On the structure of Picard-Vessiot extensions

- Joint work with Arne Ledet -

Kolchin Seminar in Differential Algebra

May 06, 2006

(Sixth Visit Since March 17, 2001)

K is assumed to be a differential field of characteristic zero with algebraically closed field of constants $\mathcal{C}$ and G, a linear algebraic group defined over $\mathcal{C}$.

A *Picard-Vessiot ring over* K for the equation $y' = Ay$, with $A \in \mathrm{M}_n(K)$, is a simple differential ring R over K such that R is generated as a ring by K, the entries of a fundamental matrix F and the inverse of the determinant of F.

Theorem (Kolchin's Main Structure Theorem). *Let R be a Picard-Vessiot ring with differential Galois group G. Then $Z = max(R)$ is a G-torsor over K.*

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

For groups such as SO_n and PGL_n, in turn, the cohomology can be interpreted in terms of quadratic forms and central simple algebras, providing a convinient way to describe the torsors.

The SO_n case

Theorem. *The elements of $H^1(K, SO_n)$ correspond bijectively to the equivalence classes of n-dimensional quadratic forms over K of discriminant 1.*

Therefore, there is a bijective correspondence between isomorphism classes of SO_n-torsors and equivalence classes of n-dimensional quadratic forms over K of discriminant 1. In particular, a quadratic form not equivalent to the unit form $\mathbf{1}_n$, will correspond to a non-trivial torsor.

From now on we will assume that $n = 3$.

By definition, we have that $\mathsf{SO}_3 \leq \mathsf{SL}_3$.

Let $a, b \in K^*$ be elements such that the quadratic form $q = \langle a, b, 1/ab \rangle$ is not equivalent to $\mathbf{1}_3 = \langle 1, 1, 1 \rangle$. Let

$$Q = \begin{pmatrix} a & & \\ & b & \\ & & 1/ab \end{pmatrix}.$$

Over K, the Hopf algebra corresponding to the special orthogonal group SO_3 is

$$H = K[X \mid X^T X = I,\ \det(X) = 1],$$

where the 3×3-matrix X is a coordinate matrix for SO_3.

On H, we have an action of $\mathsf{SO}_3(K)$ given by

$$\Sigma\colon X \mapsto X\Sigma, \quad \Sigma \in \mathsf{SO}_3(\mathcal{C}).$$

Let

$$\begin{aligned} \bar{H} &= \bar{K}[X \mid X^T X = I,\ \det(X) = 1] \\ &= \bar{K} \otimes_K H \end{aligned}$$

Over $\bar{K}$, we have the matrix

$$P = \begin{pmatrix} \sqrt{a} & & \\ & \sqrt{b} & \\ & & 1/\sqrt{a}\sqrt{b} \end{pmatrix}$$

with $P^T P = Q$. With $Y = XP$, we then have

$$Y^T Y = P^T X^T X P = P^T P = Q.$$

Also, with $e_\sigma = P\sigma P^{-1} \in \mathsf{SO}_3(\bar{K})$, we get a crossed homomorphism $e\colon \mathsf{Gal}(K) \to \mathsf{SO}_3(\bar{K})$, and therefore a twisted Galois action

$$^{\sigma}z = e_\sigma(\sigma z), \quad \sigma \in \mathsf{Gal}(K), \quad z \in \bar{H}.$$

In particular, we have

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

since $X \in K[X]$ is invariant under the original Galois action. Hence

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

so Y is invariant under this action. Thus, the fixed ring is

$$\bar{H}^{\mathsf{Gal}(K)} = K[Y] = K[Y \mid Y^T Y = Q,\ \mathrm{det}(Y) = 1].$$

Non-trivial SO_3-torsor

Let $T = K[Y]$. T is then (by construction) the coordinate ring for the SO_3-torsor corresponding to the crossed homomorphism e. By assumption, this torsor is non-trivial, since q and $\mathbf{1}_3$ are not equivalent over K.

