are finitely many minimal prime ideals $\mathfrak{p}$ of the reduced Noetherian ring R. For each, the map

$$V^* \longrightarrow R/\mathfrak{p}, \qquad L \longmapsto L(u) \bmod \mathfrak{p}$$

is a nonzero C-linear map, since the coordinates of u cannot all lie in $\mathfrak{p}$. Its kernel is proper. A finite-dimensional vector space over an infinite field is not a finite union of proper linear subspaces: choose a nonzero linear form vanishing on each such subspace and take their product, a nonzero polynomial which cannot vanish at all points. Choose L outside all these kernels and put $a = L(u)$.

The element a lies in no minimal prime. It is a nonzerodivisor: if $ar = 0$, passage to each domain $R/\mathfrak{p}$ gives $r \in \mathfrak{p}$ for every minimal prime, whence $r = 0$ because R is reduced. Thus $a \in Q(R)^*$, and also $\sigma(a) \in Q(R)^*$.

Since $\ell = Cw$ is J-stable, its one-dimensional representation is a character $\chi : J \to \mathbb{G}_m$, characterized by

$$\rho(g)w = \chi(g)w \qquad (g \in J(C)).$$

Let $\tau \in \mathrm{Aut}_\sigma(R/K)$ and write $g_\tau = Z^{-1}\tau(Z) \in J(C)$. The automorphism τ acts on $R \otimes_C V$ through the first factor. Since ρ is defined over C and $w \in V$ has constant coordinates, we have

$$\begin{aligned}\tau(u) &= \tau\big(\rho(Z)w\big) = \rho\big(\tau(Z)\big)w = \rho(Zg_\tau)w \\ &= \rho(Z)\rho(g_\tau)w = \chi(g_\tau)\rho(Z)w = \chi(g_\tau)u.\end{aligned}$$

To obtain the corresponding identity for $a = L(u)$, recall that $L \in V^* = \mathrm{Hom}_C(V, C)$ is a constant linear functional. We use the same symbol for its R-linear extension $R \otimes_C V \to R$. Choose a C-basis $e_1, \ldots, e_m$ of V and write

$$u = \sum_{i=1}^{m} u_i e_i, \qquad \lambda_i = L(e_i) \in C, \qquad a = L(u) = \sum_{i=1}^{m} \lambda_i u_i.$$

Every τ fixes $C \subseteq K$ pointwise, so $\tau(\lambda_i) = \lambda_i$. Consequently

$$\begin{aligned}\tau(a) &= \sum_{i=1}^{m} \lambda_i \tau(u_i) = L\big(\tau(u)\big) = L\big(\chi(g_\tau)u\big) \\ &= \chi(g_\tau)L(u) = \chi(g_\tau)a.\end{aligned}$$

The equality $\tau \circ L = L \circ \tau$ used here follows exactly from these constant coefficients of L. Since $a \in Q(R)^*$, it follows that

$$\tau(u/a) = \frac{\chi(g_\tau)u}{\chi(g_\tau)a} = u/a.$$

Lemma 4.3 now implies that $v = u/a$ has coordinates in K. Since $L(v) = 1$, it is nonzero. The representation is defined over the constant field, so

$$\sigma(u) = \rho(\sigma Z)w = \rho(A)u, \qquad \sigma(v) = \frac{a}{\sigma(a)}\rho(A)v.$$

Choose a nonzero coordinate of the K-vector $\rho(A)v$. Comparing that coordinate expresses $a/\sigma(a)$ as a ratio of elements of K. It is a unit of $Q(R)$ and hence a nonzero element of K. This gives the required $c \in K^*$ and the equality of the lines. □

5 Chevalley detection and the coefficient-group criterion

5.1 The line-stabilizer construction

This is Chevalley's theorem, not a new detection theorem; see [2, Theorem 4.27]. The proof uses the classical construction from a finite-dimensional translation-stable space of functions followed by an exterior power.

Lemma 5.1 (Chevalley, with an explicit construction)**.** *For a proper closed subgroup $J \subsetneq G$, there exist an algebraic representation $\rho : G \to \mathrm{GL}(V)$ and a line $\ell \subset V$ such that $J = \mathrm{Stab}_G(\ell)$.*

Proof. Use right translations $(T_g f)(t) = f(tg)$ on $C[G]$. They satisfy $T_g T_h = T_{gh}$. The representation is locally finite. Indeed, in an embedding $G \subseteq \mathrm{GL}_N$, finitely many elements of $C[G]$ are images of fractions $P(X)/\det(X)^m$ with one common m and a common bound on the degree of P. Right translation replaces this by $P(Xg)/(\det(X)^m \det(g)^m)$ and preserves the degree bound. The space of these fractions is finite dimensional and is an algebraic representation. Increase the degree bound to include 1.

Choose a finite-dimensional translation-stable $W \subset C[G]$ containing 1 and a finite set of ideal generators of $I(J)$. Put $U = W \cap I(J)$. The space U generates $I(J)$ as an ideal and satisfies $0 < e := \dim U < \dim W$. For $g \in J$, translation preserves $I(J)$ and hence U. Conversely, if g preserves U, it preserves the ideal generated by U; for each $f \in I(J)$,

$$f(g) = (T_g f)(1_G) = 0.$$

Thus $g \in J$, and $\mathrm{Stab}_G(U) = J$.

