ARTICLE IN PRESS

YJABR:11435

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Algebra ••• (••••) •••–•••

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Equivariant vector fields on non-trivial SO_n-torsors and differential Galois theory

Lourdes Juan *, Arne Ledet

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

Received 27 September 2006

Communicated by Harm Derksen

Abstract

We show how to produce SO_n-equivariant vector fields on non-trivial SO_n-torsors which correspond to quadratic forms non-equivalent to the unit form. For $n \geqslant 3$ we then give an example of a Picard–Vessiot extension with group SO_n which is the function field of a non-trivial SO_n-torsor.

Keywords: Differential Galois theory; Galois cohomology; Quadratic forms; Special orthogonal groups; Torsors; Picard–Vessiot extensions

1. Introduction

Let K be a field of characteristic $\neq 2$. It is well known that the Galois cohomology with coefficients in the special orthogonal group $H^1(K, \mathrm{SO}_n)$ is in bijective correspondence with the isomorphism classes of regular n-dimensional quadratic forms over K of discriminant 1, under Galois twist [6, Theorem 5.3.1]. It is also the case that for any linear algebraic group G defined over K, the cohomology classes in $H^1(K, G)$ correspond to isomorphism classes of G-torsors [9, Proposition 33]. Thus, in particular, the isomorphism classes of SO_n-torsors are in bijective correspondence with the isomorphism classes of regular n-dimensional quadratic forms over K of discriminant 1.

The above facts tie with differential Galois theory as follows: If K is a differential field of characteristic zero with algebraically closed field of constants $\mathcal{C}$, a Picard–Vessiot extension

* Corresponding author.
E-mail addresses: lourdes.juan@ttu.edu (L. Juan), arne.ledet@ttu.edu (A. Ledet).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2007.01.005

Please cite this article in press as: L. Juan, A. Ledet, Equivariant vector fields on non-trivial SO_n-torsors and differential Galois theory, J. Algebra (2007), doi:10.1016/j.jalgebra.2007.01.005

of K with group $G = G(\mathcal{C})$ is the function field $K(W)$ of some K-irreducible G-torsor W (see [7, Theorem 5.12] or [8, Theorem 1.28]).

If G is finite, W must be non-trivial since the trivial G-torsor is reducible unless G is the trivial group. Thus, in the finite case, Picard–Vessiot G-extensions of K correspond to function fields of non-trivial K-irreducible G-torsors. Moreover, the extension of the derivation of K to a G-equivariant derivation of a Galois G-extension is automatic and hence so is the existence of equivariant vector fields on the corresponding torsor.

So, from the point of view of differential Galois theory, the more interesting and challenging cases occur when the connected component of the group is non-trivial and, in particular, when the group G is connected.

If $K \subset E$ are differential fields and S is a subset of E, we will write $K\langle S\rangle$ to denote the differential subfield of E generated by K and S. As usual, if G acts on the ring R as automorphisms, R^G will denote the fixed ring.

A Picard–Vessiot extension $E \supset K$ with group G is also determined by the following data [7, Proposition 3.9]:

(1) A G-equivariant derivation D on the G-module E, that extends the derivation of $K = E^G$ with no new constants (note that D corresponds to a G-equivariant vector field on a K-irreducible G torsor W as above).
(2) A G-stable finite-dimensional $\mathcal{C}$-vector space V, such that $E = K\langle V\rangle$ (a $\mathcal{C}$-basis of V corresponds to an E-point of W).

All G-torsors become trivial over $\bar{K}$. Having a distinguished point, namely the identity element, the trivial G-torsor has a natural G-equivariant tangent space associated to it: the Lie algebra of G. This tangent space is isomorphic to the K-vector space of G-equivariant derivations over K on the coordinate ring $K[G]$.

When G is connected, any such derivation extends G-equivariantly to the function field $K(G)$. We then see that $K(G) = K\langle V\rangle$, where V is the G-stable $\mathcal{C}$-vector space spanned by the coordinate functions on G.

It appears that this natural G-equivariant differential structure on $K(G)$ makes it a favorite candidate when it comes to producing Picard–Vessiot extensions of K with connected group G.