Group action

The group action is induced by the homomorphism $T \to H \otimes_K T$ given by

$$Y \mapsto (X \otimes 1)(1 \otimes Y),$$

and this in turn induces an $\mathsf{SO}_3(K)$-action on T: An element $\Sigma \in \mathsf{SO}_3(K)$ defines a K-rational point $H \to K$, and by composition with

$$T \to H \otimes_K T$$

we get an automorphism $T \to T$. Taken directly, this is given by $Y \mapsto \Sigma Y$. However, this does not define a (left) group action, due to the contravariant nature of the variety/coordinate ring correspondence. Thus, to get an induced SO_3-action on T, we replace Σ by Σ^{-1}, getting

$${}^{\Sigma}Y = \Sigma^{-1}Y, \quad \Sigma \in \mathsf{SO}_3(\mathcal{C}).$$

Equivariant derivations

We define a derivation on T by

$$Y' = YB$$

for some 3×3 matrix B over K. We multiply B on from the right in order to ensure that

$$^{\Sigma}(Y') = {}^{\Sigma}(YB) = \Sigma^{-1}YB = (^{\Sigma}Y)',$$

i.e., that the $\mathrm{SO}_3(\mathcal{C})$-action is differential.

Such a derivation extends to $T \otimes_K \bar{K} = \bar{H}$, where we have

$$\begin{aligned} X' &= (YP^{-1})' = Y'P^{-1} + Y(P^{-1})' \\ &= Y(BP^{-1} + (P^{-1})') = X(PBP^{-1} + P(P^{-1})') \\ &= X(PBP^{-1} - P'P^{-1}) = XA. \end{aligned}$$

Since X is a generic point of SO_3, A must be anti-symmetric. Also,

$$A = \begin{pmatrix} b_{11} - a'/2a & \sqrt{a}/\sqrt{b} \cdot b_{12} & a\sqrt{b} \cdot b_{13} \\ \sqrt{b}/\sqrt{a} \cdot b_{21} & b_{22} - b'/2b & b\sqrt{a} \cdot b_{23} \\ 1/a\sqrt{b} \cdot b_{31} & 1/b\sqrt{a} \cdot b_{32} & b_{33} + a'/2a + b'/2b \end{pmatrix},$$

and so it is necessary and sufficient that B has the form

$$B = \begin{pmatrix} a'/2a & \alpha & \beta \\ -a\alpha/b & b'/2b & \gamma \\ -a^2b\beta & -ab^2\gamma & -a'/2a - b'/2b \end{pmatrix}$$

for $\alpha, \beta, \gamma \in K$.

For such a B, we then get an SO_3-equivariant derivation on T.

In particular,

$$A = \begin{pmatrix} 0 & \sqrt{a}/\sqrt{b}\cdot\alpha & a\sqrt{b}\cdot\beta \\ -\sqrt{a}/\sqrt{b}\cdot\alpha & 0 & b\sqrt{a}\cdot\gamma \\ -a\sqrt{b}\cdot\beta & -b\sqrt{a}\cdot\gamma & 0 \end{pmatrix} \quad (1)$$

Note that the matrices

$$\begin{pmatrix} 0 & \alpha & \beta \\ -a\alpha/b & 0 & \gamma \\ -a^2b\beta & -ab^2\gamma & 0 \end{pmatrix}$$

form a Lie algebra $\mathfrak{T}$ over K, and that

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

Thus, in a sense, $\mathfrak{T}$ is the Lie algebra associated to the torsor. Conjugating by P, we see that this Lie algebra is isomorphic to the one consisting of matrices of the form (1) above.