Take $V = \bigwedge^e W$ and $\ell = \bigwedge^e U$. For a nonzero $\omega \in \ell$,

$$U = \{z \in W : z \wedge \omega = 0\}.$$

It follows in both directions that an invertible linear map preserves ℓ if and only if it preserves U. The exterior-power representation therefore has exactly the asserted stabilizer. Equality of C-points implies equality of the closed subgroups in characteristic zero. □

5.2 Excluding every proper Galois subgroup

The standard upper inclusion of the PV group in a coefficient group is [1, Proposition 1.21(1)]. The reverse inclusion below is obtained from Theorem 3.1. This is the precise point at which the additional hypotheses of the present argument enter the inverse problem.

Theorem 5.2 (Coefficient-group criterion)**.** *Suppose $A \in G(K)$ satisfies (3.2) and $T_A = G$. Then, with the choice of R and Z in Proposition 4.2, the PV group is G.*

Proof. Let $J \subseteq G$ be that PV group. If $J \neq G$, choose ρ and $\ell = Cw$ from Lemma 5.1. Lemma 4.4 produces a difference-invariant K-line Kv. By Theorem 3.1, $Kv = Kv_0$ for some $v_0 \in V \setminus \{0\}$.

Equation (3.1), after rescaling its representative, says that $\rho(A)$ preserves Kv_0. The stabilizer $H = \mathrm{Stab}_G(Cv_0)$ is a closed constant subgroup, and this assertion is precisely $A \in H(K)$. The condition $T_A = G$ forces $H = G$.

The G-stability of Cv_0 is a representation-theoretic statement valid after arbitrary scalar extension, not just at C-points. For example, extend v_0 to a basis of V; the entries below the first entry of the first column of $\rho(g)$ vanish identically on the reduced group G, while that first entry is a character with invertible value. Thus $\rho(Z)$ and $\rho(Z)^{-1}$ preserve $Q(R)v_0$.

The equality supplied by descent gives

$$Q(R)\rho(Z)w = Q(R)v_0, \qquad \text{hence} \qquad Q(R)w = Q(R)v_0.$$

In particular $w \in Q(R)v_0$, so there exists $b \in Q(R)$ with $w = bv_0$. Both vectors are defined over C: the vector w was chosen in the C-vector space V in Chevalley's theorem, and the vector $v_0 \in V \setminus \{0\}$ is the constant generator supplied by Theorem 3.1. In a fixed C-basis $e_1, \dots, e_m$ of V, write

$$w = \sum_{i=1}^{m} w_i e_i, \qquad v_0 = \sum_{i=1}^{m} v_{0,i} e_i, \qquad w_i, v_{0,i} \in C.$$

The equality $w = bv_0$ in $Q(R) \otimes_C V$ implies the coordinate identities $w_i = bv_{0,i}$ in $Q(R)$ for every i. Since $v_0 \neq 0$, choose j with $v_{0,j} \in C^*$. The embeddings $C \hookrightarrow R \hookrightarrow Q(R)$ identify every nonzero constant with a unit whose inverse already belongs to C. Multiplying the jth coordinate identity by this constant inverse therefore gives

$$b = v_{0,j}^{-1} w_j \in C \subseteq Q(R).$$

This calculation is valid even when R has zero divisors, since the only element inverted is the nonzero constant $v_{0,j}$. Moreover $b = 0$ would imply $w = 0$, which is excluded. Hence $b \in C^*$ and $\ell = Cw = Cv_0$. The latter line is G-stable, contradicting $\mathrm{Stab}_G(\ell) = J \neq G$. □

The reverse passage through $\rho(Z)^{-1}$ is essential: the original Chevalley line and its descended constant line are not a priori the same line. The proof also explains why irreducibility in the natural representation alone would not suffice; every algebraic representation must be available to detect an arbitrary proper subgroup.

6 An explicit rational curve generating the identity component

6.1 Unipotent elements and finitely many one-parameter subgroups

Both lemmas in this subsection are consequences of classical structure theory. We give elementary proofs using polynomial exponential maps, Jordan decomposition, and containment of semisimple elements in tori [2, Theorem 9.18 and Corollary 17.36]. The subsequent use of finitely many generating points follows the strategy of [1, Proposition 3.3(2)].

Lemma 6.1 (A unipotent element lies in the identity component)**.** *If $u \in G(C)$ is unipotent, then $u \in G^\circ(C)$. More precisely, if $u \neq I$ and $N = \log(u)$, the polynomial homomorphism*

$$\mathbb{G}_a \longrightarrow \mathrm{GL}_n, \qquad t \longmapsto \exp(tN)$$

has image in G and contains u.

Proof. The logarithm and exponential are finite polynomials on a unipotent matrix and a nilpotent matrix. Their formal identities give $\exp((s+t)N) = \exp(sN)\exp(tN)$ and $\exp(N) = u$. For every integer m, $\exp(mN) = u^m \in G(C)$. For any defining equation $f \in I(G)$, the function $f(\exp(tN))$ is a polynomial in t: the determinant is 1, including in any inverse-determinant factors. It vanishes at all integers, an infinite subset of C, and hence identically. The image is consequently contained in G. It is connected and contains I, so lies in G°. If $u \neq I$, choose an entry $N_{ij} \neq 0$. The finite polynomial

$$\frac{1}{N_{ij}} \left(\sum_{k=1}^{n-1} \frac{(-1)^{k+1}}{k} (X - I)^k \right)_{ij}$$

pulls back to t, since $\log(\exp(tN)) = tN$. Thus the induced map $C[G] \to C[t]$ is surjective, proving that the parametrization is a closed immersion of $\mathbb{G}_a$. The case $u = I$ is immediate. □

