Pacific Journal of Mathematics

PICARD–VESSIOT EXTENSIONS WITH SPECIFIED GALOIS GROUP

TED CHINBURG, LOURDES JUAN AND ANDY R. MAGID

Volume 243 No. 2 December 2009

PACIFIC JOURNAL OF MATHEMATICS
Vol. 243, No. 2, 2009

PICARD–VESSIOT EXTENSIONS WITH SPECIFIED GALOIS GROUP

TED CHINBURG, LOURDES JUAN AND ANDY R. MAGID

Picard–Vessiot extensions are determined by their differential module structure. For a fixed group G, Picard–Vessiot extensions with differential Galois group G are all isomorphic as G-modules but not as differential rings. We show that isomorphism classes of Picard–Vessiot extensions with group G correspond to G-orbits in a certain finite-dimensional vector space with G-action.

1. Introduction

The normal basis theorem states that if K/L is a finite Galois extension of fields with group Γ, then K is isomorphic to the group ring $L[\Gamma]$ as an $L[\Gamma]$-module. In this paper we will consider a counterpart of this result in differential Galois theory. This counterpart leads to considering the problem of recognizing a Picard–Vessiot extension E of a differential field F from information weaker than the structure of E as a differential field.

Recall from [Van der Put and Singer 2003; Magid 1997] some basic definitions. Let F be a differential field of characteristic 0 having an algebraically closed field of constants C. A field extension E/F is a Picard–Vessiot extension if E is differentially generated over F by a full set of solutions of a monic homogeneous differential equation over F and if E has the same field of constants as F. The Picard–Vessiot ring R of E/F may be described as the ring of elements of E whose iterated images under the derivation D_E of E span a finite-dimensional vector space over F. The fraction field of R is equal to E. The differential Galois group G of E/F is the affine algebraic group over C given by the differential automorphisms of E over F. Let $C[G]$ be the affine coordinate ring of G over C, and let $F[G] = F \otimes_C C[G]$.

Our counterpart of the normal basis theorem is as follows.

Theorem 1.1. *There is an $F[G]$-comodule isomorphism between R and $F[G]$.*

MSC2000: primary 12H05, 34M15; secondary 12H20.
Keywords: differential, Galois, Picard–Vessiot.
Chinburg is supported by NSF, grant number DMS0801030.

The normal basis theorem implies that the structure of K as an $L[\Gamma]$-module is not sufficient in general to determine K as a Galois extension of F. Similarly, Theorem 1.1 shows that the $F[G]$-comodule structure of R does not in general determine R or E. It is natural to try to minimize, in various ways, the amount of information about E that is sufficient to determine E. Our first result along this line is proved in Proposition 2.1:

Theorem 1.2. *The structure of E as a differential F-module determines E.*

Generally, E has infinite dimension as an F vector space. To try to determine E from a finite amount of linear algebra data over F, one could simply note that the differential equation over F that determines E is specified by finitely many coefficients in F. More conceptually, the differential equation can be replaced by an associated finite-dimensional differential module over F that is trivialized by E; see [Van der Put and Singer 2003]. However, there is no preferred choice for a differential equation giving E or for an associated differential module. We will consider the following more canonical method, which depends on choosing a faithful finite-dimensional G-module V that admits an embedding into $C[G]$.

We will show in Proposition 2.2 that there is an isomorphism $\alpha : R \to F[G]$ respecting F- and G-module structure. Using this isomorphism, we can transport the derivation D_R of R to a G-endomorphism of $F[G]$ that makes $F[G]$ into a differential F-module. Define $\mathcal{W}$ to be the sum of the images of V in $F[G]$ under all G-homomorphisms. We will show in Lemma 4.1 that $\mathcal{W}$ is a finite-dimensional F vector space. We will also prove that $\mathcal{W}$ is a rational G-module that is stable under the above differential structure coming from D_R, and that this restriction determines D_R. Let Δ_R be the resulting differential structure on $\mathcal{W}$. The construction of $\mathcal{W}$ and Δ_R is canonical up to the choice of the F- and G-module isomorphism $\alpha : R \to F[G]$. Let $\mathrm{End}_{F\cdot G}(\mathcal{W})$ and $\mathrm{Aut}_{F\cdot G}(\mathcal{W})$ respectively be the groups of endomorphisms and automorphisms of $\mathcal{W}$ that respect the actions of F and G on $\mathcal{W}$. As a corollary of Theorem 4.2, we will prove:

Theorem 1.3. *Isomorphism classes of Picard–Vessiot extensions E of F with differential Galois group G correspond to the orbits of* $\mathrm{Aut}_{F\cdot G}(\mathcal{W})$ *on* $\mathrm{End}_{F\cdot G}(\mathcal{W})$.