In this paper we look at the case of function fields of non-trivial G-torsors, for connected groups G. In particular, we show how one can produce SO_n-equivariant vector fields on non-trivial SO_n-torsors and use this to give an explicit example of a Picard–Vessiot extension which is the function field of a non-trivial G-torsor, with G connected.

The reader is assumed to be familiar with the basic notions of the Picard–Vessiot theory. Some good sources are [7,8].

2. Quadratic forms and torsors

For the convenience of the reader we recall the following basic facts about quadratic forms and torsors.

2.1. Quadratic forms

Let K be a field of characteristic $\neq 2$. A *quadratic* form over K is a map $q : V \to K$, where V is a finite-dimensional K-vector space, such that $q(\mathbf{x}) = B(\mathbf{x}, \mathbf{x})$ for some symmetric bilinear

Please cite this article in press as: L. Juan, A. Ledet, Equivariant vector fields on non-trivial SO_n-torsors and differential Galois theory, J. Algebra (2007), doi:10.1016/j.jalgebra.2007.01.005

form $B : V \times V \to K$. Thus, if we pick a basis $\mathbf{e}_1, \dots, \mathbf{e}_n$ for V, we get

$$q(\mathbf{x}) = (x_1, \dots, x_n) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

where $\mathbf{x} = x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n$, and $A = (B(\mathbf{e}_i, \mathbf{e}_j))_{i,j}$. We say that the quadratic form is *represented* by A in the given basis.

If we choose another basis for V, the matrix B representing q in the new basis will have the form $B = P^T A P$, where $P \in \mathrm{GL}_n(K)$ is the coordinate transformation matrix for the two bases.

In particular: If q is represented by an invertible matrix in one basis, any matrix representing it will be invertible. We then refer to the quadratic form as *regular*. In this case, the determinant of a matrix representing q is called the *discriminant* of q. Since $\det(B) = \det(P)^2 \det(A)$, the discriminant is only determined up to a quadratic factor.

Two quadratic forms $q : V \to K$ and $q' : V' \to K$ are *equivalent*, if there exists a vector space isomorphism $f : V \to V'$ such that $q(\mathbf{x}) = q'(f(\mathbf{x}))$ for all $\mathbf{x} \in V$. In terms of matrices, this means: if A represents q, and B represents q', there exists an invertible matrix P with $P^T A P = B$.

An equivalence of q with itself is called an *isometry*. The isometries of q form a group, called the *orthogonal group* for q, denoted $\mathrm{O}(q)$. If we pick a basis for V, in which q is represented by A, the orthogonal group consists of all matrices P with $P^T A P = A$. In particular, an isometry must have determinant ± 1. The isometries with determinant 1 form a subgroup of $\mathrm{O}(q)$, called the *special orthogonal group* and denoted $\mathrm{SO}(q)$.

In the special case of the quadratic form $\mathbf{1}_n : K^n \to K$, given by $\mathbf{1}_n(\mathbf{x}) = x_1^2 + \cdots + x_n^2$, the orthogonal and special orthogonal groups are denoted by $\mathrm{O}_n(K)$ and $\mathrm{SO}_n(K)$, respectively.

Every regular quadratic form is *diagonalizable*, i.e., representable by a diagonal matrix.

An excellent reference for quadratic forms is [5]. For a more comprehensive review of the basic facts than the one provided here, see also Chapter 7 in [6].

We now show the following criterion which will be needed in our construction of a non-trivial SO_n-torsor:

Lemma 1. *Let k be a field containing a primitive fourth root of unity, and let $a_1, \dots, a_{n-1}$, $n \geqslant 3$, be indeterminates over k. Then the quadratic form $a_1x_1^2 + \cdots + a_nx_n^2$, where $a_n = (a_1 \cdots a_{n-1})^{-1}$, is not equivalent to $\mathbf{1}_n$ over $k(a_1, \dots, a_{n-1})$.*