More on the twisted Lie Algebra (in general)

Let $G \subseteq \mathsf{GL}_n(\mathcal{C})$ be a connected algebraic group, and let $H = K[X]$ be the coordinate ring over K, where X is a generic point of G. Given a crossed homomorphism e: $\mathsf{Gal}(K) \to G(\bar{K})$, 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 $T = \bar{H}^{\mathsf{Gal}(K)}$. Here, the G-action on H (and $\bar{H}$) is given by

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

Now, by Speiser's Theorem, there exists $P \in \mathsf{GL}_n(\bar{K})$ 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 $T = K[Y]$.

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

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

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

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

and

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

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,

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

is a Lie algebra over K of the same dimension, which we can think of as being obtained by a Galois twist of $\mathfrak{g}(K)$. (In fact, this can be made literally true by interpreting e_σ as an automorphism on $\mathfrak{g}(\bar{K})$ by conjugation.)

Proposition. *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 $C + \mathfrak{T}$.*

Picard-Vessiot extension

Let $K = \mathcal{C}\langle a, b, \alpha, \beta, \gamma\rangle$ where $a, b, \alpha, \beta, \gamma$ are differentially independent over $\mathcal{C}$.

We will show that the equation $X' = XA$ where

$$A = \begin{pmatrix} 0 & \sqrt{a}/\sqrt{b}\cdot\alpha & a\sqrt{b}\cdot\beta \\ -\sqrt{a}/\sqrt{b}\cdot\alpha & 0 & b\sqrt{a}\cdot\gamma \\ -a\sqrt{b}\cdot\beta & -b\sqrt{a}\cdot\gamma & 0 \end{pmatrix} \in \mathrm{M}_3(\overline{K})$$

has differential Galois group SO_3. Moreover, via the twisting process described above, this matrix descends to a matrix B over K with the same group and such that the corresponding Picard-Vessiot extension is the function field of a nontrivial SO_3-torsor.

Let $Z_1 = \sqrt{a}/\sqrt{b} \cdot \alpha$, $Z_2 = a\sqrt{b} \cdot \beta$ and $Z_3 = b\sqrt{a} \cdot \gamma$. Notice that $a\sqrt{b}$, $b\sqrt{a}$, Z_1, Z_2, Z_3 are differentially independent over $\mathcal{C}$ since

$$[(a\sqrt{b})^2(b\sqrt{a})^{-1}]^2 = \left(\frac{a^2}{\sqrt{a}}\right)^2 = a^3$$

$$[(b\sqrt{a})^2(a\sqrt{b})^{-1}]^2 = \left(\frac{b^2}{\sqrt{b}}\right)^2 = b^3$$

and $a^3, b^3, \alpha, \beta, \gamma \in \mathcal{C}\langle a\sqrt{b}, b\sqrt{a}, Z_1, Z_2, Z_3\rangle$ are differentially independent over $\mathcal{C}$, which forces the extension $\mathcal{C}\langle a\sqrt{b}, b\sqrt{a}, Z_1, Z_2, Z_3\rangle \supset \mathcal{C}$ to have differential transcendence degree 5.

Let $F = \mathcal{C}\langle a\sqrt{b}, b\sqrt{a}, Z_1, Z_2, Z_3\rangle$. Since $A = Z_1A_1 + Z_2A_2 + Z_3A_3$ where $A_1 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}$, $A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$, is a basis of Lie($SO_3$), by a previous result it then follows that $F(SO_3) \supset F$, is a Picard-Vessiot extension with group SO_3 for the equation $X' = XA$.

Since $a^3, b^3, \alpha, \beta, \gamma \in F$ we have that $a, b, \alpha, \beta, \gamma \in \bar{F}$ and thus $\bar{K} = \bar{F}$. Therefore, $\bar{K}(\mathrm{SO}_3) \supset F(\mathrm{SO}_3)$ is an algebraic extension. Since the field of constants of $F(\mathrm{SO}_3)$ is the algebraically closed field $\mathcal{C}$, $\bar{K}(\mathrm{SO}_3)$ must have no new constants and $\bar{K}(\mathrm{SO}_3) \supset \bar{K}$ is a Picard-Vessiot extension with group SO_3.

