On Magid's approach to the inverse problem in differential Galois theory.

Jerry Kovacic, Claude Mitschi, Michael F. Singer

On Magid's Approach to the Inverse Problem in Differential Galois Theory

J. Kovacic* C. Mitschi† M.F. Singer‡

March 25, 1996

The aim of this note is to expand on a footnote contained in our paper [4]. This footnote alluded to a counterexample (due to Kovacic) to the following Theorem (Theorem 7.13 of [3]):

> *Let* $D_1, \dots, D_n$ *be a* C*-basis of* $\mathrm{Lie}(G)$ *and let* $f_1, \dots, f_n \in F = C(x)$ *be linearly independent over* C*. With* $D_F = \frac{d}{dx}$ *let* $D = D_F \otimes 1 + \sum f_i \otimes D_i$ *be the corresponding derivation of* $F[G_F]$*. Let* P *be a maximal* $D-$*stable ideal of* $F[G_F]$ *and let* E *be the fraction field of* $F[G_F]/P$*. Then* $E \supset F$ *is a Picard-Vessiot extension with* $G(E/F) \leq G$*, where* $\mathrm{codim}_G(G(E/F) \leq 1$.
>
> *In particular, if* G *has no algebraic subgroups of codimension 1, then* $G(E/F) = G$ *and* $F(G_F) \supset F$ *is a Picard-Vessiot extension with* $G(F(G_F)/F) = G$.

This statement is incorrect as the following examples show [2]. Note that Theorem 7.3 of [3] is incorrect as well since the ideals presented in these examples have height larger than 1.

Example 1: Let G be $C \times C$, under addition. If we wish, we may consider G to be a subgroup of GL(3) by:

$$(a, b) \mapsto \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The ring of regular functions on G is $C[G] = C[X, Y]$ where X and Y are the coordinate functions: $X(a, b) = a$ and $Y(a, b) = b$. It is nothing more than the ring of polynomials in the indeterminates X and Y. The Lie algebra of right-invariant derivations (over C) has

*JYACC, 116 John Street, New York, N.Y. 10038

†Institut de Recherche Mathématique Avancée, Université Louis Pasteur et C.N.R.S., 7 rue René Descartes, 67084 Strasbourg Cedex, France.

‡North Carolina State University, Department of Mathematics, Box 8205, Raleigh, NC 27695-8205.

basis $\frac{\partial}{\partial X}$ and $\frac{\partial}{\partial Y}$, the usual partial derivatives with respect to the variables.

Define $f_1 = 1$ and $f_2 = 2x$. These are in F and are linearly independent over C . Let D be a derivation on $F[G_F] = F \otimes_C C[G]$ defined as follows:

$$D = \frac{d}{dx} \otimes 1 + 1 \otimes \frac{\partial}{\partial X} + 2x \otimes \frac{\partial}{\partial Y}$$

Consider the ideal $I = (x \otimes 1 - 1 \otimes X, x^2 \otimes 1 - 1 \otimes Y)$ of $F[G]$. Then

$$D(x \otimes 1 - 1 \otimes X) = 1 \otimes 1 - 1 \otimes 1 = 0$$

and

$$D(x^2 \otimes 1 - 1 \otimes Y) = 2x \otimes 1 - 2x \otimes 1 = 0$$

Thus I is a D-differential ideal of $F[G]$. Note that if we identify $F[G]$ with $F[X, Y]$ then $I = (X - x, Y - x^2)$.