We note that $\mathcal{W}$ is a two-sided G-module. This observation permits the F- and G-endomorphism ring of $\mathcal{W}$ to be calculated in principle. We include a number of examples in Section 5.

We retain throughout the notations of this introduction. In addition, we refer to F vector spaces with rational G action trivial on F as $F \cdot G$-modules. Some basic results on $F \cdot G$-modules are collected in Section 3 below. An $F \cdot D$-module is an F vector space having a derivation that is compatible with the derivation of F and that is the union of finite-dimensional F subspaces that are stable under the derivation. We denote by $F\langle G\rangle$ the usual group algebra of G over F.

2. Differential modules

We begin by showing that the differential F-module structure alone distinguishes Picard–Vessiot extensions.

Proposition 2.1. *Let E_1 and E_2 be Picard–Vessiot extensions of F, and assume that they are isomorphic as differential F vector spaces. Then they are isomorphic as differential fields. This is equivalent to the Picard–Vessiot rings of the E_i being isomorphic as differential F vector spaces.*

Proof. We may assume that both E_1 and E_2 are differential subfields of a Picard–Vessiot extension of F. Let $B : E_1 \to E_2$ be an F linear differential isomorphism. Let $R_i \subset E_i$ be the set of elements that satisfy monic linear homogeneous differential equations over F. Suppose $\alpha \in E_1$ is in R_1 and satisfies the differential equation $L(\alpha) = 0$, where $L(X) = X^{(n)} + a_{n-1}X^{(n-1)} + \cdots + a_0$ is a monic homogeneous linear differential operator over F. We may assume that $L^{-1}(0) \subset E_1$ and $\dim_C L^{-1}(0) = n$. Now $0 = B(L(\beta)) = L(B(\beta))$ for any $\beta \in L^{-1}(0)$, so $B(L^{-1}(0)) = L^{-1}(0)$ and $\alpha \in L^{-1}(0) = B(L^{-1}(0)) \subset R_2$. It follows that $R_1 \subseteq R_2$. Similar considerations apply to elements of R_2. We conclude that $R_1 = R_2$, and also that the isomorphism B carries R_1 to R_2. Since R_i is the Picard–Vessiot ring of E_i and E_i is the quotient field of R_i, we have $E_1 = E_2$. Thus the identity is the desired differential field isomorphism between E_1 and E_2; note that it does not, in general, coincide with B. An examination of the proof shows that it suffices to begin with an $F \cdot D$ isomorphism from R_1 to R_2. □

Proposition 2.1 implies that it is sufficient to consider the $F \cdot D$-module (R, D_R), that is, the F vector space R with its designated endomorphism D_F (which is C, but not necessarily F, linear). We now consider the $F \cdot G$-module structure of R.

Proposition 2.2. *Let R be the Picard–Vessiot ring of a Picard–Vessiot extension E of F with differential Galois group G. Then R is isomorphic to $F[G]$ as an $F \cdot G$-module.*

Proof. It is a consequence of Kolchin's theorem [Magid 1997, Theorem 5.12] that there is a finite Galois extension F_1 of F such that $F_1 \otimes_F R \cong F_1[G]$ as F_1 and G-modules. Let $n = [F_1 : F]$. As F vector spaces with G action, the two sides of the above are isomorphic to $R^{(n)}$ and $F[G]^{(n)}$, which means the two direct sums are isomorphic as $F \cdot G$-modules. This implies that the socles of the direct sums are isomorphic $F \cdot G$-modules, and then, by counting multiplicities of simple components, that the socles of R and $F[G]$ are $F \cdot G$ isomorphic. Since $F[G]$ is $F \cdot G$ injective [Cline et al. 1977], the isomorphism of the direct sums implies that R is also an injective $F \cdot G$-module. Finally, injective $F \cdot G$ modules with isomorphic socles are isomorphic. □