Lemma 6.2 (Finite one-parameter generation)**.** *Every nontrivial connected linear algebraic group H over C is generated as an algebraic group by finitely many closed subgroups isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$.*

Proof. Let

$$\mathcal{U} = \{U \subseteq H : U \text{ is a closed algebraic subgroup and } U \simeq \mathbb{G}_a \text{ or } U \simeq \mathbb{G}_m\}.$$

For a subfamily $\mathcal{F} \subseteq \mathcal{U}$, denote by

$$\Gamma_{\mathcal{F}} = \Big\langle \bigcup_{U \in \mathcal{F}} U(C) \Big\rangle \subseteq H(C), \qquad P_{\mathcal{F}} = \overline{\Gamma_{\mathcal{F}}}^{\mathrm{Zar}} \subseteq H$$

the abstract subgroup generated by its C-points and its reduced Zariski closure, respectively. The Zariski closure of a subgroup is a closed algebraic subgroup; see [2, Lemma 1.40 and Corollary 1.46]. For the empty family put $P_\varnothing = \{1_H\}$.

(i) Generation by the full family. For $g \in H(C)$, multiplicative Jordan decomposition gives

$$g = g_s g_u = g_u g_s, \qquad g_s, g_u \in H(C),$$

with g_s semisimple and g_u unipotent [2, Theorem 9.18]. By Lemma 6.1, either $g_u = 1_H$ or $g_u \in U(C)$ for some $U \in \mathcal{U}$ isomorphic to $\mathbb{G}_a$. Thus $g_u \in \Gamma_{\mathcal{U}}$. By [2, Corollary 17.36], g_s belongs to a torus $T \subseteq H$. Since C is algebraically closed, every torus is split [2, Definition 12.14 and Theorem 12.18(d)]; choose an isomorphism $\alpha : \mathbb{G}_m^r \xrightarrow{\sim} T$. For $1 \leq j \leq r$, let $\iota_j : \mathbb{G}_m \hookrightarrow \mathbb{G}_m^r$ be the jth coordinate embedding and set $T_j = \alpha(\iota_j(\mathbb{G}_m))$. Then

$$T_j \in \mathcal{U}, \qquad T(C) = T_1(C) \cdots T_r(C) \subseteq \Gamma_{\mathcal{U}}.$$

If $r = 0$, the product means $\{1_H\}$. Consequently g_s and g belong to $\Gamma_{\mathcal{U}}$, and therefore

$$\Gamma_{\mathcal{U}} = H(C). \tag{6.1}$$

(ii) Irreducibility for each finite subfamily. Let $\mathcal{F} = \{U_1, \ldots, U_r\}$ be nonempty and finite, and put

$$W_{\mathcal{F}} = U_1(C) \cdots U_r(C).$$

For every integer $q \geq 1$, the multiplication morphism

$$\mu_q : (U_1 \times \cdots \times U_r)^q \longrightarrow H, \qquad ((u_{a,j})_{j=1}^r)_{a=1}^q \longmapsto \prod_{a=1}^{q} \prod_{j=1}^{r} u_{a,j}$$

has irreducible source, since each U_j is isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$. Thus the closure $Z_q = \overline{W_{\mathcal{F}}^q}^{\mathrm{Zar}}$ is irreducible. As $1_H \in W_{\mathcal{F}}$ and $U_j(C) \subseteq W_{\mathcal{F}}$, we have

$$W_{\mathcal{F}}^q \subseteq W_{\mathcal{F}}^{q+1}, \qquad \Gamma_{\mathcal{F}} = \bigcup_{q\geq 1} W_{\mathcal{F}}^q, \qquad P_{\mathcal{F}} = \overline{\bigcup_{q\geq 1} Z_q}^{\mathrm{Zar}}.$$

The middle equality holds because the inverses of elements of $U_j(C)$ still lie in $U_j(C)$, and any finite word in these subgroups lies in a sufficiently large power of $W_{\mathcal{F}}$. The irreducible closed sets Z_q form an increasing sequence; their union, and hence its closure, is irreducible. Indeed, if this union were contained in two closed sets without being contained in either, two of its points outside the respective closed sets would lie in one sufficiently large Z_q, contradicting irreducibility of Z_q. Hence $P_{\mathcal{F}}$ is irreducible. This is also the connected-generation principle of [2, Proposition 2.53], together with the equivalence of connectedness and irreducibility for algebraic groups over an algebraically closed field [2, Corollary 1.35].