Proof. If it were, we would have

$$a_1x_1^2 + \cdots + a_nx_n^2 \sim x_1^2 + \cdots + x_n^2,$$

and since

$$x_1^2 + \cdots + x_n^2 \sim a_1x_1^2 + a_1x_2^2 + x_3^2 + \cdots + x_n^2,$$

it follows that

$$a_1x_2^2 + \cdots + x_n^2 \sim a_2x_2^2 + \cdots + a_nx_n^2,$$

Please cite this article in press as: L. Juan, A. Ledet, Equivariant vector fields on non-trivial SO_n-torsors and differential Galois theory, J. Algebra (2007), doi:10.1016/j.jalgebra.2007.01.005

and hence that the quadratic form $a_2x_2^2 + \cdots + a_nx_n^2$ represents 1. Note that $a_2, \ldots, a_n$ are algebraically independent over k. Now, by assumption we have polynomials $f, f_2, \ldots, f_n \in k[a_2, \ldots, a_n]$ such that

$$a_2 f_2^2 + \cdots + a_n f_n^2 = f^2,$$

and $f \neq 0$. Let $\tilde{f}$ be the lowest-degree term in f as a polynomial in a_2. Then $\tilde{f}^2$ is the sum of the lowest-degree terms in $a_i f_i^2$ for those $i > 2$ for which f_i has the same lowest degree in a_2 as f. The term $a_2 f_2^2$ cannot contribute, since its lowest degree in a_2 is odd. Therefore we have that

$$a_3 \tilde{f}_3^2 + \cdots + a_n \tilde{f}_n^2 = \tilde{f}^2,$$

for polynomials $\tilde{f}, \tilde{f}_3, \ldots, \tilde{f}_n \in k[a_3, \ldots, a_n]$. By recursion, we end up with one indeterminate and a statement

$$g^2 = a_n g_n^2$$

for $g, g_n \in k[x]$, $g \neq 0$, which is clearly impossible. $\square$

2.2. Torsors

Let K be a perfect field, and let it be understood in this section that all varieties are defined over K, and that they are reduced of finite type, i.e., that they are spectra of finitely generated commutative K-algebras with no nilpotents.

Given an algebraic group G, a variety V is then said to be a G-*torsor*, if G acts on V and the induced map $G \times V \to V \times V$ corresponding to $(\sigma, x) \mapsto (\sigma x, x)$ is an isomorphism of varieties (see [8]).

The algebraic group G is itself a G-torsor in the obvious way, and is said to be *trivial*. The trivial G-torsor is characterized by having K-rational points.

For a finite group G, the G-torsors are the spectra of Galois algebras over K with Galois group G. Here, the trivial G-torsor corresponds to the *split* Galois algebra $K^{|G|}$, whereas Galois field extensions correspond to irreducible G-torsors.

Scalar extensions of torsors are again torsors, over the scalar-extended group variety.

Every G-endomorphism on a G-torsor is automatically an automorphism. In the case of the trivial G-torsor G itself, the G-automorphisms form a group isomorphic to the group $G(K)$ of K-rational points.

Theorem 1. *(See [9, Proposition 33].) The isomorphism classes of G-torsors correspond bijectively to the equivalence classes of crossed homomorphisms in $H^1(K, G)$.*

Here, a *crossed homomorphism* is a continuous map $e : \mathrm{Gal}(K) \to G(\bar{K})$, where $\mathrm{Gal}(K)$ is the absolute Galois group of K, satisfying

$$e_{\sigma\tau} = e_\sigma \sigma e_\tau,$$

and two crossed homomorphisms e and e' are *equivalent* if

$$e'_\sigma = f e_\sigma \sigma f^{-1}$$

for some $f \in G(\bar{K})$.

A crossed homomorphism e gives rise to a torsor as follows: Let H be the Hopf algebra corresponding to G. On the scalar extension $\bar{H} = H \otimes_K \bar{K}$, we then have an obvious $\mathrm{Gal}(K)$-action, and we define an e-twisted action by

$${}^\sigma x = e_\sigma(\sigma x), \quad \sigma \in \mathrm{Gal}(K).$$

The fixed ring $R = \bar{H}^{\mathrm{Gal}(K)}$ under this action is then the coordinate ring for a G-torsor, with the G-action induced by the restriction $\alpha : R \to H \otimes_K R$ of the co-multiplication on $\bar{H}$.

For more on G-torsors see [9,10].

