GENERIC PICARD-VESSIOT EXTENSIONS FOR NON-CONNECTED GROUPS

LOURDES JUAN AND ARNE LEDET

Abstract. Let K be a differential field with algebraically closed field of constants $\mathcal{C}$ and G a linear algebraic group over $\mathcal{C}$. We provide a characterization of the K-irreducible G-torsors for non-connected groups G in terms of the first Galois cohomology $H^1(K, G)$ and use it to construct Picard-Vessiot extensions which correspond to non-trivial torsors for the infinite quaternion group, the infinite multiplicative and additive dihedral groups and the orthogonal groups. The extensions so constructed are generic for those groups.

1. Introduction

Let $\mathcal{C}$ denote an algebraically closed field with trivial derivation. We are concerned with the following generic form of the inverse problem in differential Galois theory: *Given a linear group G over $\mathcal{C}$, are there a differential field $\mathcal{K}$ with field of constants $\mathcal{C}$ and a Picard-Vessiot extension (PVE) $\mathcal{E} \supset \mathcal{K}$, with differential Galois group isomorphic to G, such that $\mathcal{E}$ is generated over $\mathcal{K}$ by elements satisfying universal relations, i.e., such that every PVE with differential Galois group isomorphic to G of a differential field with field of constants $\mathcal{C}$ is generated by elements satisfying at least those relations?*

We will address this problem for some instances of non-connected groups. Our approach relies on the following well known facts: If K is a differential field with field of constants $\mathcal{C}$ then a PVE of K with differential Galois group G is the function field of a K-irreducible G-torsor [13, Theorem 5.12], [14, Theorem 1.28]. In turn, the isomorphism classes of (not necessarily irreducible) G-torsors are in one-to-one correspondence with the equivalence classes of crossed homomorphisms in the first Galois cohomology set $H^1(K, G)$ [15, Proposition 33]. Thus, to each PVE of K with differential Galois group G one can associate an element of $H^1(K, G)$. Furthermore, a crossed homomorphism splits

1991 *Mathematics Subject Classification.* Primary 12H05; Secondary 12F12, 20G15.

on a Galois extension of K and the coordinate ring of the corresponding G-torsor is given by $R = K[XP, 1/\det(XP)]$ where X is a generic point of G and P is a splitting matrix. As a consequence, a PVE of K with group G is completely determined by P and our problem of finding universal generators reduces to finding the most general form of P.

The case of connected groups has been studied in [4, 5, 8, 9]. In particular, in [8] we address the case $G = \mathrm{SO}_n$, $n \geq 3$, and in [9], the case $G = \mathrm{PGL}_3$. A broader discussion of generic extensions is also included in [8]. In [5] only PVE's that are the function fields of the trivial G-torsor are considered. We point out that when G is connected all the G-torsors are automatically K-irreducible.

For non-connected G there are reducible torsors. So, our first step is to provide a characterization of K-irreducible G-torsors (Theorem 1) in terms of $H^1(K, G)$. We then proceed to a discussion of the coordinate rings and twisted Lie algebras and analyze the cases of the infinite quaternion Q_∞, the infinite dihedral groups D_m and D_a, and the orthogonal groups O_n. Finally, we show how these constructions yield solutions to the generic inverse problem for those groups, that is, we produce generic extensions (Definition 1 below) for those groups.

The case when G is a split extension $H \ltimes G^0$ of its finite group H of connected components, and the adjoint H-action on the Lie algebra of G^0 is faithful, has been partially studied in [6]. The extensions considered there are *generic relative to split G-torsors*, which means that they describe the Picard-Vessiot extensions $E \supset K$ corresponding to G-torsors of the form $G^0 \times W$, for some K-irreducible H-torsor W. In this paper we can completely remove those restrictions for the groups we study. Furthermore, we show that the stronger notion of *descent generic extension* (see comments below Definition 1) holds for these groups. We note, however, that the groups discussed in [6] cover many more cases than the ones for which the first Galois cohomology is well understood.

The notion of generic PVE is closely related to that of generic linear differential operator (equation) with group G. For more on those the reader is referred to [1, 3, 8, 10].

Throughout this paper, all fields will be standard differential fields, i.e., they will have characterstic zero and contain an algebraically closed subfield of constants denoted by $\mathcal{C}$ as before. Our base field will be K. We keep the notation G introduced above.

2. Preliminaries

For a field L, the coordinate ring for G over L is denoted $L[G]$. It has the form $L[X, 1/\det X]$, where X is a generic element in G. For $A \in G(L)$, we let $\rho_A \colon L[G] \to L[G]$ denote the L-algebra automorphism given by $X \mapsto XA$. Also, we let $\lambda_A \colon L[G] \to L[G]$ denote the L-algebra automorphism $X \mapsto A^{-1}X$.

The isomorphism classes of G-torsors over K are classified by the elements in $H^1(K, G)$ in the usual way, cf. [7]: Let $f \colon \mathrm{Gal}(K) \to G(\bar{K})$ be a crossed homomorphism. Then the corresponding *twisted Galois action* on $\bar{K}[G]$ is

$$^{\sigma}x = \rho_{f_\sigma}(\sigma(x)), \quad \sigma \in \mathrm{Gal}(K), \quad x \in \bar{K}[G],$$

meaning that it is the usual Galois action on the scalar field $\bar{K}$, with

$$^{\sigma}X = Xf_\sigma.$$

If we split the crossed homomorphism using Speiser's Theorem, i.e., write

$$f_\sigma = P\sigma(P)^{-1}$$

for some $P \in \mathrm{GL}_n(\bar{K})$, we have that the fixed ring—the coordinate ring for the torsor associated with f—is

$$R = K[Y, 1/\det Y],$$

where $Y = XP$.

The $G(K)$-action on R is the one induced by left multiplication, i.e., through λ.

