Spring Central Sectional Meeting Texas Tech University, Lubbock, Texas

Special Session on Differential Algebra and Galois Theory

April 11th 2014

Real and p-adic Picard-Vessiot fields

Teresa Crespo, Universitat de Barcelona, Spain
Zbigniew Hajto, Uniwersytet Jagielloński, Kraków, Poland
Marius van der Put, Rijksuniversiteit Groningen, The Netherlands

Theorem. Let K be differential field with field of constants k. Let M/K be a differential module. We assume that K is a real (resp., p-adic) field and k is real closed (resp. p-adically closed).

(1). Existence. There exists a real (resp., p-adic) Picard–Vessiot extension for M/K.

(2). Unicity for the real case. Let L_1, L_2 denote two real Picard–Vessiot extensions for M/K. Suppose that L_1 and L_2 have total orderings which induce the same total ordering on K. Then there exists a K-linear isomorphism $\phi : L_1 \to L_2$ of differential fields.

(3). Unicity for the p-adic case. Let L_1, L_2 denote two p-adic Picard–Vessiot extensions for M/K. Suppose that L_1 and L_2 have p-adic closures L_1^+ and L_2^+ such that the p-adic valuations of L_1^+ and L_2^+ induce the same p-adic valuation on K and such that $K \cap (L_1^+)^n = K \cap (L_2^+)^n$ for every integer $n \geq 2$ (where $F^n := \{f^n | f \in F\}$). Then there exists a K-linear isomorphism $\phi : L_1 \to L_2$ of differential fields.

A *real field* is a field K which can be endowed with a total ordering compatible with sum and product. Equivalently, -1 is not a sum of squares in K.
A *real closed field* is a real field that has no nontrivial real algebraic extensions.

Let p be a prime integer. A *p-adic field* is a field which admits a valuation $v : K \to \Gamma$, where Γ is a totally ordered abelian group such that $v(p)$ is the smallest positive value in $v(K)$.
A *p-adically closed field* is a p-adic field that has no nontrivial p-adic algebraic extensions.

Proposition. Let $k \subset K$ denote fields of characteristic zero such that:

(i) For every smooth variety V of finite type over k, $V(K) \neq \emptyset$ implies $V(k) \neq \emptyset$.

(ii) The natural map $Gal(\overline{K}/K) \to Gal(\overline{k}/k)$ is bijective.

Let G be any linear algebraic group over k, then the map of pointed sets

$$H^1(k, G(\overline{k})) \to H^1(K, G(\overline{K})),$$

induced by the inclusion $G(\overline{k}) \subset G(\overline{K})$ and the group isomorphism $Gal(\overline{K}/K) \simeq Gal(\overline{k}/k)$ is bijective.

Conditions (i) and (ii) are fulfilled when k and K are both real closed or p-adically closed.

Reduction to the case K real closed (resp. p-adically closed)

Existence. *Let $\tilde{K} \supset K$ be an extension of real (resp., p-adic) differential fields such that the field of constants of $\tilde{K}$ is k. Suppose that $\tilde{K} \otimes M$ has a real (resp., p-adic) Picard–Vessiot field $\tilde{L}$, then M has a real (resp., p-adic) Picard–Vessiot field.*

Unicity. *Let L_1, L_2 be two real Picard–Vessiot fields for M over the real differential field K. Suppose that L_1 and L_2 have total orderings extending a total ordering τ on K. Let $K^r \supset K$ be the real closure of K inducing the total ordering τ. Then the fields L_1, L_2 induce Picard–Vessiot fields $\tilde{L}_1, \tilde{L}_2$ for $K^r \otimes M$ over K^r. These fields are isomorphic as differential field extensions of K^r if and only if L_1 and L_2 are isomorphic as differential field extensions of K.*

Let, for $j = 1, 2$, τ_j be a total ordering on L_j inducing τ on K and let L_j^r be the real closure of L_j which induces the ordering τ_j. We may identify the real closure K_j of K in L_j^r with K^r.

Let $V_j \subset L_j$ denote the solution space of M. Then the field $\tilde{L}_j := K^r < V_j > \subset L_j^r$ is a real Picard–Vessiot field for $K^r \otimes M$.

If $\psi : K^r < V_1 > \to K^r < V_2 >$ is a K^r-linear differential isomorphism, $\psi(V_1) = V_2$ and ψ induces a K-linear differential isomorphism $L_1 = K < V_1 > \to L_2 = K < V_2 >$. On the other hand, a K-differential isomorphism $\phi : L_1 \to L_2$ extends to an isomorphism $\tilde{\phi} : L_1^r \to L_2^r$ which maps $\tilde{L}_1$ to $\tilde{L}_2$.

Picard-Vessiot extensions and fibre functors.
Let $< M >_\otimes$ denote the Tannakian category generated by the differential module M, $\rho :< M >_\otimes \to vect(K)$ the forgetful functor.