3. $F \cdot G$-modules

We recall that $F[G] = F \otimes_C C[G]$. We associate F-valued functions on G to elements of $F[G]$: If $f = \sum a_i \otimes \phi_i$, then $f(g) = \sum \phi_i(g) a_i$ for $g \in G$. It is clear that elements of $F[G]$ are determined by their associated functions. Using this functional representation, the actions of G on $F[G]$ are the left action $\lambda(g) f = g \cdot f$ where $g \cdot f(x) = f(xg)$ and the right action $\rho(g) f = f \cdot g^{-1}$ where $f \cdot g(x) = f(gx)$.

Note that $\lambda(g)\rho(h) = \rho(h)\lambda(g)$.

We have evaluation functionals given by $\mathrm{ev}_g : F[G] \to F$, $f \mapsto f(g)$. Note that the only element of $F[G]$ in the kernel of all the evaluation functionals is 0.

If $X \subset F[G]$ is a left (or right) $F \cdot G$-submodule, we use λ (or ρ) to denote the G action on X, and we use $\mathrm{ev}_g : X \to F$ for the evaluation restrictions. In $\mathrm{End}_F(X)$ we let $\Lambda = \sum_g F\lambda(g)$ (or $P = \sum_g F\rho(g)$). If X is both a left and right $F \cdot G$-submodule, then Λ and P commute.

Suppose X is finite-dimensional. Then the fact that intersections of the kernels of the evaluation functionals is trivial means that they span $\mathrm{Hom}_F(X, F)$.

That $F[G]$ is $F \cdot G$ injective and that the multiplicities of the simple components of its socle are finite follow from the next lemma, whose proof and use are the same as the familiar case where $F = C$ [Cline et al. 1977, Proposition 1.4, page 9]:

Lemma 3.1. *Let W be a finite-dimensional $F \cdot G$-module, with associated $F[G]$ comodule structure $\gamma_W : W \to W \otimes_F F[G]$. Let $ev_e : F[G] \to F$ be evaluation at the identity. Then there is an isomorphism as (right) G-modules and F vector spaces given by*

$$\mathrm{Hom}_{F \cdot G}(W, F[G]) \to \mathrm{Hom}_F(W, F)$$

with $\Phi \mapsto ev_e \circ \Phi$ and $f \mapsto (1 \otimes f) \circ \gamma_W$.

This “duality” lemma also implies a structural result about endomorphism rings:

Lemma 3.2. *Let $W \subset F[G]$ be a finite-dimensional $F \cdot G$-submodule that is also a right G-submodule, and suppose every $F \cdot G$-morphism $W \to F[G]$ has image in W. Then $\mathrm{End}_{F \cdot G}(W) = P$.*

Proof. By assumption we have $\mathrm{End}_{F \cdot G}(W) = \mathrm{Hom}_{F \cdot G}(W, F[G])$, and Lemma 3.1 says that

$$\mathrm{Hom}_{F \cdot G}(W, F[G]) \to \mathrm{Hom}_F(W, F), \quad \Phi \mapsto \mathrm{ev}_e \circ \Phi$$

is an isomorphism. For $g \in G$ we have that $\rho(g^{-1})$ is an $F \cdot G$-endomorphism of W, and one checks that $\mathrm{ev}_e \circ \rho(g^{-1}) = \mathrm{ev}_g$. Since W is finite-dimensional, $\mathrm{Hom}_F(W, F)$ is spanned by evaluations, which means that the subring P of the $F \cdot G$-endomorphism ring maps onto $\mathrm{Hom}_F(W, F)$ and hence coincides with the endomorphism ring. □

Another way to state the result of Lemma 3.2 is that the ring homomorphism $F\langle G\rangle \to \mathrm{End}_{F\cdot G}(W)$ induced from $\rho : G \to \mathrm{End}_{F\cdot G}(W)$ is surjective.