3. Irreducible torsors

For our purposes—the construction of Picard-Vessiot extensions—we must have that the torsors are irreducible, i.e., that the coordinate ring R is a domain. This is automatically the case if G is connected, since $\bar{K}[G]$ is then a domain. However, we are interested in non-connected groups:

Let $N \triangleleft G$ be the connected component of G, and let $H = G/N$ be the (finite) factor group.

In the coordinate ring $K[G]$, we have a prime ideal $\mathfrak{p}$ defining N, i.e., the coordinate ring for N is $K[G]/\mathfrak{p}$. If NA is another irreducible component of G, it is then given by the prime ideal $\rho_{A^{-1}}(\mathfrak{p})$. In particular, we have an induced isomorphism $\rho_{A^{-1}} \colon K[N] \simeq K[NA]$.

The prime ideals defining the cosets of N in G (i.e., the irreducible components of G) are pair-wise co-maximal and have trivial intersection. By the Chinese Remainder Theorem [12, p. 94], we therefore have

$$K[G] \simeq \bigoplus_{h \in H} K[NA_h]e_h,$$

where the e_h's are orthogonal idempotents, introduced for convenience, and A_h is a pre-image of h in $G(K)$, with $A_1 = I$. The isomorphism is

$$X \mapsto \sum_{h \in H} X_h e_h,$$

with X_h denoting the generic element for NA_h, i.e., the image of X in $K[NA_h]$. The $G(K)$-actions on $K[G]$ of course carry over to this decomposition. We will not need to describe them in detail, but just observe the following: Let $e \in K[G]$ be an element such that $e \equiv 1 \pmod{\mathfrak{p}}$, whereas $e \in \rho_{A_h^{-1}}(\mathfrak{p}) = \mathfrak{p}_h$ for all $h \in H \setminus 1$. Then $e \mapsto e_1$. For $B \in G(K)$, we let $h \in H$ be the image of B, and get that $\rho_{B^{-1}}(e) \mapsto e_h$. Thus,

$$\rho_B \colon e_h \mapsto e_1.$$

It follows immediately that

$$\rho_B \colon e_g \mapsto e_{gh^{-1}}, \quad g \in H :$$

Write $B = C^{-1}D$, where $D \in G(K)$ is a pre-image of g, and $C \in G(K)$ is a pre-image of gh^{-1}. Then ρ_D takes e_g to e_1, and $\rho_{C^{-1}}$ takes e_1 to $e_{gh^{-1}}$.

In a similar manner, we see that

$$\lambda_B \colon e_g \mapsto e_{hg}, \quad g \in H.$$

Now, let once again $f\colon \mathrm{Gal}(K) \to G(\bar{K})$ be a crossed homomorphism, and let P, Y and R be as in the previous section.

We then have a homomorphism $\varphi\colon \mathrm{Gal}(K) \to H$, given by composing f with $G \twoheadrightarrow H$. Let M be the fixed field of $\ker\varphi$ inside $\bar{K}$. Then M/K is a Galois extension, and the Galois group $\mathrm{Gal}(M/K)$ can be canonically identified with a subgroup H' of H. Moreover, we have M embedded in R by

$$\alpha \mapsto \alpha' = \sum_{g \in H'} g^{-1}(\alpha) e_g.$$

If $H' \subsetneq H$, we can find an $h \in H \setminus H'$, and would then have that $\alpha' \cdot \lambda_{A_h}(\alpha') = 0$ for $\alpha \in M$, meaning that R would not be a domain. It is therefore necessary that φ be onto.

Remark. φ is a crossed homomorphism $\mathrm{Gal}(K) \to H$, and consequently represents a Galois algebra over K with Galois group H, cf. [2, p.10]. The Galois twist producing this algebra happens automatically when we take Galois twist to produce R, meaning that the Galois algebra sits inside R. Since a Galois algebra is only a domain if it is a field, and since the Galois algebra is a direct sum of $[H : H']$ copies of M, this means that R cannot be a domain unless $H = H'$. The argument above simply establishes this directly.

Assuming φ to be onto, we then have the H-extension M/K inside R, by

$$\alpha \mapsto \sum_{g \in H} g^{-1}(\alpha) e_g \in R, \quad \alpha \in M.$$

Additionally, the left action of $G(K)$ on R then restricts to the Galois action:

$$\lambda_B(\sum_{g\in H} g^{-1}(\alpha)e_g) = \sum_{g\in H} g^{-1}(\alpha)e_{hg} = \sum_{g\in H} g^{-1}(h(\alpha))e_g,$$

when $B \in G(K)$ is a pre-image of $h \in H$.

We have a restricted crossed homomorphism $f\colon \operatorname{Gal}(M) \to N(\bar{M})$, and accordingly the coordinate ring for an N-torsor $S = M[Z, 1/\det Z]$ over M, where $Z = X_1 P$. We also have a K-algebra homomorphism $\psi\colon R \to S$, given by $\psi(Y) = Z$, obtained by restricting the canonical map $\bar{K}[G] \to \bar{K}[N] = \bar{M}[N]$. Clearly, ψ is onto.

The kernel of ψ is $(\mathfrak{p} \otimes_K \bar{K}) \cap R$. For every $h \in H$, we can find a $\sigma \in \operatorname{Gal}(K)$ with $\varphi(\sigma) = h^{-1}$, and hence ${}^{\sigma}(\mathfrak{p} \otimes_K \bar{K}) = \mathfrak{p}_h \otimes_K \bar{K}$. Thus, an element in $\ker \psi$ must be in all the $\mathfrak{p}_h \otimes_K \bar{K}$'s, i.e., it must be 0. Therefore, ψ is injective.