1. *There exists a fibre functor* $\omega :< M >_\otimes \to vect(k)$.
The field K contains a finitely generated k-subalgebra R, which is invariant under differentiation, such that there exists a fibre functor $< M >_\otimes \to vect(R/\underline{m})$, for $\underline{m}$ a maximal ideal of R. Since K is a real field (resp., p-adic field) and therefore R is a real (resp., p-adic) algebra, finitely generated over a real closed (resp., p-adically closed) field k, there exists $\underline{m}$ such that $R/\underline{m} = k$

2. *There is a bijection between the (isomorphy classes of) fibre functors* $\omega :< M >_\otimes \to vect(k)$ *and the (isomorphy classes of) Picard–Vessiot fields* L *for* M/K.
The functor $\underline{Aut}^\otimes(\omega)$ is represented by a linear algebraic group G over k; the functor $\underline{Isom}_K^\otimes(K \otimes \omega, \rho)$ is represented by a torsor P over $G_K := K \times_k G$. This torsor is affine, irreducible and the field of fractions $K(P)$ of its coordinate ring $O(P)$ is a Picard–Vessiot field for M/K and G identifies with the group of the K-linear differential automorphisms of $K(P)$.
If L be a Picard–Vessiot field for M/K, define the fibre functor $\omega_L :< M >_\otimes \to vect(k)$ by $\omega_L(N) = \ker(\partial : L \otimes_K N \to L \otimes_K N)$.

3. *Suppose that K is real closed (resp., p-adically closed). Let L be a Picard–Vessiot field for M/K. Then L is a real field (resp., a p-adic field) if and only if the torsor $\underline{Isom}^{\otimes}_K(K \otimes \omega_L, \rho)$ is trivial.*

If L is a real Picard–Vessiot field, then $O(P) \subset L$ is a finitely generated real K-algebra. From the real Nullstellensatz and the assumption that K is real closed it follows that there exists a K-linear homomorphism $\phi : O(P) \to K$ with $\phi(1) = 1$. The torsor $P = Spec(O(P))$ has a K-valued point and is therefore trivial.

If the torsor $P = Spec(O(P))$ is trivial, then the affine variety P has a K-valued point. It follows that the Picard–Vessiot field L, which is the function field of this variety, is real.

Proof of unicity.

Let L_1, L_2 be two real Picard-Vessiot fields for a differential module M/K; $\omega_j = \omega_{L_j} :< M >_{\otimes} \to vect(k)$ the corresponding fibre functors.

Put $G = \underline{Aut}_k^{\otimes}(\omega_1)$. Then $\underline{Isom}_k^{\otimes}(\omega_1, \omega_2)$ is a G-torsor over k corresponding to an element $\xi \in H^1(k, G(\overline{k}))$.

The G_K-torsor $\underline{Isom}_K^{\otimes}(K \otimes \omega_1, K \otimes \omega_2)$ corresponds to an element $\eta \in H^1(K, G(\overline{K}))$.

$$\begin{array}{ccc} H^1(k, G(\overline{k})) & \to & H^1(K, G(\overline{K})) \\ \xi & \mapsto & \eta \end{array}$$

Since L_j is real, the torsor $\underline{Isom}_K^{\otimes}(K \otimes \omega_j, \rho)$ is trivial for $j = 1, 2$. Thus there exists isomorphisms

$$\alpha_j : K \otimes \omega_j \to \rho,$$

for $j = 1, 2$. The isomorphism

$$\alpha_2^{-1} \circ \alpha_1 : K \otimes \omega_1 \to K \otimes \omega_2$$

implies that η is trivial.

Since the map $H^1(k, G(\overline{k})) \to H^1(K, G(\overline{K}))$ is an injective map between pointed sets, ξ is trivial. Hence there is an isomorphism $\omega_1 \to \omega_2$, which implies that L_1 and L_2 are isomorphic as differential field extensions of K.

Proof of existence.
Let M be a differential module over a real closed differential field K. We fix a fibre functor

$$\omega_0 :< M >_{\otimes} \to vect(k)$$

and write $G_0 := \underline{Aut}^{\otimes}(\omega_0)$.
Let $G_\rho := \underline{Aut}^{\otimes}(\rho)$, where $\rho :< M >_{\otimes} \to vect(K)$ is the forgetful functor.

$$\begin{aligned} H^1(k, G_0(\overline{k})) &\leftrightarrow \{\omega :< M >_{\otimes} \to vect(k)\} \\ H^1(K, G_\rho(\overline{K})) &\leftrightarrow \{G_\rho\text{-torsors}\}\,. \end{aligned}$$

Thus $\omega \mapsto \underline{Isom}(K \otimes \omega, \rho)$ induces a map $\Phi : H^1(k, G_0(\overline{k})) \to H^1(K, G_\rho(\overline{K}))$.
$1 = \Phi(\omega) \Rightarrow L_\omega$ is a *real* Picard–Vessiot field.

$$\Phi : H^1(k, G_0(\overline{k})) \stackrel{natG_0}{\longrightarrow} H^1(K, G_0(\overline{K})) \stackrel{composition}{\longrightarrow} H^1(K, G_\rho(\overline{K})).$$

The map "*composition*" is defined as follows. An element in $H^1(K, G_0(\overline{K}))$ is a right $K \times_k G_0$-torsor. One can compose with $\underline{Isom}^{\otimes}(K \otimes \omega_0, \rho)$ which is a left $K \otimes_k G_0$-torsor and a right G_ρ-torsor. The result is a right G_ρ-torsor and thus an element in $H^1(K, G_\rho(\overline{K}))$. The map "*composition*" is clearly bijective. Since the map $natG_0$ is bijective, this finishes the proof of the existence.