This is not necessarily the case for automorphisms. However:

Lemma 3.3. *Let W be an $F \cdot G$-submodule of $F[G]$. The morphisms*

$$\mathrm{End}_{F\cdot G}(F[G]) \to \mathrm{End}_{F\cdot G}(\mathcal{W}) \quad \textit{and} \quad \mathrm{Aut}_{F\cdot G}(F[G]) \to \mathrm{Aut}_{F\cdot G}(\mathcal{W})$$

induced from restriction are surjective.

Proof. By construction, $\mathcal{W}$ is an $F \cdot G$-submodule of the injective $F \cdot G$-module $F[G]$. This means that $F[G]$ contains an injective hull I of $\mathcal{W}$. Then I is an essential extension of $\mathcal{W}$, which in our context means that they have the same socle, and I, being injective, is also a direct summand of $F[G]$. Let B be an automorphism of $\mathcal{W}$. Composing B with the inclusion of $\mathcal{W}$ in I is a monomorphism. Since I is injective, the inclusion of $\mathcal{W}$ into I factors through this monomorphism, so that B lifts to an endomorphism B_0 of I. The same argument, in the case that B is only an endomorphism, also proves the first claim of the lemma. The kernel of B_0, if nontrivial, contains a simple submodule, which belongs to the socle of I and therefore the socle of $\mathcal{W}$. This simple module then is contained in $\mathcal{W}$, and hence in the kernel of B. That kernel is trivial, and thus so is the kernel of B_0. The image $I_0 = B_0(I)$ is then an injective submodule of I (being isomorphic to I) and contains $B(\mathcal{W}) = \mathcal{W}$. Again, because I is an essential extension of $\mathcal{W}$, this implies that $I = I_0$ and B_0 is onto, and hence an automorphism of I_0. Now take B_1 to be an automorphism of $F[G]$ that is B_0 on I and the identity on a complementary direct summand. □

There is a derivation of $F[G]$ coming from F given by $D_F \otimes 1$. We denote this by ∂ in this section. Note that ∂ is a G-morphism. Suppose that X is a finite-dimensional $F \cdot G$-submodule of $F[G]$ with $\partial(X) \subset X$ and that $T : X \to X$ is an $F \cdot G$-endomorphism. We define

$$T' = \partial \circ T - T \circ \partial.$$

It is straightforward to check that T' is also an $F \cdot G$-endomorphism. If $T = 1 \otimes \tau$ for τ a G endomorphism of $C[G]$, then T commutes with ∂ and $T' = 0$. It follows that

$$\text{if } T = \sum f_i \rho(g_i) \quad \text{then } T' = \sum f_i' \rho(g_i).$$

which we call the *differentiation of coefficients formula*. In these notation, we also have the following conjugation formula:

Lemma 3.4. *Let X be a finite-dimensional $F \cdot G$-submodule of $F[G]$ such that $\partial(X) \subset X$, and let $B : X \to X$ be an $F \cdot G$-automorphism. Then*

$$B^{-1}\partial B = \partial + B^{-1}B'.$$

More generally, if (X, Δ) *is an* $F \cdot D$ *structure on* X *and* $T = \Delta - \partial$, *then we have* $B^{-1}\Delta B = \partial + B^{-1}B' + B^{-1}TB$.

Proof. Let $S = B^{-1}\partial B$, so $BS = \partial \circ B$. By definition, $\partial \circ B = B' + B \circ \partial$, so $S = B^{-1}(B' + B \circ \partial) = B^{-1}B' + \partial$, as desired. The second formula is immediate from the first. □

4. Isomorphism classes of Picard–Vessiot extensions

Let V be a faithful finite-dimensional G-module over C.

Definition 1. Let Y be any rational G-module over C. Then

$$\mathcal{W}(Y) = \sum\{\phi(V) \mid \phi \in \operatorname{Hom}_G(V, Y)\}.$$

For $Y = F[G]$, we let $\mathcal{W}$ denote $\mathcal{W}(F[G])$.