All in all: $\psi\colon R \to M[Z, 1/\det Z]$ is an isomorphism. Since a torsor for a connected group is irreducible, it follows that R is a domain. Thus, we have

Theorem 1. *The torsor given by f is irreducible if and only if φ is onto.*

The isomorphism $R \simeq M[Z, 1/\det Z]$ also tells us how to construct the coordinate ring: Given $f\colon \operatorname{Gal}(K) \to G(\bar{K})$ as above, with φ onto, we let M/K be an associated H-extension, and $P \in \mathrm{GL}_n(\bar{K})$ a matrix splitting f: $f_\sigma = P\sigma(P)^{-1}$. If X_1 is a generic point for N, the coordinate ring R is $M[Z, 1/\det Z]$, where $Z = X_1 P$, and the G-action on R is given by

$$Z \mapsto B^{-1}Z, \quad \forall \alpha \in M\colon \alpha \mapsto h(\alpha)$$

for $B \in G(\mathcal{C})$ with image $h \in H$.

4. Derivations

Given $R = M[Z, 1/\det Z]$ as above, we impose a derivation on R by

$$Z' = ZA$$

for some $n \times n$ matrix A over M. To see what the possible A's are, we basically recapitulate the general argument in [7]:

On $\bar{R} = \bar{M} \otimes_M R$, we have a generic N-point $X = ZP^{-1}$, and an induced derivation

$$X' = (ZP^{-1})' = X(PAP^{-1} - P'P^{-1}),$$

and it is therefore necessary that $PAP^{-1} - P'P^{-1}$ is in the Lie algebra $\mathfrak{n}(\bar{M})$ for N over $\bar{M}$, i.e., that

$$A \in P^{-1}\mathfrak{n}(\bar{M})P + P^{-1}P'.$$

To ensure that $G(\mathcal{C})$ acts as differential automorphisms, it is also necessary that

$$\lambda_B(Z') = B^{-1}Zh(A) = \lambda_B(Z)' = (B^{-1}Z)' = B^{-1}ZA$$

for $B \in G(\mathcal{C})$, i.e., that A has coefficients in K.

From $f_\sigma = P\sigma(P)^{-1}$ we get that

$$\sigma(P^{-1}\mathfrak{n}(\bar{M})P) = P^{-1}f_\sigma\mathfrak{n}(\bar{M})f_\sigma^{-1}P = P^{-1}\mathfrak{n}(\bar{M})P,$$

so $P^{-1}\mathfrak{n}(\bar{M})P$ is closed under the action of $\mathrm{Gal}(K)$. By the Invariant Basis Lemma it is therefore a K-vector space of dimension $\dim G$.

Also, on $M[G] = M[\hat{X}, 1/\det \hat{X}]$ we can of course define $\hat{X}' = O$, or more generally $(\hat{X}f_\sigma)' = O$ since $\hat{X}f_\sigma$ is also a generic point, and get that $-f_\sigma' f_\sigma^{-1} \in \mathfrak{n}(\bar{M})$, meaning that

$$\sigma(P^{-1}P') - P^{-1}P' = P^{-1}(-f_\sigma' f_\sigma^{-1})P \in P^{-1}\mathfrak{n}(\bar{M})P.$$

Thus, $\sigma \mapsto \sigma(P^{-1}P') - P^{-1}P'$ is an additive crossed homomorphism $\mathrm{Gal}(K) \to P^{-1}\mathfrak{n}(\bar{M})P$, and it follows that it is principal:

$$\sigma(P^{-1}P') - P^{-1}P' = \sigma C - C$$

for some $C \in P^{-1}\mathfrak{n}(\bar{M})P$. But then

$$\begin{aligned}(P^{-1}\mathfrak{n}(\bar{M})P + P^{-1}P')^{\mathrm{Gal}(K)} &= \\ (P^{-1}\mathfrak{n}(\bar{M})P + P^{-1}P' - C)^{\mathrm{Gal}(K)} &= \\ (P^{-1}\mathfrak{n}(\bar{M})P)^{\mathrm{Gal}(K)} + P^{-1}P' - C.\end{aligned}$$

Thus, we have

Theorem 2. *The possible derivations on $M[Z, 1/\det Z]$ are given by*

$$Z' = Z(A + P^{-1}P' - C),$$

where $A \in (P^{-1}\mathfrak{n}(\bar{M})P)^{\mathrm{Gal}(K)}$, and $C \in P^{-1}\mathfrak{n}(\bar{M})P$ satisfies

$$\sigma(P^{-1}P') - P^{-1}P' = \sigma C - C, \quad \sigma \in \mathrm{Gal}(K).$$

Remark. Consider the special case of a finite Galois extension M/K with Galois group $G = \mathrm{Gal}(M/K)$. Here, the crossed homomorphism $f\colon \mathrm{Gal}(K) \to G$ is simply the restriction map, and if we represent G as a matrix group inside some $\mathrm{GL}_n(\mathcal{C})$, we have that there exists an invertible $n \times n$ matrix P over M, such that $M = K(P)$ and $\sigma(P) = \sigma^{-1} \cdot P$ for $\sigma \in G$. (If G happens to be Abelian, it allows a diagonal representation, and we recover classical Kummer theory.) The matrix P is then the generic point Z for the torsor, since after all the generic point for the connected component is I. The derivation is (of course) $Z' = ZP^{-1}P'$, and of necessity $P^{-1}P'$ must be a matrix over K.

5. Special Case: Triviality on N

Let $f\colon \mathrm{Gal}(K) \to G(\bar{K})$ be a crossed homomorphism with φ surjective, and assume that the restriction to $\mathrm{Gal}(M)$ is principal. For instance, this would be the case if the connected component has trivial cohomology. We can then assume that $f_\sigma = 1$ for $\sigma \in \mathrm{Gal}(M)$, from which it follows that f is in fact induced by a crossed homomorphism $\mathrm{Gal}(M/K) \to G(M)$, which we will also denote f. In this case, we then get that φ is the identity on $H = \mathrm{Gal}(M/K)$.