Then,

$$B = \begin{pmatrix} a'/2a & \alpha & \beta \\ -a\alpha/b & b'/2b & \gamma \\ -a^2b\beta & -ab^2\gamma & -a'/2a - b'/2b \end{pmatrix}$$

defines a derivation on the coordinate ring $T = K[Y|Y^TY = Q]$ of the non-trivial SO_3-torsor corresponding to the quadratic form given by the matrix

$$Q = \begin{pmatrix} a & & \\ & b & \\ & & 1/ab \end{pmatrix}.$$

Since $\bar{K}(Y) = \bar{K}(X)$, as a differential field it will be isomorphic to $\bar{K}(\mathsf{SO}_3)$. 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_3-torsor corresponding to Y is a Picard-Vessiot extension of K with group SO_3.

Generic Extensions

Definition. Suppose that $Y_1, \ldots, Y_n$ are differentially independent over $\mathcal{C}$ and put $\mathcal{F} = \mathcal{C}\langle Y_1, \ldots, Y_n \rangle$. We say that a Picard-Vessiot G-extension $\mathcal{E} \supset \mathcal{F}$ for the matrix equation $X' = X\mathcal{A}(Y_1, \ldots, Y_n)$, with $\mathcal{A}(Y_1, \ldots, Y_n) \in \mathrm{gl}_m(\mathcal{F})$ *is generic for G* if,

1. For every Picard-Vessiot extension $E \supset F$ with differential Galois group $H \leq G$, such that the field of constants of F is $\mathcal{C}$, there is a specialization $Y_i \to f_i \in F$ such that the equation $X' = X\mathcal{A}(f_1, \ldots, f_n)$ gives rise to this extension.

2. For every specialization$Y_i \to f_i \in F$, the differential equation $X' = X\mathcal{A}(f_1, \ldots, f_n)$ gives rise to a Picard-Vessiot extension $E \supset F$ with differential Galois group $H \leq G$.

Theorem. *The extension $K(Y) \supset K$ is a generic Picard-Vessiot extension for* SO_3.

Proof. We let $Y_i = Z_i$, $i = 1, \ldots, 3$, $Y_4 = a\sqrt{b}$, $Y_5 = b\sqrt{a}$ and $A(Y_1, \ldots, Y_5) = B$.

Suppose that $E \supset F$ is a Picard-Vessiot extension with differential Galois group $H \leq SO_3$. Let X, X_H respectively denote generic points of SO_3 and H. Then $E = F(Y)$ where $Y = X_H P$, for some invertible matrix P with coefficients in $\bar{F}$. Moreover, there is an F-algebra homomorphism of coordinate rings

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

Since $X_H P$ is a generic point for an H-torsor we have that XP is a generic point for an SO_3-torsor and therefore the (twisted) Lie algebra associated to the H-torsor is contained in that for the SO_3-torsor. In turn, this implies that the generic point Y satisfies a matrix equation with matrix $\tilde{B} = \mathcal{A}(f_1, \ldots, f_5)$ for some $f_i \in F$.

Likewise, a specialization $\mathcal{A}(f_1, \ldots, f_5)$ of $\mathcal{A}(Y_1, \ldots, Y_5)$ with $f_i \in F$, gives a derivation on the coordinate ring $F[XP, \det(XP)^{-1}]$ of an SO_3-torsor, which may not be irreducible. The corresponding Picard-Vessiot extension will be the quotient field of the factor ring

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

where M is a maximal differential ideal. The differential Galois group therefore is the closed subgroup of SO_3 consisting of those elements that stabilize M. $\square$

Observe that the trivial torsor case is also covered in this situation. For, if we let $a = b = 1$ in

$$B = \begin{pmatrix} a'/2a & \alpha & \beta \\ -a\alpha/b & b'/2b & \gamma \\ -a^2b\beta & -ab^2\gamma & -a'/2a - b'/2b \end{pmatrix}$$

it becomes

$$A = \begin{pmatrix} 0 & \alpha & \beta \\ -\alpha & 0 & \gamma \\ -\beta & -\gamma & 0 \end{pmatrix}$$

which is a typical element in $\mathrm{Lie}(\mathrm{SO}_3)$.