(iii) Reduction to a finite subfamily. The set

$$\mathcal{D} = \{\dim P_{\mathcal{F}} : \mathcal{F} \subseteq \mathcal{U} \text{ finite}\} \subseteq \{0, 1, \ldots, \dim H\}$$

is nonempty. Choose a finite $\mathcal{F}_0$ with $\dim P_{\mathcal{F}_0} = \max \mathcal{D}$, and put $P = P_{\mathcal{F}_0}$. For every $U \in \mathcal{U}$, let $P' = P_{\mathcal{F}_0 \cup \{U\}}$. Then

$$P \subseteq P', \qquad \dim P \leq \dim P' \leq \max \mathcal{D} = \dim P.$$

Both P and P' are irreducible by (ii), including the trivial case $P = \{1_H\}$. A proper closed subset of an irreducible variety has strictly smaller dimension [2, Appendix A.47], so $P = P'$. In particular $U \subseteq P$ for every $U \in \mathcal{U}$. Using (6.1), we obtain

$$H(C) = \Gamma_{\mathcal{U}} \subseteq P(C) \subseteq H(C).$$

Since $H(C)$ is Zariski dense in the reduced affine C-variety H, the closed subgroup P equals H; compare [2, Corollary 1.18]. Thus the finite family $\mathcal{F}_0$ generates H. Since $H \neq \{1_H\}$, this family is nonempty. □

Fix such a finite list, with embeddings

$$u_i : \mathbb{G}_a \hookrightarrow H \quad \text{or} \quad \lambda_i : \mathbb{G}_m \hookrightarrow H, \qquad 1 \leq i \leq r.$$

For an additive subgroup put $g_i = u_i(1)$, and for a multiplicative subgroup put $g_i = \lambda_i(2)$. The powers of g_i are respectively $u_i(m)$, $m \in \mathbb{Z}$, or $\lambda_i(2^m)$, $m \in \mathbb{Z}$. These parameter sets are infinite in characteristic zero. Every infinite subset of $\mathbb{A}^1$ or $\mathbb{G}_m$ is Zariski dense, since a nonzero one-variable polynomial has finitely many roots. Therefore

$$H = \overline{\langle g_1, \ldots, g_r \rangle}^{\mathrm{Zar}}. \tag{6.2}$$

Only these finitely many points will be prescribed on a rational curve.

6.2 Interpolation with a vanishing first jet

Prescribing finitely many group values is the interpolation step of [1, Proposition 3.3(2)]. Prescribing values while making a group curve approach the identity to high order also occurs in [1, proof of Theorem 8.11], there for connection data in a different variable. The formulas here implement the required second-order condition in the coefficient variable x by elementary

Lagrange interpolation on one-parameter subgroups. Their singularities can then be controlled independently of the matrix entries defining those subgroups. For $1 \le i \le r$, define

$$M = r+1, \qquad L_i(z) = \prod_{\substack{1\le j\le r\\ j\neq i}} \frac{z-j}{i-j}, \qquad p_i(z) = \frac{i^M L_i(z)}{z^M}. \tag{6.3}$$

An empty product is 1. Since distinct nonzero integers remain distinct in C, these formulas are valid. They satisfy

$$p_i(j) = \delta_{ij}, \qquad p_i(z) = O(z^{-2}) \quad (z=\infty). \tag{6.4}$$

The second assertion follows from $\deg L_i = r-1 = M-2$. Set

$$F_i(z) = \begin{cases} u_i(p_i(z)), & \text{for an additive subgroup,}\\ \lambda_i(1+p_i(z)), & \text{for a multiplicative subgroup,}\end{cases} \qquad B(z) = F_1(z)\cdots F_r(z). \tag{6.5}$$

The rational function $1+p_i$ is nonzero since its value at infinity is 1, so the multiplicative expression defines a point over $C(z)$. All factors are $H(C(z))$-points.

At $z=j$, every additive parameter is 0 except possibly the jth, and every multiplicative parameter is 1 except possibly the jth, which is 2. All evaluations are defined. Hence

$$B(j) = g_j, \qquad B(z) = I + O(z^{-2}), \qquad B(\infty) = I. \tag{6.6}$$

The order estimate holds because each regular group homomorphism maps its identity to I and preserves congruence modulo z^{-2}. Multiplying finitely many matrices congruent to I modulo z^{-2} preserves that congruence. No commutativity of the factors is used. By (6.2), the values of B generate H.

6.3 A finite algebraic set containing all singularities

The entries of $u_i(t)$ and $u_i(t)^{-1} = u_i(-t)$ are polynomials in t. Thus an additive factor in (6.5) has no finite pole except possibly $z=0$. The entries of $\lambda_i(t)$ and its inverse are Laurent polynomials, since $C[\mathbb{G}_m] = C[t,t^{-1}]$. Consequently a multiplicative factor and its inverse have finite poles only among

$$0 \quad \text{and the zeros of} \quad Q_i(z) = z^M + i^M L_i(z).$$

These Q_i are monic polynomials in $\mathbb{Q}[z]$. Thus

$$S_0 = \{0\} \cup \bigcup_{i \text{ multiplicative}} \{\alpha \in \overline{\mathbb{Q}} : Q_i(\alpha) = 0\} \quad \text{satisfies} \quad S(B) \subseteq S_0. \tag{6.7}$$

Here we choose an algebraic closure of $\mathbb{Q}$ inside C. Products and inverse products create no pole outside the union of the factor singularities. Possible cancellations only shrink $S(B)$. The points of S_0 are algebraic even when the entries defining H and its one-parameter subgroups are arbitrary constants in C.

7 Arithmetic dilation and realization of the full group

The dilation below is an elementary finite-dimensional $\mathbb{Q}$-linear avoidance argument. Its role in this proof is to arrange the hypothesis of Theorem 3.1; it does not use a specialization theorem or an uncountability assumption.