3. The twisted Lie algebra

Let $G \subseteq \mathrm{GL}_n(\mathcal{C})$ be a connected linear algebraic group, and let $H = K[X, 1/\det(X)]$ be the coordinate ring over K, where X is a generic point of G. Given a crossed homomorphism $e : \mathrm{Gal}(K) \to G(\bar{K})$, we get an e-twisted Galois action on $\bar{H} = \bar{K} \otimes_K H$ by

$${}^\sigma z = e_\sigma(\sigma z),$$

and a corresponding coordinate ring for a torsor $T = \bar{H}^{\mathrm{Gal}(K)}$. Here, the G-action on H (and $\bar{H}$) is given by

$${}^g X = Xg, \quad g \in G.$$

Now, by Speiser's Theorem (see [6, Exercise 1.61]), there exists $P \in \mathrm{GL}_n(\bar{K})$ with $e_\sigma = P\sigma P^{-1}$, and with $Y = XP$ we have

$${}^\sigma Y = XP\sigma P^{-1}\sigma P = XP = Y,$$

from which it follows that we can realize T explicitly inside $\bar{H}$ as $T = K[Y, 1/\det(Y)]$.

We then have a G-action on T given by

$${}^g Y = g^{-1} Y, \quad g \in G.$$

Define a derivation on T by

$$Y' = YB$$

for some $B \in M_n(K)$. The fact that the derivation is expressed by multiplication from the right guarantees that the G-action on T is differential.

It then extends to $\bar{H}$, where

$$X' = XA = X\big(PBP^{-1} - P'P^{-1}\big),$$

Please cite this article in press as: L. Juan, A. Ledet, Equivariant vector fields on non-trivial SO_n-torsors and differential Galois theory, J. Algebra (2007), doi:10.1016/j.jalgebra.2007.01.005

and hence, if we let $\mathfrak{g}$ denote the Lie algebra $\mathrm{Lie}(G)$, we see that

$$A \in \mathfrak{g}(\bar{K})$$

and

$$B = P^{-1}AP + P^{-1}P' \in \left[P^{-1}P' + P^{-1}\mathfrak{g}(\bar{K})P\right] \cap M_n(K).$$

Here, $P^{-1}\mathfrak{g}(\bar{K})P$ is a Lie algebra, and since $e_\sigma = P\sigma P^{-1} \in G(\bar{K})$, meaning that conjugation by e_σ is an automorphism on $\mathfrak{g}(\bar{K})$, we see that this Lie algebra is closed under the (un-twisted) Galois action. Thus, by the Invariant Basis Lemma (see [3], [6, Exercise 1.61], or [2, Lemma 5]),

$$\mathfrak{T} = \left(P^{-1}\mathfrak{g}(\bar{K})P\right)^{\mathrm{Gal}(K)}$$

is a Lie algebra over K of the same dimension, which we can think of as being obtained by a Galois twist of $\mathfrak{g}(K)$.

Remark. The Galois twist can be realized by interpreting e_σ as an automorphism of $\mathfrak{g}(\bar{K})$ by conjugation which gives rise to a Galois twist $P\mathfrak{T}P^{-1}$ ($\cong \mathfrak{T}$) of $\mathfrak{g}(K)$. For that reason, we call $\mathfrak{T}$ the *twisted Lie algebra* associated to the torsor with coordinate ring T.

Proposition 1. *The possible choices of B form a co-space with respect to $\mathfrak{T}$. I.e., there exist possible B's, and if C is one of them, all the others are the elements of $C + \mathfrak{T}$.*

Proof. Clearly we can define a derivation on $\bar{H}$ by $X' = 0$, and get by computations as above that $Y' = YP^{-1}P'$. Applying the twisted Galois action, we get conjugate derivations $Y' = Y\sigma P^{-1}\sigma P'$ for all $\sigma \in \mathrm{Gal}(K)$, for which we have

$$X' = X\left(P\sigma P^{-1}\sigma P'P^{-1} - P'P^{-1}\right),$$

and therefore

$$P\sigma P^{-1}\sigma P'P^{-1} - P'P^{-1} \in \mathfrak{g}(\bar{K}),$$

or

$$\sigma\left(P^{-1}P'\right) - P^{-1}P' \in P^{-1}\mathfrak{g}(\bar{K})P.$$

Obviously, $\sigma \mapsto \sigma(P^{-1}P') - P^{-1}P'$ is an additive crossed homomorphism, and since $P^{-1}\mathfrak{g}(\bar{K})P$ is a finite-dimensional $\bar{K}$-vector space with a semilinear $\mathrm{Gal}(K)$-action, the additive Hilbert 90 gives us that it is principal, i.e., that there exists a $D \in P^{-1}\mathfrak{g}(\bar{K})P$ with