The PGL_2 case

Theorem. *There is a bijective correspondence between 4-dimensional central simple algebras and the elements of* $H^1(K, PGL_2)$.

A 4-dimensional CSA is a quaternion algebra and is given by a quadratic form.

Representation as a matrix group

We have a homomorphism $\varphi\colon \mathrm{PGL}_2 \to \mathrm{SL}_3$, given by

$$\varphi\colon \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \mapsto$$
$$\frac{1}{\det(x_{ij})} \begin{pmatrix} x_{11}^2 & x_{11}x_{12} & x_{12}^2 \\ 2x_{11}x_{21} & x_{11}x_{22} + x_{12}x_{21} & 2x_{12}x_{22} \\ x_{21}^2 & x_{21}x_{22} & x_{22}^2 \end{pmatrix}.$$

This homomorphism arises as follows: Let GL_2 act on the polynomial ring in two variables s and t in the obvious manner, and consider the resulting action of a matrix on the three-dimensional space of homogeneous quadratic polynomials, represented in the basis s^2, st, t^2. This gives a homomorphism $\mathrm{GL}_2 \to \mathrm{GL}_3$, and after dividing by the determinant, we get φ.

Lemma 1. φ: $\mathsf{PGL}_2 \to \mathsf{SL}_3$ *is injective, and the image is an algebraic subgroup of* SL_3.

Lie Algebra

Lemma 2. *The Lie algebra associated with* PGL_2 *is* $\mathfrak{pgl}_2$*, consisting of the matrices*

$$\begin{pmatrix} x & y & 0 \\ z & 0 & 2y \\ 0 & z/2 & -x \end{pmatrix}.$$

Proof. We use the representation of PGL_2 as an algebraic subgroup of SL_3 given in Lemma 1. By definition, a 3×3 matrix A is then in the Lie algebra if and only if $1 + \varepsilon A$ satisfies the conditions defining PGL_2, where ε is an 'algebraic infinitesimal', i.e., a non-zero quantity satisfying $\varepsilon^2 = 0$.

Since

$$\begin{pmatrix} 1+\varepsilon x & \varepsilon y & 0 \\ \varepsilon z & 1 & 2\varepsilon y \\ 0 & \frac{1}{2}\varepsilon z & 1-\varepsilon x \end{pmatrix} = \varphi \begin{pmatrix} 1+\frac{1}{2}\varepsilon x & \varepsilon y \\ \frac{1}{2}\varepsilon z & 1-\frac{1}{2}\varepsilon x \end{pmatrix},$$

we see that $\mathfrak{pgl}_2$ certainly contains the required matrices, and since $\mathfrak{pgl}_2$ has dimension 3 (as PGL_2 itself has), they constitute the entire Lie algebra.

□

The cohomology

Let K be a field. From the short-exact sequence

$$1 \to \bar{K}^* \to \mathrm{GL}_2(\bar{K}) \to \mathrm{PGL}_2(\bar{K}) \to 1,$$

we get (part of) a long-exact cohomology sequence

$$1 \to H^1(K, \mathrm{PGL}_2) \underset{\delta}{\to} H^2(K, \mathbb{G}_\mathrm{m}),$$

and if we identify $H^2(K, \mathbb{G}_\mathrm{m})$ with the Brauer group $\mathrm{Br}(K)$, it is known that

Lemma 3. *For $e \in H^1(K, \mathrm{PGL}_2)$ we have $\delta[e] = [\mathrm{M}_2(K)_e]$, where $\mathrm{M}_2(K)_e$ is the Galois twist of $\mathrm{M}_2(K)$ by e.*