Lemma 7.1 (Dilation of a finite singularity set)**.** *For every finite $S_0 \subset C$ there is $t \in C^*$ such that $1 \notin \operatorname{span}_{\mathbb{Q}}(tS_0)$. If S_0 lies in a number field F of degree D, any root $t \in C$ of $T^{D+1} - 2$ is such a choice.*

Proof. The space $W = \operatorname{span}_{\mathbb{Q}} S_0$ is finite dimensional. The field C has infinite dimension over $\mathbb{Q}$, since it contains algebraic numbers of arbitrarily large degree. Choose $a \in C \setminus W$ and put $t = a^{-1}$; $a \neq 0$ because $0 \in W$. The relation $1 \in tW$ would imply $a \in W$.

For the explicit assertion, Eisenstein's criterion at 2 gives $[\mathbb{Q}(t) : \mathbb{Q}] = D + 1$. Hence $t \notin F$ and $t^{-1} \notin F$. Since $\operatorname{span}_{\mathbb{Q}}(tS_0) \subseteq tF$, it cannot contain 1. □

The following choice of a lift of a generator of G/G° occurs in the proof of [1, Theorem 8.10]: take the semisimple part of an arbitrary representative. That source subsequently chooses a finite-order element for its analytic construction. The present argument needs only the semisimple representative, so no splitting of the exact sequence $1 \to G^\circ \to G \to G/G^\circ \to 1$ is required.

Lemma 7.2 (A semisimple lift of a quotient generator)**.** *If G/G° is cyclic, there is a semisimple $h \in G(C)$ whose image generates that quotient. Moreover $G(C) = \langle G^\circ(C), h \rangle$.*

Proof. Choose $g \in G(C)$ whose image generates G/G° and write $g = g_s g_u$. Lemma 6.1 gives $g_u \in G^\circ$, so $h = g_s$ has the same image in the quotient. If that image has order m, each element of $G(C)$ belongs to a coset $h^j G^\circ(C)$, $0 \leq j < m$, proving the last assertion. If the quotient is trivial, one may simply take $h = I$. □

No assertion that $h^m = I$ is used. In particular the exact sequence $1 \to G^\circ \to G \to G/G^\circ \to 1$ need not split, and no finite-order lifting result is required.

Proof of Theorem 1.1. Put $H = G^\circ$. Suppose first that $H \neq 1$. Choose B from (6.5), h from Lemma 7.2, and t from Lemma 7.1 for the set (6.7). Define

$$\boxed{A(x) = hB(x/t).} \tag{7.1}$$

Then $A \in G(K)$ and

$$A(x) = h + O(x^{-2}), \qquad S(A) \subseteq tS_0, \qquad 1 \notin \operatorname{span}_{\mathbb{Q}} S(A).$$

Left multiplication by the constant h and right multiplication by its inverse introduce no singularities.

It remains to check the group generated by A. It is contained in G. For every equation $f \in I(T_A)$ the rational function $f(A(x))$ is zero. The matrix A is regular and invertible at infinity, so evaluation there yields $f(h) = 0$. Thus $h \in T_A(C)$. Also, using (6.6),

$$A(ti) = hg_i, \qquad g_i = h^{-1}A(ti) \in T_A(C).$$

These evaluations are defined and invertible, as verified above. Since the g_i generate H and the image of h generates G/G°, $T_A = G$. Theorem 5.2 proves the required realization.

If $H = 1$, then G is a finite cyclic group. Take its generator h and put $A = h$. In characteristic zero a finite-order matrix is semisimple, because its minimal polynomial divides a separable polynomial $T^m - 1$. Now $S(A) = \varnothing$, $A = h + O(x^{-2})$, and $T_A = G$. The same criterion applies, including the trivial group. □

8 Explicit realizations

8.1 A one-singularity realization of SL_2

Let

$$u_+(s) = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, \qquad u_-(s) = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix},$$

and set

$$p(x) = \frac{2-x}{x^3}, \qquad q(x) = \frac{8(x-1)}{x^3}, \qquad A(x) = u_+(p(x))u_-(q(x)) = \begin{pmatrix} 1+pq & p \\ q & 1 \end{pmatrix}.$$

Both A and its inverse have no finite pole outside $\{0\}$ and $A = I + O(x^{-2})$. Moreover $A(1) = u_+(1)$ and $A(2) = u_-(1)$. The Zariski closure of the subgroup generated by each value is its entire root subgroup, and those two root subgroups generate SL_2; for instance their Lie algebras contain E_{12}, E_{21} and their bracket, a basis of $\mathfrak{sl}_2$. Thus $T_A = \mathrm{SL}_2$ and the criterion applies without any dilation.

8.2 A multiplicative group

Take $B(z) = 1 + z^{-2}$, with singularities $0, i, -i$. Choose t satisfying $t^3 = 2$ and consider the system

$$A(x) = \left(1 + \frac{t^2}{x^2}\right) \in \mathrm{GL}_1(K), \qquad \sigma Y = A(x)Y$$

Since $t^{-1} \notin \mathbb{Q}(i)$, we have $1 \notin \mathrm{span}_{\mathbb{Q}}\{0, it, -it\}$, and $A = I + O(x^{-2})$. Its nonconstant coefficient has infinitely many values, which generate $\mathbb{G}_m$. Thus its PV group is $\mathbb{G}_m$. Dilation is not always necessary; for example $1 \notin \mathrm{span}_{\mathbb{Q}}\{0, i, -i\}$ already holds. The chosen t illustrates a uniform algebraic rule which works without first testing the individual singularity set.