If $f : Y \to Z$ is a G-module morphism, then $f(\mathcal{W}(Y)) \subseteq \mathcal{W}(Z)$, and in particular $\mathcal{W}(Y)$ is stable under G-endomorphisms of Y. It is clear that $\mathcal{W}(Y)$ is a G-submodule of Y, and that $\mathcal{W}(Y)$ is the image of

$$\operatorname{Hom}_G(V, Y) \otimes_C V \to Y, \quad \phi \otimes y \mapsto \phi(y).$$

In the special case $Y = F[G]$ and $W = F \otimes_C V$, we have

$$\operatorname{Hom}_G(V, F[G]) = \operatorname{Hom}_{F \cdot G}(W, F[G]) \quad \text{and} \quad \otimes_C V = \otimes_F W,$$

so that $\operatorname{Hom}_G(V, F[G]) \otimes_C V = \operatorname{Hom}_{F \cdot G}(W, F[G]) \otimes_F W$, from which it follows that $\mathcal{W}(F[G])$ is the image of

$$\operatorname{Hom}_{F \cdot G}(W, F[G]) \otimes_F W \to F[G], \quad \psi \otimes w \mapsto \psi(w).$$

Since $\operatorname{Hom}_{F \cdot G}(W, F[G]) = \operatorname{Hom}_F(W, F)$ is a finite-dimensional F-module, this shows that $\mathcal{W}(F[G])$ is a finite-dimensional $F \cdot G$-module, and that $\mathcal{W}(F[G]) = \sum\{\psi(W) \mid \psi \in \operatorname{Hom}_{F \cdot G}(W, F[G])\}$. Since R is $F \cdot G$ isomorphic to $F[G]$, we see that $\mathcal{W}(R)$ is also a finite-dimensional $F \cdot G$-submodule of R. Moreover, the restriction of D_E to $\mathcal{W}(R)$ determines D_E, as we now note:

Lemma 4.1. $\mathcal{W}(R)$ *is finite-dimensional over* F *and an* $F \cdot G$- *and* $F \cdot D$-*submodule of* R. *The* F *subalgebra of* R *generated by* $\mathcal{W}(R)$ *has quotient field* E. *In particular, the restriction of* D_E *to* $\mathcal{W}(R)$ *determines* D_E.

Proof. D is a G-endomorphism of R, and hence preserves $\mathcal{W}(R)$. This makes $\mathcal{W}(R)$ an $F \cdot D$-submodule of R, and hence the subalgebra generated over F by $\mathcal{W}(R)$ is a differential subalgebra of R, and its quotient field K is then an intermediate differential field of the Picard–Vessiot extension $E \supset F$, and so is of the form E^H for a subgroup H of G. By assumption, we have an embedding $V \to C[G]$, hence $V \to F[G]$, and therefore, by Proposition 2.2, an embedding $\phi : V \to R$.

Then $\phi(V)$ is a faithful G-submodule of $\mathcal{W}(R)$ and hence of K. Since no element of G other then e acts trivially on K, we have H trivial and $K = E$. □

We are now ready to construct the invariant. We recall from Proposition 2.1 that if we have two Picard–Vessiot rings R_1 and R_2 with corresponding derivations D_1 and D_2, then they are isomorphic as Picard–Vessiot rings if and only if there is an F vector space isomorphism $B : R_1 \to R_2$ such that $D_2 = BD_1B^{-1}$. If there is such a B, then there will be one that is an $F \cdot G$-isomorphism.

We can select an $F \cdot G$-isomorphism $A_i : R_i \to F[G]$, as per Proposition 2.2, and consider the G endomorphisms $A_i D A_i^{-1}$ of $F[G]$.

We have $A_i(\mathcal{W}(R_i)) = \mathcal{W}$, and hence, by Lemma 4.1, that $\Delta_i = A_i D A_i^{-1}$ is determined by its restriction to $\mathcal{W}$, which we denote by the same symbol. As previously noted, the structures $\mathcal{M}_i = (\mathcal{W}, \Delta_i)$ are $F \cdot D$-modules. If the R_i are isomorphic, then clearly so are the $\mathcal{M}_i$, where by the latter we mean that there is an $F \cdot G$-module automorphism of $\mathcal{W}$ carrying Δ_1 to Δ_2. We record this and its converse in the following result:

Theorem 4.2. *For $i = 1, 2$, let E_i be Picard–Vessiot extensions of F with group G, let R_i be the Picard–Vessiot ring of E_i, and let $A_i : R_i \to F[G]$ be an $F \cdot G$-isomorphism. Then the E_i are isomorphic if and only if there is an $F \cdot G$-automorphism B of $\mathcal{W}$ such that*

$$BA_1D_{R_1}A_1^{-1}B^{-1}|_{\mathcal{W}} = A_2D_{R_2}A_2^{-1}|_{\mathcal{W}}.$$

Proof. If the E_i are isomorphic, then there is a differential $F \cdot G$-isomorphism $R_1 \to R_2$ that produces B. Conversely, suppose we have B. If B is the restriction to $\mathcal{W}$ of an $F \cdot G$-automorphism B_1 of $F[G]$, then replacing A_1 by B_1A_1 gives an isomorphism of R_1 to $F[G]$ such that the resulting $F \cdot D$-module structure on $\mathcal{W}$ coincides with that for R_2, so that the R_i and hence E_i are isomorphic. So the theorem follows from Lemma 3.3. □

Theorem 4.2 says that an isomorphism class of Picard–Vessiot extensions corresponds to an equivalence class of differential structures on $\mathcal{W}$, the equivalence relation coming from conjugation by $F \cdot G$-automorphisms. We always have the differential structure ∂ on $\mathcal{W}$ induced from $D_F \otimes 1$ on $F[G]$ as in Section 3. Then $(\mathcal{W}, \Delta)$ is an $F \cdot D$-module if and only if $\Delta - \partial$ is an $F \cdot G$-endomorphism of $\mathcal{W}$. The action of $F \cdot G$-automorphisms on differential structures on $\mathcal{W}$ then translates to the following action on $F \cdot G$-endomorphisms:

For $B \in \mathrm{Aut}_{F.G}(\mathcal{W})$ and $T \in \mathrm{End}_{F.G}(\mathcal{W})$, let $T^B = BTB^{-1} + B^{-1}B'$, where $B' = \partial \circ B - B \circ \partial$. This defines a right action of automorphisms on endomorphisms, called, for obvious reasons, conjugation plus logarithmic differentiation. Then Theorem 4.2 and Lemma 3.4 imply the following:

Corollary 4.3. *Isomorphism classes of Picard–Vessiot extensions of F with group G correspond to* $\mathrm{Aut}_{F\cdot G}(\mathcal{W})$ *orbits on* $\mathrm{End}_{F\cdot G}(\mathcal{W})$ *under the conjugation plus logarithmic differentiation right action.*

5. Examples

We use $\mathrm{dlog}(x)$ to denote the logarithmic derivative x'/x.

We begin with the case of finite G. Finite Galois extensions $E \supset F$ are Picard–Vessiot: There is a unique extension of the derivation D_F to E, and this turns out to have field of constants C. Moreover, in this case the Picard–Vessiot ring R coincides with E. On the other hand, it is never the case that R is isomorphic as an F algebra with $F[G]$, as the latter is always just a finite product of copies of F.

Example 1. $G = \mathbb{Z}/2\mathbb{Z}$. A Picard–Vessiot extension of F with group G is then of the form $E = F(\sqrt{d})$, where d is a nonsquare of F. Assume D_F is extended to E. Differentiating the equation $(\sqrt{d})^2 = d$ shows that $(\sqrt{d})' = d'/(2\sqrt{d})$ which we write as $\frac{1}{2}\,\mathrm{dlog}(d)\sqrt{d}$.

Let e denote the identity and g denote the nontrivial element of G. The ring $F[G]$ is all functions F^G, which is isomorphic as a G-module to the group algebra $F\langle G\rangle = Fe + Fg$. (The isomorphism has e corresponding to the constant function 1 and g to the function that is 1 on the identity and -1 on g.) There is a G isomorphism $A : E \to F\langle G\rangle$ by $1 \mapsto e+g$ and $\sqrt{d} \mapsto e-g$. (This is, of course, a special case of the normal basis theorem.) In terms of coordinates, $A(a+b\sqrt{d}) = (a+b)e+(a-b)g$ while $A^{-1}(\alpha e+\beta g) = \frac{1}{2}(\alpha+\beta)+\frac{1}{2}(\alpha-\beta)\sqrt{d}$. Then if $D = D_E$, we calculate

$$ADA^{-1}(\alpha e+\beta g) = (\alpha' + \tfrac{1}{2}(\alpha-\beta)\tfrac{1}{2}\,\mathrm{dlog}(d))e + (\beta' - \tfrac{1}{2}(\alpha-\beta)\tfrac{1}{2}\,\mathrm{dlog}(d))g.$$