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

In particular, $P^{-1}P' - D$ is $\mathrm{Gal}(K)$-invariant, and so

Please cite this article in press as: L. Juan, A. Ledet, Equivariant vector fields on non-trivial SO_n-torsors and differential Galois theory, J. Algebra (2007), doi:10.1016/j.jalgebra.2007.01.005

$$\begin{aligned}\left[P^{-1}P' + P^{-1}\mathfrak{g}(\bar{K})P\right]^{\mathrm{Gal}(K)} &= \left[\left(P^{-1}P' - D\right) + P^{-1}\mathfrak{g}(\bar{K})P\right]^{\mathrm{Gal}(K)} \\ &= \left(P^{-1}P' - D\right) + \left[P^{-1}\mathfrak{g}(\bar{K})P\right]^{\mathrm{Gal}(K)} = \left(P^{-1}P' - D\right) + \mathfrak{T}.\end{aligned}$$

Thus, the possible choices for B form a co-space for $\mathfrak{T}$, as claimed. □

4. The special orthogonal groups

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

$$\mathrm{SO}_n = \left\{X \in \mathrm{GL}_n \;\middle|\; X^t X = I,\ \det(X) = 1\right\}$$

of GL_n.

The corresponding Lie algebra $\mathfrak{so}_n$ consists of all antisymmetric $n \times n$ matrices, from which we immediately get that SO_n has dimension $\frac{1}{2}n(n-1)$.

Let K be a field of characteristic $\neq 2$ as before, and let $\bar{K}_{\mathrm{sep}}$ denote its separable closure. The correspondence between the cohomology classes in $H^1(K, \mathrm{SO}_n)$ and the isomorphism classes of regular n-dimensional quadratic forms of discriminant 1 can be realized as follows:

Given a crossed homomorphism $e : \mathrm{Gal}(K) \to \mathrm{O}_n(\bar{K}_{\mathrm{sep}})$, we define the e-twisted Galois action on $\bar{K}_{\mathrm{sep}}^n$ by

$${}^{\sigma}\mathbf{x} = e_\sigma(\sigma\mathbf{x}), \quad \mathbf{x} \in \bar{K}_{\mathrm{sep}}^n,\ \sigma \in \mathrm{Gal}(K),$$

and get the twisted quadratic space by restricting the quadratic form $\mathbf{1}_n$ to the K-vector space V_e of fixed points under this action. This defines a quadratic form $q : V_e \to K$, since e_σ is an isometry, so that $\mathbf{1}_n({}^{\sigma}\mathbf{x}) = \mathbf{1}_n(\sigma\mathbf{x}) = \sigma\mathbf{1}_n(\mathbf{x})$, making the image of a fixed point a fixed point, i.e., an element in K. If e maps into $\mathrm{SO}_n(\bar{K}_{\mathrm{sep}})$, this space will have discriminant 1.

Thus, the isomorphism classes of SO_n-torsors correspond to those of quadratic forms with square discriminant. In particular, a quadratic form not equivalent to the unit form $\mathbf{1}_n$ will correspond to a non-trivial torsor.

Assume that K is a differential field of characteristic zero with algebraically closed field of constants $\mathcal{C}$. Let

$$q = a_1x_1^2 + \cdots + a_nx_n^2$$

be a regular quadratic form with $a_1, \ldots, a_n \in K^*$ and (say) $d(q) = a_1 \cdots a_n = 1$. Put

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

with the square roots chosen to have product 1 as well, and

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

We then have $P^t P = Q$, and get a crossed homomorphism $f : \mathrm{Gal}(K) \to \mathrm{SO}_n(\bar{K})$ by $f_\sigma = P\sigma P^{-1}$ for $\sigma \in \mathrm{Gal}(K)$. This establishes the correspondence between isomorphism classes of regular n-dimensional quadratic spaces with square discriminant over K and cohomology classes of crossed homomorphisms (and between the former and the isomorphism classes of SO_n-torsors).