Now, split f by a matrix $P \in \mathrm{GL}_n(M)$: $f_h = Ph(P)^{-1}$. Then the coordinate ring for the torsor is

$$R = M[Z, 1/\det Z] = M[XP, 1/\det(XP)],$$

where X is a generic point for N, and $B \in G(\mathcal{C})$ acts on Z by left multiplication with B^{-1} and on M as its image in $H = \mathrm{Gal}(M/K)$.

Of course, a more natural generator for R over M is X itself. Here, we see that

$$\lambda_B\colon X = ZP^{-1} \mapsto B^{-1}Zh(P^{-1}) = B^{-1}ZP^{-1}f_h = B^{-1}Xf_h.$$

Our result about derivations takes the following form in this case:

Proposition 1. *The possible derivations on R are given by*

$$X' = X(B + C),$$

where $C \in P(P^{-1}\mathfrak{n}(M)P)^H P^{-1} \subseteq \mathfrak{n}(M)$, and $B \in \mathfrak{n}(M)$ satisfies

$$f_h h(B) f_h^{-1} - B = f_h' f_h^{-1}, \quad h \in H.$$

5.1. **The infinite quaternion group, initial discussion.** Let Q_∞ denote the group generated by $\mathbb{G}_m$ and j, subject to the conditions $j^2 = -1 \in \mathbb{G}_m$ and $jxj^{-1} = x^{-1}$ for $x \in \mathbb{G}_m$. Then Q_∞ is generated by the matrices

$$a = \begin{pmatrix} 1/a & 0 \\ 0 & a \end{pmatrix}, \quad j = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

where $a \in \mathbb{G}_m$. This group contains all the quaternion groups $Q_{4n} = \langle \zeta, j \rangle$, where ζ is a primitive $2n^{\text{th}}$ root of unity, hence the name Q_∞.

Since the connected component $\mathbb{G}_m$ has trivial cohomology, we can take the crossed homomorphism to be of the form $f\colon \mathrm{Gal}(M/K) \to Q_\infty(M)$, where M/K is a quadratic extension. Let τ be a generator for $\mathrm{Gal}(M/K)$, and let $f_\tau = cj$, $c \in M^*$. Since $1 = f_1 = f_\tau \tau(f_\tau) = cj\tau(c)j = -c/\tau(c)$, we have $\tau(c) = -c$, and can write $M = K(\sqrt{b})$, where $b = c^2$ and $c = \sqrt{b}$. Thus,

$$f_\tau = \begin{pmatrix} 0 & i/\sqrt{b} \\ i\sqrt{b} & 0 \end{pmatrix}.$$

The coordinate ring for the torsor is $R = M[x, 1/x]$, where $\left(\begin{smallmatrix} x & 0 \\ 0 & 1/x \end{smallmatrix}\right)$ is the generic element in $\mathbb{G}_m$. The $Q_\infty(\mathcal{C})$-action on R is then given by

$$a\colon X \mapsto \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} X = \begin{pmatrix} ax & 0 \\ 0 & 1/ax \end{pmatrix}$$

and

$$j\colon X \mapsto j^{-1} X f_\tau = \begin{pmatrix} \sqrt{b}/x & 0 \\ 0 & x/\sqrt{b} \end{pmatrix},$$

i.e., by

$$\begin{aligned} a\colon \sqrt{b} &\mapsto \sqrt{b}, \quad & x &\mapsto ax, \\ j\colon \sqrt{b} &\mapsto -\sqrt{b}, & x &\mapsto \sqrt{b}/x. \end{aligned}$$

As the matrix P splitting f, we can take

$$P = \begin{pmatrix} i/\sqrt{b} & -i \\ 1 & \sqrt{b} \end{pmatrix},$$

from which we get the derivations

$$X' = X \begin{pmatrix} \alpha\sqrt{b} + b'/4b & 0 \\ 0 & -\alpha\sqrt{b} - b'/4b \end{pmatrix}, \quad \alpha \in K,$$

i.e.,

$$x' = \left(\frac{b'}{4b} + \alpha\sqrt{b}\right)x.$$

Of course, we only get a Picard-Vessiot extension if there are no new constants, i.e., if α is not a rational multiple of a logarithmic derivative in $K(\sqrt{b})$. In that case, the extension $K(\sqrt{b}, x)/K$ is the Picard-Vessiot extension for the differential equation

$$y'' - (\frac{\alpha'}{\alpha} + \frac{b'}{b})y' - \Big((\frac{b'}{4b})' - (\frac{\alpha'}{\alpha} + \frac{3b'}{4b})\frac{b'}{4b} + \alpha^2 b\Big)y = 0,$$

which has x and $\sqrt{b}/x$ as linearly independent solutions.

For instance: Let $K = \mathcal{C}(t)$, with $t' = 1$, and take $b = t$. Since all logarithmic derivatives in $\mathcal{C}(\sqrt{t})$ are rational functions in $\sqrt{t}$ of negative degree, we can then take $\alpha = 1$, and get a $Q_\infty(\mathcal{C})$-extension

$$\mathcal{C}(\sqrt{t}, x)/\mathcal{C}(t),$$

where $t' = 1$ and $x' = (1/4t + \sqrt{t})x$.

More 'generically', we can let $K = \mathcal{C}\langle \alpha, b\rangle$, where α and b are differential indeterminates.

Remark. Let $K = \mathcal{C}((1/t))$ be the Laurent series field in $1/t$, with the usual derivation. Then the Ricatti equation $v' + v^2 = t$ has exactly two solutions in $M = K(\sqrt{t}) = \mathcal{C}((1/\sqrt{t}))$, and these are conjugate under the Galois action. We let

$$a = \sqrt{t} + \sum_{n=0}^{\infty} a_n t^{-n/2}$$

be one of them.

The differential equation $w' - 2aw = 1$ has a (unique) solution in M, which we will simply call w. Then $w'/w - a$ is a solution to the Ricatti equation, i.e., $w'/w - a = \tau(a)$, when τ is the generator for $\mathrm{Gal}(M/K)$. In particular, $w'/w = a + \tau(a) \in K$, which means that w and $\tau(w)$ have the same logarithmic derivative, and therefore that they differ by a constant: $\tau(w) = cw$ for some $c \in \mathcal{C}^*$. Since $w \notin K$ and $\tau^2 = 1$, we get $c = -1$ and $\tau(w) = -w$.