8.3 A nonsplit extension with quotient of order two

Let

$$T = \{\mathrm{diag}(s, s^{-1}) : s \in C^*\}, \qquad h = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad G = N_{\mathrm{SL}_2}(T) = T \cup hT.$$

To see the displayed description of the normalizer, an element normalizing T must permute its two distinct weight lines in C^2 and is therefore diagonal or antidiagonal; the determinant-one condition gives exactly $T \cup hT$. The quotient G/T has order 2. Conjugation by h inverts T and $h^2 = -I$, so $(h\,\mathrm{diag}(s, s^{-1}))^2 = -I$ for every s. Thus the extension by C_2 does not split: there is no element of order 2 in the nonidentity component.

Take $t^3 = 2$ and $q(x) = 1 + t^2/x^2$. Then

$$A(x) = h\,\mathrm{diag}(q(x), q(x)^{-1}) = \begin{pmatrix} 0 & -q(x)^{-1} \\ q(x) & 0 \end{pmatrix}$$

has semisimple limit h, no first-order term, and singularities among $0, it, -it$. Its coefficient group contains h and T, hence equals G. Its PV group is therefore the nonsplit normalizer.

8.4 A finite cyclic group and a nonintegral PV ring

The construction is classical. In the supplied correspondence, Singer [4, Section 2a and Proposition 1] writes the finite cyclic PV ring using cyclically permuted idempotents and an element u with $\sigma(u) = \zeta u$. We give the equivalent quotient-algebra presentation and verify its prescribed matrix representation. Let $G = \langle h \rangle$ have order m. Choose a primitive mth root $\zeta \in C$ and write $h = P \operatorname{diag}(\zeta^{e_1}, \dots, \zeta^{e_n}) P^{-1}$. Put

$$R = K[t]/(t^m - 1), \qquad \sigma(t) = \zeta t, \qquad Z = P \operatorname{diag}(t^{e_1}, \dots, t^{e_n}) P^{-1}.$$

The ring is isomorphic to K^m and σ permutes its primitive idempotents transitively. An ideal is a product of ideals in these field factors, so no nonzero proper ideal is σ-stable. Also $\sigma Z = hZ$. Since h has order m, $\gcd(m, e_1, \dots, e_n) = 1$. The diagonal entries of $P^{-1} Z P$ give t^{e_i}, and their inverses are the diagonal entries of $P^{-1} Z^{-1} P$. They belong to the algebra generated by the entries of Z and $(\det Z)^{-1}$ because $Z^{-1} = \operatorname{adj}(Z)/\det Z$. Bézout's identity modulo m therefore recovers t in this algebra. Thus R is generated by the fundamental matrix and its inverse determinant, and is a PV ring. The K-automorphisms are permutations of the m field factors. A permutation commuting with a full cycle is determined by the image of one factor, so the commuting automorphisms are precisely $t \mapsto \zeta^j t$, with right-action matrices h^j.

For $m = 2$, a unimodular vector such as $(1+t, 1-t)^{\mathsf{T}}$ can have every coordinate a zerodivisor. This is why the descent proof selects a *linear combination* outside the minimal primes: here the sum of the coordinates is the unit 2.

9 Counterexamples and sharpness of the hypotheses

9.1 Dropping the singularity condition, or forgetting the inverse

Let $a(x) = 1 - x^{-2}$ and $y = x/(x-1)$. Then

$$\frac{y(x+1)}{y(x)} = \frac{(x+1)(x-1)}{x^2} = a(x).$$

The one-dimensional system with coefficient matrix $A = (a)$ has the fundamental matrix $Z = (y) \in \mathrm{GL}_1(K)$. Thus its PV group is trivial, while its coefficient group is $\mathbb{G}_m$. The infinity normalization holds, but $S(a) = \{0, 1, -1\}$ violates the arithmetic condition. Counting only poles of a, and not of a^{-1}, would give the erroneous set $\{0\}$.

The degree identity can be checked exactly in the representation $\rho(s) = \operatorname{diag}(s, 1)$:

$$v = \begin{pmatrix} x \\ x-1 \end{pmatrix}, \qquad \sigma v = \frac{x}{x-1} \rho(a) v.$$

The vector is primitive and $d = 1$. The multiplier has $k_0 = 1$, $k_1 = -1$, so $\sum_s k_s s = -1$ and $d + \sum_s k_s s = 0$.

9.2 Dropping semisimplicity

Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad Z(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Then $\sigma Z = AZ$ and $Z \in \mathrm{GL}_2(K)$. Thus the PV group is trivial, whereas $T_A \simeq \mathbb{G}_a$. The singularity set is empty, but the limit at infinity is not semisimple. Correspondingly, $v = (x, 1)^{\mathsf{T}}$ satisfies $\sigma v = Av$ and has nonconstant direction. This is precisely the failure of $\ker(M - I) \cap \operatorname{im}(M - I) = 0$ in the proof of rigidity.

9.3 Allowing a first-order term at infinity

Consider

$$A(x) = \begin{pmatrix} 1 + x^{-1} + x^{-2} & -x^{-1} \\ x^{-2} & 1 - x^{-1} \end{pmatrix}, \qquad v(x) = \begin{pmatrix} x \\ 1 \end{pmatrix}.$$

Direct multiplication gives $\det A = 1$ and $\sigma v = Av$. Both A and A^{-1} have finite poles only at 0, and $A(\infty) = I$ is semisimple. Nevertheless Kv is not a constant line. Thus even all these other conditions together do not permit dropping the absence of the x^{-1} term.