Proof of the Proposition ($H^1(k, G(\overline{k})) \leftrightarrow H^1(K, G(\overline{K}))$)

Surjectivity

(1). Let U be the unipotent radical of G. The maps $H^1(k, G) \to H^1(k, G/U)$ and $H^1(K, G) \to H^1(K, G/U)$ are bijective, hence we may assume that the neutral component G^o of G is reductive.

(2). Consider a commutative group C over k. Since the commutative group $C(\overline{K})/C(\overline{k})$ is torsion free and divisible and so it has trivial Galois cohomology, the natural maps $H^n(k, C) \to H^n(K, C)$ are bijective for all $n > 0$.

(3). Let T be a maximal torus of G, and let N be its normalizer. The map $H^1(K, N) \to H^1(K, G)$ is surjective. Hence it will be enough to prove surjectivity for N.

(4). After replacing G by N, we have an exact sequence $1 \to C \to G \to F \to 1$, where C is a torus and F a finite group. This gives us a commutative diagram:

$$\begin{array}{ccccccc} 1 & \to & H^1(k, C) & \to & H^1(k, G) & \to & H^1(k, F) \\ & & \updownarrow & & \downarrow & & \updownarrow \\ 1 & \to & H^1(K, C) & \to & H^1(K, G) & \to & H^1(K, F) \end{array}$$

Let x be an element of $H^1(K, G)$ and let y be its image in $H^1(K, F)$. Thus we view y as an element of $H^1(k, F)$.

Proof of the Proposition ($H^1(k, G(\overline{k})) \leftrightarrow H^1(K, G(\overline{K}))$)

Surjectivity

(1). Let U be the unipotent radical of G. The maps $H^1(k, G) \to H^1(k, G/U)$ and $H^1(K, G) \to H^1(K, G/U)$ are bijective, hence we may assume that the neutral component G^o of G is reductive.

(2). Consider a commutative group C over k. Since the commutative group $C(\overline{K})/C(\overline{k})$ is torsion free and divisible and so it has trivial Galois cohomology, the natural maps $H^n(k, C) \to H^n(K, C)$ are bijective for all $n > 0$.

(3). Let T be a maximal torus of G, and let N be its normalizer. The map $H^1(K, N) \to H^1(K, G)$ is surjective. Hence it will be enough to prove surjectivity for N.

(4). After replacing G by N, we have an exact sequence $1 \to C \to G \to F \to 1$, where C is a torus and F a finite group. This gives us a commutative diagram:

$$\begin{array}{ccccccccc} 1 & \to & H^1(k, C) & \to & H^1(k, G) & \to & H^1(k, F) & \xrightarrow{\delta} & H^2(k, C_y) \\ & & \updownarrow & & \downarrow & & \updownarrow & & \updownarrow \\ 1 & \to & H^1(K, C) & \to & H^1(K, G) & \to & H^1(K, F) & \xrightarrow{\delta} & H^2(K, C_y) \end{array}$$

Let x be an element of $H^1(K, G)$ and let y be its image in $H^1(K, F)$. Thus we view y as an element of $H^1(k, F)$.

The element y belongs to the image of $H^1(k, G) \to H^1(k, F)$.

The element x belongs to the image of $H^1(k, G) \to H^1(K, G)$.

Injectivity
Let ξ_1, ξ_2 be elements in $H^1(k, G(\overline{k}))$ such that their images in $H^1(K, G(\overline{K}))$ coincide. Let c_i be a 1-cocycle with values in $G(\overline{k})$ representing $\xi_i, i = 1, 2$.

There is an element $h \in G(\overline{K})$ such that

$$c_2(\alpha) = h^{-1} c_1(\alpha) \alpha(h) \tag{1}$$

for all $\alpha \in Gal(\overline{K}/K) = Gal(\overline{k}/k)$.

There exists a finitely generated k-algebra $B \subset K$ with $h \in G(\overline{k}B)$. Since B is real and k is real closed, there exists a k-linear homomorphism $\phi : B \to k$ with $\phi(1) = 1$. Further ϕ extends to a $\overline{k}$-linear homomorphism $\overline{k}B \to \overline{k}$, commuting with the actions of $Gal(\overline{K}/K) = Gal(\overline{k}/k)$. Applying ϕ to the identity (1) one obtains

$$c_2(\alpha) = \phi(h)^{-1} c_1(\alpha) \alpha(\phi(h)).$$

Thus $\xi_1 = \xi_2$.