Consequently, $b = w^2 \in K$, and $M = K(\sqrt{b})$, with $\sqrt{b} = w$.

Now, with $\alpha = -\frac{1}{2}w^{-1}$, we get $a = b'/4b + \alpha\sqrt{b}$. A logarithmic derivative in M has no terms in degree ≥ -1, so a is not a rational multiple of a logarithmic derivative, and if we let $x' = ax$, we get a Picard-Vessiot extension with differential Galois group $Q(\mathcal{C})$. The corresponding differential equation is the Airy equation

$$y'' - ty = 0.$$

5.2. **Matrix form equation over K.** In order to construct a generic extension we need a description of the coordinate ring over K as well as the corresponding Q_∞-equivariant derivations on it.

First, we note that a generic point for Q_∞ is

(1)
$$X = e\begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} + (1-e)\begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} j = \begin{pmatrix} ex & (1-e)ix \\ (1-e)i/x & e/x \end{pmatrix},$$

where e is a non-trivial idempotent: the generic point for the multiplicative group is $\left(\begin{smallmatrix} x & 0 \\ 0 & 1/x \end{smallmatrix}\right)$, and the other coset in Q_∞ has representative j.

Therefore a generic point for the torsor corresponding to the matrix P is given by

$$Y = XP = \begin{pmatrix} (e/\sqrt{b} + 1 - e)ix & (-e + (1-e)\sqrt{b})ix \\ (e - (1-e)/\sqrt{b})/x & (1 - e + e\sqrt{b})/x \end{pmatrix} \tag{2}$$

To get a Q_∞-equivariant derivation $Y' = YB$ on the coordinate ring $K[Y, 1/\det(Y)]$, we must then have

$$B = P^{-1}AP + P^{-1}P' = \begin{pmatrix} -\frac{b'}{4b} & -a\sqrt{b} + \frac{b'}{4\sqrt{b}} \\ -\frac{a}{\sqrt{b}} + \frac{b'}{4b\sqrt{b}} & \frac{b'}{4b} \end{pmatrix},$$

where

$$A = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}.$$

For B to be defined over K, we must have

$$a = \frac{b'}{4b} - \frac{\alpha}{\sqrt{b}}, \quad \alpha \in K,$$

and hence

$$B = \begin{pmatrix} -b'/4b & \alpha \\ \alpha/b & b'/4b \end{pmatrix}. \tag{3}$$

Thus, the general matrix form equation over K for the quaternion group is

$$Y' = Y\begin{pmatrix} -b'/4b & \alpha \\ \alpha/b & b'/4b \end{pmatrix}.$$

5.3. **The multiplicative dihedral group.** An easier example is the dihedral group D_m, generated by $\mathbb{G}_m$ and τ, where $\tau^2 = 1$ and $\tau x \tau^{-1} = x^{-1}$ for $x \in \mathbb{G}_m$. As a linear algebraic group, it is generated by the matrices

$$a = \begin{pmatrix} 1/a & 0 \\ 0 & a \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

for $a \in \mathbb{G}_m$. The computations proceed like for Q_∞ above, except that we get $f_1 = f_\tau \tau(f_\tau) = 1$, and hence $\tau(c) = c$, i.e.,

$$f_\tau = \begin{pmatrix} 0 & 1/c \\ c & 0 \end{pmatrix}.$$

A generic point is

$$X = \begin{pmatrix} ex & (1-e)x \\ (1-e)/x & e/x \end{pmatrix}, \tag{4}$$

and we have

$$P = \begin{pmatrix} 1 & -\sqrt{b} \\ c & c\sqrt{b} \end{pmatrix}. \tag{5}$$

Consequently,

$$Y = XP = \begin{pmatrix} (e+(1-e)c)x & (-e+(1-e)c)\sqrt{b}\,x \\ (1-e+ec)/x & (ex+e-1)\sqrt{b}/x \end{pmatrix}. \tag{6}$$

The derivations $Y' = YB$ must have

$$B = P^{-1}AP + P^{-1}P' = \begin{pmatrix} \frac{c'}{2c} & \frac{(c'-2ac)\sqrt{b}}{2c} \\ \frac{c'-2ac}{2\sqrt{b}\,c} & \frac{b'}{2b} + \frac{c'}{2c} \end{pmatrix}$$

for

$$A = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$$

and a of the form

$$a = \frac{c'}{2c} - \frac{d}{\sqrt{b}}, \quad d \in K,$$

meaning that

$$B = \begin{pmatrix} c'/2c & d \\ d/b & b'/2b + c'/2c \end{pmatrix}. \tag{7}$$

The equation for D_m is therefore

$$Y' = Y \begin{pmatrix} c'/2c & d \\ d/b & b'/2b + c'/2c \end{pmatrix}.$$

5.4. **The additive dihedral group.** An even easier example is the dihedral group D_a, generated by $\mathbb{G}_a$ and τ, with relations $\tau^2 = 0$ and $\tau a \tau^{-1} = -a$ for $a \in \mathbb{G}_a$. As a matrix group, it is generated by

$$a = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The crossed homomorphism can then be taken to be $f_\tau = \tau$.