More generally, if $B = H + B_1/x + O(x^{-2})$ and $\sigma v = cBv$, the same two-coefficient calculation gives, for $M = \gamma H$,

$$Mv_d = v_d, \qquad (d+q)v_d = (M - I)v_{d-1} + \gamma B_1 v_d.$$

When H is semisimple, projection Π_1 onto the 1-eigenspace of M yields $(d+q)v_d = \gamma \Pi_1 B_1 v_d$. The proof requires this extra term to vanish; our construction arranges the stronger condition $B_1 = 0$ uniformly in every representation.

9.4 Why the scalar multiplier need not be constant

Take $A = 1 + x^{-2}$ in $\mathbb{G}_m$. It satisfies the criterion with $S(A) = \{0, i, -i\}$. For the constant vector $v = 1$, equation (3.1) holds with $c = x^2/(x^2+1)$, which is not constant. Its divisor gives $k_0 = 2$, $k_i = k_{-i} = -1$, and both required sums are zero. This rules out an incorrect strengthening from constancy of the line to constancy of the multiplier.

9.5 Rational gauges of constant systems

Lemma 9.1 (A scalar coboundary creates an integer resonance)**.** *If $f \in C(x)^*$ is nonconstant, the finite zero–pole support of $\sigma(f)/f$ contains two distinct points differing by a nonzero integer.*

Proof. A nonconstant rational function has a finite zero or pole. In an orbit $a + \mathbb{Z}$ containing one, put $n_k = \operatorname{ord}_{a+k}(f)$. This is a nonzero finitely supported sequence. Let m and M be the least and greatest indices with $n_k \neq 0$. Then

$$\operatorname{ord}_{a+k}(\sigma(f)/f) = n_{k+1} - n_k$$

is nonzero at $k = m - 1$ and at $k = M$. These are distinct indices and the corresponding points differ by $M - m + 1 \in \mathbb{Z}_{>0}$. □

Suppose A satisfies (3.2) and $A = \sigma(P)DP^{-1}$ with $P \in \mathrm{GL}_n(K)$ and constant semisimple D. After a constant eigenbasis change for D, each column p_j of P satisfies $\sigma(p_j) = \lambda_j^{-1} A p_j$. Rigidity gives $p_j = f_j v_j$ with v_j constant. The v_j form a basis, since P is invertible. In that constant basis A is diagonal, with entries $\lambda_j \sigma(f_j)/f_j$. Both these entries and their inverses have singularities contained in $S(A)$. Lemma 9.1 would contradict $1 \notin \operatorname{span}_{\mathbb{Q}} S(A)$ if any f_j were nonconstant. Therefore P is constant. This excludes an entire class of rational gauge counterexamples, rather than just isolated matrices.

10 An alternative interpolation construction

The main proof uses one-parameter subgroups. For comparison, one can instead construct the generating curve by prescribing tangent vectors. The rational chart is the same classical ingredient used in [1, Proposition 3.3(2)]; the prescribed first derivatives are supplied by

elementary Hermite interpolation. The deduction from spanning tangent vectors to group generation uses smoothness and connectedness. This section assembles these standard ingredients into an alternative curve construction and is independent of the realization proof already completed.

A connected linear algebraic group over C is a rational variety. One may obtain this from the Levi decomposition, polynomial coordinates on the unipotent radical, and the big cell of a reductive group. By translating a rational chart one obtains an open subset $U \subset \mathbb{A}^d$ and a regular map, an isomorphism onto an open subset,

$$F : U \longrightarrow H, \qquad 0 \in U, \quad F(0) = I, \quad dF_0 : C^d \xrightarrow{\sim} \mathrm{Lie}(H).$$

For $d > 0$ put $b_i = i$, $M = 2d + 1$, and

$$L_i(z) = \prod_{j \neq i} \frac{z - b_j}{b_i - b_j}, \qquad u_i(z) = \frac{b_i^M (z - b_i) L_i(z)^2}{z^M}.$$

At $z = b_i$ the factor $z - b_i$ gives derivative 1 after multiplication by b_i^M / z^M. At $z = b_j$, $j \neq i$, the square of L_i has a double zero. Hence

$$u_i(b_j) = 0, \qquad u_i'(b_j) = \delta_{ij}, \qquad u_i = O(z^{-2}).$$

The last estimate follows because the numerator has degree $2d - 1$. The curve $B(z) = F(u_1(z), \ldots, u_d(z))$ is defined generically and at the specified nodes and infinity: those parameter values are $0 \in U$. It satisfies

$$B(z) = I + O(z^{-2}), \qquad B(b_j) = I, \qquad B'(b_j) = dF_0(e_j).$$

If a closed subgroup $P \subseteq H$ contains all regular values of B, then its Lie algebra contains these derivatives, a basis of $\mathrm{Lie}(H)$. Smoothness in characteristic zero gives $\dim P = \dim H$; connectedness of H implies $P = H$. Its finite singularities need not be algebraic over $\mathbb{Q}$, but the first assertion of Lemma 7.1 works for every finite set. Thus $A(x) = hB(x/t)$ gives a second construction under the same rigidity criterion.

A Earlier contributions and the scope of the present argument

A.1 Published inverse results

Van der Put and Singer [1] supply both the foundational PV theory and the principal earlier formulation of the shift inverse problem. The coefficient-group characterization in Proposition 3.2(1) and the construction in Proposition 3.3(2) provide the starting point for the coefficient-curve method used here.