By Section 3, the derivation $\partial = D_F \otimes 1$ of $F\langle G\rangle$ is given by $\partial(\alpha e+\beta g) = \alpha' e+\beta' g$, and hence the determining $F\cdot G$-module endomorphism $T = ADA^{-1} - \partial$ is given by

$$T(\alpha e+\beta g) = \tfrac{1}{2}\,\mathrm{dlog}(d)(\tfrac{1}{2}(\alpha-\beta)e + \tfrac{1}{2}(\beta-\alpha)g).$$

We now specify the faithful G-module V: We choose the one-dimensional module on which g acts nontrivially, which appears here as the module spanned by $e-g$. It then follows that we may choose $F(e-g)$ for $\mathcal{W}$. On $\mathcal{W}$, T becomes multiplication by $\frac{1}{2}\,\mathrm{dlog}(d)$. Now suppose B is any $F\cdot G$-automorphism of $\mathcal{W}$. Then B is multiplication by some nonzero element α of F, so that B commutes with T and $B^{-1}B'$ is multiplication by $\mathrm{dlog}(\alpha)$ and $B^{-1}TB + B^{-1}B'$ is multiplication by $\frac{1}{2}\,\mathrm{dlog}(d) + \mathrm{dlog}(\alpha)$, which can be written $\frac{1}{2}\,\mathrm{dlog}(\alpha^2 d)$.

This is interpreted as follows: Picard–Vessiot extensions of F with group G are quadratic extensions of F. Those isomorphic to $F(\sqrt{d})$ are of the form $F(\sqrt{c})$ where c is equivalent to d modulo squares, or $c = \alpha^2 d$ for some $\alpha \in F$.

Example 2. $G = \mathbb{G}_m$. For Picard–Vessiot extensions $E \supset F$ with group $\mathbb{G}_m$, we have $E = F(y)$, where y is transcendental over F and satisfies $y' = ay$ for some $a \in F$. Furthermore, there is no $\alpha \in F$ with $\alpha' = a\alpha$, which says that a is not a logarithmic derivative in F. The Picard–Vessiot ring here is $F[y, y^{-1}]$, which is isomorphic as an F-algebra and G-module to $F[\mathbb{G}_m]$, the isomorphism A carrying y to the coordinate t on $\mathbb{G}_m$. For V we can take the C-module spanned by t, and then $\mathcal{W}$ turns out to be Ft. We compute ADA^{-1} on $\mathcal{W}$ as $\alpha t \mapsto \alpha y \mapsto (\alpha' + a)y \mapsto (\alpha' + a)t$. So $T = ADA^{-1} - \partial$ is multiplication by a. As in Example 1, an $F \cdot G$-automorphism B of $\mathcal{W}$ is multiplication by some nonzero element b of F, and so $B^{-1}TB + B^{-1}B'$ is multiplication by $a + \operatorname{dlog}(b)$.

Suppose K is a Picard–Vessiot extension of F with group $\mathbb{G}_m$ such that K is $\mathbb{G}_m$ differentially isomorphic to $C(y)$. Modeling E on $C(y)$, we see that E is generated by $z = by$ for some nonzero $b \in F$. Then z satisfies $z' = (b' + ab)y = (\operatorname{dlog}(b) + a)z$. Thus the invariant corresponding to K is $a + \operatorname{dlog}(b)$.

Example 3. $G = \mathrm{SL}_2(C)$. As with Example 2, here all Picard–Vessiot rings are isomorphic to $F[\mathrm{SL}_2(C)]$; see [Magid 1997, Theorem 5.12] and [Serre 1997, Proposition 33]. However, in this case the classification of extensions is not available, and so we confine our attention to the specific case $F = C(x)$, the field of rational functions with constant coefficients and with $x' = 1$, and the Picard–Vessiot extension $E \supset F$ for the Airy equation $Y'' - xY$. Then the Picard–Vessiot ring R is known to be $F[y, z, y', z']/(yz' - zy' - 1)$, where y, z are solutions of the Airy equation [Magid 1997, Example 4.29].