A generic point for D_a is

$$X = \begin{pmatrix} 1 & (2e-1)x \\ 0 & 2e-1 \end{pmatrix},$$

and

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{b} \end{pmatrix}. \tag{8}$$

Therefore, a generic point for the torsor corresponding to P is

$$Y = YP = \begin{pmatrix} 1 & (2e-1)\sqrt{b}\,x \\ 0 & (2e-1)\sqrt{b} \end{pmatrix}. \tag{9}$$

The D_a-equivariant derivations on the coordinate ring are then $Y' = YB$ with

$$B = P^{-1}AP + P^{-1}P' = \begin{pmatrix} 0 & a\sqrt{b} \\ 0 & b'/2b \end{pmatrix},$$

where

$$A = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}.$$

Clearly, we must have $a = c/\sqrt{b}$, and hence

$$B = \begin{pmatrix} 0 & c \\ 0 & b'/2b \end{pmatrix}. \tag{10}$$

The equation for D_a is thus

$$Y' = Y \begin{pmatrix} 0 & c \\ 0 & b'/2b \end{pmatrix}.$$

5.5. **The orthogonal group.** For $n \in \mathbb{N}$, the *orthogonal group* is the subgroup

$$\mathrm{O}_n = \{X \in \mathrm{GL}_n \mid X^t X = I\}$$

of GL_n. Its connected component is the *special orthogonal group*

$$\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n.$$

The associated Lie algebra $\mathfrak{so}_n$ consists of all anti-symmetric $n \times n$ matrices. It follows easily that $\dim \mathrm{O}_n = \frac{1}{2}n(n-1)$.

The cohomology $H^1(\mathrm{Gal}(K), \mathrm{O}_n(\bar{K}))$ can be interpreted as classifying regular quadratic spaces of dimension n over K: Given a regular quadratic form

$$q = a_1 x_1^2 + \cdots + a_n x_n^2$$

with $a_1, \ldots, a_n \in K^*$, we let

$$P = \begin{pmatrix} \sqrt{a_1} & & & \\ & \sqrt{a_2} & & \\ & & \ddots & \\ & & & \sqrt{a_n} \end{pmatrix} \tag{11}$$

and

$$Q = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}.$$

Then $P^t P = Q$, and we have a crossed homomorphism $f\colon \mathrm{Gal}(K) \to \mathrm{O}_n(\bar{K})$ given by $f_\sigma = P\sigma(P)^{-1}$ for $\sigma \in \mathrm{Gal}(K)$. In this way, isomorphism classes of regular n-dimensional quadratic spaces over K correspond bijectively to cohomology classes of crossed homomorphisms.

Thus, the quadratic form q gives rise to a torsor, and this torsor will be irreducible if $\varphi = \det(f)\colon \mathrm{Gal}(K) \to C_2 = \{\pm 1\}$ is onto, i.e., if $d(q) = a_1 \cdots a_n$ is not a square in K.

So, assume that $d(q)$ is not a square. Then the coordinate ring for the torsor is $R = K[Z, 1/\det(Z)]$, where

$$Z = XP \tag{12}$$

for a generic O_n-point X. The defining relation for Z is

$$Z^t Z = Q,$$

and in R, $\det(Z)$ is a square root of $d(q)$.

A matrix $U \in \mathrm{O}_n(\mathcal{C})$ acts on R by $U\colon Z \mapsto U^{-1}Z$.

To find the derivations on R, we note that

$$P^{-1}\begin{pmatrix} 0 & b_{12} & b_{13} & \dots & b_{1n} \\ -b_{12} & 0 & b_{23} & \dots & b_{2n} \\ -b_{13} & -b_{23} & 0 & \dots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_{1n} & -b_{2n} & -b_{3n} & \dots & 0 \end{pmatrix} P =$$
$$\begin{pmatrix} 0 & \frac{\sqrt{a_2}}{\sqrt{a_1}}b_{12} & \frac{\sqrt{a_3}}{\sqrt{a_1}}b_{13} & \dots & \frac{\sqrt{a_n}}{\sqrt{a_1}}b_{1n} \\ -\frac{\sqrt{a_1}}{\sqrt{a_2}}b_{12} & 0 & \frac{\sqrt{a_3}}{\sqrt{a_2}}b_{23} & \dots & \frac{\sqrt{a_n}}{\sqrt{a_2}}b_{2n} \\ -\frac{\sqrt{a_1}}{\sqrt{a_3}}b_{13} & -\frac{\sqrt{a_2}}{\sqrt{a_3}}b_{23} & 0 & \dots & \frac{\sqrt{a_n}}{\sqrt{a_3}}b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\frac{\sqrt{a_1}}{\sqrt{a_n}}b_{1n} & -\frac{\sqrt{a_2}}{\sqrt{a_n}}b_{2n} & -\frac{\sqrt{a_3}}{\sqrt{a_n}}b_{3n} & \dots & 0 \end{pmatrix},$$

and that this matrix has coefficients in K if and only if $b_{ij} = \sqrt{a_i}/\sqrt{a_j} \cdot c_{ij}$ for some $c_{ij} \in K$.

The O_n-equivariant derivations are then

$$Z' = ZB,$$

where

$$B = \begin{pmatrix} \frac{a_1'}{2a_1} & c_{12} & c_{13} & \dots & c_{1n} \\ -\frac{a_1}{a_2}c_{12} & \frac{a_2'}{2a_2} & c_{23} & \dots & c_{2n} \\ -\frac{a_1}{a_3}c_{13} & -\frac{a_2}{a_3}c_{23} & \frac{a_3'}{2a_3} & \dots & c_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\frac{a_1}{a_n}c_{1n} & -\frac{a_2}{a_n}c_{2n} & -\frac{a_3}{a_n}c_{3n} & \dots & \frac{a_n'}{2a_n} \end{pmatrix} \tag{13}$$

and $c_{ij} \in K$.