Now consider the substitution homomorphism $\pi : X \mapsto x, Y \mapsto x^2$ over F. In other words, $\pi : F[G] = F \otimes C[G] \to F$ is given by $\sum(k_i \otimes h_i) \mapsto \sum(k_i h_i(x, x^2))$. One can show that this is a D to d/dx differential homomorphism whose kernel is I. Since the image of π is a field (*i.e.,* F), I is a maximal ideal, and therefore a maximal differential ideal. But $E = F[G]/I$ is isomorphic to F. The Galois group $G(E/F)$ is the identity, which is of codimension 2 in G. We note that arbitrary codimension can be achieved by using $G = C^n$ and elements $f_i = ix^{i-1}, i = 1, \ldots, n$. ∎

Analyzing this example further shows where the argument in the proof of Theorem 7.3 is not valid. With notations as before, let $V = \text{Spec } C[x] = \mathrm{A}^1_C$ as in the proof of Theorem 7.3 in [3] (the f_i here have no denominators). Then $V \times G = \text{Spec } C[x, X, Y]$ and the irreducible variety defined by the ideal I is the rational curve $W = \text{Spec } C[x, X, Y]/(X - x, Y - x^2)$. The generic point Spec F of V (as before, $F = C(x)$) becomes an F-point of $V \times G$ via the natural homomorphism $C[x, X, Y] \to C[x, X, Y]/(X, Y)] \to F$. It extends to an $\overline{F}$-point of $V \times G$ which is *not* an $\overline{F}$-point of W, since the ideal I is not contained in the kernel (X, Y) of $C[x, X, Y] \to \overline{F}$. On line 24 of [3], an implicit assumption is made that (using the notation of [3]) $(\overline{\eta}, e)$ is a point of $W_{\overline{\eta}}$, that is, (t, e) is a point of $W(\overline{F})$ for all $t \in \overline{F}$. In the above example $(t, e) = (t, 0, 0)$ and $W(\overline{F}) = \{(t, t, t^2), t \in \overline{F}\}$ and so we see that this is not the case.

One can also construct a counterexample for a reductive group.

Example 2: Let $G = \mathrm{GL}(n)$. Let ξ_{ij} be the coordinate functions on G. Thus $\xi_{ij}(g) = g_{ij}$ whenever $g \in \mathrm{GL}(n)$. The ring of regular functions $C[G]$ is $C[\xi_{ij}, \frac{1}{\det \xi}]$. The derivations $D_{ij} = \sum_k \xi_{jk} \frac{\partial}{\partial \xi_{ik}}$ form a basis of Lie(G) (*cf.* [1], p. 329). As before, let $F = C(x)$.

One wishes to find $f_{11}, \ldots, f_{nn} \in F$ and $p_{11}, \ldots, p_{nn} \in F$ such that:
1) the f_{ij} are linearly independent over C,

2) the ideal P generated by $p_{ij} \otimes 1 - 1 \otimes \xi_{ij}$ is a maximal ideal of $F[G_F]$,
3) if $D = \frac{d}{dx} \otimes 1 + \sum_{ij} f_{ij} \otimes D_{ij}$ then P is a D-stable ideal.
We will then have a counterexample to the theorem.

Leave condition 1 aside for the moment. Condition 2 is satisfied so long as $\det(p)$ is not 0. This is equivalent to saying that $p \in G_F$. Condition 3 is more interesting.

$$\begin{aligned} D(p_{\mu\nu} \otimes 1 - 1 \otimes \xi_{\mu\nu}) &= p'_{\mu\nu} \otimes 1 - \sum_{ij} f_{ij} \otimes D_{ij}\xi_{\mu\nu} \\ &= p'_{\mu\nu} \otimes 1 - \sum_{ijk} f_{ij} \otimes \xi_{jk} \frac{\partial \xi_{\mu\nu}}{\partial \xi_{ik}} \\ &= p'_{\mu\nu} \otimes 1 - \sum_{j} f_{\mu j} \otimes \xi_{j\nu} \\ &\equiv p'_{\mu\nu} \otimes 1 - \sum_{j} f_{\mu j} p_{j\nu} \otimes 1 \qquad (\mathrm{mod} P). \end{aligned}$$

So it suffices to find a matrix $p = (p_{\mu\nu})$ such that $p'_{\mu\nu} = \sum_j f_{\mu j} p_{j\nu}$, or, in matrix form, $f = p'p^{-1}$.