Assuming the quadratic form to be as above, the coordinate ring for the corresponding torsor is then $T = K[Y, 1/\det(Y)]$, where $Y = XP$ for a generic SO_n-point X. The defining relations for Y are

$$Y^t Y = Q \quad \text{and} \quad \det(Y) = 1$$

(thus we can omit $1/\det(Y)$ in the description of T). The $\mathrm{SO}_n(\mathcal{C})$-action on T is given by

$$\Sigma : Y \mapsto \Sigma^{-1} Y, \quad \Sigma \in \mathrm{SO}_n(\mathcal{C}).$$

To find the derivations on T, we first conjugate a typical element of $\mathfrak{so}_n(\bar{K})$:

$$P^{-1} \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ -a_{12} & 0 & a_{23} & \cdots & a_{2n} \\ -a_{13} & -a_{23} & 0 & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{1n} & -a_{2n} & -a_{3n} & \cdots & 0 \end{pmatrix} P$$

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

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

The relevant derivations on T thus have the form

$$Y' = YB,$$

where

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

and $b_{ij} \in K$.

Please cite this article in press as: L. Juan, A. Ledet, Equivariant vector fields on non-trivial SO_n-torsors and differential Galois theory, J. Algebra (2007), doi:10.1016/j.jalgebra.2007.01.005

Note that in this case the twisted Lie algebra $\mathfrak{T}$ over K consists of the matrices

$$\begin{pmatrix} 0 & b_{12} & b_{13} & \cdots & b_{1n} \\ -\frac{a_1}{a_2}b_{12} & 0 & b_{23} & \cdots & b_{2n} \\ -\frac{a_1}{a_3}b_{13} & -\frac{a_2}{a_3}b_{23} & 0 & \cdots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\frac{a_1}{a_n}b_{1n} & -\frac{a_2}{a_n}b_{2n} & -\frac{a_3}{a_n}b_{3n} & \cdots & 0 \end{pmatrix} \tag{1}$$

and that

$$B \in P'P^{-1} + \mathfrak{T},$$

since $P'P^{-1}$ has coefficients in K.

5. Picard–Vessiot extension

Since the special orthogonal group SO_2 is isomorphic to the multiplicative group, the case $n = 2$ is completely trivial and we shall assume that $n \geqslant 3$ in what follows.

From (1) we can go back to an element $A = (a_{ij}) \in \mathfrak{so}_n(\bar{K})$ through conjugation by P:

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

We now show that there are $a_1, \dots, a_n$ and b_{ij}, $1 \leqslant i \leqslant n-1$, $2 \leqslant j \leqslant n$, such that the equation $X' = XA$ has differential Galois group SO_n and the corresponding quadratic form $\langle a_1, \dots, a_n \rangle$ is not equivalent to $\mathbf{1}_n = \langle 1, \dots, 1 \rangle$. From this, we produce a matrix B in the twisted Lie algebra associated to the non-trivial torsor for the crossed homomorphism given by P with differential Galois group SO_n.

Please cite this article in press as: L. Juan, A. Ledet, Equivariant vector fields on non-trivial SO_n-torsors and differential Galois theory, J. Algebra (2007), doi:10.1016/j.jalgebra.2007.01.005

Let $a_1, \ldots, a_{n-1}$ be differentially independent over $\mathcal{C}$ and $a_n = 1/a_1 \cdots a_{n-1}$. Put $b_{i,i+1} = a_{i+1}$, for $i < n-1$, $b_{n-1,n} = a_n$ if n is odd and $b_{n-1,n} = a_{n-1}a_n$ otherwise. We let b_{ij}, $i+1 < j$, be differentially independent over $\mathcal{C}$ as well. If n is odd one has,