Over $\bar{K}[Z] = \bar{K}[\mathrm{O}_n]$, this means that

$$X' = XA$$

for

$$A = \begin{pmatrix} 0 & \frac{\sqrt{a_1}}{\sqrt{a_2}}c_{12} & \frac{\sqrt{a_1}}{\sqrt{a_3}}c_{13} & \cdots & \frac{\sqrt{a_1}}{\sqrt{a_n}}c_{1n} \\ -\frac{\sqrt{a_1}}{\sqrt{a_2}}c_{12} & 0 & \frac{\sqrt{a_2}}{\sqrt{a_3}}c_{23} & \cdots & \frac{\sqrt{a_2}}{\sqrt{a_n}}c_{2n} \\ -\frac{\sqrt{a_1}}{\sqrt{a_3}}c_{13} & -\frac{\sqrt{a_2}}{\sqrt{a_3}}c_{23} & 0 & \cdots & \frac{\sqrt{a_3}}{\sqrt{a_n}}c_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\frac{\sqrt{a_1}}{\sqrt{a_n}}c_{1n} & -\frac{\sqrt{a_2}}{\sqrt{a_n}}c_{2n} & -\frac{\sqrt{a_3}}{\sqrt{a_n}}c_{3n} & \cdots & 0 \end{pmatrix}. \tag{14}$$

6. Generic extensions

Next, we set up the machinery to show that the above calculations yield solutions to the generic inverse differential Galois problem for those groups.

Let $\mathfrak{gl}_m(\cdot)$ denote the Lie algebra of $m \times m$ matrices with coefficients in some specified field and consider the differential rational field $\mathcal{K} = \mathcal{C}\langle Z_1, \ldots, Z_k\rangle$, where the Z_i are differentially independent indeterminates over $\mathcal{C}$.

We will use the terminology 'Picard-Vessiot G-extension' with the obvious meaning 'PVE with differential Galois group isomorphic to G'.

Definition 1. A Picard-Vessiot G-extension $\mathcal{E} \supset \mathcal{K}$ for the equation $X' = X\mathcal{A}(Z_i)$, with $\mathcal{A}(Z_i) \in \mathfrak{gl}_m(\mathcal{K})$ for some m, is said to be *a generic extension for* G when the following condition holds: for any differential field K with field of constants $\mathcal{C}$ there is a PVE $E \supset K$ with differential Galois group $H \leq G$ if and only if there are $k_i \in K$, $i = 1, \ldots, n$, such that the matrix $\mathcal{A}(k_i)$ is well defined, the equation $X' = X\mathcal{A}(k_i)$ gives rise to the extension $E \supset K$, and any fundamental solution matrix maps to one for the specialized equation.

In our earlier papers [8, 9] generic extensions as in Definition 1 were called *descent generic* and discussed separately. In those papers and in [6] the term *generic extension* was used in a weaker sense, that is, not requiring specialization to H-extensions for proper subgroups H of G. That distinction is especially important in [6]: the PVE's studied there are restricted to function fields of split G-torsors, limiting the class of subgroups H for which PVE's with group H can be obtained by specialization. In [8, 9] and here the description of the torsors that we provide makes possible the specialization to all PVE's corresponding to proper subgroups.

We proceed now to the construction of generic extensions. The first step is to produce a suitable PVE for each of the groups.

For Q_∞ we put $\mathcal{K} = \mathcal{C}\langle \alpha, b\rangle$ with α and b differentially independent indeterminates over $\mathcal{C}$, and let $\mathcal{E}$ be the differential field $\mathcal{K}(Y)$, $Y' = YB$, where Y and B are given by (2)-(3) in Section 5.1. Since α is obviously not a rational multiple of a logarithmic derivative in $\mathcal{K}(\sqrt{b})$ the discussion in Section 5.1 shows that $\mathcal{E} \supset \mathcal{K}$ is a PVE with differential Galois group Q_∞.

For the multiplicative dihedral D_m we let b, c, and d be differentially independent indeterminates over $\mathcal{C}$ and put $\mathcal{K} = \mathcal{C}\langle b, c, d\rangle$. Then

$$a = \frac{c'}{2c} - \frac{d}{\sqrt{b}}$$

is differentially transcendental over $\mathcal{C}$. By abuse of notation, we will also let $\sqrt{b}$ denote the element $-\sqrt{b}e + \sqrt{b}(1-e) \in \mathcal{K}[Y, 1/\det(Y)]$ and x the element $x(\frac{e}{\sqrt{b}} + (1-e))$. Then [5, Theorem 4.1.2] implies that the extension $\mathcal{K}(\sqrt{b})(Z) \supset \mathcal{K}(\sqrt{b})$, with $Z = \left(\begin{smallmatrix} x & 0 \\ 0 & 1/x \end{smallmatrix}\right)$ a generic $\mathbb{G}_m$-point and derivation given by $Z' = ZA$,

$$A = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix},$$

is a PVE with differential Galois group the multiplicative group $\mathbb{G}_m$. Since a generic point for an irreducible D_m-torsor is of the form $Y = XP$ for X and P as in (4)-(5) we have that $\mathcal{K}(\sqrt{b})(Y) = \mathcal{K}(\sqrt{b})(Z) \supset \mathcal{K}(\sqrt{b})$, with $Y' = YB$, for B as in (7), is a no new constant extension and so is $\mathcal{K}(Y) \supset \mathcal{K}$, $Y' = YB$. The discussion in Section 5.3 then implies that the latter is a PVE with differential Galios group D_m.

In the case of the additive dihedral D_a, for the differentially independent indeterminates over $\mathcal{C}$ we take b and c and put $\mathcal{K} = \mathcal{C}\langle c, d\rangle$. Then $\mathcal{K}(Y) \supset \mathcal{K}$, $Y' = YB$ with Y, B as in (9)-(10), is a PVE with differential Galois group D_a corresponding to a non-trivial torsor associated to a matrix P of the form (8). The proof is almost identical to the one for D_m and we will omit the details.