In terms of the familiar matrix coordinates we can write

$$F[\mathrm{SL}_2] = F[x_{11}, x_{12}, x_{21}, x_{22}]/(x_{11}x_{22} - x_{12}x_{21} - 1).$$

There is an obvious F algebra isomorphism

$$A : R \to F[\mathrm{SL}_2], \quad y \mapsto x_{11},\ z \mapsto x_{21},\ y' \mapsto x_{12},\ z' \mapsto x_{22}.$$

For V, we are going to use the SL_2-module C^2 (column 2-tuples with the usual left matrix multiplication action of SL_2). V appears in R as $Cy + Cz$, which we will use. For A to be SL_2 linear, we need to use the *right* action of SL_2 on $F[\mathrm{SL}_2]$: Thus if X is the matrix $[x_{ij}]$ and $g \in \mathrm{SL}_2(C)$ is the matrix $[x_{ij}(g)]$, then $x_{ij}^g = x_{ij}(gX) = x_{i1}(g)x_{1j} + x_{i2}(g)x_{2j}$.

One checks then that $\mathcal{W}$ is 4-dimensional over F, and hence equals $\sum Fx_{ij}$. Then $T = ADA^{-1}$ is given by $T(x_{i1}) = x_{i2}$ and $T(x_{i2}) = xx_{i1}$.

To determine the class of T, we need to know about the $F \cdot G$-automorphisms of $\mathcal{W}$. According to Lemma 3.2, all $F \cdot G$-endomorphisms of $\mathcal{W}$ are F linear combinations of "right" (here left) SL_2 translations symbolized by $X \mapsto Xg$. Every 2-by-2 matrix P in $M_2(F)$ can be written as an F-linear combination of matrices in $\mathrm{SL}_2(C)$. Thus every $F \cdot G$-endomorphism B of $\mathcal{W}$ can be written as $X \mapsto XP$ for some P in $M_2(F)$. For example, T is represented by the matrix $\left[\begin{smallmatrix} 0 & x \\ 1 & 0 \end{smallmatrix}\right]$. An endomorphism B will be an automorphism if and only if the representing matrix P is invertible, in which case B^{-1} will be represented by P^{-1}. By the derivation of coefficients formula below, we know that B' is given by the matrix obtained from P by differentiating entries.

So let B be an $F \cdot G$-automorphism of $\mathcal{W}$ represented by an invertible matrix P, which we write in the form δQ, where Q has determinant 1.

Let $Q = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$. Then $B^{-1}TB + B^{-1}B'$ is represented by the matrix

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} 0 & x \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} + \mathrm{dlog}(\delta).$$

References

[Cline et al. 1977] E. Cline, B. Parshall, and L. Scott, "Induced modules and affine quotients", *Math. Ann.* **230**:1 (1977), 1–14. MR 57 #9861 Zbl 0378.20033

[Magid 1997] A. R. Magid, *Lectures on differential Galois theory*, 2nd ed., University Lecture Series **7**, American Mathematical Society, Providence, RI, 1997. MR 95j:12008 Zbl 0855.12001

[Serre 1997] J.-P. Serre, *Galois cohomology*, Springer, Berlin, 1997. MR 98g:12007 Zbl 0902.12004

[Van der Put and Singer 2003] M. van der Put and M. F. Singer, *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften **328**, Springer, Berlin, 2003. MR 2004c:12010 Zbl 1036.12008

Received January 19, 2009. Revised April 13, 2009.

TED CHINBURG
UNIVERSITY OF PENNSYLVANIA
DEPARTMENT OF MATHEMATICS
PHILADELPHIA, PA 19104-6317
UNITED STATES
ted@math.upenn.edu

LOURDES JUAN
DEPARTMENT OF MATHEMATICS AND STATISTICS
TEXAS TECH UNIVERSITY
LUBBOCK, TX 79409-1042
UNITED STATES
lourdes.juan@ttu.edu

ANDY R. MAGID
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF OKLAHOMA
NORMAN, OK 73019
UNITED STATES
amagid@math.ou.edu