In order that all the conditions be satisfied (including condition 1), we need to find examples of $p \in G_F$ such that the coordinates of its logarithmic derivative are linearly independent over C. We now do this for GL(2). Let

$$\begin{aligned} a &= 2^u \\ b &= 2^v \\ c &= 2^w \\ d &= 2^x \end{aligned}$$

where the u, v, w, x are positive integers chosen so that with $u < v < w < x$ (in fact $a = 2, b = 2^2, c = 2^3, d = 2^4$ will work). Let $p = (p_{\mu\nu}) =$

$$\begin{pmatrix} \frac{1}{x^a} & \frac{1}{x^b} \\ \frac{1}{x^c} & \frac{1}{x^d} \end{pmatrix}$$

We then have that $p'p^{-1} =$

$$\begin{pmatrix} \frac{1}{x^a} & \frac{1}{x^b} \\ \frac{1}{x^c} & \frac{1}{x^d} \end{pmatrix}' \begin{pmatrix} \frac{1}{x^d} & -\frac{1}{x^b} \\ -\frac{1}{x^c} & \frac{1}{x^a} \end{pmatrix} \frac{x^{a+b+c+d}}{x^{b+c} - x^{a+d}}$$

To show that the entries of this matrix are linearly independent over the constants, it is enough to show that the entries of the follwoing matrix are linearly independent

$$\begin{aligned} \begin{pmatrix} \frac{1}{x^a} & \frac{1}{x^b} \\ \frac{1}{x^c} & \frac{1}{x^d} \end{pmatrix}' \begin{pmatrix} \frac{1}{x^d} & -\frac{1}{x^b} \\ -\frac{1}{x^c} & \frac{1}{x^a} \end{pmatrix} &= \begin{pmatrix} \frac{-a}{x^{a+1}} & \frac{-b}{x^{b+1}} \\ \frac{-c}{x^{c+1}} & \frac{-d}{x^{d+1}} \end{pmatrix} \begin{pmatrix} \frac{1}{x^d} & -\frac{1}{x^b} \\ -\frac{1}{x^c} & \frac{1}{x^a} \end{pmatrix} \\ &= \begin{pmatrix} \frac{-a}{x^{a+d+1}} + \frac{b}{x^{c+b+1}} & \frac{a}{x^{a+b+1}} - \frac{b}{x^{a+b+1}} \\ \frac{-c}{x^{c+d+1}} + \frac{d}{x^{c+d+1}} & \frac{c}{x^{b+c+1}} - \frac{d}{x^{a+d+1}} \end{pmatrix} \end{aligned}$$

Assume we have a relation $0 =$

$$A(\frac{-a}{x^{a+d+1}} + \frac{b}{x^{c+b+1}}) + B(\frac{a}{x^{a+b+1}} - \frac{b}{x^{a+b+1}}) + C(\frac{-c}{x^{c+d+1}} + \frac{d}{x^{c+d+1}}) + D(\frac{c}{x^{b+c+1}} - \frac{d}{x^{a+d+1}})$$

for some constants A, B, C, D. Since $d+c+1 > d+a+1 > c+b+1 > a+b+1$ (these are 2-adic expansions) we must have that

$$\begin{aligned} C(d-c) &= 0 \\ A(-a) + D(-d) &= 0 \\ A(b) + D(c) &= 0 \\ B(a-b) &= 0 \end{aligned}$$

Since $d > c$ and $b > a$, we have that $C = B = 0$. Since $ac > bd$ we have that $-ac + bd \neq 0$ so $A = D = 0$. Therefore the entries of $p'p^{-1}$ are linearly independent. A similar idea should work for $\mathrm{GL}(n), n > 2$ as well.

References

[1] E. R. Kolchin *Differential Algebra and Algebraic Groups*, Academic Press, 1973.

[2] J. Kovacic, *E-mail communication to A. Magid, C. Mtschi, M.F. Singer, et. al.* March 2, 1995.

[3] A. Magid, *Lectures on Differential Galois Theory*, 7, *University Lecture Series*, Vol. 7, American Mathematical Society, 1994.

[4] C. Mitschi, M.F. Singer, *Connected linear groups as differential Galois groups over* $C(x)$, to appear in *Journal of Algebra*.