$$A = \begin{pmatrix} 0 & \sqrt{a_1}\sqrt{a_2} & \frac{\sqrt{a_1}}{\sqrt{a_3}}b_{13} & \cdots & \frac{\sqrt{a_1}}{\sqrt{a_n}}b_{1n} \\ -\sqrt{a_1}\sqrt{a_2} & 0 & \sqrt{a_2}\sqrt{a_3} & \cdots & \frac{\sqrt{a_2}}{\sqrt{a_n}}b_{2n} \\ -\frac{\sqrt{a_1}}{\sqrt{a_3}}b_{13} & -\sqrt{a_2}\sqrt{a_3} & 0 & \cdots & \frac{\sqrt{a_3}}{\sqrt{a_n}}b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\frac{\sqrt{a_1}}{\sqrt{a_{n-1}}}b_{1,n-1} & -\frac{\sqrt{a_2}}{\sqrt{a_{n-1}}}b_{2,n-1} & -\frac{\sqrt{a_3}}{\sqrt{a_{n-1}}}b_{3,n-1} & \cdots & \sqrt{a_{n-1}}\sqrt{a_n} \\ -\frac{\sqrt{a_1}}{\sqrt{a_n}}b_{1n} & -\frac{\sqrt{a_2}}{\sqrt{a_n}}b_{2n} & -\frac{\sqrt{a_3}}{\sqrt{a_n}}b_{3n} & \cdots & 0 \end{pmatrix}$$

for n even,

$$A = \begin{pmatrix} 0 & \sqrt{a_1}\sqrt{a_2} & \frac{\sqrt{a_1}}{\sqrt{a_3}}b_{13} & \cdots & \frac{\sqrt{a_1}}{\sqrt{a_n}}b_{1n} \\ -\sqrt{a_1}\sqrt{a_2} & 0 & \sqrt{a_2}\sqrt{a_3} & \cdots & \frac{\sqrt{a_2}}{\sqrt{a_n}}b_{2n} \\ -\frac{\sqrt{a_1}}{\sqrt{a_3}}b_{13} & -\sqrt{a_2}\sqrt{a_3} & 0 & \cdots & \frac{\sqrt{a_3}}{\sqrt{a_n}}b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\frac{\sqrt{a_1}}{\sqrt{a_{n-1}}}b_{1,n-1} & -\frac{\sqrt{a_2}}{\sqrt{a_{n-1}}}b_{2,n-1} & -\frac{\sqrt{a_3}}{\sqrt{a_{n-1}}}b_{3,n-1} & \cdots & \sqrt{a_{n-1}}\sqrt{a_n}a_{n-1} \\ -\frac{\sqrt{a_1}}{\sqrt{a_n}}b_{1n} & -\frac{\sqrt{a_2}}{\sqrt{a_n}}b_{2n} & -\frac{\sqrt{a_3}}{\sqrt{a_n}}b_{3n} & \cdots & 0 \end{pmatrix}.$$

Let Z_{ij}, $i < j$, denote the corresponding ij-entry in either of the above matrices. We show that the Z_{ij} are differentially independent over $\mathcal{C}$ as follows: let $K = \mathcal{C}\langle a_i, b_{ij}\rangle$, $\mathcal{F} = \mathcal{C}\langle Z_{ij}\rangle$, $i = 1, \ldots, n-1$, $i+2 \leqslant j \leqslant n$. For odd n one has,

$$Z_{n-1,n} \prod_{i<n,\, i \text{ odd}} Z_{i,i+1} = \sqrt{a_{n-1}} \prod_{i=1}^{n} \sqrt{a_i} = \sqrt{a_{n-1}},$$

and for even n,

$$\prod_{i<n,\, i \text{ odd}} Z_{i,i+1} = a_{n-1} \prod_{i=1}^{n} \sqrt{a_i} = a_{n-1}.$$

Thus, in either case $a_{n-1} \in \mathcal{F}$. This immediately implies that $a_i, b_{ij} \in \mathcal{F}$, $i = 1, \ldots, n-1$, $i+2 \leqslant j \leqslant n$, thus $\mathcal{F} \supset K \supset \mathcal{C}$. Therefore the differential transcendence degree [4, Definition 3.2.33 and Theorem 5.4.12] of $\mathcal{F}$ over $\mathcal{C}$ must be $\frac{1}{2}(n-1)n$. This proves our claim.