The analytic results in Chapter 8 have the following respective base fields and hypotheses. Theorem 8.10 concerns the local field of convergent Laurent series at infinity, not the rational-function field. Theorem 8.11 gives a global realization over the complex rational-function field when a finite-order element whose image generates G/G° lies in the identity component of the normalizer of G° in the ambient general linear group. In particular it applies when G is connected. Lemma 8.12 separately realizes cyclic extensions of tori. Thus these results do not, as stated, supply the full global theorem for every G such that G/G° is cyclic.

Feng's contribution in [3, Theorem 1.2] is preservation of a specified difference Galois group under suitable specialization; the basic open sets used for this purpose are Zariski dense [3, Theorem 2.16]. His Theorem 6.3 proves that validity of the inverse conjecture over the complex numbers implies validity over every algebraically closed field of characteristic zero. Corollary 6.4

thereby establishes these realizations over all such fields when G is connected, or when G° is a torus and G/G° is cyclic. This is a substantial existence and transfer result. The proof in the present manuscript instead constructs its coefficients over the given C and establishes their Galois group directly by Theorems 3.1 and 5.2.

A.2 The supplied correspondence and the q-difference paper

The file `Feng_8_26_15.pdf` is a letter addressed to Ruyong and signed Michael, dated 26 August 2015. It is therefore cited here as Singer's letter [4], rather than attributing authorship from the filename. Its Section 1 reduces the problem to a finite cyclic semidirect product followed by a finite quotient. Sections 2–3 describe cyclic idempotents, passage to an iterate of the shift, and a criterion using a twisted product in the connected group. These are substantive antecedents for the treatment of components and for the finite cyclic example.

The note `inverseproblem.pdf`, dated 16 January 2016 and addressed to Michael, gives the coordinate-ring formulation of the inverse problem and reductions through the unipotent radical, finite isogenies, and cyclic semidirect products [5]. The supplied copy has no signature or author byline, so its author is left unspecified in the bibliography. These reductions explain the structural approach pursued in the correspondence. None is assumed as a general realization theorem in the present proof.

Ramis and Sauloy [6] study the wild fundamental group and the inverse problem for q-difference equations. Their local analytic results and global connected reductive realizations concern the multiplicative operator $f(z) \mapsto f(qz)$, with $|q| \neq 1$. They provide context for a different inverse problem. No theorem from that paper is used to infer a realization for the additive shift $x \mapsto x + 1$.

A.3 What is proved here and what is imported

The substantive PV foundation imported without proof is the algebraic-group and torsor theorem [1, Theorem 1.13], in the form (4.1). The constant lemma and invariant-ring assertions are classical results from the same monograph, with expanded proofs included here. Chevalley's theorem is also classical; its standard construction is included to make the subgroup-detection step explicit. Jordan decomposition, torus containment, smoothness in characteristic zero, constructibility, the Nullstellensatz, and faithful flatness are the other standard foundations used in the main argument.

The specific deductions established within this manuscript are the representation-uniform degree identity and rigidity theorem, the resulting coefficient-group equality under its stated hypotheses, and the assembly of interpolating curves with arithmetic dilation to satisfy those hypotheses. Their proofs are given in full, rather than being attributed to an earlier inverse theorem. The interpolation strategy, the use of lifts of quotient generators, the finite cyclic PV construction, and the classical descent results retain the source attributions stated above. The optional tangent construction additionally uses rationality of connected linear algebraic groups, obtainable from the Levi decomposition and a reductive big cell; this extra input is not needed by the main construction.

References

[1] M. van der Put and M. F. Singer, *Galois Theory of Difference Equations*, Lecture Notes in Mathematics 1666, Springer, 1997. Relevant foundations: Lemmas 1.7–1.8, Theorems 1.13 and 1.32, Corollary 1.15, Proposition 1.21, and Lemma 1.28(1). For coefficient curves and

earlier inverse results, see Propositions 3.2(1) and 3.3(2), Theorems 8.10–8.11, and Lemma 8.12.

[2] J. S. Milne, *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*, Cambridge Studies in Advanced Mathematics 170, Cambridge University Press, 2017. Corollary 1.18 (determination by points), Corollary 1.35 (connectedness and irreducibility), Lemma 1.40 and Corollary 1.46 (Zariski closure of subgroups), Proposition 2.53 (generation by connected varieties), Theorem 4.27 (Chevalley), Theorem 9.18 (Jordan decomposition), Definition 12.14 and Theorem 12.18(d) (tori), Corollary 17.36 (torus containment), and Appendix A.47 (dimension of closed subvarieties). Author's online text.

[3] R. Feng, *Difference Galois groups under specialization*, Transactions of the American Mathematical Society **374** (2021), 61–96. arXiv:1708.07944, v5.

[4] M. F. Singer, Letter to Ruyong Feng, 26 August 2015, unpublished correspondence, 5 pp. Supplied file: `Feng_8_26_15.pdf`.

[5] Unsigned note addressed to Michael, 16 January 2016, on reductions for the shift difference inverse Galois problem, unpublished manuscript. No author is specified in the supplied copy. Supplied file: `inverseproblem.pdf`.

[6] J.-P. Ramis and J. Sauloy, *The q-analogue of the wild fundamental group and the inverse problem of the Galois theory of q-difference equations*, Annales scientifiques de l'École normale supérieure, 4th series, **48** (2015), 171–226. Supplied file: `ens_ann-sc_48_171-226.pdf`.