Our last case corresponds to the orthogonal groups O_n. In [8] we showed that if $a_1, \ldots, a_{n-1}$, c_{ij}, $1 \le i \le n-1$, $2 \le j \le n$, $i < j$, are differentially independent indeterminates over $\mathcal{C}$ and $a_n = 1/a_1 \cdots a_{n-1}$, then the equation $X' = XA$, with A as in (13), has differential Galois group SO_n over $\mathcal{L} = \mathcal{C}\langle a_i, Z_{ij}\rangle$ where $Z_{ij} = \frac{\sqrt{a_i}}{\sqrt{a_j}} c_{ij}$, $1 \le i \le n-1$, $2 \le j \le n$, $i < j$. Working inside the coordinate ring of the O_n-torsor, this immediately implies that the equation $Y' = YB$ where Y, B are as in (12)-(14) has differential Galois group O_n over $\mathcal{K} =$

$\mathcal{C}\langle a_1, \ldots, a_{n-1}, c_{12}, \ldots, c_{n-1,n}\rangle$. Furthermore the torsor corresponding to the PVE arising from this equation has associated matrix P of the form (11), and thus is non-split over $\mathcal{K}$. In particular, this feature makes the construction here more general than the one in [6].

Finally we will show that the PVE for the infinite quaternion discussed above is generic for this group. The proof for the other groups can be done in a similar way and will be omitted. We proceed as in [8, 9]: First, we let $Z_1 = \alpha$, $Z_2 = b$ and the matrix $\mathcal{A}(Z_i)$ in Definition 1 be the matrix B in (3). Assume that $E \supset K$ is a PVE with differential Galois group $H \leq \mathrm{Q}_\infty$ and let X (respectively X_H) denote the generic point of Q_∞ (respectively of H). We have that $E = K(Y)$, where $Y = X_H P$ for some invertible matrix P with coefficients in $\bar{K}$ and there is a K-algebra homomorphism of coordinate rings

$$K[XP, \det(XP)^{-1}] \twoheadrightarrow K[X_H P, \det(X_H P)^{-1}].$$

Since $X_H P$ is a generic point for an H-torsor we have that XP is a generic point for a Q_∞-torsor, and therefore any H-equivariant derivation on the coordinate ring of the H-torsor arises from a Q_∞-equivariant derivation on the coordinate ring of Q_∞. This implies that the generic point Y satisfies an equation with matrix $\tilde{B} = \mathcal{A}(K_i)$ for some $k_i \in K$.

Likewise, a specialization $\mathcal{A}(k_i)$ of $\mathcal{A}(Z_i)$ with $k_i \in K$, gives a derivation on the coordinate ring $F[XP, \det(XP)^{-1}]$ of a Q_∞-torsor, which may have new constants. We get a PVE of K by taking the quotient field of the factor ring

$$K[XP, \det(XP)^{-1}]/M,$$

where M is a maximal differential ideal. The differential Galois group in this case is the closed subgroup H of Q_∞ consisting of those elements that stabilize M.

Finally, it is clear that a fundamental matrix for the equation $\eta' = \eta\mathcal{A}(Z_i)$ specializes to one for $\eta' = \eta\mathcal{A}(k_i)$ since, on the one hand, a solution of $\eta' = \eta\mathcal{A}(Z_i)$ is given by a generic point XP of the Q_∞-torsor corresponding to the the matrix

$$P = \begin{pmatrix} i/\sqrt{b} & -i \\ 1 & \sqrt{b} \end{pmatrix},$$

and X a generic point of Q_∞.

On the other hand, a solution of $\eta' = \eta\mathcal{A}(k_i)$ is given by the generic point $XP(k_i)$ of the Q_∞-torsor corresponding to the matrix

$$P(k_i) = \begin{pmatrix} i/\sqrt{k}_2 & -i \\ 1 & \sqrt{k}_2 \end{pmatrix},$$

Clearly the matrix P allows specialization to any nonzero values of b.

References

[1] A. K. Bhandari and N. Sankaran, Generic differential equations and Picard-Vessiot extensions. Ren. Sem. Mat. Univ. Pol. Torino 52 (1994) 353–358.

[2] S. Garibaldi, A. Merkurjev and J. P. Serre, Cohomological Invariants in Galois Cohomology, University Lecture Series, 28, American Mathematical Society (2003).

[3] L. Goldman, Specialization and Picard–Vessiot theory, Trans. Amer. Math. Soc. 85 (1957). 327–356.

[4] Principal differential ideals and a generic inverse differential Galois problem for GL_n, Comm. Algebra 30 (2002), 6071–6103.

[5] L. Juan, Pure Picard-Vessiot extensions with generic properties, Proc. Amer. Math. Soc., 9 (2004) 2549-2556.

[6] L. Juan, Generic Picard-Vessiot extensions for connected by finite groups, J. Alg. 312 (2007), 194–206.

[7] L. Juan and A. Ledet, Equivariant vector fields on non-trivial SO_n-torsors and Differential Galois Theory, J. Alg., to appear.

[8] L. Juan and A. Ledet, On generic SO_n-extensions (preprint).

[9] L. Juan and A. Ledet, On Picard-Vessiot extensions with group PGL_3 (preprint).

[10] L. Juan and A. Magid, Generic rings for Picard-Vessiot extensions and generic differential equations, J. Pure Appl. Algebra, 209 (2007) 793–800.

[11] M. V. Kondratieva, A. B. Levin, A. V. Mikhalev and E. V. Pankatriev, Differential and Difference Dimension Polynomials, Kluwer Academic Publishers, Dordrecht, 1999.

[12] S. Lang, Algebra, Revised Third Edition, Springer-Verlag, 2002.

[13] A. Magid, Lectures in Differential Galois Theory, University Lecture Series, 7, American Mathematical Society (1994).

[14] M. Van der Put and M. Singer, Galois Theory of Linear Differential Equations, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 328, Springer-Verlag, Berlin, 2003.

[15] J. P. Serre, Galois Cohomology, Springer-Verlag, 1997.

[16] T. A. Springer, Linear Algebraic Groups, Birkh auser, 1998.

Department of Mathematics and Statistics, Texas Tech University, Box 41042, Lubbock, Texas 79409-1042, USA

E-mail address: `lourdes.juan@ttu.edu and arne.ledet@ttu.edu`