Now, we observe that $A = \sum_{j=i+2}^{n} \sum_{i=1}^{n-1} Z_{ij} A_{ij}$, where A_{ij} are the basis of $\mathfrak{so}_n(\mathcal{C})$ consisting of the antisymmetric matrices with 1 in the ij-entry, -1 in the ji-entry and 0 otherwise. By [1, Theorem 4.1.2] it then follows that $\mathcal{F}(\mathrm{SO}_n) \supset \mathcal{F}$, is a Picard–Vessiot extension with group SO_n for the equation $X' = XA$.

Since $\bar{K} = \bar{\mathcal{F}}$ we have that $\bar{K}(\mathrm{SO}_n) \supset \mathcal{F}(\mathrm{SO}_n)$ is an algebraic extension. Since the field of constants of $\mathcal{F}(\mathrm{SO}_n)$ is algebraically closed, $\bar{K}(\mathrm{SO}_n)$ must have no new constants and $\bar{K}(\mathrm{SO}_n) \supset \bar{K}$ is a Picard–Vessiot extension with group SO_n.

The discussion in the previous section implies that the matrix

$$B = \begin{pmatrix} \frac{a_1'}{2a_1} & a_2 & b_{13} & \cdots & b_{1n} \\ -a_1 & \frac{a_2'}{2a_2} & a_3 & \cdots & b_{2n} \\ -\frac{a_1}{a_3} b_{13} & -a_2 & \frac{a_3'}{2a_3} & \cdots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\frac{a_1}{a_n} b_{1n} & -\frac{a_2}{a_n} b_{2n} & -\frac{a_3}{a_n} b_{3n} & \cdots & \frac{a_n'}{2a_n} \end{pmatrix}$$

defines a derivation on the coordinate ring $T = K[Y]$ of the SO_n-torsor corresponding to the quadratic form given by the matrix

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

which by Lemma 1 is non-trivial (let $k(a_1, \ldots, a_{n-1})$ in the lemma be $\mathcal{C}\langle a_1, \ldots, a_{n-1}\rangle$).

Since $\bar{K}(Y) = \bar{K}(X)$, as a differential field it will be isomorphic to $\bar{K}(\mathrm{SO}_n)$. Therefore, the field of constants of $\bar{K}(Y)$ is $\mathcal{C}$. In particular, this implies that $K(Y) \supset K$ is a no new constant extension. This shows that the function field of the non-trivial SO_n-torsor corresponding to Y is a Picard–Vessiot extension of K with group SO_n.

Acknowledgment

We are grateful to Michael Singer for suggesting the approach that we followed in finding G-equivariant vector fields on non-trivial G-torsors.

References

[1] L. Juan, Pure Picard–Vessiot extensions with generic properties, Proc. Amer. Math. Soc. 9 (2004) 2549–2556.
[2] G. Kemper, G. Malle, Invariant fields of finite irreducible reflection groups, Math. Ann. 315 (1999) 569–586.
[3] E. Kolchin, S. Lang, Existence of invariant bases, Proc. Amer. Math. Soc. 11 (1960) 140–148.
[4] M.V. Kondratieva, A.B. Levin, A.V. Mikhalev, E.V. Pankatriev, Differential and Difference Dimension Polynomials, Kluwer Academic Publishers, Dordrecht, 1999.
[5] T.Y. Lam, Introduction to Quadratic Forms over Fields, Grad. Stud. Math., vol. 67, American Mathematical Society, 2005.
[6] A. Ledet, Brauer Type Embedding Problems, Fields Monogr. Math., vol. 21, American Mathematical Society, 2005.
[7] A. Magid, Lectures in Differential Galois Theory, Univ. Lecture Ser., American Mathematical Society, 1994.
[8] M. Van der Put, M. Singer, Galois Theory of Linear Differential Equations, Grundlehren Math. Wiss. (Fundamental Principles of Mathematical Sciences), vol. 328, Springer-Verlag, Berlin, 2003.
[9] J.P. Serre, Galois Cohomology, Springer-Verlag, 1997.
[10] T.A. Springer, Linear Algebraic Groups, Birkhäuser, 1998.